Copyright © 2015, 2017, Hitachi, Ltd.

MAINTENANCE PC SECTION

Copyright © 2015, 2017, Hitachi, Ltd.

Contents

1. Maintenance PC Setup MPC01-10
1.1 Specifications for the Maintenance PC MPC01-10
1.2 Attachment / Removal Procedure of Maintenance PC MPC01-20
1.2.1 Attachment Procedure of Maintenance PC MPC01-20
1.2.2 Removal Procedure of Maintenance PC MPC01-40
1.3 Maintenance PC Connection Procedure MPC01-50
1.3.1 IP Address Setting Method of Maintenance PC MPC01-50
1.3.2 Troubleshooting of IP Address Setting MPC01-71
1.3.3 Troubleshooting of the Proxy Setting MPC01-72
1.4 Shutting down the Maintenance PC MPC01-80
1.5 Maintenance PC Initial Installation/Update Installation MPC01-90
1.5.1 Before Connecting to the Storage System MPC01-90
1.5.2 Setting Method of Negotiation MPC01-90
1.5.3 Checking Overlap of Port Number for the Maintenance PC MPC01-102
1.5.4 Maintenance PC Software Installation MPC01-110
1.5.5 Storage Device List Update MPC01-150
1.5.6 How to use Flash Player that is installed on Windows Server 2012 or later MPC01-210
1.5.6.1 Using Flash Player in Windows Server 2012 ..... MPC01-210
1.5.7 Precautions Related to the Use of the Virus Detection Program MPC01-220
1.5.8 Function List MPC01-221
1.6 Connecting to the Storage System MPC01-230
1.6.1 Precautions on Maintenance PC Connection MPC01-230
1.6.2 Procedures for Connecting to the Storage System MPC01-240
1.6.2.1 Register the Storage System MPC01-240
1.6.2.2 Starting Web Console MPC01-280
1.6.2.3 Stopping Web Console MPC01-291
1.6.3 Storage System Icon MPC01-300
1.6.4 Stopping/Starting the Service of Storage System MPC01-310
1.6.4.1 Stopping the Service of Storage System MPC01-310
1.6.4.2 Starting the Service of Storage System MPC01-313
1.6.5 Changing Storage System Information and Updating Software of Web Console MPC01-320
1.6.6 Switching the Storage System MPC01-330
1.6.7 Deleting the Storage System Icon MPC01-332
1.6.8 Incorrect display errors MPC01-340
1.6.9 Specifications of Web Server Status List MPC01-350
1.7 Setting the IIS/FTP Server MPC01-390
1.7.1 Installing IIS/FTP MPC01-390
1.7.2 Setting IIS/FTP MPC01-400
1.8 Starting Windows MPC01-440
1.8.1 Maintenance PC Window MPC01-440
1.8.1.1 Open the Window MPC01-440
1.8.1.2 Starting the Maintenance PC Window Only MPC01-450
1.8.1.3 Close the Window MPC01-450

Copyright © 2015, 2017, Hitachi, Ltd.

1.8.2 Maintenance Utility Window MPC01-460
1.8.2.1 Starting the Web Console Window MPC01-460
1.8.2.2 Starting the MPC Window MPC01-470
1.8.2.3 Starting the Browser MPC01-470
1.8.2.4 Close the Window MPC01-470
1.8.2.5 Basic Framework MPC01-471
1.8.2.6 Header Area Configuration MPC01-472
1.8.2.7 Navigation Area Configuration MPC01-473
1.8.2.8 Application Area Configuration MPC01-476
1.8.3 NAS Manager Window MPC01-477
1.8.3.1 Starting the Window MPC01-477
1.8.3.2 Closing the Window MPC01-477
1.8.4 BALI (Console) Window MPC01-478
1.8.4.1 Starting the Window MPC01-478
1.8.5 Setting the Browser Compatibility Display to OFF MPC01-480
1.9 Check the Version of Third Party Software MPC01-490
1.10 Stopping/Starting the Storage Navigator Services MPC01-491
1.10.1 Stopping the Storage Navigator Services MPC01-491
1.10.2 Starting the Storage Navigator Services MPC01-493
1.11 Troubleshooting of Storage Device List MPC01-500
1.12 Troubleshooting of Web Console MPC01-510
1.13 Troubleshooting of Maintenance Utility MPC01-530
1.14 Troubleshooting during Operation in Connection with External Server MPC01-570

2. Local Setting of Maintenance PC MPC02-10
2.1 Before using Web Console MPC02-10
2.2 Check of Configuring Web Console Over a Firewall MPC02-20
2.3 Internal Communication Ports Used by the Maintenance PC MPC02-20
2.4 Initial Setting Wizard MPC02-30

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 MPC03-90
3.3.1 Setting up User Account MPC03-90
3.3.2 Disabling User Accounts MPC03-110
3.3.3 Changing User Account Authentication MPC03-130
3.3.4 Removing User Accounts MPC03-150
3.3.5 User Account Information MPC03-170
3.3.5.1 Backup User Accounts MPC03-170
3.3.5.2 Restore of User Account Information MPC03-170
3.3.6 Roles to be Required for the Operation Window of Maintenance Utility MPC03-171

Copyright © 2015, 2017, Hitachi, Ltd.

3.4 Alert Notifications MPC03-180
3.4.1 Setting up Email Notification when Storage System Failures Occur MPC03-190
3.4.1.1 Prerequisites MPC03-190
3.4.1.2 Procedure MPC03-190
3.4.1.3 Example of Test Mail MPC03-212
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 MPC03-230
3.4.3.1 Procedure MPC03-230
3.4.3.2 Adding SNMP Trap Notification Destinations MPC03-232
3.4.3.3 Adding the Request Permission Setting that Accepts GET REQUEST and GETNEXT REQUEST MPC03-233
3.4.3.4 Deleting the SNMP Trap Notification MPC03-235
3.4.3.5 Deleting an IP Address and Community of the SNMP Manager which Accepts GET REQUEST and GETNEXT REQUEST MPC03-236
3.4.3.6 Changing the Sending Trap Settings MPC03-236B
3.4.3.7 Changing the Request Permission Setting MPC03-236E
3.4.3.8 Performing the Trap Report Test MPC03-237
3.5 Time Setting MPC03-240
3.5.1 Setting Synchronization Information MPC03-240
3.6 Network Setting MPC03-270
3.6.1 Network Setting MPC03-270
3.6.2 Network Permissions MPC03-290
3.7 Setting up License Keys MPC03-310
3.7.1 Types of License Keys MPC03-310
3.7.1.1 Using the Permanent Key MPC03-310
3.7.1.2 Using the Term Key MPC03-320
3.7.1.3 Using the Temporary Key MPC03-320
3.7.1.4 Using the Emergency Key MPC03-320
3.7.2 Software Packaging MPC03-330
3.7.3 Software and Licensed Capacity MPC03-350
3.7.4 Calculating Licensed Capacity MPC03-370
3.7.4.1 Calculating Capacity for a Normal Volume (LDEV) MPC03-370
3.7.4.2 Calculating Licensed Capacity for an External Volume Mapped to the Storage System MPC03-370
3.7.4.3 Calculating Pool Capacity MPC03-370
3.7.4.4 Implementation Capacity of the Parity Group whose Accelerated Compression Setting is Enabled MPC03-370
3.7.5 Installing Software Using a License Key Code MPC03-380
3.7.6 Enabling a License MPC03-410
3.7.7 Disabling a License MPC03-420
3.7.8 Removing Program Product MPC03-430
3.7.9 Verifying License MPC03-440
3.7.9.1 Examples of the displayed window MPC03-441

Copyright © 2015, 2017, Hitachi, Ltd.

3.7.10 Cautions on Licensed Capacity in Non-License-Related Windows MPC03-450
3.7.11 Troubleshooting related to licenses MPC03-460
3.7.12 Precautions related to the pool capacity when using Dynamic Provisioning MPC03-470
3.8 Audit Log Settings MPC03-480
3.8.1 Verifying the Settings to Transfer the Syslog Server MPC03-480
3.8.2 Transferring Audit Log to the Syslog Server MPC03-490
3.8.2.1 Prerequisites MPC03-490
3.8.2.2 Operation Procedure MPC03-490
3.8.3 Exporting Audit Log MPC03-520
3.8.3.1 Exporting Audit Log (Maintenance Utility) MPC03-520
3.8.3.2 Exporting Audit Log (Web Console) MPC03-522
3.8.4 Sending a Test Message to the Syslog Server MPC03-530
3.9 Turn on/off Locate LEDs MPC03-540
3.9.1 Trun on Locate LED MPC03-540
3.9.2 Trun off Locate LED MPC03-560
3.10 Power on Storage System MPC03-580
3.11 Power off Storage System MPC03-600
3.12 Edit UPS Mode MPC03-620
3.13 Edit Login Message MPC03-640
3.14 Select Cipher Suite MPC03-660
3.15 Update Certificate Files MPC03-670
3.16 Edit System Parameters MPC03-690
3.17 Force Release System Lock MPC03-710
3.18 Reboot GUM MPC03-730
3.19 Change Password MPC03-750
3.20 Boot System Safe Mode MPC03-770
3.21 Alert Display MPC03-790
3.22 Alert Display Related to FRU (Field Replacement Unit) MPC03-810
3.23 Management Menu MPC03-840
3.24 Power Supply Management MPC03-850
3.25 System Management MPC03-860
3.26 Resetting GUM MPC03-870
3.27 Acquiring System Dumps MPC03-880
3.28 Confirming the NAS Module Status MPC03-900
3.28.1 Displaying the NAS Module Status MPC03-900
3.28.2 Resetting Unified Hypervisor MPC03-910
3.28.3 Resetting Hypervisor Network Module MPC03-940
3.28.4 Resetting NAS Unified Firmware MPC03-970
3.28.5 Editing Unified Hypervisor Maintenance Mode MPC03-1000
3.29 Changing Java Security Settings When Electronic Certificate is Expired MPC03-1020
3.29.1 Confirm Java Version MPC03-1021
3.29.2 Changing Java Security Settings MPC03-1030

Copyright © 2015, 2017, Hitachi, Ltd.

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 Verifying LDEVs 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 Construct iSCSI Target or Host Group MPC04-170
4.1.4.2 Configuring iSCSI Target Information 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
4.2.2 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
4.2.3 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 MPC04-400
4.2.3.8 Releasing Logical Device Assignments MPC04-420
4.3 Managing Port MPC04-440
4.3.1 Editing Fibre Channel MPC04-440
4.3.2 Editing iSCSI MPC04-460
4.3.3 Deleting Host Group Information MPC04-490
4.3.4 Deleting iSCSI Target Information MPC04-500
4.3.5 Using CHAP Authentication with iSCSI Ports MPC04-520
4.3.5.1 Configuring One-Way CHAP MPC04-530
4.3.5.2 Changing One-Way CHAP Settings MPC04-560
4.3.5.3 Deleting a One-Way CHAP User MPC04-590
4.4 Logical Device Maintenance MPC04-600
4.4.1 Blocking LDEVs MPC04-600
4.4.2 Restoring Blocked LDEVs MPC04-620
4.4.3 Editing an LDEV Name MPC04-640
4.4.4 Force Restore LDEVs MPC04-660
4.5 WebConsole Operation MPC04-680
4.5.1 Local Replication MPC04-690
4.5.1.1 Initializing Local Replica Pairs MPC04-690

4.5.2 Data Retention Utility MPC04-700
4.5.3 Universal Volume Manager MPC04-710
4.5.4 Remote Replication MPC04-720
4.5.4.1 Remote Replica Function Switch MPC04-720
4.5.4.2 Assign Remote Command Devices Window MPC04-750
4.5.5 Dynamic Provisioning/Dynamic Tiering/active flash/Thin Image MPC04-760
4.5.6 Performance Monitor MPC04-780
4.6 Copy Back Setting MPC04-790
4.6.1 Setting the Copy Back MPC04-790
4.6.2 Changing the Copy Back MPC04-790
4.7 Verify（Parity Consistency Check） MPC04-810
4.7.1 Executing Verify（Parity Consistency Check） MPC04-810
4.7.2 Interrupting Verify MPC04-840
4.7.3 Checking the Progress MPC04-850
4.7.3.1 Checking the Progress in the “Parity Group” Window MPC04-860
4.7.3.2 Checking the Progress in the “LDEV” Window MPC04-870
4.7.3.3 Checking the Progress in the Task MPC04-880
4.8 Managing Resource Group MPC04-900
4.8.1 Adding LDEVs to Resource Group MPC04-900
4.8.2 Removing LDEVs from Resource Group MPC04-930

5. Maintenance Function of Maintenance PC MPC05-10
5.1 Mode MPC05-10
5.2 Dump MPC05-40
5.3 Log MPC05-170
5.3.1 Log Indication MPC05-170
5.3.2 Log Delete MPC05-370
5.4 Online Read Margin (ORM) MPC05-390
5.5 Management of Drive Threshold Values MPC05-650
5.6 Setting Machine Install Data MPC05-730
5.7 System Option MPC05-750
5.8 Setting System Option Mode MPC05-800
5.9 System Tuning MPC05-850
5.10 Config Backup MPC05-910
5.11 Initializing the Configuration Information MPC05-940
5.12 Maintenance Screen MPC05-960
5.12.1 Start MPC05-960
5.12.2 Terminate MPC05-990
5.12.3 Update MPC05-1000
5.13 Maintenance Procedure MPC05-1010
5.13.1 Copy Status View MPC05-1010
5.13.2 Version of Firmware MPC05-1020
5.13.2.1 Basic Info MPC05-1030
5.13.2.2 MP Ver.(Curt./Running) MPC05-1050
5.13.2.3 MP Ver.(Curt./FM) MPC05-1070

5.13.2.4 CFM/GUM Ver. MPC05-1090
5.13.2.5 Unified Hypervisor Ver. MPC05-1100
5.13.2.6 HDD Ver. MPC05-1110
5.13.2.7 ENC Ver. MPC05-1120
5.13.3 Pin Data Indication MPC05-1140
5.13.4 PCB/SFP Revision Display MPC05-1170
5.13.5 Inter-PCB Logical Path MPC05-1180
5.13.6 Restoring Failed MP MPC05-1210
5.13.7 Failed CTL Recovery MPC05-1260
5.13.8 Error or Failure Status Action MPC05-1320

6. Main Operation Items of NAS Manager MPC06-10
6.1 Logging into/Logging out NAS Manager MPC06-10
6.1.1 Logging into NAS Manager MPC06-10
6.1.2 Logging out from NAS Manager MPC06-20
6.2 Collecting IP Address Information MPC06-30
6.3 Confirming the Node Status MPC06-50
6.4 Migrating EVS MPC06-80
6.4.1 Migration before the Maintenance Operations MPC06-80
6.4.2 Migration after the Maintenance Operations MPC06-120
6.5 Adding License Keys MPC06-150
6.6 Backup of Node Registry MPC06-170
6.7 Restoring the NAS Unified Firmware Configuration Information MPC06-190
6.8 DNS Settings and Confirmation MPC06-250
6.9 Setting the Time and the NTP Server MPC06-270
6.10 Confirming the Event Log MPC06-290
6.11 Confirming the Firmware Version of the Node MPC06-310
6.12 Collecting Logs of Node and SMU MPC06-330

7. Maintenance CLI MPC07-10
7.1 Operation Procedure of the Command MPC07-10
7.1.1 Before Using the Command MPC07-10
7.1.2 Logging into the Node MPC07-10
7.1.3 How to Run the Command MPC07-20
7.1.4 Logging out of the Node MPC07-30
7.2 Logging into Node MPC07-40
7.3 Dumps for NAS MPC07-80
7.3.1 Collecting NAS Dumps Manually MPC07-80
7.3.2 Collecting NAS-OS Dump MPC07-110
7.4 List of Commands to be Used MPC07-130
7.5 Displaying the Network Status (ifconfig) MPC07-150
7.5.1 Command Line MPC07-150
7.5.2 ifconfig Output Format MPC07-150
7.5.3 ifconfig -v Output Format MPC07-170
7.5.4 Procedure for Isolating Failure Causes MPC07-190

Copyright © 2015, 2017, Hitachi, Ltd.

7.6 Shutting down NAS Modules MPC07-200
7.6.1 Command Line MPC07-200
7.6.2 shutdown Output Format MPC07-200
7.7 Displaying Hardware Status (status) MPC07-210
7.7.1 Command Line MPC07-210
7.7.2 status Output Format MPC07-210
7.7.3 status -h Option Output Format MPC07-220
7.7.4 status -s Option Output Format MPC07-230
7.7.5 status -a Option Output Format MPC07-240
7.8 Setting Date and Confirmation (setdate) MPC07-260
7.8.1 Command Line MPC07-260
7.8.2 setdate Output Format MPC07-260
7.9 Setting Time and Confirmation (settime) MPC07-270
7.9.1 Command Line MPC07-270
7.9.2 settime Output Format MPC07-270
7.10 Confirming the Version of NAS Modules (ver) MPC07-280
7.10.1 Command Line MPC07-280
7.10.2 ver Output Format MPC07-280
7.10.3 ver -h Option Output Format MPC07-290
7.11 Managing IP Addresses (ipaddr) MPC07-300
7.11.1 Command Line MPC07-300
7.11.2 ipaddr Output Format MPC07-300
7.12 Displaying the NAS Module Status (cluster-show) MPC07-310
7.12.1 Command Line MPC07-310
7.12.2 cluster-show -a Option Output Format MPC07-320
7.13 EVS Migration (evs migrate) MPC07-350
7.13.1 Command Line MPC07-350
7.13.2 evs migrate Output Format MPC07-350
7.14 EVS Information (evs list) MPC07-360
7.14.1 Command Line MPC07-360
7.14.2 evs list Output Format MPC07-360
7.15 Stopping EVS (evs disable) MPC07-370
7.15.1 Command Line MPC07-370
7.15.2 evs disable Output Format MPC07-370
7.16 Booting EVS (evs enable) MPC07-380
7.16.1 Command Line MPC07-380
7.16.2 evs enable Output Format MPC07-380
7.17 Setting IP Address (evsipaddr) MPC07-390
7.17.1 Command Line MPC07-390
7.17.2 evsipaddr Output Format MPC07-400
7.18 Confirming SUM Version (smu-version) MPC07-410
7.18.1 Command Line MPC07-410
7.18.2 smu-version Output Format MPC07-410

Copyright © 2015, 2017, Hitachi, Ltd.

7.19 Confirming SMU Running Status (smu-service-status) MPC07-420
7.19.1 Command Line MPC07-420
7.19.2 smu-service-status Output Format MPC07-420
7.20 Rebooting NAS Module (reboot) MPC07-430
7.20.1 Command Line MPC07-430
7.20.2 reboot Output Format MPC07-430
7.21 Confirming Command Contents (help) MPC07-440
7.21.1 Command Line MPC07-440
7.21.2 help Output Format MPC07-440
7.22 Displaying List of Directories (ls) MPC07-450
7.22.1 Command Line MPC07-450
7.22.2 ls Output Format MPC07-450
7.23 Confirming Network Communication (ping) MPC07-460
7.23.1 Command Line MPC07-460
7.23.2 ping Output Format MPC07-460
7.24 Displaying List of Spans (span-list) MPC07-470
7.24.1 Command Line MPC07-470
7.24.2 span-list Output Format MPC07-470
7.25 Enabling Access to Spans (span-assign-to-cluster) MPC07-480
7.25.1 Command Line MPC07-480
7.25.2 span-assign-to-cluster Output Format MPC07-480
7.26 Displaying List of System Drives (sd-list) MPC07-490
7.26.1 Command Line MPC07-490
7.26.2 sd-list Output Format MPC07-490
7.27 Displaying Disk Utilization Ratio (df) MPC07-500
7.27.1 Command Line MPC07-500
7.27.2 df Output Format MPC07-500
7.28 Deleting Clusters (cluster-node-delete) MPC07-510
7.28.1 Command Line MPC07-510
7.28.2 cluster-node-delete Output Format MPC07-510
7.29 Mounting File System (mount) MPC07-520
7.29.1 Command Line MPC07-520
7.29.2 mount Output Format MPC07-520
7.30 Power On Self Test (POST) Result (post-status) MPC07-530
7.30.1 Command Line MPC07-530
7.30.2 post-status Output Format MPC07-530
7.31 Expanding Specific File System (expandfs) MPC07-540
7.31.1 Command Line MPC07-540
7.31.2 expandfs Output Format MPC07-540
7.32 Displaying NVRAM utilization ratio (nvpages) MPC07-550
7.32.1 Command Line MPC07-550
7.32.2 nvpages Output Format MPC07-550

8. Monitoring MPC08-10

Copyright © 2015, 2017, Hitachi, Ltd.

9. Installing the Maintenance PC Tool MPC09-10
9.1 Use of OnlineDumpTool MPC09-10
9.1.1 Installation MPC09-10
9.1.2 Uninstallation MPC09-50
9.1.3 Upload Procedure MPC09-60
9.1.4 Reference of Uploaded Results MPC09-130
9.1.5 Message Table MPC09-140
9.2 Dump file name Conversion Tool MPC09-170
9.2.1 Installation of Dump file name Conversion Tool MPC09-170
9.2.2 Uninstallation of Dump file name Conversion Tool MPC09-190
9.2.3 Operating procedure of Dump file name Conversion Tool MPC09-190

10. Maintenance PC Uninstallation MPC10-10
10.1 OSS Uninstallation MPC10-10
10.2 Maintenance PC Software Uninstallation MPC10-20

11. Description of Windows MPC11-10
11.1 Names of Elements of Windows (Maintenance PC) MPC11-10
11.2 WARNING LED Status Window MPC11-20
11.3 Maintenance Window MPC11-30
11.3.1 Main Window MPC11-30
11.3.2 Operation Menu MPC11-40
11.3.3 Dialog Bar MPC11-50
11.3.4 Information Display View MPC11-60
11.3.4.1 Storage System Information View MPC11-70
11.3.4.2 DKC Information View MPC11-80
11.3.4.3 HDD Information View MPC11-110
11.3.4.4 Dialog MPC11-140

12. Changing/Initializing Port Numbers Used by the SVP MPC12-10
12.1 Changing Port Numbers Used by the SVP MPC12-20
12.2 Initializing Port Numbers Used by the SVP MPC12-30
12.3 Reallocating Automatically Allocated Port Numbers MPC12-40
12.4 Initializing Automatically Allocated Port Numbers MPC12-50
12.5 Changing Range of Port Numbers to be Allocated Automatically MPC12-60
12.6 Initializing Range of Port Numbers to be Allocated Automatically MPC12-70
12.7 See the Port Number to be Used in the SVP MPC12-80
12.8 Checking the Application Using the Port Number Used by the SVP MPC12-90

13. Appendix MPC13-10
13.1 IP Addresses of Maintenance Ports and Internal Network MPC13-10
13.1.1 Maintenance Port Addresses MPC13-10
13.1.2 Internal Network Addresses MPC13-20
13.2 Port Number Used by Hitachi Command Suite MPC13-30
13.3 Port Number Used by the Maintenance PC MPC13-40

Copyright © 2015, 2017, Hitachi, Ltd.

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

1. Maintenance PC Setup

1.1 Specifications 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 (*4)	Adobe Reader	
Web Browser	Internet Explorer 11.0 (*2) (*3) (*5)	
Locale	English (United States), Japanese (Japan)	

Copyright © 2015, 2017, Hitachi, Ltd.

*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: When using Internet Explorer, turn off the compatibility display to use it.
For the procedure for turning off the compatibility display, see “1.8.5 Setting the Browser Compatibility Display to OFF”.

*3: Disable the pop-up block on the Web browser in accordance with the following procedure.
1. Click [Control Panel] – [Internet Options] from the [Start] menu of Windows and display the “Internet Options” window.
2. Select the [Privacy] tab in the “Internet Options” window.
3. Uncheck the checkbox of [Turn on Pop-up Blocker] and click [OK] button.

*4: RAID Manager cannot be installed in the Maintenance PC.

*5: This browser supports only the Internet Explorer of the latest version operating in each OS in accordance with the Microsoft support policy.

Copyright © 2015, 2017, Hitachi, Ltd.

1.2 Attachment / Removal Procedure of Maintenance PC

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.

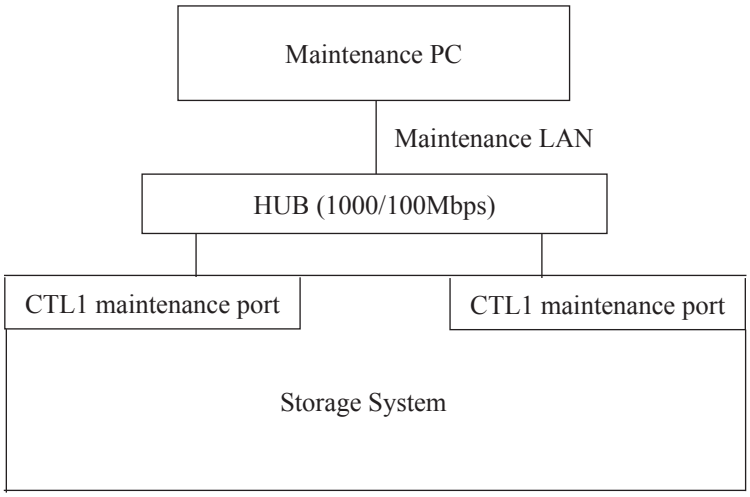
1.2.1 Attachment Procedure of Maintenance PC

See Step 5 for the network configuration when 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 1-2.)
   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.
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.
5. The configuration when monitoring
   When collecting the monitor information using the following functions of the Maintenance PC, communicating with the DKC by connecting the Maintenance PC to CTL1 and CTL2 using HUB is required.
   - Using the performance monitor function by Web Console
   - Using the monitoring function in the “Monitor” window

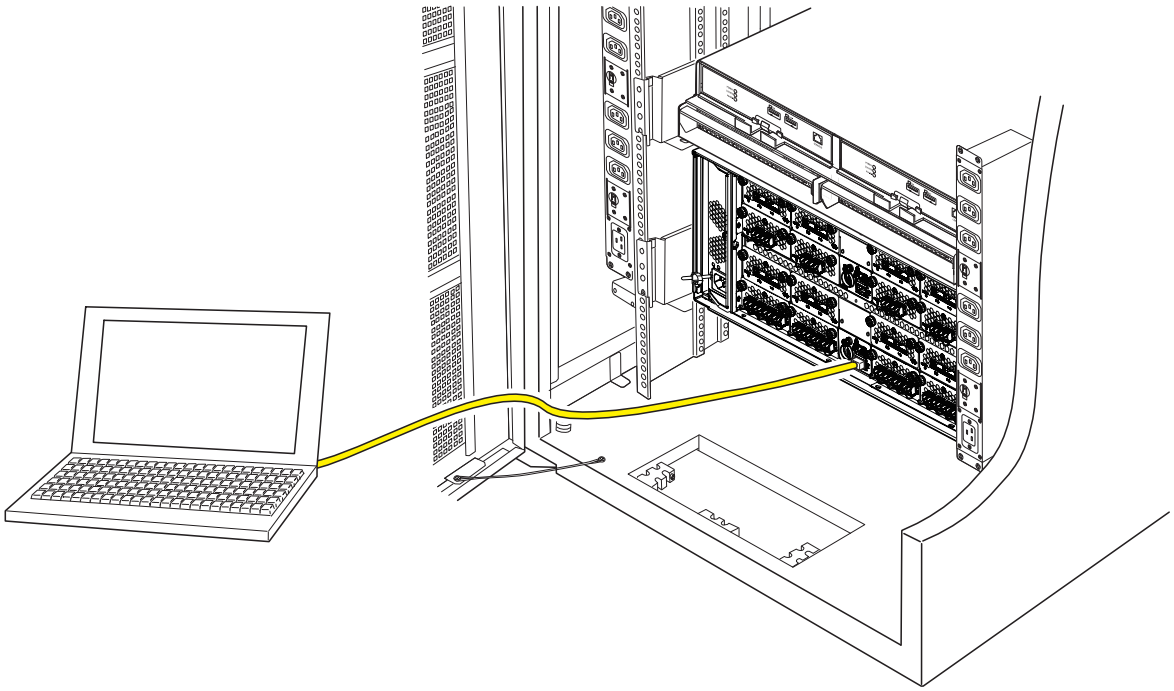
   NOTE: If CTL1 and CTL2 are not connected simultaneously, monitor data might be missed. Connect the Maintenance PC to the Storage System with the following connection configuration diagram.

Figure 1-1 Connection Configuration Diagram

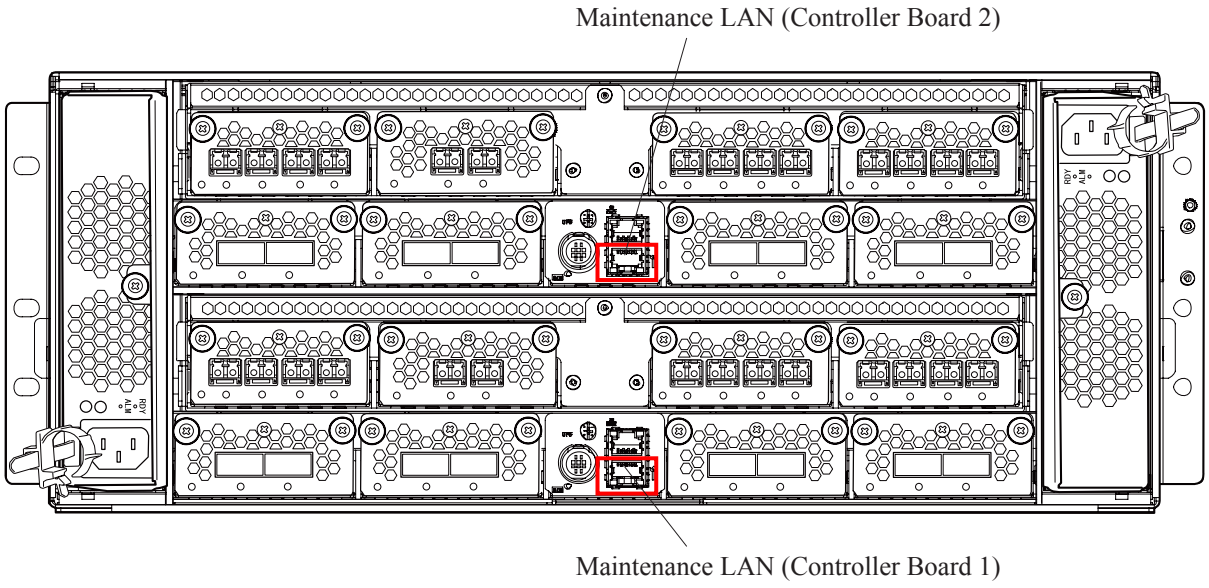


Copyright © 2015, 2017, Hitachi, Ltd.

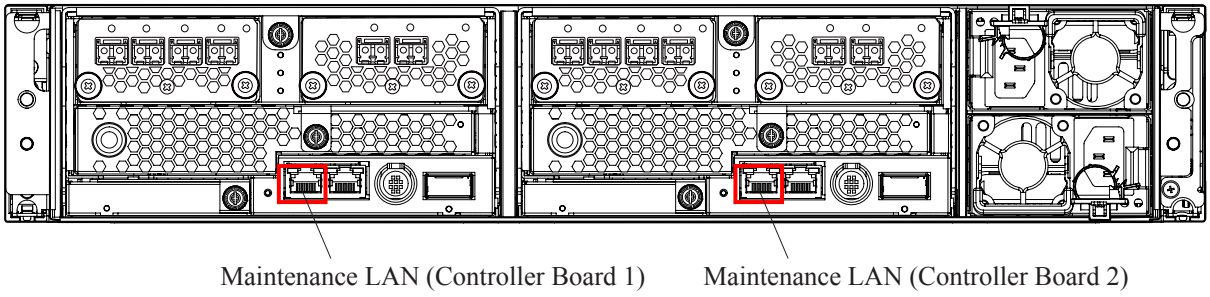
Figure 1-2 Connection of Cables



• CBLM2/CBLH3 (Rear view)



• CBSS/CBSL (Rear view)



Copyright © 2015, 2017, Hitachi, Ltd.

1.2.2 Removal Procedure of Maintenance PC

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 1-2.)
4. Disconnect the power cable and LAN cable from the Maintenance PC.

1.3 Maintenance PC Connection Procedure

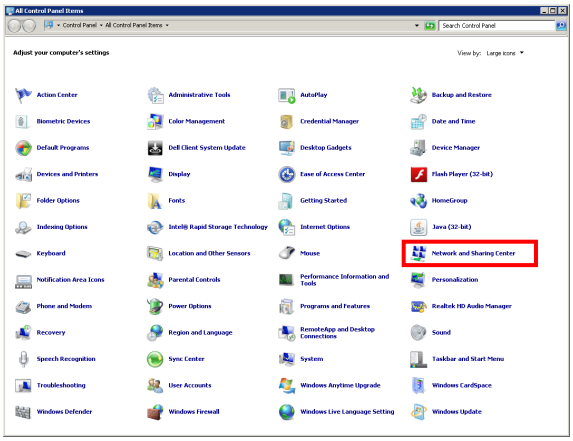
1.3.1 IP Address Setting Method of Maintenance PC

NOTE: If you have already done the operations of "1.6 Connecting to the Storage System", confirm all of the icon's status on the "Storage Device List" are "Service stop status", before executing the following operations. Otherwise, you have to reboot the Maintenance PC.

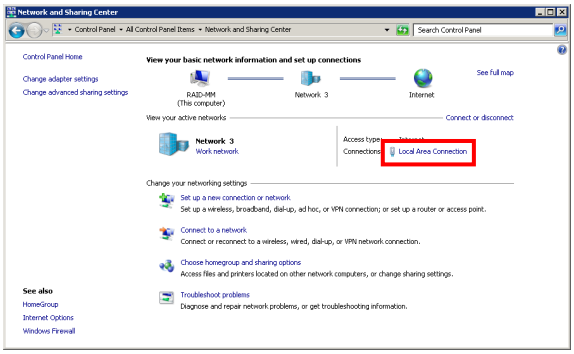
- Example of Service stop status icon



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

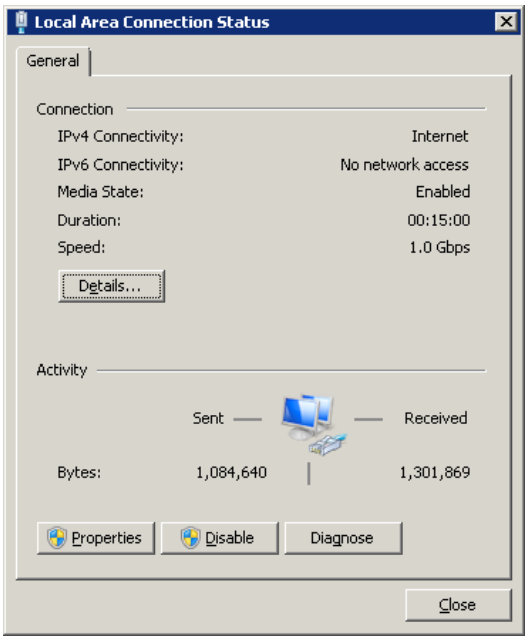


2. Click the [Local Area Connection].

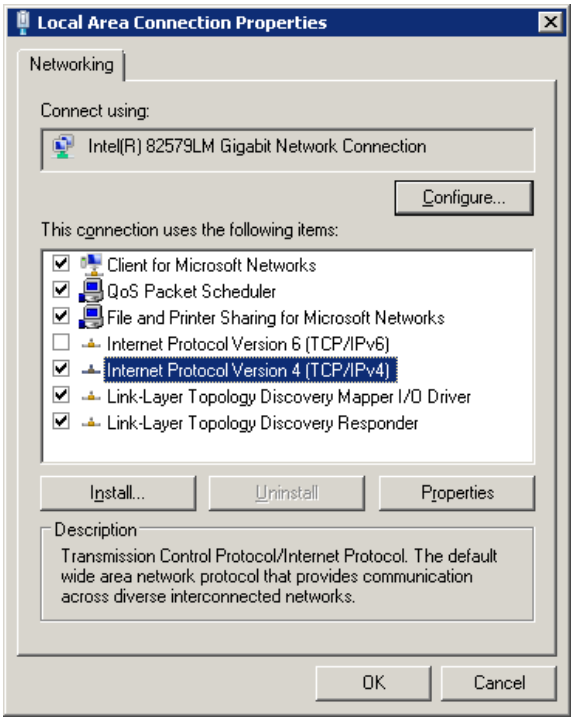


Copyright © 2015, 2017, Hitachi, Ltd.

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



4. 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.

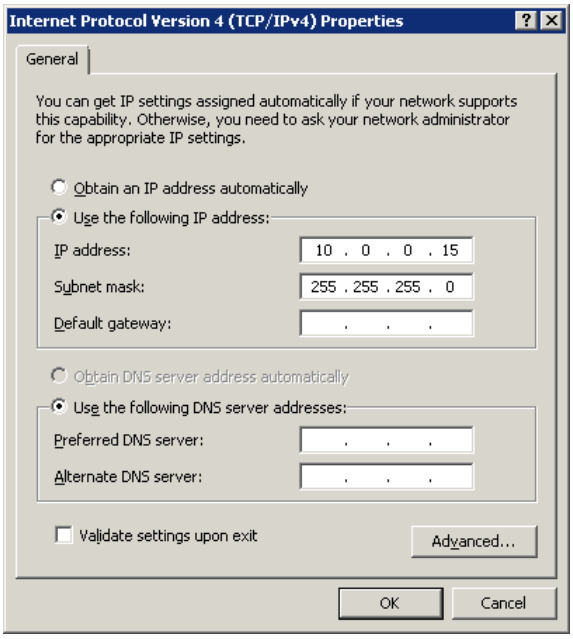


Table 1-2 Operation Environment shows two types of IP addresses of the maintenance LAN port.
Item No. 1: Initial setting status
Item No. 2: Network already set up at factory shipment

Table 1-2 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 (*2).
*2: The maintenance port addresses of CTL consist of the Storage System, Unified Hypervisor and NAS Platform. See “13.1 IP Addresses of Maintenance Ports and Internal Network” for the details.

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

7. Close the network connection window.

8. Connect to the Storage System from the launcher (connection icon) on the desktop.

Copyright © 2015, 2017, Hitachi, Ltd.

1.3.2 Troubleshooting of IP Address Setting

If the following conditions are met, you might be displayed as “LOCALHOST” to the IP address of 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

Please apply the KB2883200 If you display the IP address of the audit log correctly.

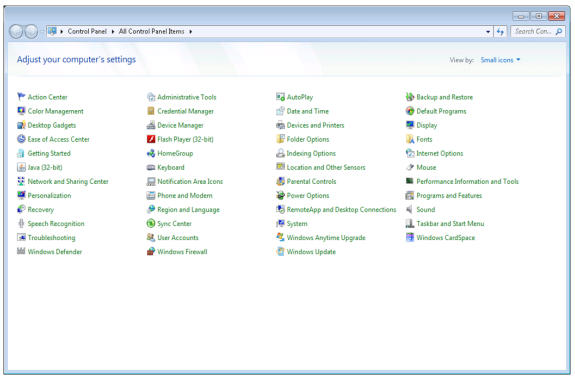
Copyright © 2015, 2017, Hitachi, Ltd.

1.3.3 Troubleshooting of the Proxy Setting

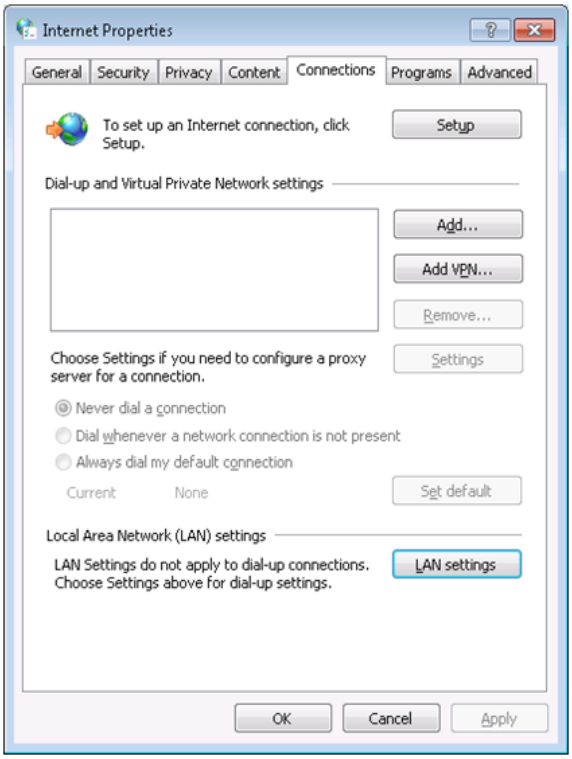
When Internet Explorer uses the proxy, the pages of Storage Navigator or Maintenance Utility might not be found.
Set the IP address of GUM and the IP address of the service PC to [Exceptions] of the proxy.

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

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

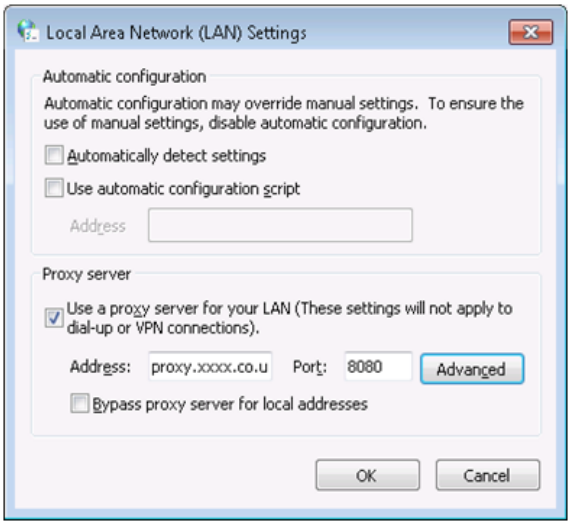


2. Select [LAN settings] of the [Connections] tab.

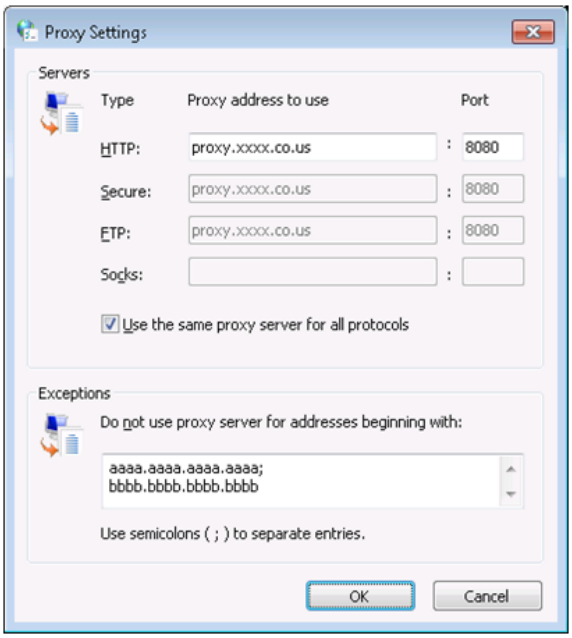


Copyright © 2015, 2017, Hitachi, Ltd.

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



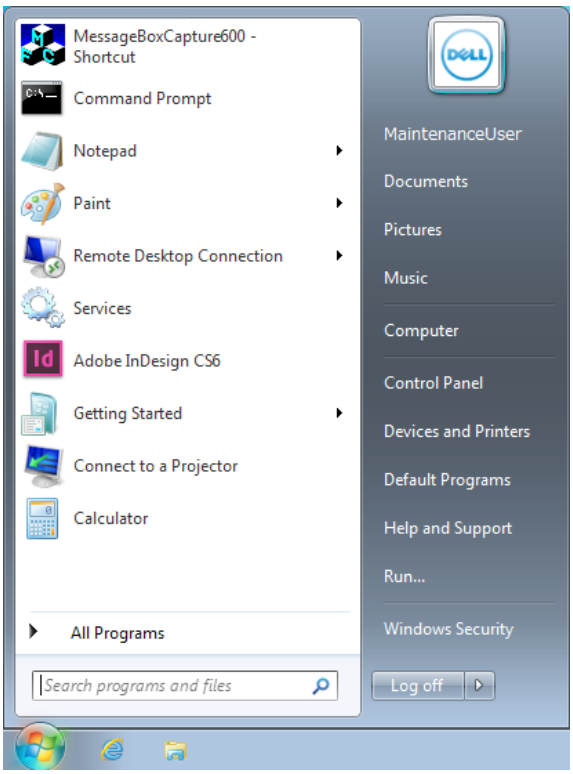
4. Add the IP address of GUM and the IP address of the service PC to [Exceptions], and then select [OK].



Copyright © 2015, 2017, Hitachi, Ltd.

1.4 Shutting down the Maintenance PC

Close all the open windows.
Click the [Windows] button and then [Shut Down].
For Windows 10, click the [Windows] button, select [Power], and select [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.

Copyright © 2015, 2017, Hitachi, Ltd.

1.5 Maintenance PC Initial Installation/Update Installation

1.5.1 Before Connecting to the Storage System

Before connecting to the Storage System, perform "1.7 Setting the IIS/FTP Server".
If the IIS/FTP server is not set, a warning message (21542-005033) occurs in the following operation.

- When the checkbox of [Not start service after addition immediately] is unchecked in the "Add System" window at the time of the Storage System registration and [Apply] is clicked
- When the services of the Storage System icon registered in Storage Device List start

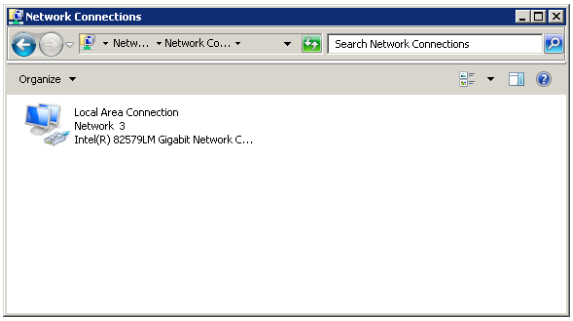
1.5.2 Setting Method of Negotiation

The negotiation setting methods differ depending on the types of Maintenance PCs.
The following shows an example of the setting methods.

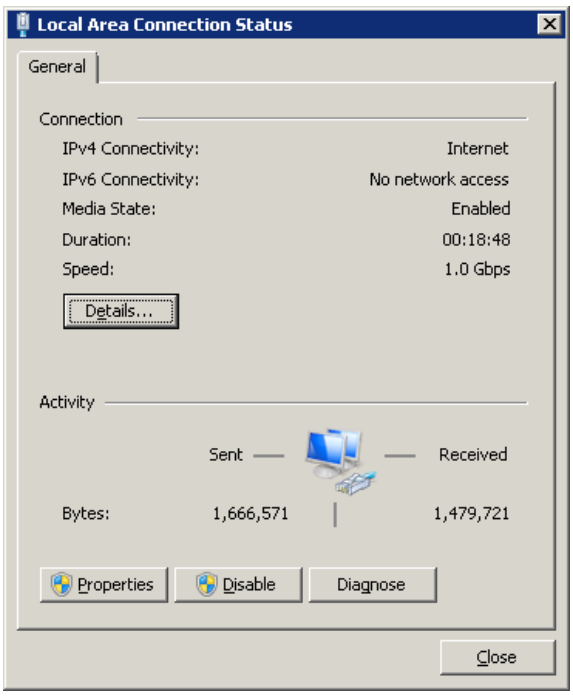
1. Open [Network and Shared Center] from [Control Panel].

2. Click [Change Adapter Settings] from the menu in the left side of the window.

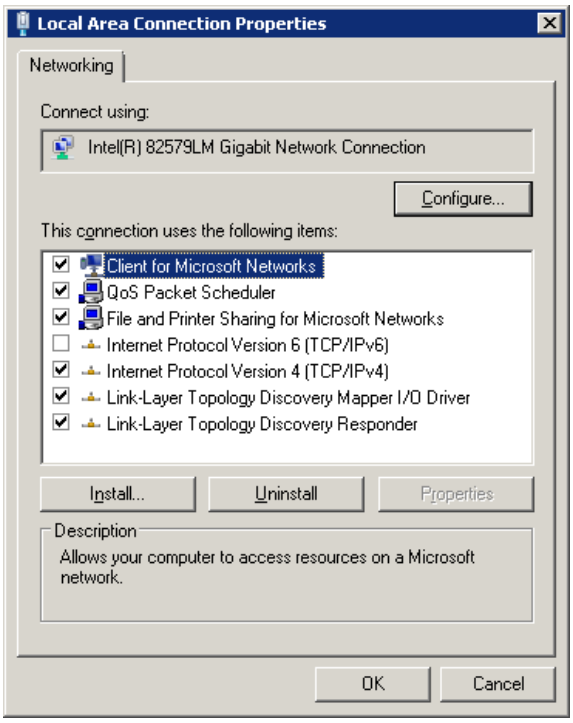
3. Click [Local Area Connection].



4. The “Local Area Connection Status” window is displayed. Click [Properties].

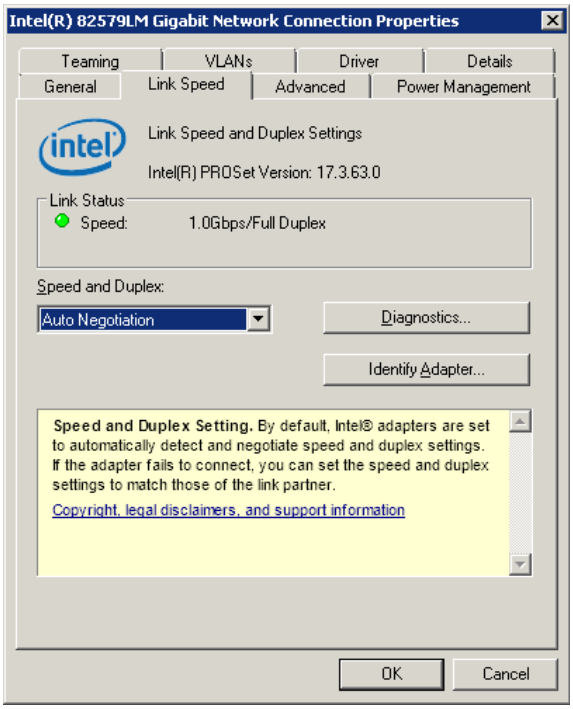


5. The “Local Area Connection Properties” window is displayed. Click the [Configure] button.



Copyright © 2015, 2017, Hitachi, Ltd.

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



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

Copyright © 2015, 2017, Hitachi, Ltd.

1.5.3 Checking Overlap of Port Number for the Maintenance PC

See "12.1 Changing Port Numbers Used by the SVP" to check if the port number is not used by a different application before installing the software on the Maintenance PC.
See "12.8 Checking the Application Using the Port Number Used by the SVP" for the procedure to check if the port number is used by a different application.
If the port number is already used, change the port number used by the application. If it cannot be changed, change the port number to be used after installation referring to "12.1 Changing Port Numbers Used by the SVP".
When Hitachi Command Suite is installed, a port number described in "13.3 Port Number Used by the Maintenance PC" is used. Change the port number not to be the same port number used by Hitachi Command Suite.

Copyright © 2015, 2017, Hitachi, Ltd.

1.5.4 Maintenance PC Software Installation

The software of the following version is installed in the Maintenance PC.
See "1.9 Check the Version of Third Party Software" for how to check the software version.

Installation media	Software							
	JRE	JRE (Client)	Perl	Apache	Jetty	OpenSSL	Flash	PuTTY
When the firmware version is less than 83-01-03-x0/xx	1.7.67	1.7.67	5.18.1	2.4.10	9.0.7	1.0.1j	15	-
When the firmware version is 83-01-03-x0/xx or later and less than 83-01-21-x0/xx	1.8.31	1.7.67	5.18.1	2.4.10	9.0.7	1.0.1j	15	-
When the firmware version is 83-01-21-x0/xx or later and less than 83-02-01-x0/xx	1.8.45	1.8.45	5.18.1	2.4.10	9.2.10	1.0.1j	15	-
When the firmware version is 83-02-01-x0/xx or later and less than 83-03-21-x0/xx	1.8.51	1.8.51	5.18.1	2.4.16	9.2.10	1.0.1p	18	-
When the firmware version is 83-03-21-x0/xx or later and less than 83-04-01-x0/xx	1.8.74	1.8.74	5.18.1	2.4.16	9.2.10	1.0.1r	20	0.64
When the firmware version is 83-04-01-x0/xx or later and less than 83-04-02-x0/xx	1.8.74	1.8.74	5.18.1	2.4.16	9.2.10	1.0.2h	20	0.64
When the firmware version is 83-04-02-x0/xx or later	1.8.74	1.8.74	5.18.1	2.4.16	9.2.10	1.0.2j	20	0.64

NOTICE: When performing update installation, stop the Storage System by the device list, and then install the Maintenance PC. (See "1.6.4 Stopping/Starting the Service of Storage System").

NOTICE: See "1.5.5 Storage Device List Update" for procedure of the firmware update.

Copyright © 2015, 2017, Hitachi, Ltd.

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 JRE1.6 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: Before performing the installation/update or uninstallation, close the Event Viewer of Windows.

⚠ CAUTION

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 "10.2 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: When the firmware version of the Storage System in operation is less than 83-01-04/00, install the JRE whose version is less than 1.8.45 as the JRE (Client), and then install the software of the Maintenance PC.

NOTICE: If JRE1.8 on the Maintenance PC starts, the JRE (Client) setting in JRE1.7 or earlier that is installed in the customer environment might partly return to the default setting. When this phenomenon occurs, perform the setting again.

Copyright © 2015, 2017, Hitachi, Ltd.

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.

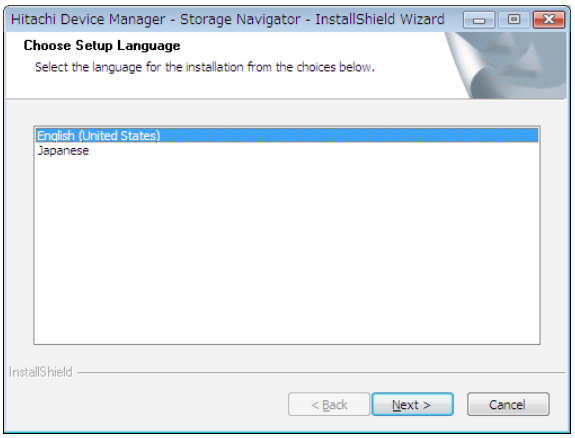
Copyright © 2015, 2017, Hitachi, Ltd.

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

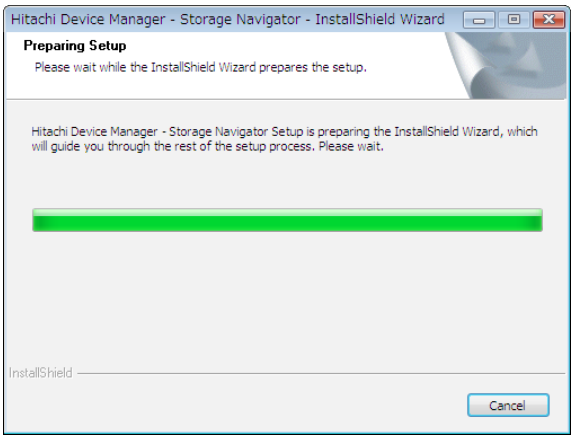
2. Right-click Setup.exe immediately under the drive to select [Execute as Administrator].

   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”.

3. Checking languages
   Select either English or Japanese.



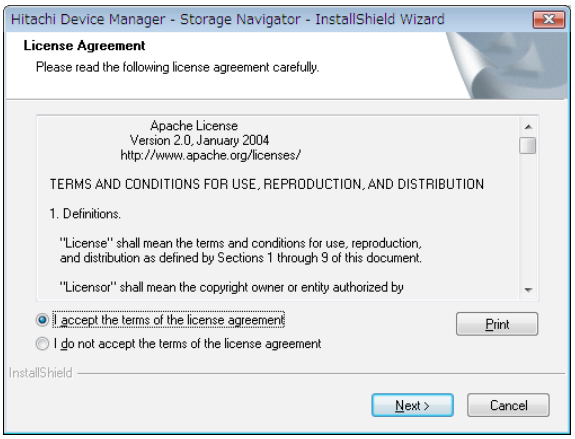
4. Preparing for installation
   The “Preparing Setup” window is displayed.
   Wait until the preparation is completed.

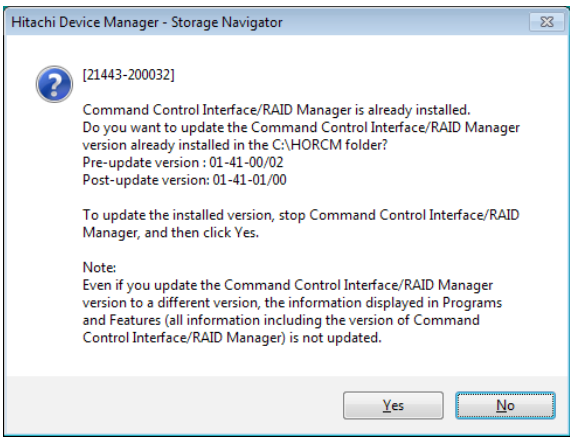


5. Installation start
   The “InstallShield” window is displayed when the preparation is completed.
   Click the [Next >] button.



6. Confirming OSS licenses
   The “Confirmation” window of the JRE, Perl, Apache, Jetty, Openssl and Flash licenses is displayed.
   When the firmware version is 83-03-21-x0/xx or later, PuTTY is displayed as well as those above.
   Select [I accept the terms of the license agreement] and click the [Next >] button.

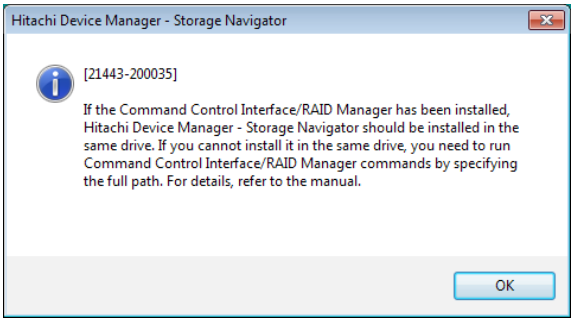




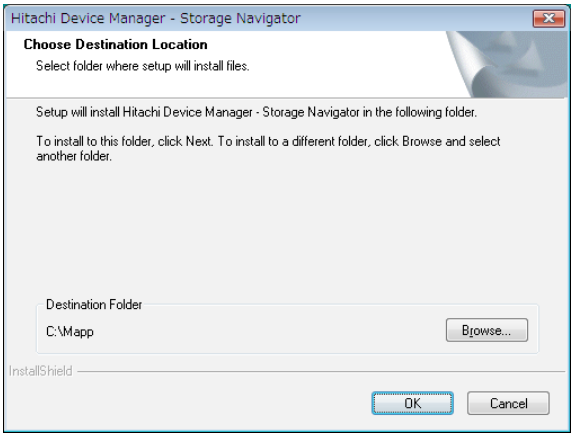
Copyright © 2015, 2017, Hitachi, Ltd.

- 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.

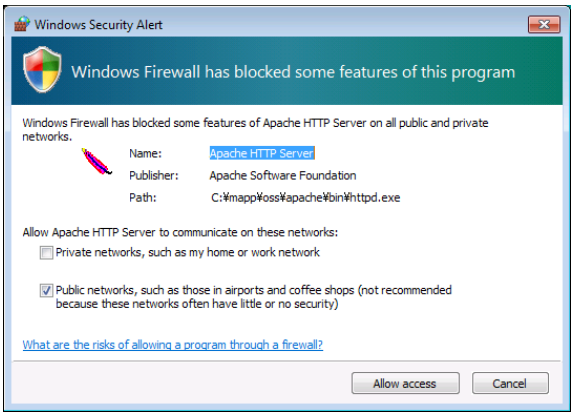
7. Selecting an installation directory
   This window is not displayed when performing update installation of the Maintenance PC software.
   Go to Step 8.
   (1) The confirmation message concerning the installation drive for the storage management software is displayed. Check the content and click [OK].



   (2) Select a directory to be installed and click [OK].
   (3) Specify [C:\Mapp] for the directory.

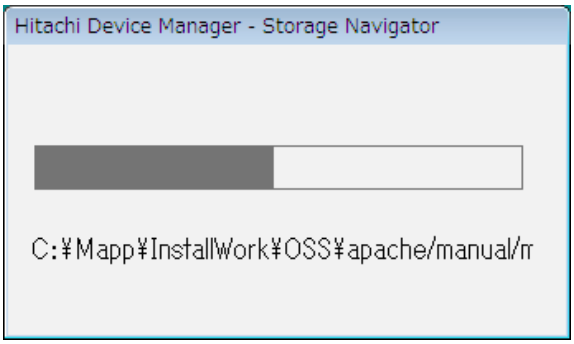


NOTE:
- The directory selection is the procedure required at the time of initial installation only.
- When OSS is installed, the skip confirmation message is displayed. Click [Yes].
- When the “Windows Security Alert” window is displayed, click [Allow Access].
- To change the default directory to a different 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.

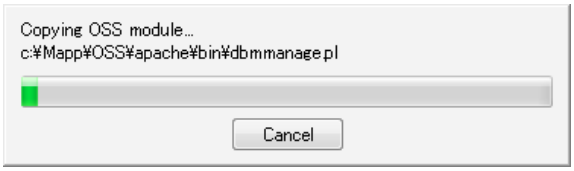


8. Decompressing and copying the Firmware
   Decompress the files in the media and copy them to the folder selected in Step 7.
   The following window is displayed during the processing.
   Wait until the decompression and copy are completed.

   <Decompressing Files>

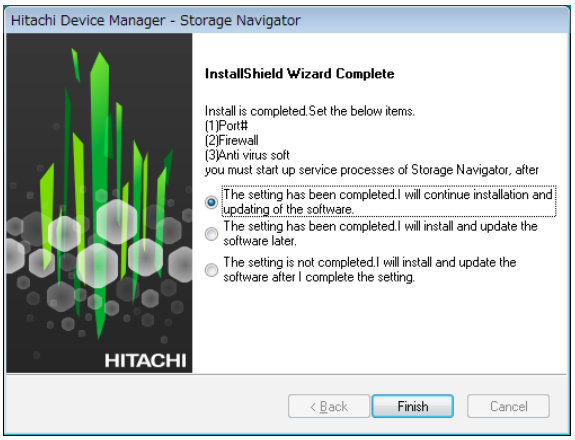


   <Copying Files>



Copyright © 2015, 2017, Hitachi, Ltd.

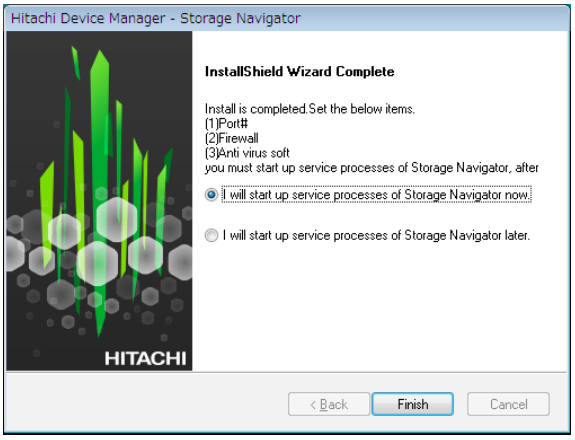
9. Completion message
   - When the firmware version of Installation Media for Maintenance PC is 83-01-21-x0/xx or later
     (1) Select [The setting has been completed. I will continue installation and updating of the software.] and click the [Finish] button.
     Select [The setting has been completed I will install and update the software later.] for New Installation.



     Select [The setting is not completed. I will install and update the software after I complete the setting] and click the [Finish] button. The window is closed and the software installation of the Maintenance PC is complete.

     (2) Go to Step 10.

   - When the firmware version of Installation Media for Maintenance PC is earlier than 83-01-21-x0/xx
     (1) Select [I will start up service processes of Storage Navigator now.] and click the [Finish] button.
     Select [I will start up service processes of Storage Navigator later.] for New Installation.

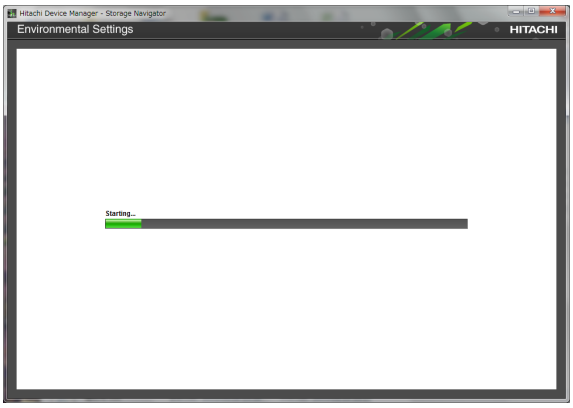


     (2) The installation completes.
     Do not remove the media from the DVD Drive.
     Go to "1.6 Connecting to the Storage System".

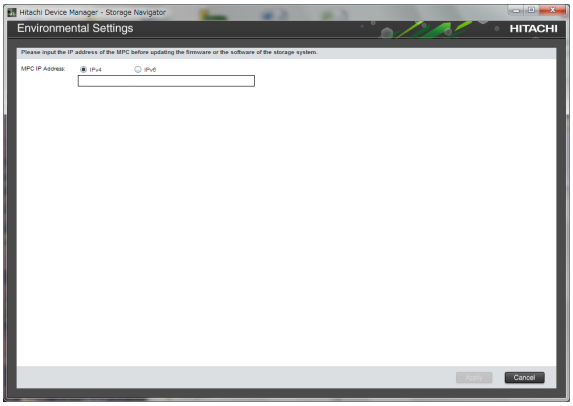
Copyright © 2015, 2017, Hitachi, Ltd.

10. Starting
    When Storage Navigator is installed completely, the Environmental Settings tool starts.

11. Prepare update processing
    The “Preparing Setup” window is displayed. Wait until the preparation is complete.



12. Enter MPC IP Address window
    The “Enter MPC IP Address” window is displayed when the preparation is complete. Click the [Cansel] button.



NOTE: When IP addresses of the Maintenance PC and the storage system are already set, enter the IP addresses without clicking Cancel.Refer to “1.6.2 Procedures for Connecting to the Storage System”.

Copyright © 2015, 2017, Hitachi, Ltd.

1.5.5 Storage Device List Update

Updates the Storage Device List that installed in the maintenance PC or SVP.
When the firmware version is less than 83-01-21-x0/xx, perform the procedure from Step 1.
Start from Step 3 when the Firmware version is 83-01-21-x0/xx or more.

NOTICE: If confirm the version of software that is updated in Maintenance PC, refer to "1.5.4 Maintenance PC Software Installation").

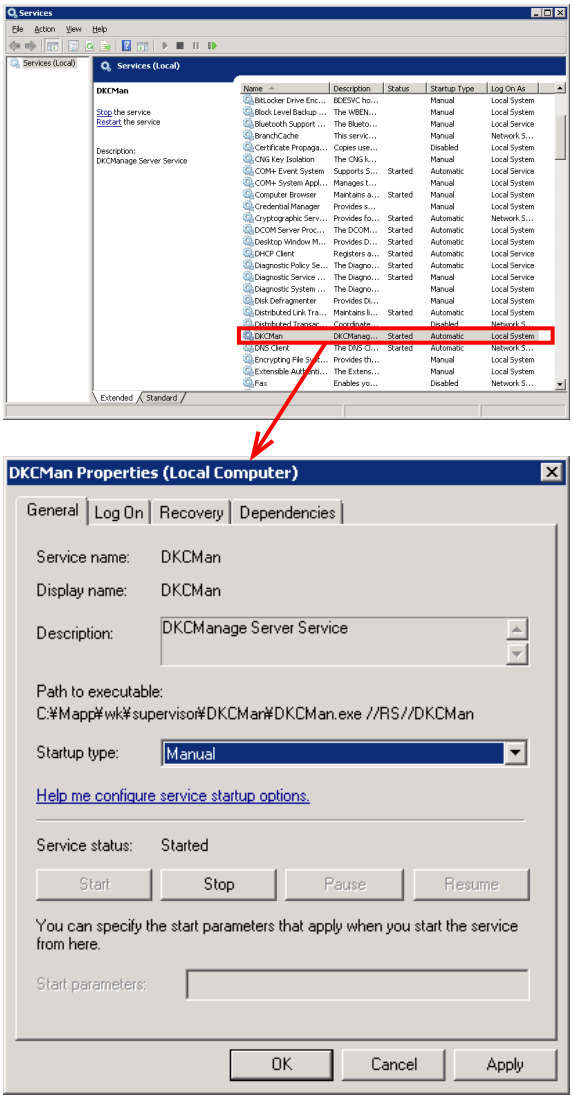
1. Stop the Storage system
   Stop the Storage System by the device list, and then update the Maintenance PC.
   Refer to "1.6.4 Stopping/Starting the Service of Storage System" for detail.

---

2. Stop service processes of Windows
   Stop service processes of Windows, and then update the Maintenance PC.
   (1) Select [Control Panel]-[Administrative Tools]-[Services] from Windows start menue.

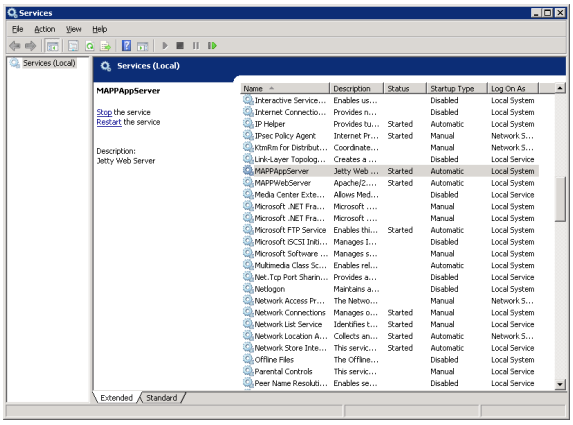
   NOTE: When the Windows user account control starts, select [Continue].

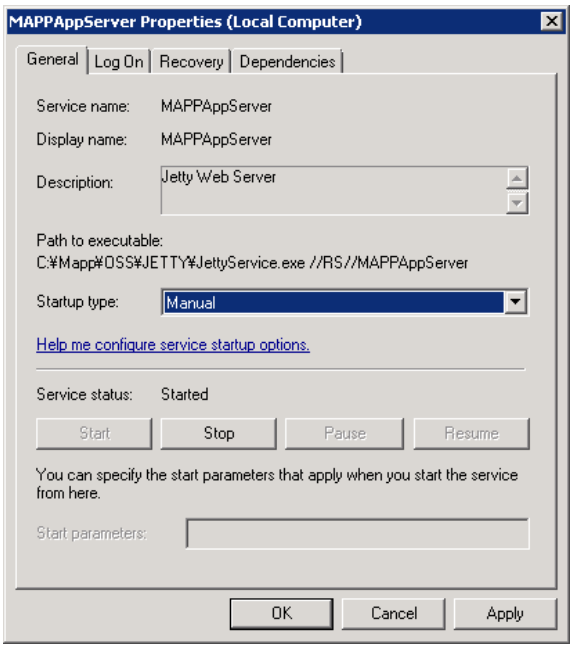
(2) Display the property of DKCMan and set [Startup type] of the [General] tab to [Manual]. Then, select [Apply] and [OK] in order.

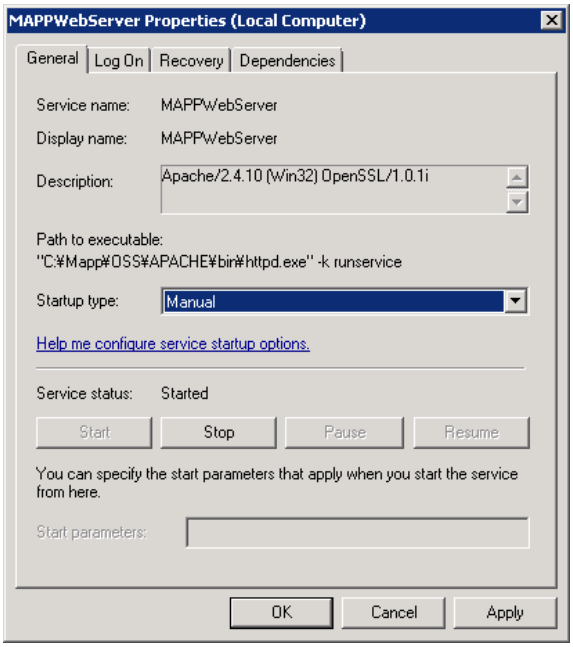


Copyright © 2015, 2017, Hitachi, Ltd.

(3) Set [Startup type] to [Manual] for MAPPAppServer and MAPPWebServer.







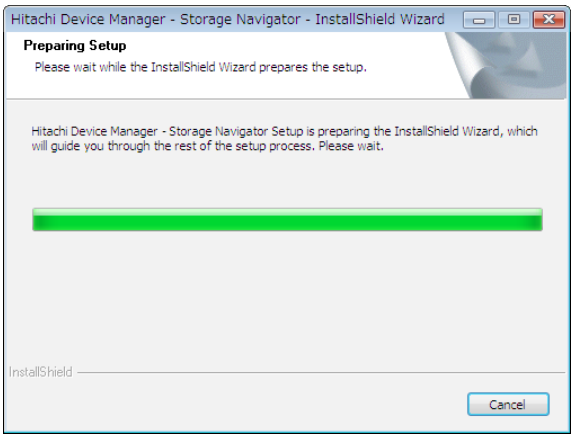
(4) Reboot the Maintenance PC or SVP when you complete to change the setting of the service.

3. Performing Setup. exe

⚠ CAUTION

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 "10.2 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. Once the media is removed, the set information is initialized. Therefore, set the information that was set before the removal again.

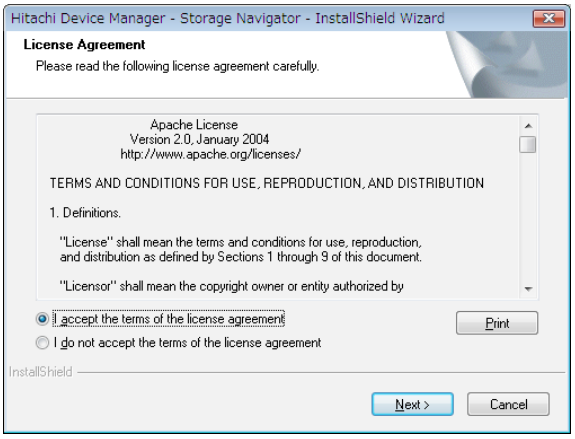
(1) Insert [Installation Media] into the DVD Drive of the Maintenance PC/SVP.
(2) Right-click the "Setup.exe" in the [Installation Media], and select of [Execute as Administrator].
(3) The "Preparing Setup" window is displayed. (The displayed contents is the same as the installation.)



4. Update start
   The “InstallShield” window is displayed when the preparation is completed.
   Click the [Next >] button.



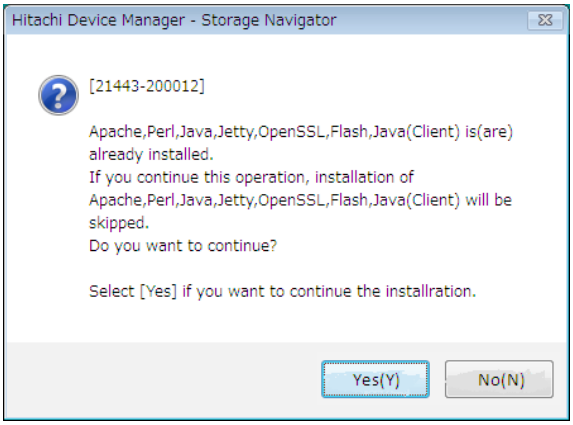
5. Confirming OSS licenses
   The “Confirmation” window of the JRE, Perl, Apache, Jetty, Flash and OpenSSL licenses is displayed.
   When the firmware version is 83-03-21-x0/xx or later, PuTTY is displayed as well as those above.
   Select “I accept the terms of the license agreement” and click the [Next >] button.



NOTE: The Check Languages window is not displayed. The language selected at the time of installation is selected automatically.

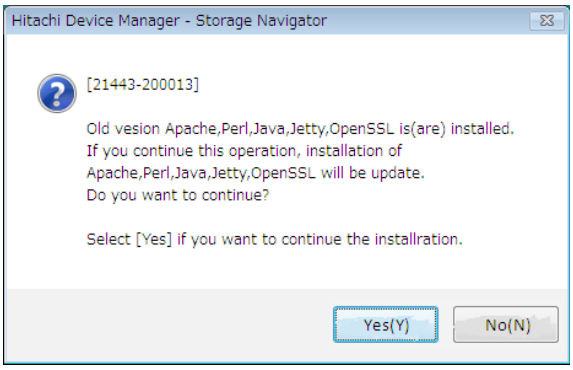
Copyright © 2015, 2017, Hitachi, Ltd.

6. Confirm OSS Version check
   Displays the result of the version check of JRE, JRE(Client), Perl, Apache, Jetty, Flash, OpenSSL.
   When the firmware version is 83-03-21-x0/xx or later, PuTTY is displayed as well as those above.
   If JRE, Perl, JRE(Client), Apache, Jetty, Flash, OpenSSL have been already installed in the Maintenance PC or SVP, the following message will be displayed. Click [Yes] to continue.



NOTE: The “Select Installation Directory” window is not displayed. The update is executed for the directory entered at the time of installation.

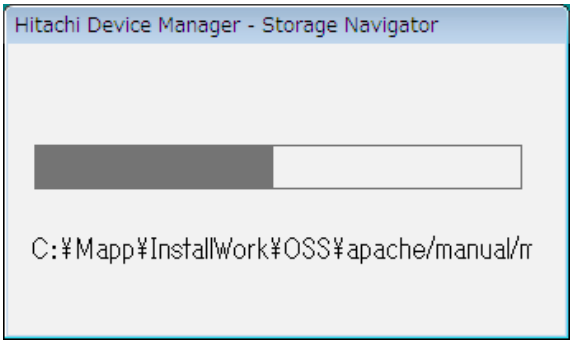
7. Confirm OSS update
   If old versioned JRE, Perl, Apache, Jetty, Flash, OpenSSL have been installed in the Maintenance PC or SVP, the following message will be displayed. Click [Yes] to continue.



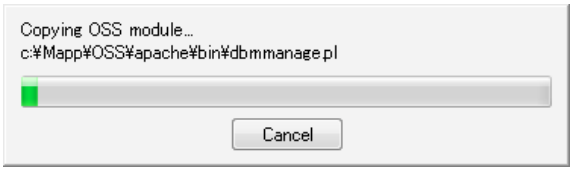
NOTE: The displayed window shows only the third party software name to be updated.

8. Decompressing and copying the Firmware
   Decompress the files in the media and copy them to the folder selected in Step 5.
   The following window is displayed during the processing.
   Wait until the decompression and copy are completed.

   <Decompressing Files>

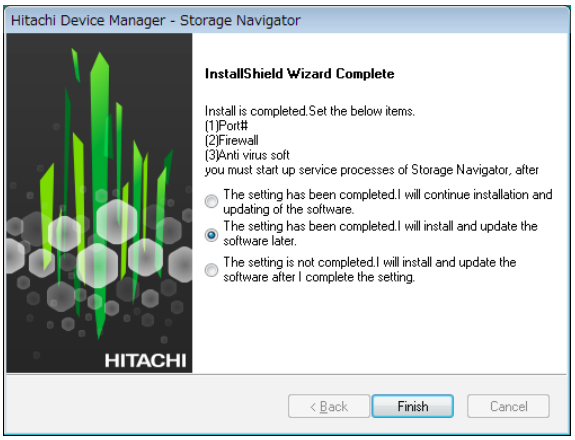


   <Copying Files>



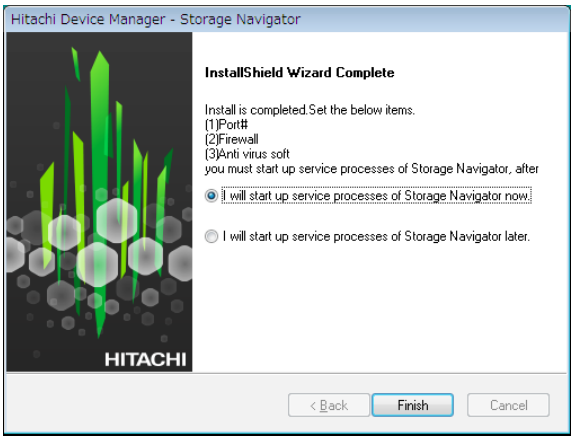
Copyright © 2015, 2017, Hitachi, Ltd.

9. Completion message
   - When the firmware version of Installation Media for Maintenance PC is 83-01-21-x0/xx or later
     (1) Select [The setting has been completed. I will install and update the software later.] and click the [Finish] button.



     (2) To update the software, go to "1.6.5 Changing Storage System Information and Updating Software of Web Console". To start the software, go to "1.6.4.2 Starting the Service of Storage System".

   - When the firmware version of Installation Media for Maintenance PC is earlier than 83-01-21-x0/xx
     (1) Select [I will start up service processes of Storage Navigator now.] and click the [Finish] button.



     (2) To update the software, go to "1.6.5 Changing Storage System Information and Updating Software of Web Console".
     To start the software, go to "1.6.4.2 Starting the Service of Storage System".

Copyright © 2015, 2017, Hitachi, Ltd.

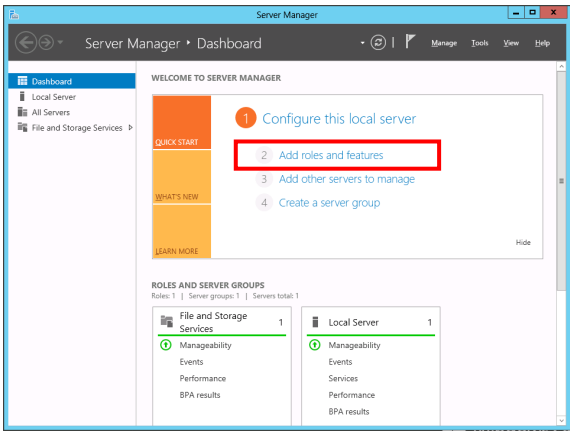
1.5.6 How to use Flash Player that is installed on Windows Server 2012 or later

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.

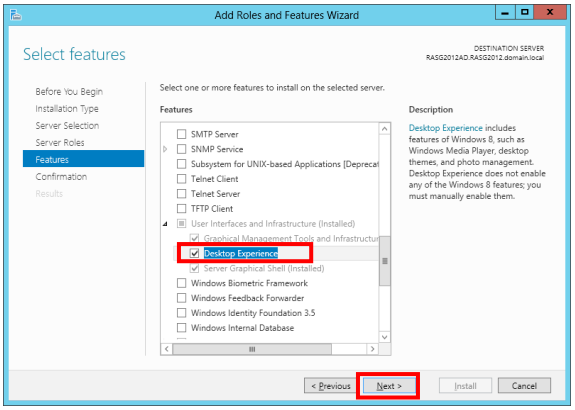
1.5.6.1 Using Flash Player in Windows Server 2012

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

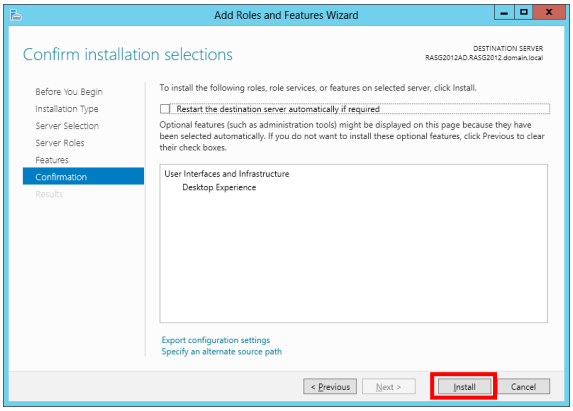
1. Click [Add roles and features] in [Server Manager > Dashboard] - [WELCOME TO SERVER MANAGER] - [QUICK START].



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.

Copyright © 2015, 2017, Hitachi, Ltd.

1.5.7 Precautions Related to the Use of the Virus Detection Program

When using Web Console on the Maintenance PC in which the virus detection program is installed, the operation of Web Console might be affected.
Threrfore, exclude the following directories from the real time virus scan targets by the virus detection program.

C:\Mapp\wk

“C:\Mapp” indicates a Web Console installation directory.
When other than “C:\Mapp” is specified for an installtion 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.

Copyright © 2015, 2017, Hitachi, Ltd.

1.5.8 Function List

Tool Kind	Function	Refer
Storage Device List → Right-click the icon on the desktop and select [Run as administrator] to start the Storage System.	Stopping and connectiong the Storage System	1.6.2 Procedures for Connecting to the Storage System 1.6.4 Stopping/Starting the Service of Storage System
	Changing Storage System information and updating Web Console software	1.6.5 Changing Storage System Information and Updating Software of Web Console
Web Console → Refer to "1.6.2 Procedures for Connecting to the Storage System".	Connecting to the Host	4.1 Connecting to the Host
		4.1.1 Creating Parity Groups
		4.1.2 Verifying LDEVs
		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)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

Tool Kind	Function	Refer
MPC Window (old SVP tool) → Refer to "1.8.1 Maintenance PC Window" • When the "Web Console" window is not running, refer to "1.8.1.2 Starting the Maintenance PC Window Only" to start the Storage System.	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
	Config Backup	5.10 Config Backup
	Initializing the Configuration Information	5.11 Initializing the Configuration Information
	Maintenance Screen	5.12 Maintenance Screen
		5.13 Maintenance Procedure
		5.13.1 Copy Status View
		5.13.2 Version of Firmware
		5.13.3 Pin Data Indication
		5.13.4 PCB/SFP Revision Display
		5.13.5 Inter-PCB Logical Path
		5.13.6 Restoring Failed MP
		5.13.7 Failed CTL Recovery
		5.13.8 Error or Failure Status Action
	Monitoring	8. Monitoring
	Removing Cache Memory/ Cache Flash Memory/ Battery	INSTALLATION SECTION "4.7 Removing Cache Memory/Cache Flash Memory/Battery"

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

Tool Kind	Function	Refer
Maintenance Utility → Refer to "1.8.2 Maintenance Utility Window"	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 NAS Module	INSTALLATION SECTION "3.6 Adding NAS Module"
	Adding Disk Board (DKB)/ Replacing Disk Board	INSTALLATION SECTION "3.7 Adding Disk Board (DKB)/Replacing Disk Board (DKB) (Type Change)"
	Adding Cache Memory/ Cache Flash Memory/ Battery	INSTALLATION SECTION "3.8 Adding Cache Memory/ Cache Flash Memory/Battery"
	Adding Shared Memory	INSTALLATION SECTION "3.9 Adding Shared Memory (SM)"
	Changing the Type of Small Form-Factor Pluggable	INSTALLATION SECTION "3.10 Changing the Type of Small Form-Factor Pluggable (SFP)"
	Adding PDUs for a Rack and PDU Power Codes	INSTALLATION SECTION "3.11 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 NAS Module	INSTALLATION SECTION "4.6 Removing NAS Module"
	Removing Disk Board	INSTALLATION SECTION "4.7 Removing Disk Board (DKB)"
	Removing Shared Memory	INSTALLATION SECTION "4.9 Removing Shared Memory (SM)"
	Removing PDUs for a Rack and PDU Power Codes	INSTALLATION SECTION "4.10 Removing PDUs for a Rack and PDU Power Codes"
	New Installation of the NAS Unified Firmware	INSTALLATION SECTION "7.1 New Installation of the NAS Unified Firmware"
	Removing the NAS Unified Firmware	INSTALLATION SECTION "7.2 Removing the NAS Unified Firmware"
	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)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

Tool Kind	Function	Refer
Maintenance Utility → Refer to "1.8.2 Maintenance Utility Window"	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 a 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"
	Replacing a Air Filters	REPLACEMENT SECTION "2.22 Air Filters"
	Replacing a NAS Module	REPLACEMENT SECTION "2.29.1 Replacing a NAS Module "
		REPLACEMENT SECTION "2.29.2 Replacing a Cache Memory for NAS Module"
		REPLACEMENT SECTION "2.29.3 Replacing a Small Form-Factor Pluggable (SFP+) for NAS Module"
	Initial Setting Wizard	2.4 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)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

Tool Kind	Function	Refer
Maintenance Utility → Refer to "1.8.2 Maintenance Utility Window"	Setting up License Keys	3.7 Setting up License Keys
		3.7.1 Types of License Keys
		3.7.2 Software Packaging
		3.7.3 Software and Licensed Capacity
		3.7.4 Calculating Licensed Capacity
		3.7.5 Installing Software Using a License Key Code
		3.7.6 Enabling a License
		3.7.7 Disabling a License
		3.7.8 Removing Program Product
		3.7.9 Verifying License
		3.7.10 Cautions on Licensed Capacity in Non-License-Related Windows
		3.7.11 Troubleshooting related to licenses
		3.7.12 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
		3.8.4 Sending a Test Message to the Syslog Server
	Locate LED	3.9 Turn on/off Locate LEDs
		3.9.1 Trun on Locate LED
		3.9.2 Trun 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 System Parameters	3.16 Edit 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 System Dumps	3.27 Acquiring System Dumps
	NAS Module Status	3.28 Confirming the NAS Module Status
		3.28.1 Displaying the NAS Module Status
		3.28.2 Resetting Unified Hypervisor
		3.28.3 Resetting Hypervisor Network Module
		3.28.4 Resetting NAS Unified Firmware
		3.28.5 Editing Unified Hypervisor Maintenance Mode

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

Tool Kind	Function	Refer
NAS Manager (*1) → Refer to "6.1 Logging into/Logging out NAS Manager" for how to start	Logging into NAS Manager	6.1 Logging into/Logging out NAS Manager
	Collecting IP address information	6.2 Collecting IP Address Information
	Confirming node status	6.3 Confirming the Node Status
	Migrating EVS	6.4 Migrating EVS
		6.4.1 Migration before the Maintenance Operations
		6.4.2 Migration after the Maintenance Operations
	Adding license keys	6.5 Adding License Keys
	Backup of node registry	6.6 Backup of Node Registry
	DNS settings and confirmation	6.8 DNS Settings and Confirmation
	Setting the time and the NTP Server	6.9 Setting the Time and the NTP Server
	Confirming the event log	6.10 Confirming the Event Log
	Confirming the firmware version of the node	6.11 Confirming the Firmware Version of the Node
	Collecting logs of node and SMU	6.12 Collecting Logs of Node and SMU
Maintenance CLI → Refer to "7.1.2 Logging into the Node" for how to start		7. Maintenance CLI
	Operation Procedure of the Command	7.1 Operation Procedure of the Command
	Logging into Node	7.2 Logging into Node
	Dumps for NAS	7.3 Dumps for NAS
		7.3.1 Collecting NAS Dumps Manually
		7.3.2 Collecting NAS-OS Dump
	List of Commands to be Used	7.4 List of Commands to be Used

*1: NAS Manager is a tool used for the NAS Module failure investigation and the EVS operation.

Copyright © 2015, 2017, Hitachi, Ltd.

1.6 Connecting to the Storage System

Multiple storage systems can be registered in Storage Device List.
A maximum number of Maintenance PCs and SVP that can be registered for each firmware version are shown below.

	When the firmware version is less than 83-01-21-x0/xx	When the firmware version is 83-01-21-x0/xx or later
Maintenance PC	16	256
SVP	1	256

1.6.1 Precautions on Maintenance PC Connection

(1) Procedure for connecting to another Storage System with the same IP address via LAN
When maintaining multiple Storage System with the same IP address by connecting to an Maintenance PC via LAN, if one Storage System connects to the Maintenance PC, the Maintenance PC stores the IP address and physical address of the Storage System in pairs. As a result, if another Storage System connects to the Maintenance PC via LAN, the physical address differs and the IP address is not accepted.
For connecting via LAN, execute the following command from an MS-DOS prompt on a Windows PC and delete the IP address information stored in an arp table on the Maintenance PC.

```
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
```

Execute the following command from the MS-DOS prompt on the Windows PC to check if the IP address stored in the arp table was deleted.

```
arp –a
```

If a message “No specified IP address exists” or “No ARP Entries Found” is returned from the Storage System, the IP address has been deleted from the arp table.

Copyright © 2015, 2017, Hitachi, Ltd.

1.6.2 Procedures for Connecting to the Storage System

1.6.2.1 Register the Storage System

For the register the Storage System, see the following table to register the Storage System.

	When the firmware version in the installation media is 83-01-21-x0/xx or earlier	When the firmware version in the installation media is 83-01-21-x0/xx or later
When the firmware version of the running Storage System is 83-01-21-x0/xx or earlier	See the following to register the Storage System. (MPC01-249F)	See the following to register the Storage System. (MPC01-249F)
When the firmware version of the running Storage System is 83-01-21-x0/xx or later	It is version down of the Firmware. It is necessary to contact TSD (Technical support Division) for approval.	See the following to register the Storage System. (MPC01-240)

[When collectively]

⚠ CAUTION

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 "10.2 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. Once the media is removed, the set information is initialized. Therefore, set the information that was set before the removal again.

NOTICE: Before performing the installation/update or uninstallation, close the Event Viewer of Windows.

NOTICE: If the window indicating the expiration of the electronic certificate is displayed at the start-up of the Maintenance window when the installed Java version is Java 1.7.0_55 or later or Java 1.8.0_5 ro later, the Java security settings must be changed.
For the details, see "3.29. Changing Java Security Settings When Electronic Certificate is Expired".

NOTICE: Before downgrading the firmware version, ask the technical support division about the appropriateness of the operation.

- Do not perform the version downgrade during initial copy and resynchronization of TrueCopy, Universal Replicator, and global-active device. If it is performed, the firmware update might fail.
- You cannot downgrade a revision number (RR of 83-RR-XX-XX/XX) of the DKCMAIN firmware when the firmware version of the DKC in operation is as follows: If the version is as follows, update the firmware offline.
  - 83-03-30-x0/xx or less
  - 83-04-01-x0/xx or later and 83-04-28-x0/xx or less
  - 83-04-41-x0/xx or later and 83-04-44-x0/xx or less

Copyright © 2015, 2017, Hitachi, Ltd.

1. Checking and recording EVS status to deal with NAS Modules
   When the firmware version is 83-03-21-x0/xx or later and NAS Modules are already installed, follow the procedure below to update the firmware (Unified Hypervisor, NASFWINST, and NASFW) for NAS Module.
   Go to Step 2 for other than the above-mentioned status.

   Before starting the firmware update, check and record the running EVS status in the NAS Module.
   See Step 1 to Step 5 in "6.4.1 Migration before the Maintenance Operations" for the procedure for checking EVS.

2. Clearing the cache of the browser
   (1) Clear the cache of the browser.
      (a) When using Internet Explorer
         (i) Open [Start] - [Control Panel] - [Internet Options].
         (ii) Click the [Delete] button of [Browser History] in the [General] tab.
         (iii) Check that the check box of [Internet Temporary File] is checked and click the [Delete] button.
      (b) When using Firefox
         (i) Select the [Network] tab of [Details] in the "Option" window and click the [Erase Immediately] of [Cached Web Page].

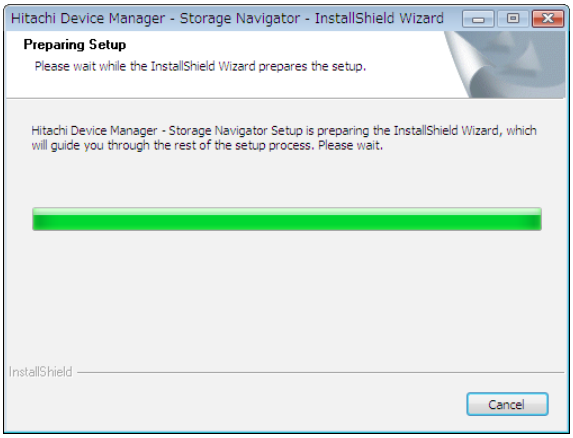
   (2) Close all the open browsers

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

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

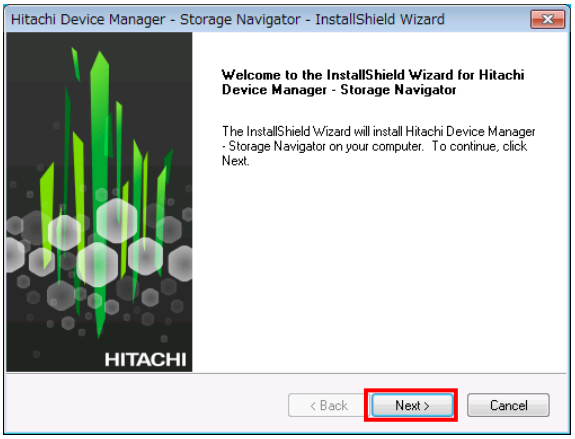
   NOTE: If a DVD drive is not mounted on a PC, copy all the files of installation media for the Maintenance PC to "work folder". For a "work folder" name, do not use a double -byte character because Setup.exe might not start if a double-byte character is included in the name.
   Then, use the files in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

5. The "Preparing Setup" window is displayed. Wait until the preparation is completed.



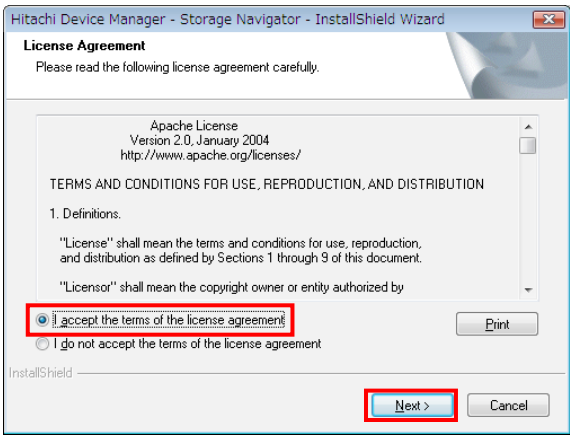
Copyright © 2015, 2017, Hitachi, Ltd.

6. The “Welcome” window is displayed when the preparation is completed. Click the [Next >] button.

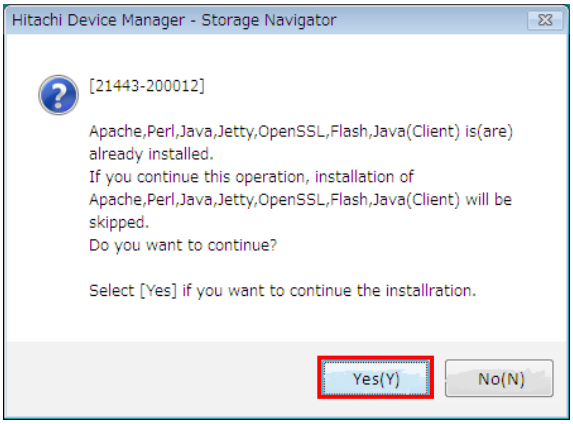


Copyright © 2015, 2017, Hitachi, Ltd.

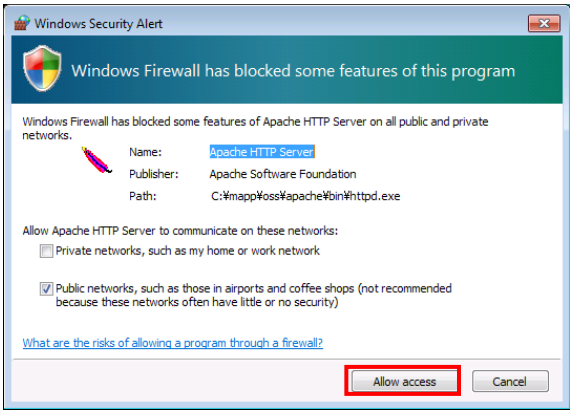
7. The “Confirmation” window of the JRE, Perl, Apache, Jetty, Openssl and Flash licenses is displayed. When the firmware version is 83-03-21-x0/xx or later, PuTTY is displayed as well as those above. Select [I accept the terms of the license agreement] and click the [Next >] button.



8. The skip confirmation message is displayed. Click the [Yes] button.

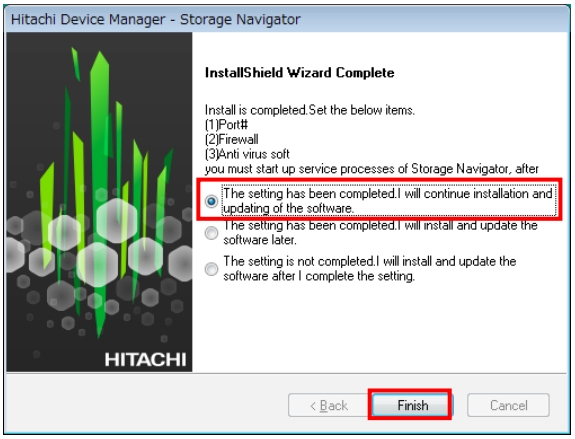


NOTE: When the “Windows Security Alert” window is displayed, click [Allow Access].

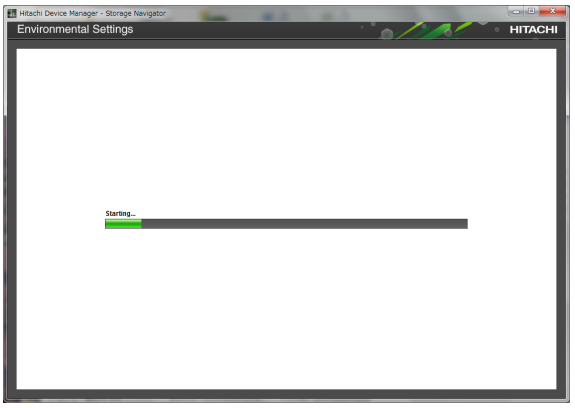


Copyright © 2015, 2017, Hitachi, Ltd.

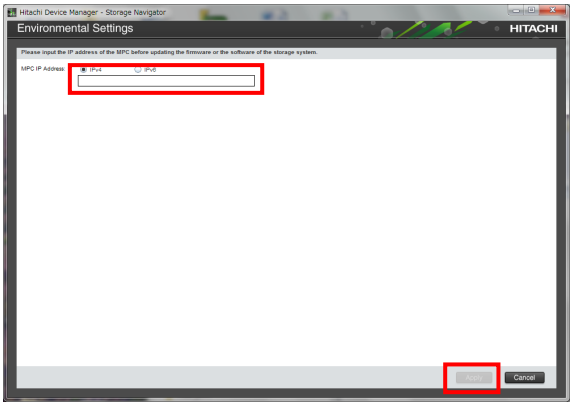
9. The installation completion message is displayed. Select [The setting has been completed. I will continue installallation and updating of the software.] and click the [Finish] button.



10. Prepare update processingThe Preparing update window is displayed. Wait until the preparation is complete.



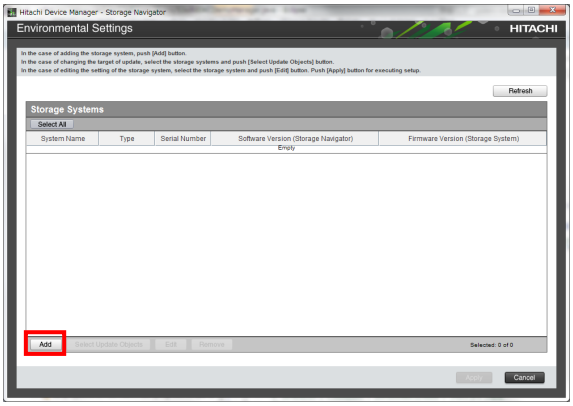
11. The Enter MPC IP Address window is displayed when the preparation is complete. Enter the IP address of the port used for connecting the Maintenance PC and the storage system and click the [Apply] button.



NOTE: This window does not open in the second time and later, and when the IP address of the Maintenance PC is set in the procedure of Setting Up IP Address on "1.6.2 Procedures for Connecting to the Storage System".

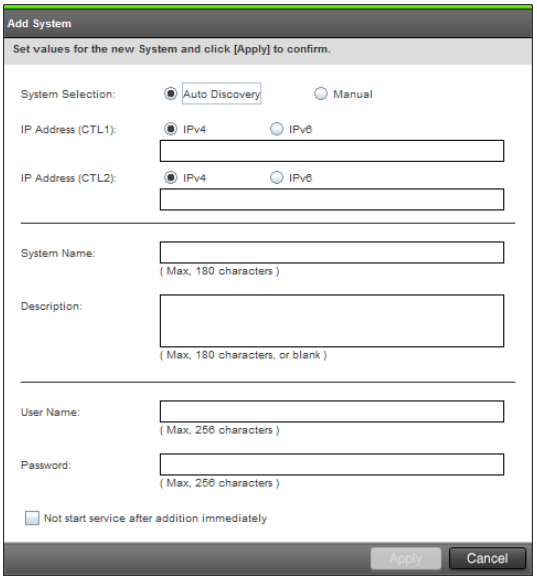
Copyright © 2015, 2017, Hitachi, Ltd.

12. The target storage systems list window is displayed. Click the [Add] button.



13. The "Add System" window appears. Enter each setting item as follows and click the [Apply] button. See the next page to perform it manually.

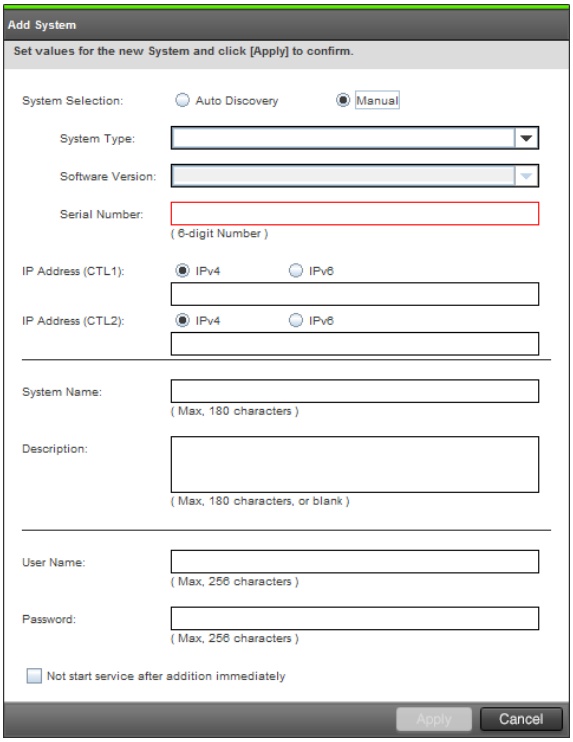
- When selecting [Auto Discovery]



Copyright © 2015, 2017, Hitachi, Ltd.

Item	Description
System Selection	Select the input method of the Storage System information. • [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)	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	Set the display name of the storage system. The number of characters you can enter up to 180. Allowed characters are one-byte alphanumeric characters, symbols (# $ % & ' * + - . / = ? @ ^ _ ` { | } ~). You cannot use one-byte spaces.
Description	Enter the description of the Storage System. The number of characters you can enter is zero to 180.
User Name	Enter a user name.
Password	Enter the password of the Storage System.
Not start service after addition immediately	Select whether to connect the registered Storage System immediately. To update the firmware, check the checkbox. If the checkbox is unchecked, the service starts and Web Console gets ready to start immediately. (Default is unchecked)

- When selecting [Manual]

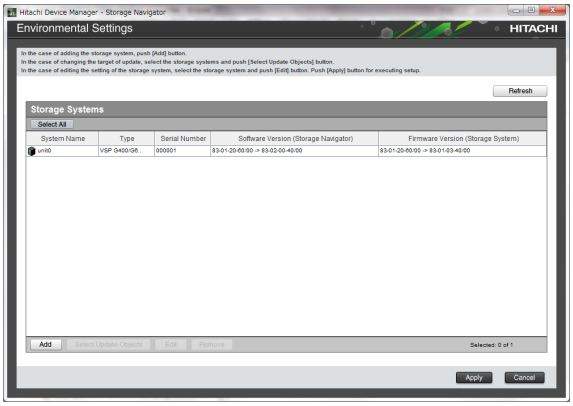


Copyright © 2015, 2017, Hitachi, Ltd.

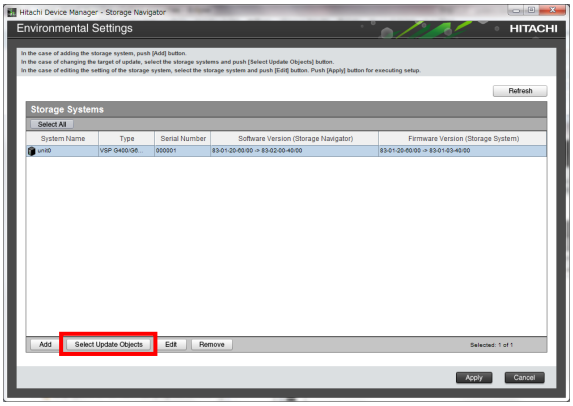
<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>System Selection</td><td>Select the input method of the Storage System information.
• [Auto Discovery] (default selection): Acquire the Storage System information automatically.
• [Manual]: Set each of the displayed items, [System Type], [Software Version] and [Serial Number].</td></tr>
<tr><td>System Selection - System Type</td><td>Select a Storage System type.
[VSP G800 and VSP F800]
[VSP G400/G600 and VSP F400/F600]
[VSP G200]</td></tr>
<tr><td>System Selection - Software Version</td><td>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.
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.
<Example>
xx-xx-xx-xx/xx(xx-xx-xx/60) for Japan domestic
xx-xx-xx-xx/xx(xx-xx-xx/00) for global
• Notes:
When a Config version model is 60, “for Japan domestic” is displayed; when a Config version model is 00, “for global” is displayed.
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.
<table>
<tr><th>Model name of the Storage System</th><th>Model of Config version to be selected</th></tr>
<tr><td>HT-40SB, HT-40SC, HT-40SD</td><td>60</td></tr>
<tr><td>DW800</td><td>00</td></tr>
</table>
</td></tr>
<tr><td>System Selection - Serial Number</td><td>Enter the serial number. The serial number consists of a six digit number beginning with “4”. Only numbers are usable.</td></tr>
<tr><td>IP Address (CTL1)</td><td>Enter the CTL1 IP address. Select IPv4 (Default) or IPv6, and then enter the IP address.</td></tr>
<tr><td>IP Address (CTL2)</td><td>Enter the CTL2 IP address. Select IPv4 (Default) or IPv6, and then enter the IP address.</td></tr>
<tr><td>System Name</td><td>Set the display name of the storage system.
The number of characters you can enter up to 180.
Allowed characters are one-byte alphanumeric characters, symbols (# $ % & ' * + - . / = ? @ ^ _ ` { | } ~).
You cannot use one-byte spaces.</td></tr>
<tr><td>Description</td><td>Enter the description of the Storage System.
The number of characters you can enter is zero to 180.</td></tr>
<tr><td>User Name</td><td>Enter a user name.</td></tr>
<tr><td>Password</td><td>Enter the password of the Storage System.</td></tr>
<tr><td>Not start service after addition immediately</td><td>Select whether to connect the registered Storage System immediately.
To update the firmware, check the checkbox.
If the checkbox is unchecked, the service starts and Web Console gets ready to start immediately. (Default is unchecked)</td></tr>
</table>

Copyright © 2015, 2017, Hitachi, Ltd.

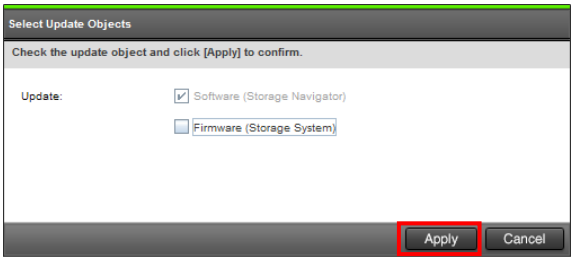
14. The entered storage system is added to the target storage systems list window.



15. Select whether to update the firmware and add the storage system simultaneously. Select the storage systems that change the state whether to update and click the [Select Update Objects] button.



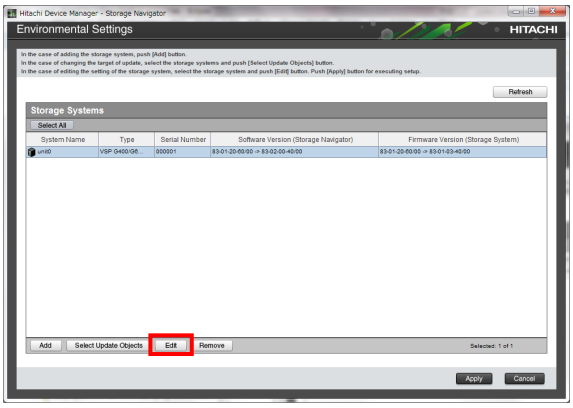
16. The “Select Update Objects” window is displayed. Check the Firmware (Storage System) to update the firmware. If not, uncheck it and click the [Apply] button.



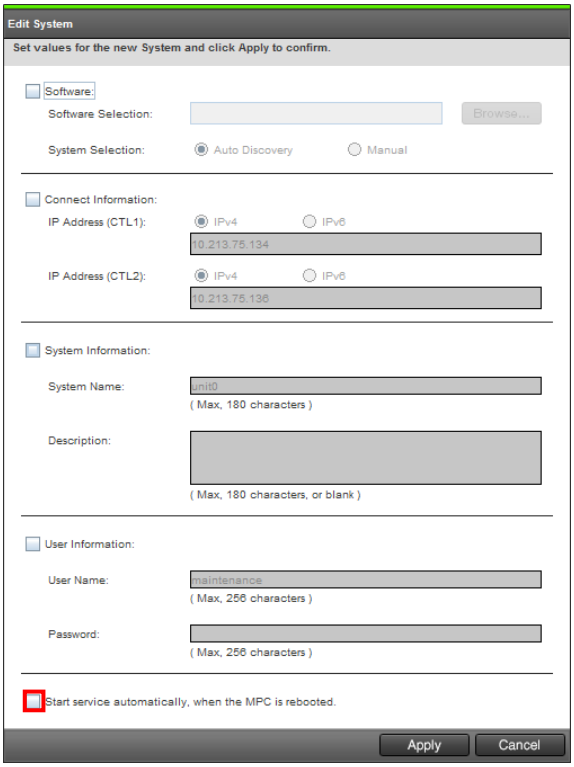
NOTE: The storage system to be registered cannot be changed because the check box of [Software (Storage Navigator)] is automatically checked. When the firmware is set as an update target, two versions are displayed in the form of [Current version] → [Updated version] in Firmware Version (Storage System) shown in the target storage system list window. When these two versions are identical, the firmware update is not required.

Copyright © 2015, 2017, Hitachi, Ltd.

17. When the [Apply] button is clicked, the display is returned to the [Environmental Settings] window. To update the firmware, perform the following operations.
    (1) Select the target storage system and click the [Edit] button.



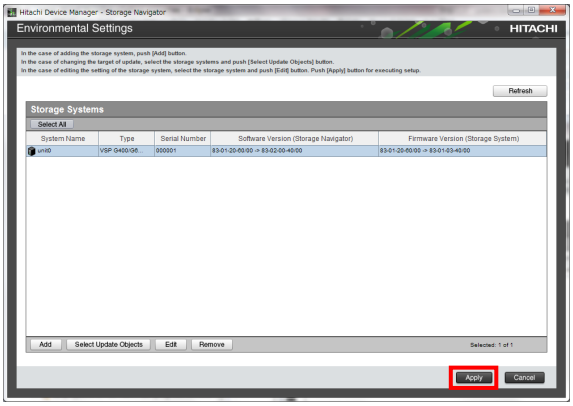
    (2) Confirm that the checkbox of "Start service automatically, when the MPC is rebooted." is unchecked. If the checkbox is checked, uncheck it.



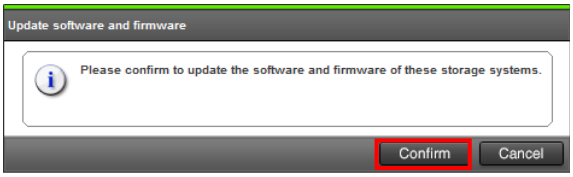
    (3) When the confirmation and the input are completed, click the [Apply] button.

Copyright © 2015, 2017, Hitachi, Ltd.

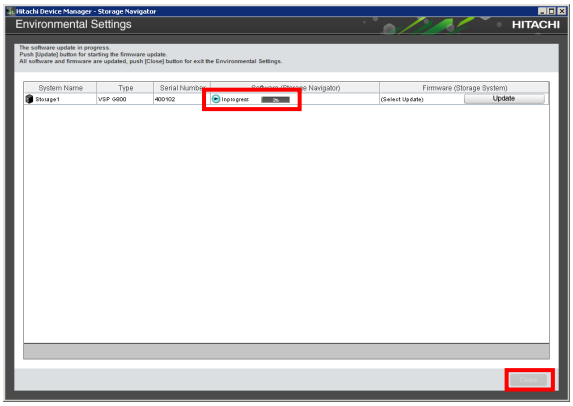
18. Repeat Step 15 to Step 17 for all the storage systems.
    Check whether the current software version/firmware version and the new software version/firmware version are correct.
    When the settings and version confirmation are completed for all the storage systems, click the [Apply] button in the target storage system list window.



19. The Update software and firmware window is displayed. Click the [Confirm] button.



20. The run update firmware window is displayed and the software update of the storage system starts automatically. You can check the software update status in the Software (Storage Navigator) row.

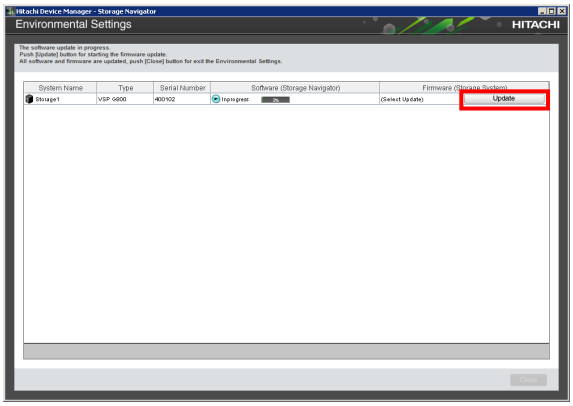


Copyright © 2015, 2017, Hitachi, Ltd.

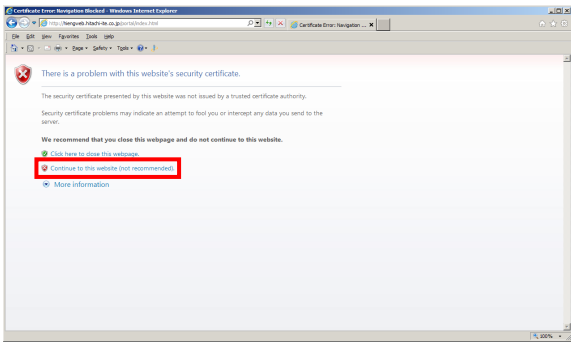
The software update status is as shown below.

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. When an error occurs, see (MPC01-249F) and update the software again.
(Not Update)	This is not selected as a software update target. If storage systems were added, this state does not appear.

21. Access the storage system and update the firmware.To update the firmware, click the [Update] button in the Firmware (Storage System) row.
This procedure is required only when the Firmware is selected as an update target.



(1) If the Security warning window is displayed, click the [Continue to this website] to display the Update Firmware window. Then, close the browser.



NOTE: If Firmware was not selected as an update target, this step is not required.
Perform it again from "1.6.2 Procedures for Connecting to the Storage System".

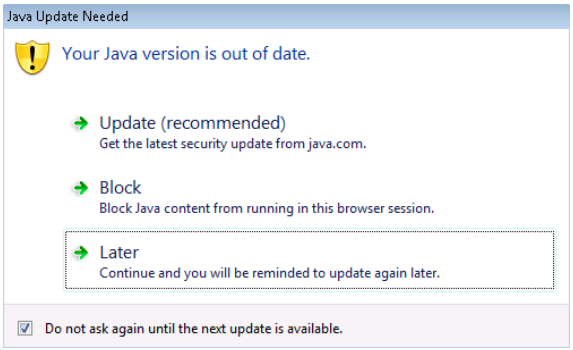
Copyright © 2015, 2017, Hitachi, Ltd.

(2) Java start

The displayed windows differ according to the JRE (Java Runtime Environment) versions.
In the case of JRE7 or JRE8, go to Step (a).In the case of JRE6, go to Step (b)

(a) In the case of JRE7 or JRE8

(a-1) The update of the Java application may be promoted.



When using Maintenance Utility 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], close the window of the Web browser and restart Maintenance Utility. When checking the checkbox of [Do not ask again until the next update is available.] and selecting [Update(recommended)] or [Block], Maintenance Utility cannot update the firmware. To allow Maintenance Utility to update the firmware, execute the following procedures.

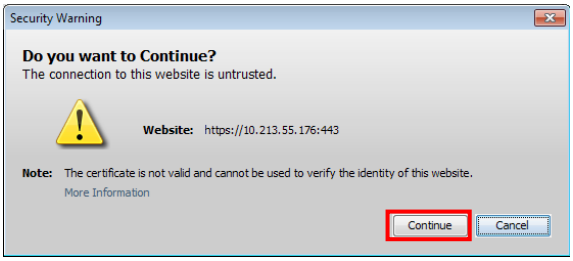
(i) Click [All Programs]-[Java]-[Configure Java] from the [Start] menu of Windows and start [Java Control Panel].
(ii) Click the [Security] tab of [Java Control Panel].
(iii) If the checkbox of [Enable Java content in the browser] in the [Security] tab is checked, uncheck it once and click the [Apply] 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 Maintenance Utility.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

(a-2) When the message “Do you want to Continue?” is displayed, click the [Continue] button.

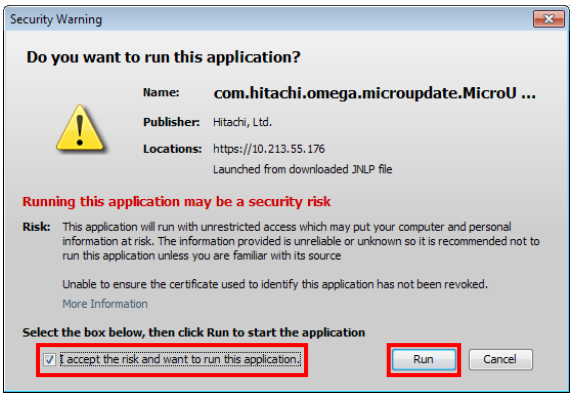
NOTE: This window may not be displayed.



NOTE: If you press the [Cancel] button in the window, the firmware update is not complete. Perform it again from “1.6.2 Procedures for Connecting to the Storage System”.

(a-3) 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. Go to Step (3).

NOTE: This window may not be displayed.



NOTE: If you press the [Cancel] button in the window, the firmware update is not complete.

NOTE: When the “Application Blocked by Java Security” or “Application Blocked by Security Settings” window is displayed, refer to TROUBLESHOOTING SECTION “3.28.1.1 Troubleshooting Related to Installation and Upgrade” and register the storage system in the exception site.
After the registration, perform the procedure of “1.6.2 Procedures for Connecting to the Storage System” again.

Copyright © 2015, 2017, Hitachi, Ltd.

(b) In the case of JRE6

(b-1) When the message "The web site's certificate cannot be verified. Do you want to continue?" is displayed, click the [Yes] button.

NOTE: This window may not be displayed.



NOTE: If you press the [No] button in the window, the firmware update is not complete. Perform it again from "1.6.2 Procedures for Connecting to the Storage System".

(b-2) 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. Go to Step (3).

NOTE: This window may not be displayed.



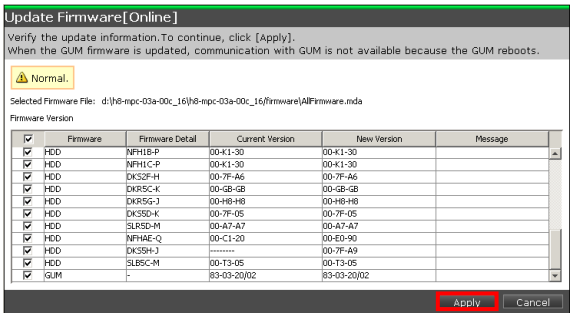
NOTE: If you press the [Cancel] button in the window, the firmware update is not complete. Perform it again from "1.6.2 Procedures for Connecting to the Storage System".

Copyright © 2015, 2017, Hitachi, Ltd.

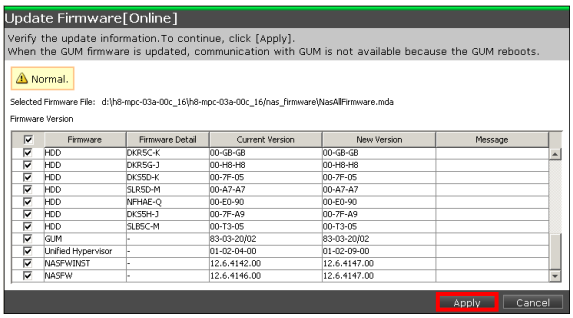
(3) The Update Firmware window is displayed. Click the [Apply] button.

NOTE: The update window varies whether NAS Modules are installed or not. "Unified Hypervisor", "NASFWINST" and "NASFW" are displayed only when NAS Modules are installed.

(a) When NAS Modules are not installed

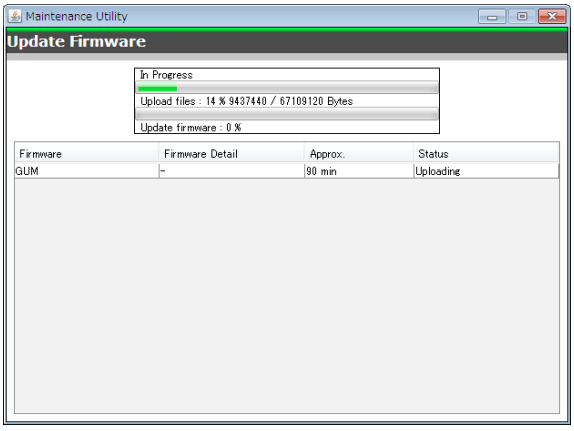


(b) When NAS Modules are installed



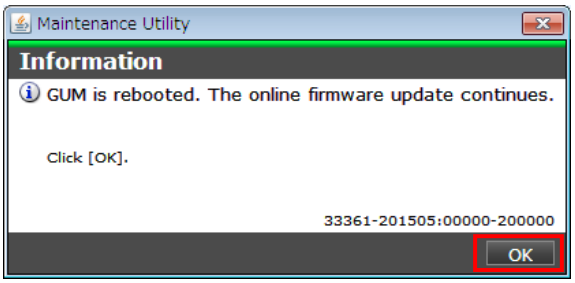
NOTE:
- Clicking Cancel in this window does not complete the firmware update.
- Terminate the tool after completing the software update. Update the firmware again in "1.6.2 Procedures for Connecting to the Storage System".

(4) The progress of the firmware update is displayed.

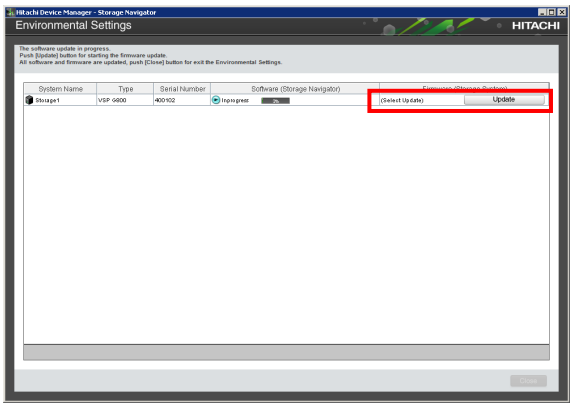


Copyright © 2015, 2017, Hitachi, Ltd.

(5) Once the firmware update proceeds, the following window is displayed and the Update window closes.
Click the [OK] button.



22. You can check the firmware update status in the Firmware (Storage System) row.
Wait until the firmware update is complete.



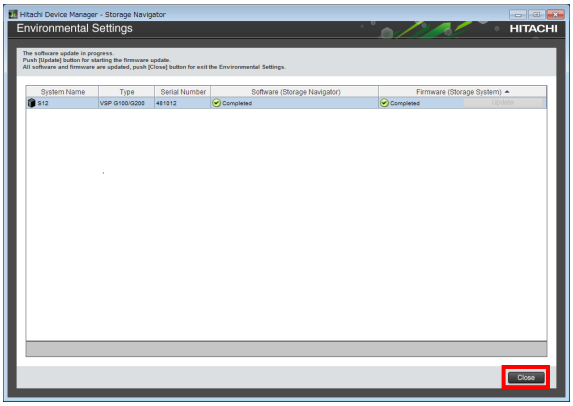
The firmware update status is as shown below.

Status	Description
(Select Update)	Wait for starting the Update Firmware window. Click the [Update] button to display the Update Firmware window.
In Progress	The Update Firmware window started and the firmware update is not complete. This state appears even if the firmware update is cancelled.
Completed	Firmware update is complete.
Failed	Firmware update failed. Click the [Update] button to display the Update Firmware window and check the error details.
Communication Timeout	The completion of the firmware update in time (*1) is not confirmed. Check the state in the Update Firmware window.
(Not Update)	This is not selected as a firmware update target.

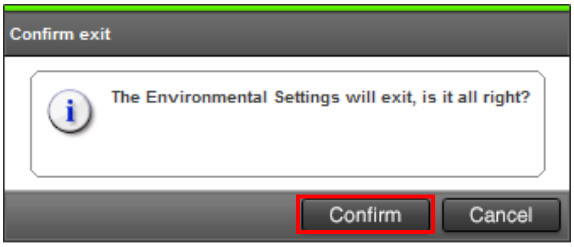
*1: When NAS Modules are not installed: 200 minutes
When NAS Modules are installed: 540 minutes

Copyright © 2015, 2017, Hitachi, Ltd.

23. After completing the update of the software and the firmware, click the [Close] button.



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



25. Restoring EVS to deal with NAS Modules
When the firmware (Unified Hypervisor, NASFWINST, and NASFW) for NAS Module was updated in the state that the firmware version is 83-03-21-x0/xx or later and NAS Modules are already installed, follow the procedure below.
Go to Step 26 for other than the above-mentioned status.

After completing the firmware update, check the running EVS status in the NAS Module.
See Step 1 to Step 5 in "6.4.1 Migration before the Maintenance Operations" for the procedure for checking EVS.

If the checked EVS status is different from the information recorded in Step 1, migrate the EVS to return to the recorded status.
See "6.4.2 Migration after the Maintenance Operations" for the procedure for EVS migration.

26. Start the service of the storage system in accordance with the procedure of "1.6.4.2 Starting the Service of Storage System".

27. If the setting of "Start service automatically, when the MPC is rebooted." is changed, restore the setting.

Copyright © 2015, 2017, Hitachi, Ltd.

28. Clearing the cache of the browser

Perform the following procedure only when the firmware version is less than 83-03-0x-x0/xx.

(1) Clear the cache of the browser.

(a) When using Internet Explorer

(i) Open [Start] - [Control Panel] - [Internet Options].

(ii) Click the [Delete] button of [Browser History] in the [General] tab.

(iii) Check that the check box of [Internet Temporary File] is checked and click the [Delete] button.

(b) When using Firefox

(i) Select the [Network] tab of [Details] in the “Option” window and click the [Erase Immediately] of [Cached Web Page].

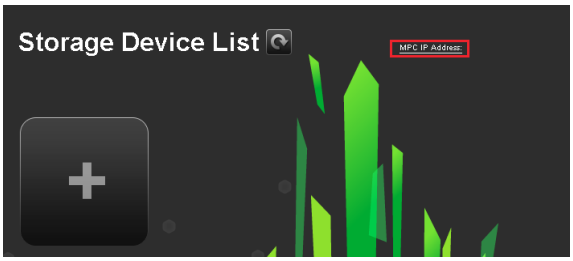
(2) Close all the open browsers

Copyright © 2015, 2017, Hitachi, Ltd.

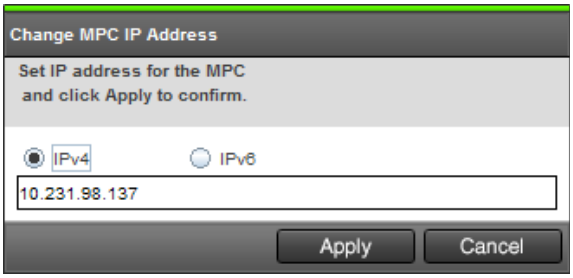
[When Register the Storage System]

1. Right-click the connection icon “Open Storage Device List” on the desktop of the Maintenance PC and select [Run as administrator].

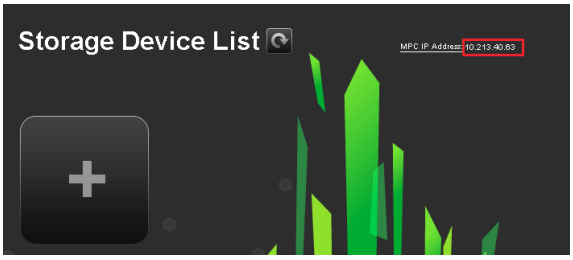
2. Set an IP Address.
   (1) Click the [MPC IP Address] link in the “Storage Device List” window.



   (2) Enter the IP address set in section “1.3.1 IP Address Setting Method of Maintenance PC” into the “Change MPC IP Address” window and click the [Apply] button.

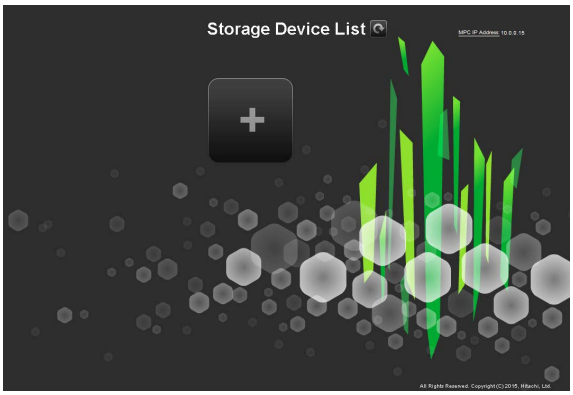


   (3) Check that the IP address set in Step (2) is displayed beside the [MPC IP Address] link.



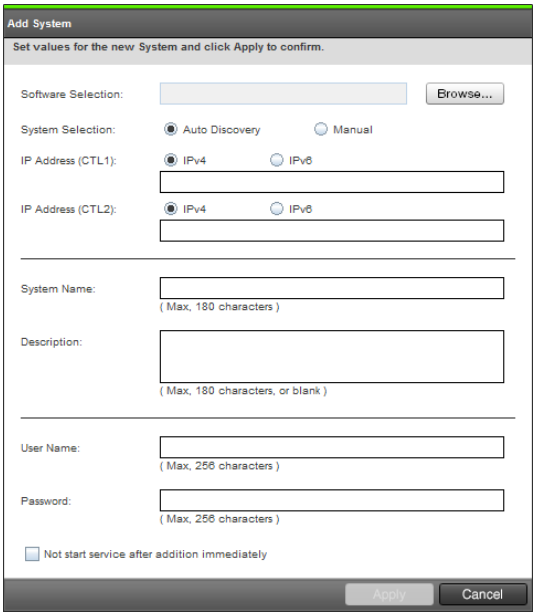
3. Create a Storage System icon.
   If the icon already exists, go to “1.6.2.2 Starting Web Console”.

   (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 MPC01-261 to perform it manually.

   • When selecting [Auto Discovery]

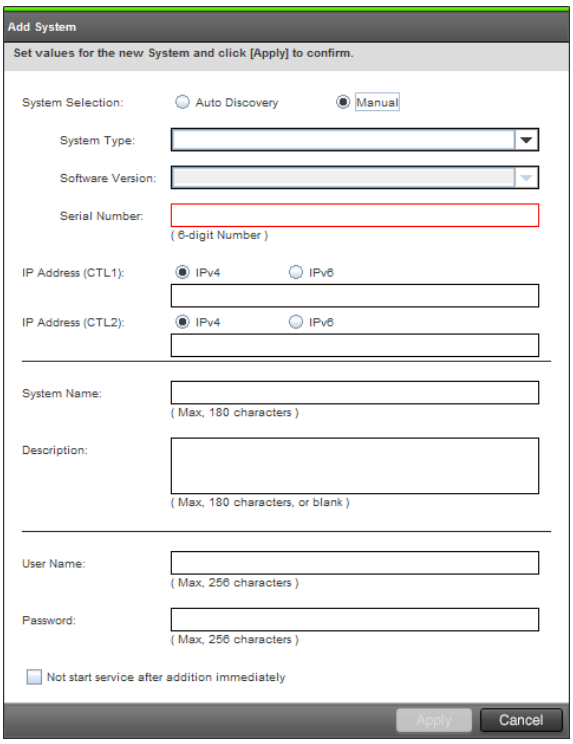


Copyright © 2015, 2017, Hitachi, Ltd.

Item	Description
Software Selection	Specify installation media for the Maintenance PC or “Software\productname.inf” in “work folder” by the [Browse] button to acquire the installation information.
System Selection	Select the input method of the Storage System information. • [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)	• 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)	• 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	Enter a Storage System display name. The number of characters you can enter is zero to 180. Allowed characters are one-byte alphanumeric characters, symbols (# $ % & ' * + - . / = ? @ ^ _ ` { | } ~). You cannot use one-byte spaces.
Description	Enter the description of the Storage System. The number of characters you can enter is zero to 180.
User Name	Enter a user name. The number of characters you can enter is one to 256. Only alphanumeric characters and signs (! # $ % & ' * + - . / = ? @ ^ _ ` { | } ~) are usable.
Password	Enter a password. The number of characters you can enter is six to 256.
Not start service after addition immediately	Select whether to connect the registered Storage System immediately. Check the checkbox for New Installation. If the checkbox is unchecked, the service starts and Web Console gets ready to start immediately. (Default is unchecked)

Copyright © 2015, 2017, Hitachi, Ltd.

- When selecting [Manual]



Item	Description
Software Selection	Specify installation media for the Maintenance PC or “Software\productname.inf” in “work folder” by the [Browse] button to acquire the installation information.
System Selection	Select the input method of the Storage System information. • [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 G800 and VSP F800] [VSP G400/G600 and VSP F400/F600] [VSP G200]

(To be continued)

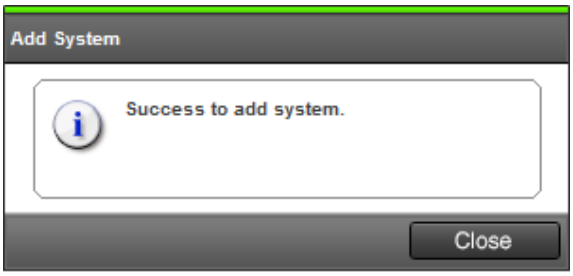
Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>System Selection - Software Version</td><td>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.
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.
<Example>
xx-xx-xx-xx/xx(xx-xx-xx/60) for Japan domestic
xx-xx-xx-xx/xx(xx-xx-xx/00) for global
• Notes:
When a Config version model is 60, “for Japan domestic” is displayed; when a Config version model is 00, “for global” is displayed.
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.
<table>
<tr><th>Model name of the Storage System</th><th>Model of Config version to be selected</th></tr>
<tr><td>HT-40SB, HT-40SC, HT-40SD</td><td>60</td></tr>
<tr><td>DW800</td><td>00</td></tr>
</table>
</td></tr>
<tr><td>System Selection - Serial Number</td><td>Enter the serial number. The serial number consists of a six digit number beginning with “4”. Only numbers are usable.</td></tr>
<tr><td>IP Address (CTL1)</td><td>Enter the CTL1 IP address. Select IPv4 (Default) or IPv6, and then enter the IP address.</td></tr>
<tr><td>IP Address (CTL2)</td><td>Enter the CTL2 IP address. Select IPv4 (Default) or IPv6, and then enter the IP address.</td></tr>
<tr><td>System Name</td><td>Set the display name of the storage system.
The number of characters you can enter up to 180.
Allowed characters are one-byte alphanumeric characters, symbols (# $ % & ' * + - . / = ? @ ^ _ ` { | } ~).
You cannot use one-byte spaces.</td></tr>
<tr><td>Description</td><td>Enter the description of the Storage System.
The number of characters you can enter is zero to 180.</td></tr>
<tr><td>User Name</td><td>Enter a user name.</td></tr>
<tr><td>Password</td><td>Enter the password of the Storage System.</td></tr>
<tr><td>Not start service after addition immediately</td><td>Select whether to connect the registered Storage System immediately.
If the checkbox is unchecked, the service starts and Web Console gets ready to start immediately. (Default is unchecked)</td></tr>
</table>

Copyright © 2015, 2017, Hitachi, Ltd.

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



(4) A Storage System icon is added.

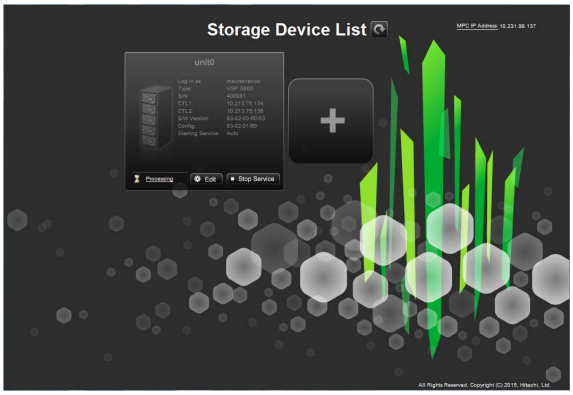


Table 1-3 Icon Display Item

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.

1.6.2.2 Starting Web Console

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.



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”.



Copyright © 2015, 2017, Hitachi, Ltd.

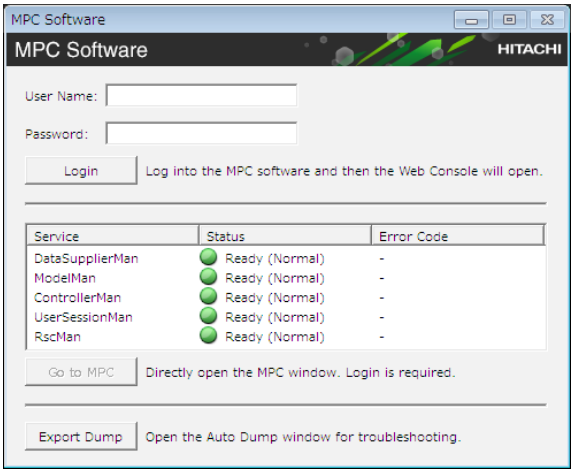
5. Click the Storage System icon.



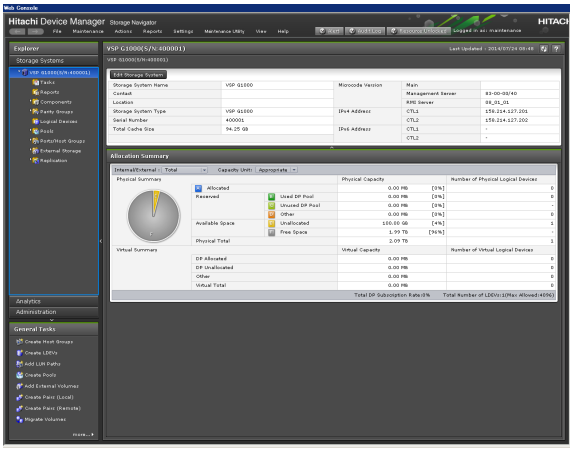
NOTE: When the Firmware version is less than 83-01-21-x0/xx, the [Stop Service] button is not displayed.

6. "MPC Software" is displayed and the service status is checked automatically.
Enter a user name and password and click the [Login] button.
When all become [Ready (Normal)], go to Step 7.

NOTE: If not logged in, the "Web Console" window is not displayed. Check that the [Login] button is inactive.



7. Web Console starts.

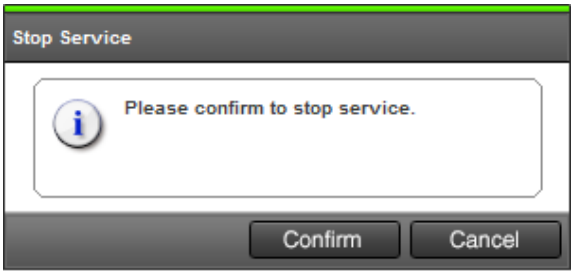


1.6.2.3 Stopping Web Console

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.



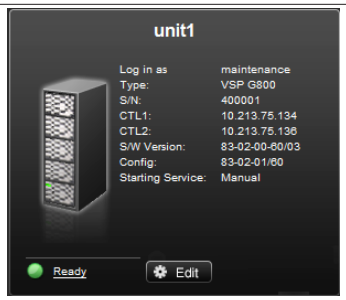
Web Console is automatically stop.

Copyright © 2015, 2017, Hitachi, Ltd.

1.6.3 Storage System Icon

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

Table 1-4 Storage System Icon Type

Status Name	Overview	Icon
Default	Display the Storage System information.	
Operation enabled status	The operation button display is enabled. The mouseover changes the status.	 (*1)
Service stop status	The service is stopped.	

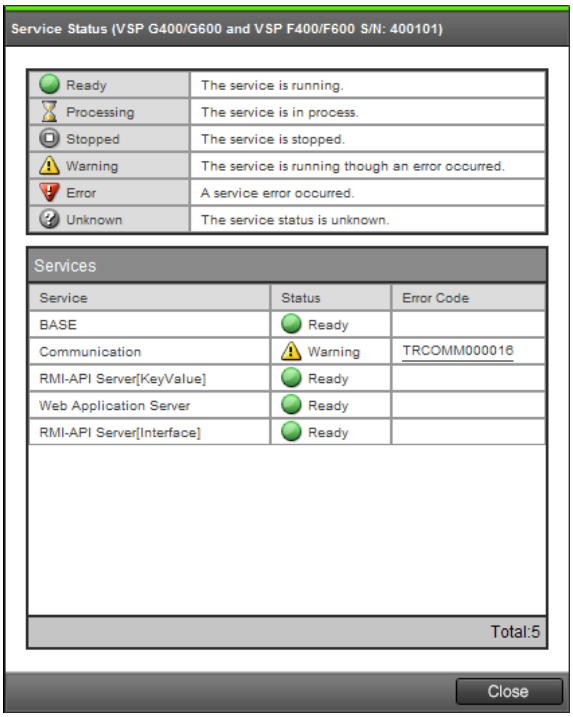
*1: When the Firmware version is less than 83-01-21-x0/xx, the [Stop Service] button is not displayed.

Copyright © 2015, 2017, Hitachi, Ltd.

Table 1-5 Operation Button

Item	Button	Description
Status icon	[Stopped] [Ready]	"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.
Edit button	[Edit]	"Edit System" window is displayed. Refer to "1.6.4 Stopping/Starting the Service of Storage System" or "1.6.5 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.



NOTE: When the firmware version is 83-03-01-x0/xx or later, [Error Code] is displayed in Services.

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".

Copyright © 2015, 2017, Hitachi, Ltd.

1.6.4 Stopping/Starting the Service of Storage System

1.6.4.1 Stopping the Service of Storage System

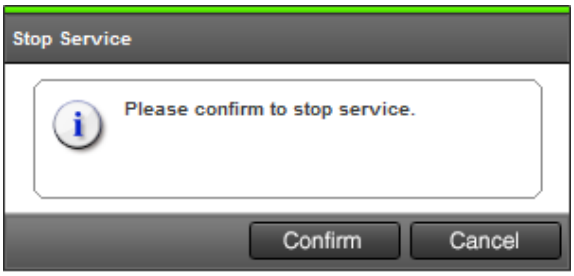
The following shows the procedure for stopping the service of the Storage System.

[When the Firmware version is 83-01-21-x0/xx or more]

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.



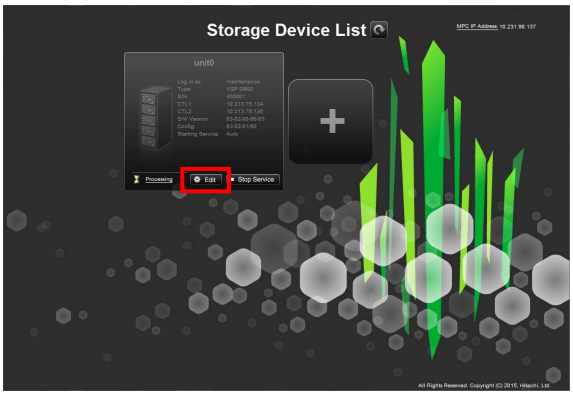
2. The confirmation message is displayed. Click the [Confirm] button.



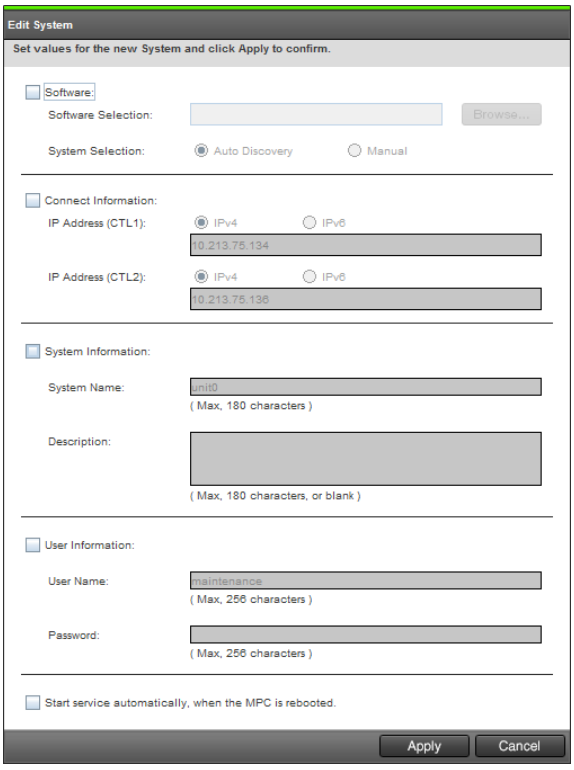
Copyright © 2015, 2017, Hitachi, Ltd.

[When the Firmware version is less than 83-01-21-x0/xx]

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 [Edit] button of the registered Storage System in the “Storage Device List” window.

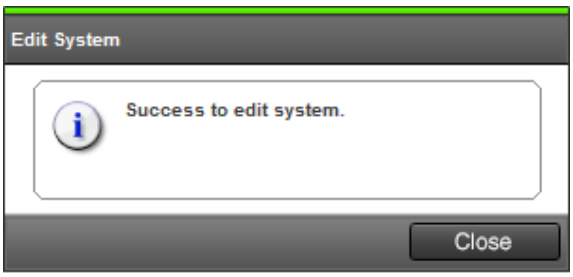


2. Confirm that the checkbox of [Start service automatically, when the MPC is rebooted] is unchecked, and then click the [Apply] button.



Copyright © 2015, 2017, Hitachi, Ltd.

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



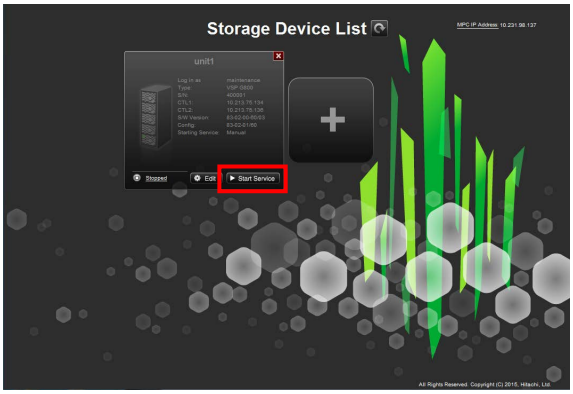
4. Restart the Maintenance PC.

5. Right-click the connection icon “Open Storage Device List” on the desktop of the Maintenance PC and select [Run as administrator].
   It starts with the services stopped.

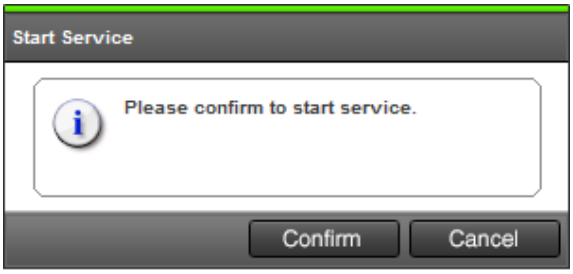
1.6.4.2 Starting the Service of Storage System

[When the Firmware version is less than 83-01-21-x0/xx]

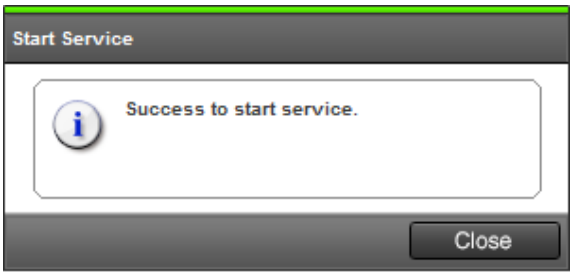
1. Click the [Start Service] button of the registered Storage System on the “Storage Device List” window.



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”.



Copyright © 2015, 2017, Hitachi, Ltd.

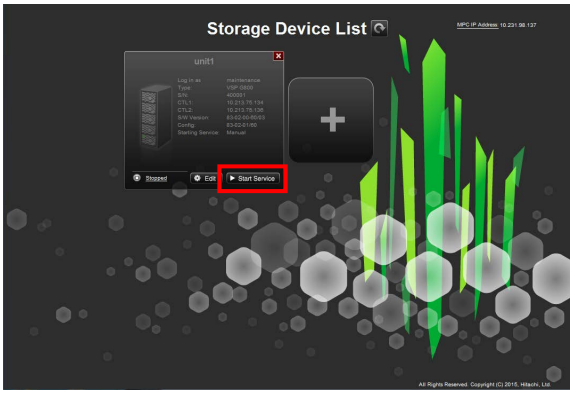
4. Check that Starting Service of the registered Storage System in the “Storage Device List” window is “Auto”.



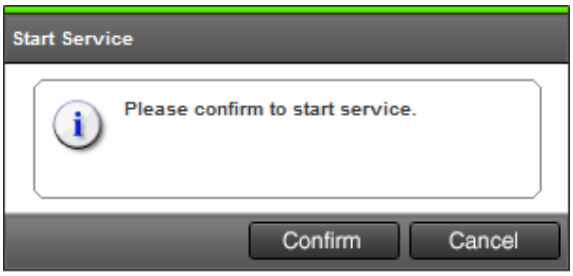
Copyright © 2015, 2017, Hitachi, Ltd.

[When the Firmware version is less than 83-01-21-x0/xx]

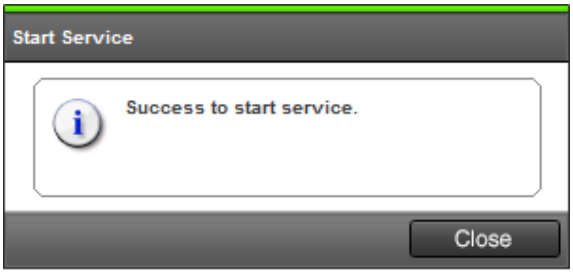
1. Click the [Start Service] button of the registered Storage System on the “Storage Device List” window.



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

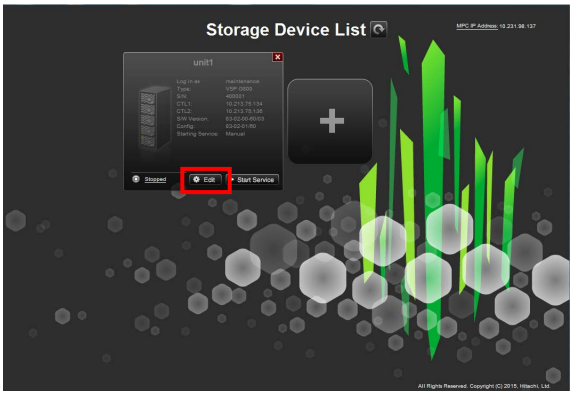


3. The “Starting Service Completed” window is displayed. Click the [Close] button.
   The status of the registered Storage System in the “Storage Device List” window becomes “Ready”.

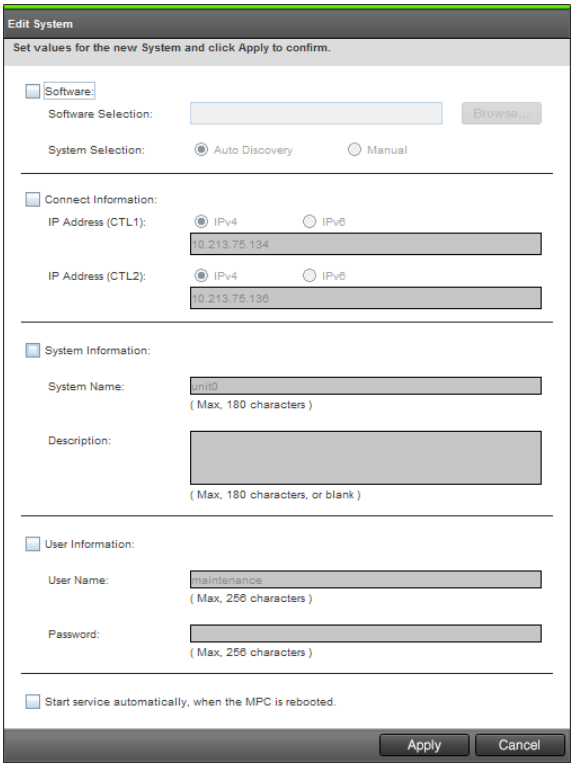


Copyright © 2015, 2017, Hitachi, Ltd.

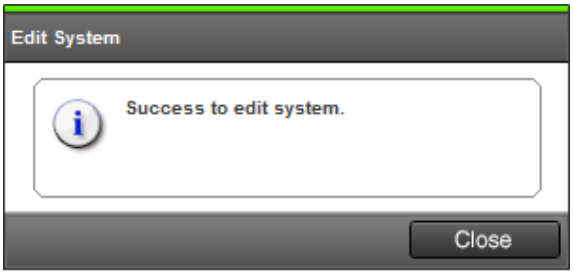
4. Click the [Edit] button of the registered Storage System on the “Storage Device List” window.



5. Check the check box of [Start service automatically, when the MPC is rebooted] and click the [Apply] button.



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



Copyright © 2015, 2017, Hitachi, Ltd.

7. Check that Starting Service of the registered Storage System in the “Storage Device List” window is “Auto”.



Copyright © 2015, 2017, Hitachi, Ltd.

1.6.5 Changing Storage System Information and Updating Software of Web Console

1. Stop the Storage System by the storage device list (Refer to "1.6.4.1 Stopping the Service of Storage System").

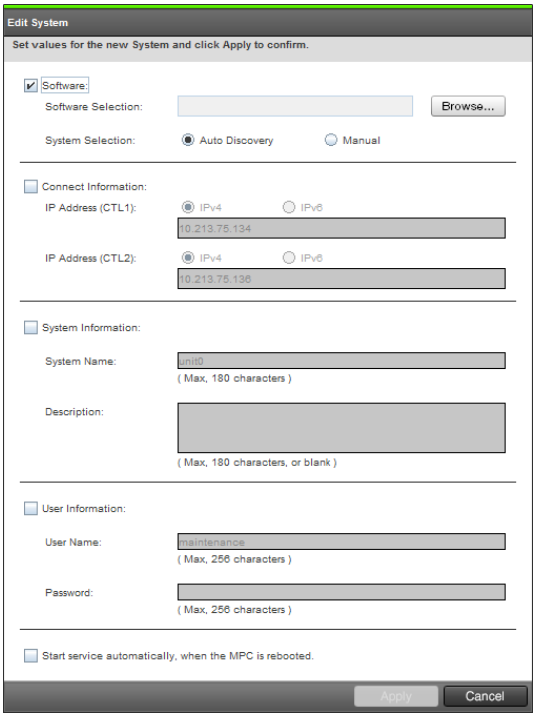
2. Click the [Edit] button of the registered Storage System on the storage device list.

3. Check the check box of [Software].

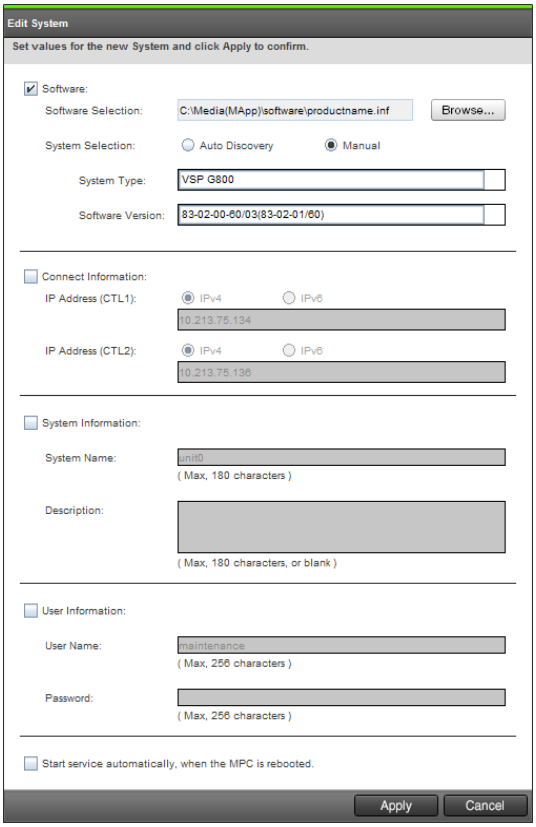
4. Specify "Software\productname.inf" in the setup media by the [Browse...] button of Software Selection in [Software].

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

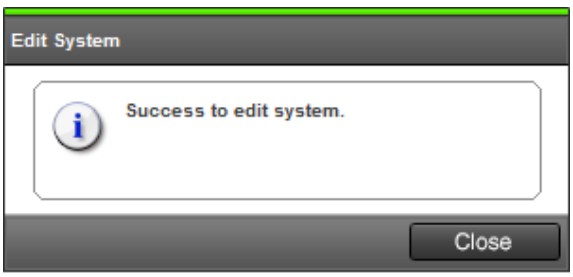
When selecting [Auto Discovery]



When selecting [Manual]



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

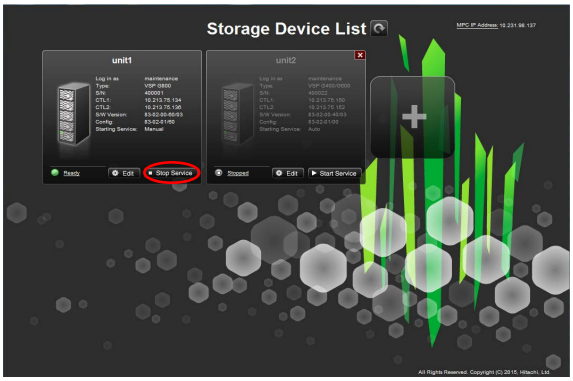


Copyright © 2015, 2017, Hitachi, Ltd.

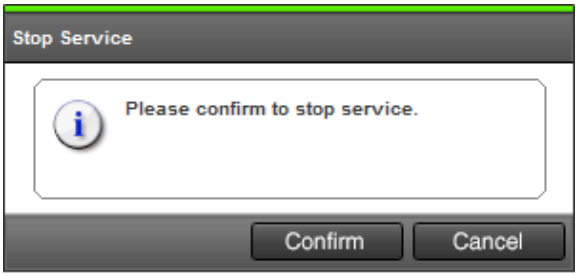
1.6.6 Switching the Storage System

When two or more Storage Systems are registered, only one Storage System that the service started can be operated.
To operate the Storage System that the service did not start, switch the Storage System.

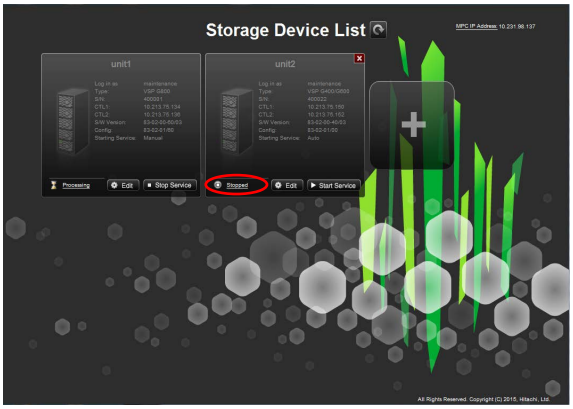
1. Click the [Stop Service] button of the Storage System that the service already started in the “Storage Device List”. (If no Storage System started, skip this operation and run Step 4 and later)



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

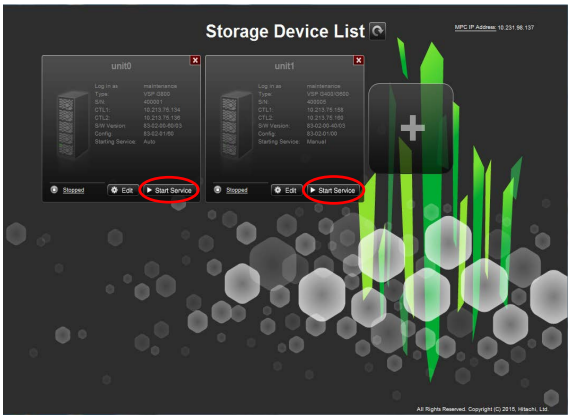


3. Wait until the service status of the Storage System changes to Stopped.

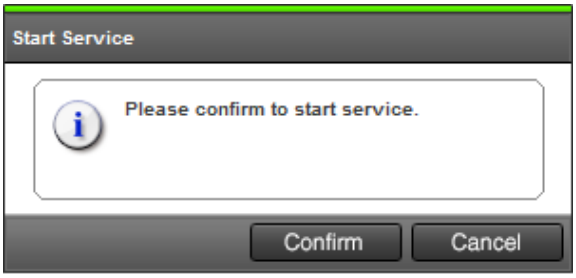


Copyright © 2015, 2017, Hitachi, Ltd.

4. Click the [Start Service] button of the Storage System to be operated in the “Storage Device List” window.



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



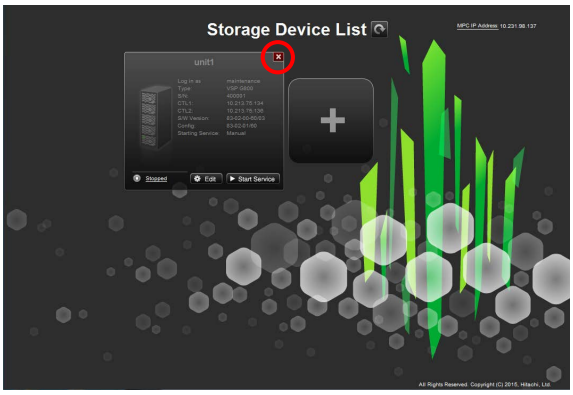
Copyright © 2015, 2017, Hitachi, Ltd.

1.6.7 Deleting the Storage System Icon

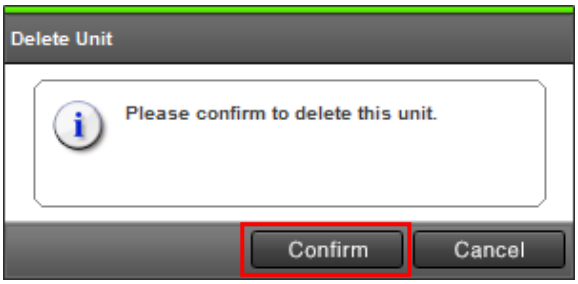
NOTICE:	Before deleting the Storage System icon, close the Event Viewer of Windows.

Perform the following procedure to delete the Storage System icon. You can delete it when the Storage System icon is stopped.

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

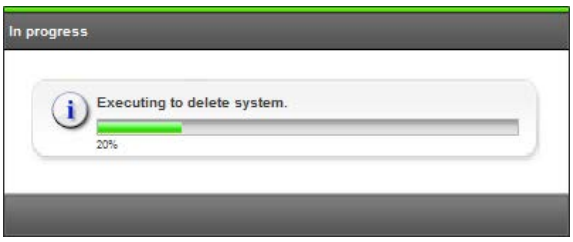


2. The “Delete Unit” window is displayed. Click the [Confirm] button.

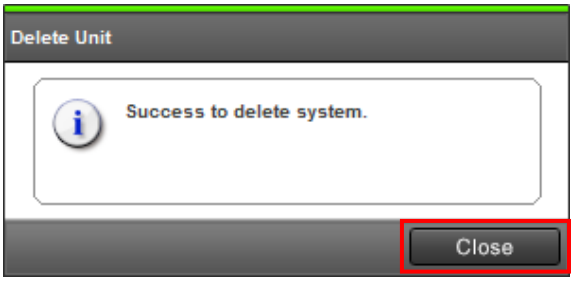


Copyright © 2015, 2017, Hitachi, Ltd.

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



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



Copyright © 2015, 2017, Hitachi, Ltd.

1.6.8 Incorrect display errors

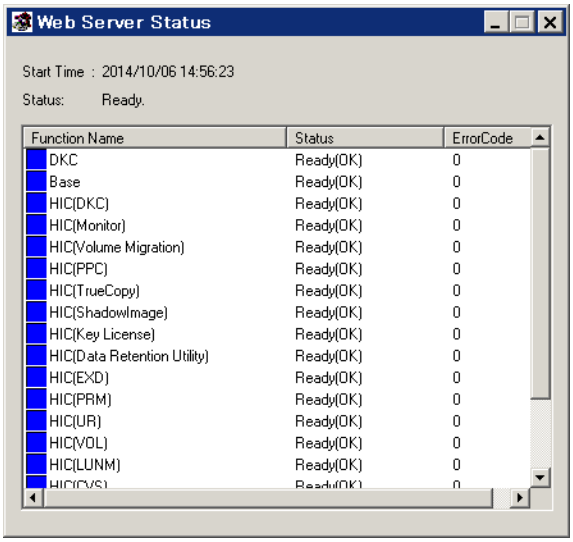
The following table lists incorrect display errors:

Error condition	Probable cause / Recommended action
A question mark (?) displays in a table or other area of the window.	• 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.	Log out. Then, press the [Ctrl] key and the [F5] key at the same time to read it again forcibly. After that, if the phenomenon is still not resolved even logged in again, contact the Technical Support Division.
The window is stuck during the window operation.	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.
The image display is unclear after completing the input setting in the window.	The window becomes unclear when entering slashes sequentially. There is no problem if you use it as is.
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.	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.

Copyright © 2015, 2017, Hitachi, Ltd.

1.6.9 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.



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.

Copyright © 2015, 2017, Hitachi, Ltd.

- 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

Copyright © 2015, 2017, Hitachi, Ltd.

• 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(Stat) / 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 (RAID Manager 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.

Copyright © 2015, 2017, Hitachi, Ltd.

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

Copyright © 2015, 2017, Hitachi, Ltd.

1.7 Setting the IIS/FTP Server

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 Windows7/Windows8.1 have the restrictions on the maximum number of simultaneous connections.
When IIS/FTP is already installed, see "1.7.2 Setting IIS/FTP".
If IIS configuration conflicts with a different application, back up the IIS configuration before performing "1.7.2 Setting IIS/FTP". The procedure can be performed in the Windows command prompt only as an administrator.

- Backup command
  %systemroot%\system32\inetsrv\appcmd add BACKUP "NAME_OF_BACKUP_A"

  NOTE: "NAME_OF_BACKUP_A" can be changed to a different name.
  After performing the backup, run the following command and confirm that the name specified at the backup is displayed.

- Backup list display command
  %systemroot%\system32\inetsrv\appcmd list BACKUP

When the IIS/FTP server is not installed or set, the following maintenance operation cannot be performed.

- INSTALLATION SECTION "6. New Installation (Auto Define Configuration, All Firmwares)"
- FIRMWARE SECTION "5.1 New Installation (Offline Configuration Definition, All Firmwares)"
- FIRMWARE SECTION "5.2 Procedure of New Installation (Restore Configuration)"

1.7.1 Installing IIS/FTP

Install IIS/FTP at the time of initial installation of the Maintenance PC.
The procedure for Windows7 is shown below as an example.

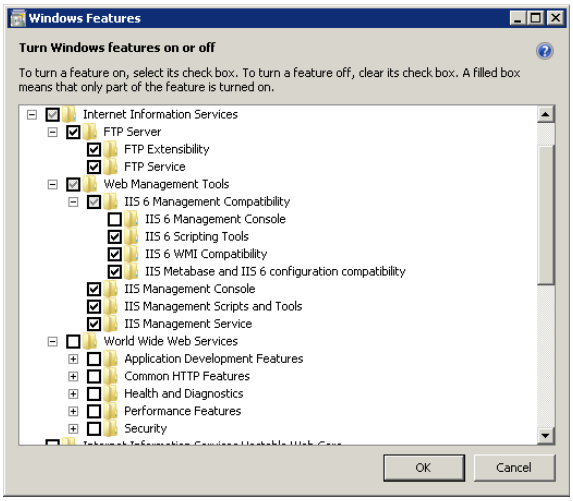
1. Installing IIS/FTP
   (1) Click the [Control Panel] button.
   (2) Click the [Programs and Features] button.
   (3) Click [Turn Windows features on or off].

Copyright © 2015, 2017, Hitachi, Ltd.

(4) Select [Internet Information Services] and set the following items.

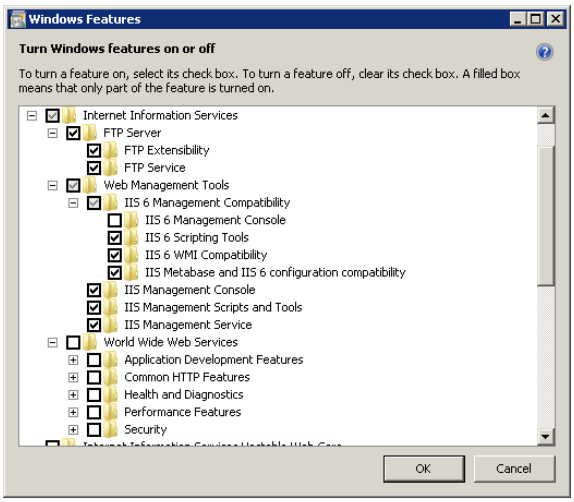
(a) Check the check boxes of the following items.

- 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



Copyright © 2015, 2017, Hitachi, Ltd.

1.7.2 Setting IIS/FTP

Set IIS/FTP at the time of initial installation/update installation of the Maintenance PC.
The procedure for Windows7 is shown below as an example.

NOTE: When the firmware version is 83-02-00-x0/xx or later, the procedures from Step 2. to Step 5. are performed automatically at the time of starting the services of the Storage System icon registered in Storage Device List. Perform the procedure from Step 1, Step 6, Step 7.

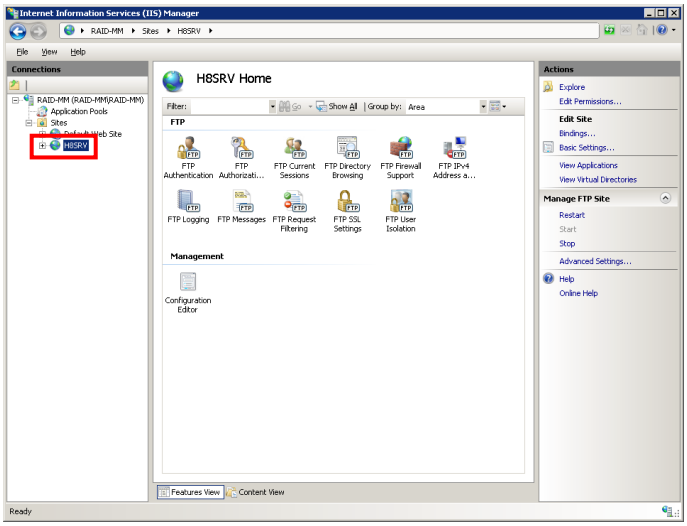
1. Restoring MPC IIS configuration

   NOTE:
   - Perform this procedure only when backup has been performed in "7. Backing up MPC IIS configuration" and the backed-up IIS configuration will be restored on the MPC.
   - When this procedure is performed, skip the following procedure.
   - The procedure can be performed in the Windows command prompt only as an administrator.

   - Restoring MPC IIS configuration
     %systemroot%\system32\inetsrv\appcmd restore BACKUP "NAME_OF_BACKUP_B"
     For "NAME_OF_BACKUP_B", specify the name obtained in "7. Backing up MPC IIS configuration", "1.7.2 Setting IIS/FTP".
   - Backup list display command
     %systemroot%\system32\inetsrv\appcmd list BACKUP

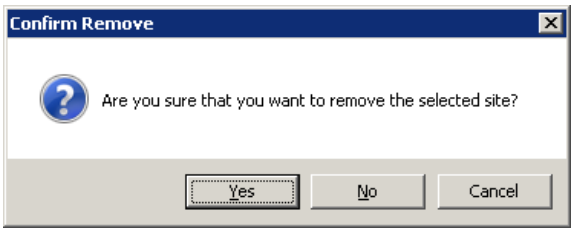
2. Starting the Internet Information Service (IIS) manager
   Open [Administrative Tools] from [Control Panel] and start [Internet Information Services (IIS) Manager].

3. Deleting Default Web Site and the existing FTP server
   If Default Web Site and the existing FTP server (including H8SRV) are registered, delete all of them in the following procedure.
   (1) Right-click the FTP server under [Sites] and click [Delete].
   Example: If H8SRV is registered as the FTP server



Copyright © 2015, 2017, Hitachi, Ltd.

(2) Click the [Yes] button in the “Confirm Remove” window.

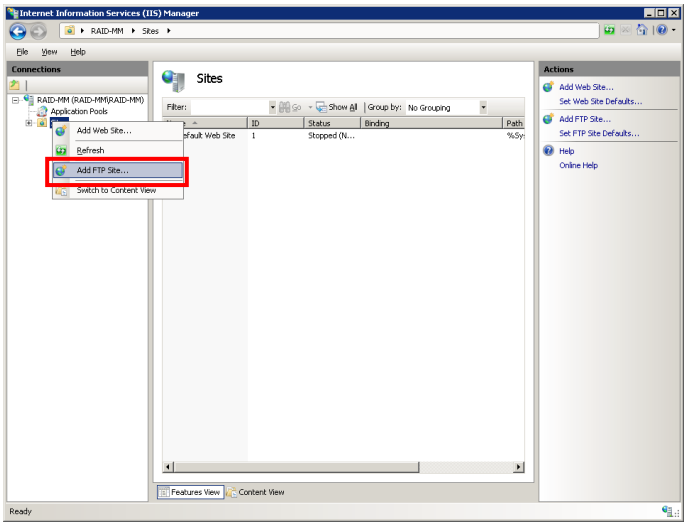


(3) For Default Web Site and other FTP servers, also repeat Step (1) to Step (2) to delete them.

Copyright © 2015, 2017, Hitachi, Ltd.

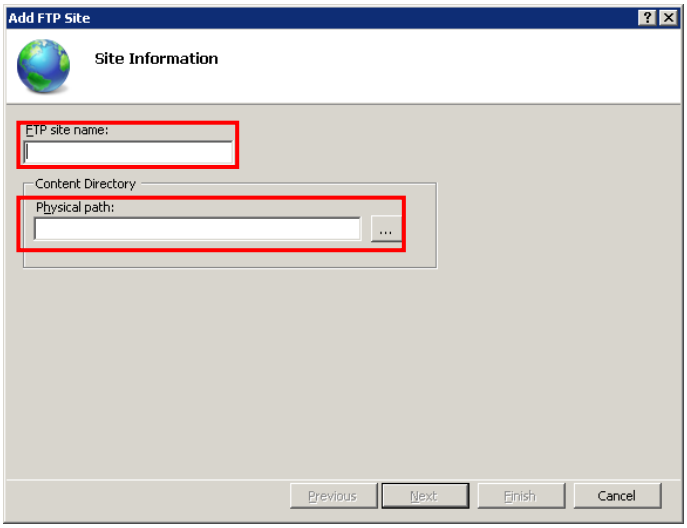
4. Adding the FTP site

(1) Right-click [Sites] and click [Add FTP Site...].



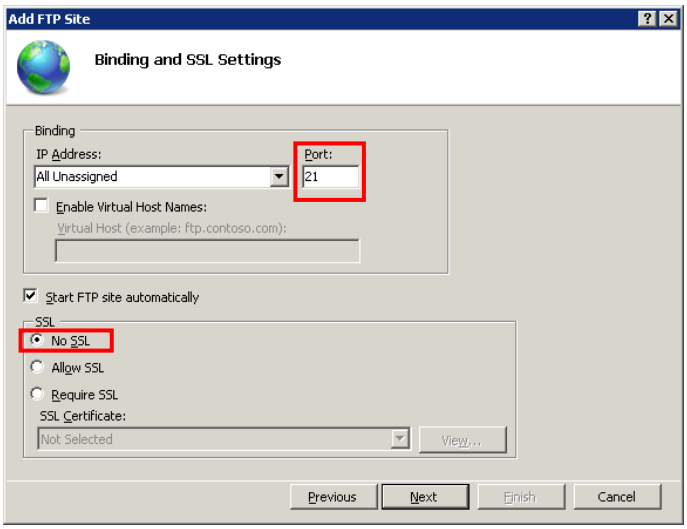
(2) Enter “H8SRV” in [FTP site name] and “C:\Mapp\wk\83xxxxyyyyyy\DKC200\HOME\micro” in [Content Directory] and click the [Next] button.

NOTE: “83xxxxyyyyyy” is a directory that is created when the Storage System is registered in the Storage Device List.
xxxx: “6000” in case of [VSP G800]
“4000” in case of [VSP G400/G600]
“2000” in case of [VSP G200]
yyyyyy: serial number

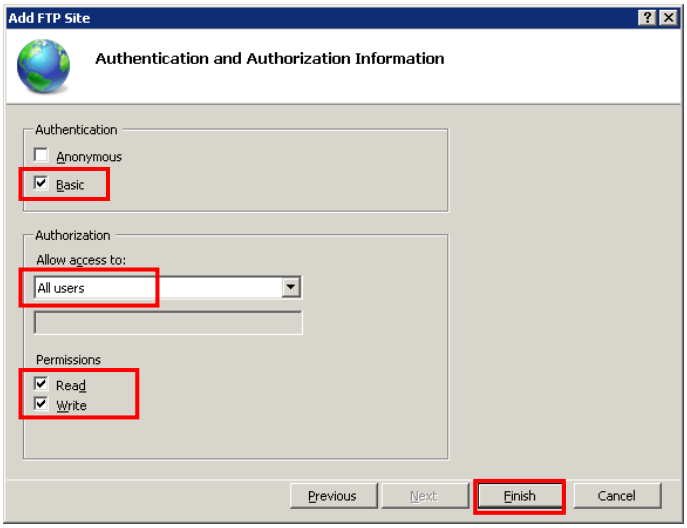


Copyright © 2015, 2017, Hitachi, Ltd.

(3) Use “21” as [Port].
Select [No SSL] for [SSL] and click the [Next] button.



(4) Check [Basic] for [Authentication].
Select [All users] in [Allow access to] of [Authorization] and check [Read] and [Write] for [Permissions]. Click the [Finish] button.

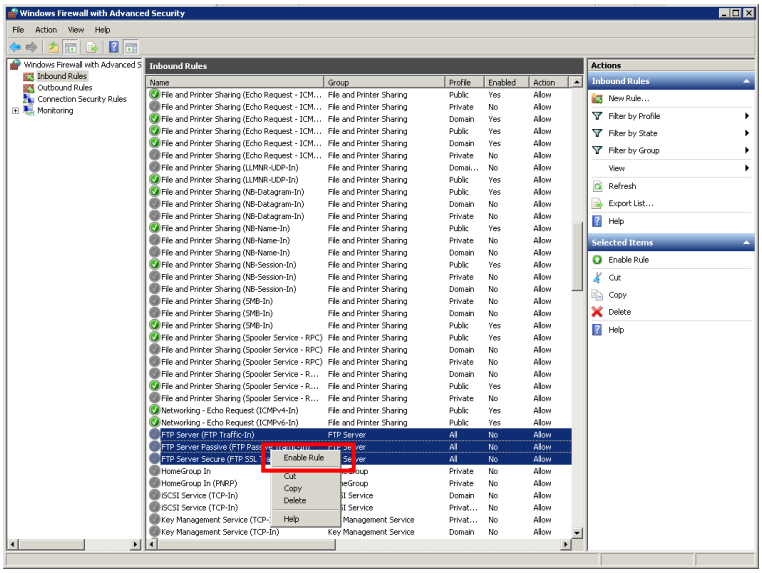


Copyright © 2015, 2017, Hitachi, Ltd.

5. 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.

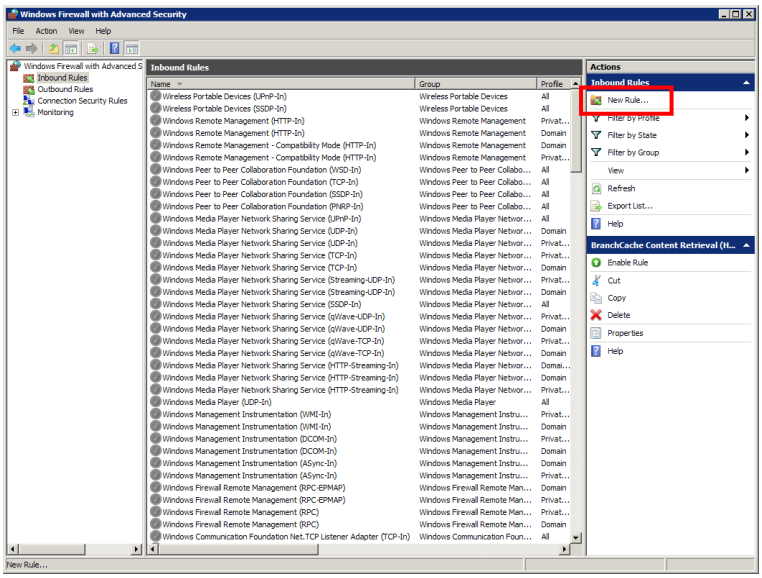


6. Release the blocked port for NAS unified firmware installation

NOTE: Perform this operation only when installing the NAS unified firmware.

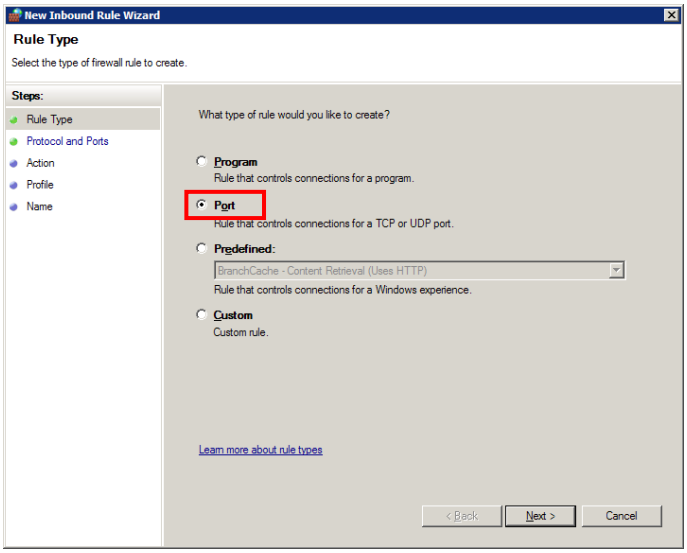
(1) Click [Control Panel] - [Administrative Tools] to open, and then start [Windows Firewall with Advanced Security].

(2) Click [Inbound Rules] in the tree on the left, and click [New Rule...] in the operation panel on the right.

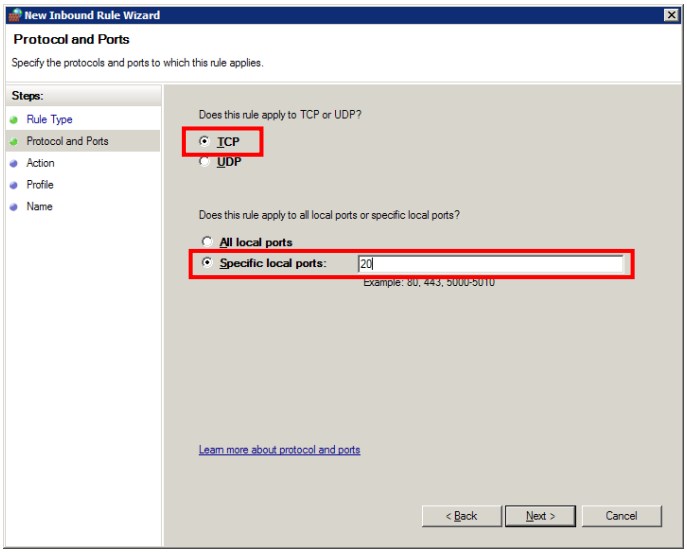


Copyright © 2015, 2017, Hitachi, Ltd.

(3) New Inbound Rule Wizard appears and Rule type to create is asked. Select [Port] and then click [Next] button.

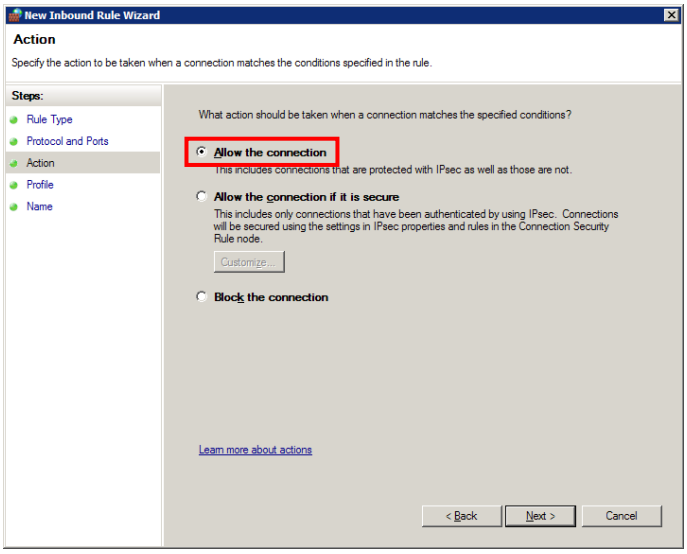


(4) In the "Protocol and Ports" window, select [TCP] and [Specific local ports], enter [20] in the text box, and then click [Next] button.

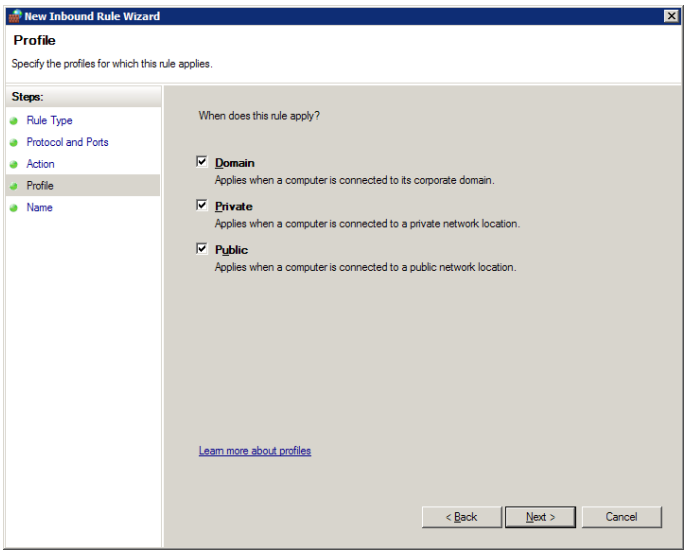


Copyright © 2015, 2017, Hitachi, Ltd.

(5) In the Actions window, select [Allow the connection], and then click [Next] button.

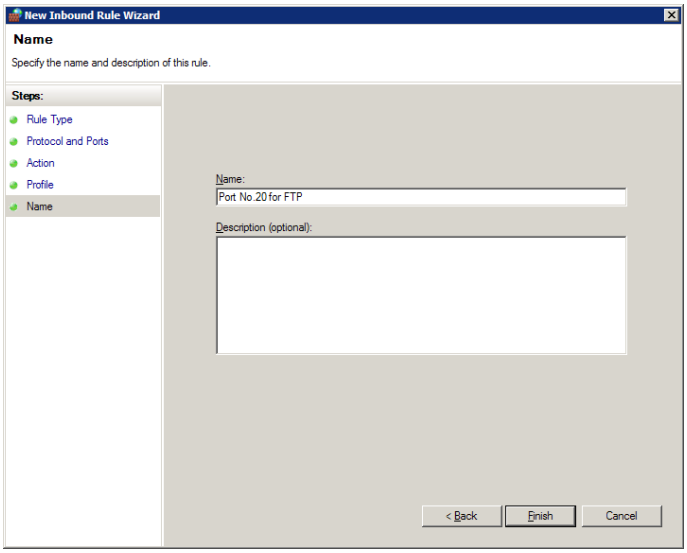


(6) In the Profile window, check that all checkboxes are checked, and then click [Next] button.

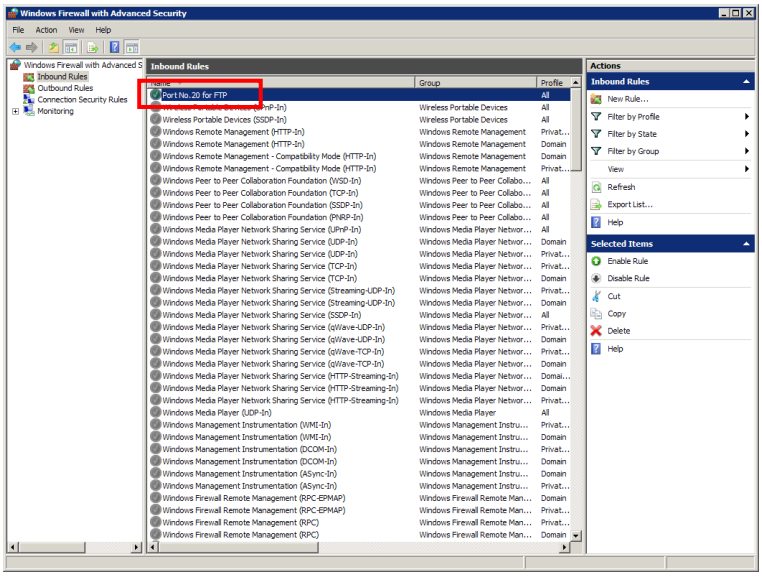


Copyright © 2015, 2017, Hitachi, Ltd.

(7) In the Name window, enter an appropriate name for a rule to be added in the text box, and then click [Finish] button.



(8) Check that the new rule is added in the Inbound Rules list.



Copyright © 2015, 2017, Hitachi, Ltd.

7. Backing up MPC IIS configuration

NOTE:
- When backup has been performed, skip this procedure.
- The procedure can be performed in the Windows command prompt only as an administrator.

(1) How to back up MPC IIS configuration
%systemroot%\system32\inetsrv\appcmd add BACKUP “NAME_OF_BACKUP_B”

NOTE: “NAME_OF_BACKUP_B” can be changed to a different name.

(2) Backup list display command
%systemroot%\system32\inetsrv\appcmd list BACKUP

NOTE: Confirm that the name specified at the backup is displayed.

Copyright © 2015, 2017, Hitachi, Ltd.

1.8 Starting Windows

Two types of windows necessary for maintenance are displayed from Web Console. They are an “MPC” window and a “Maintenance Utility” window.

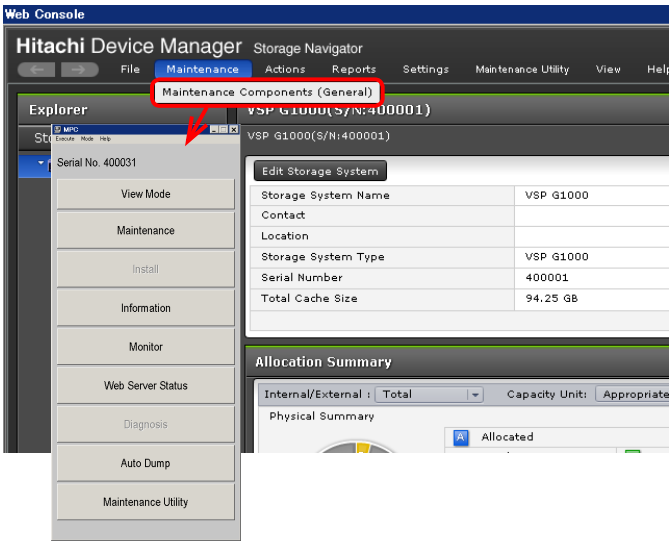
1.8.1 Maintenance PC Window

A window for service personnel work is called an “MPC” window and only accessed by Maintenance PC. A display method of the “MPC” window is as follows.

1.8.1.1 Open the Window

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 “1.12 Troubleshooting of Web Console” to register the Storage System to Java exception site.

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



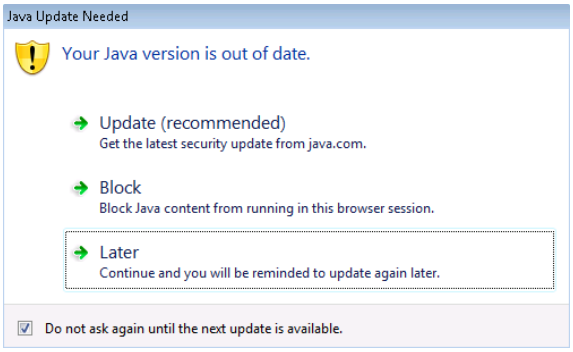
NOTE: When the “Web Console” window is not running, refer to “1.8.1.2 Starting the Maintenance PC Window Only”.

Copyright © 2015, 2017, Hitachi, Ltd.

(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.

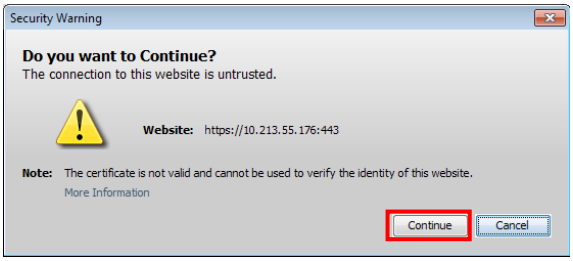
(i) Click [All Programs]-[Java]-[Configure Java] from the [Start] menu of Windows and start [Java Control Panel].
(ii) Click the [Security] tab of [Java Control Panel].
(iii) If the checkbox of [Enable Java content in the browser] in the [Security] tab is checked, uncheck it once and click the [Apply] 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.

Copyright © 2015, 2017, Hitachi, Ltd.

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

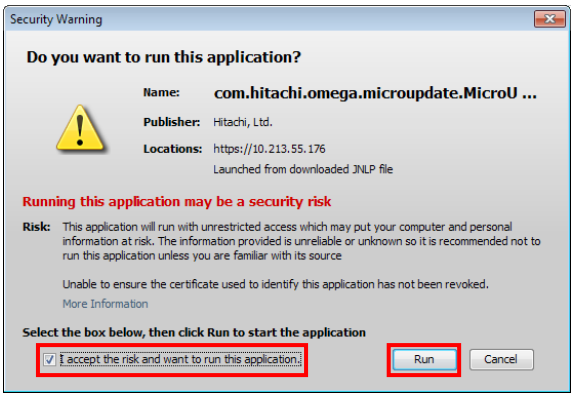
NOTE: This window may not be displayed.



NOTE: If you press the [Cancel] button in the window, the “MPC” window cannot be opened. Perform it again from “1.8.1.1 Open the Window”.

(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.

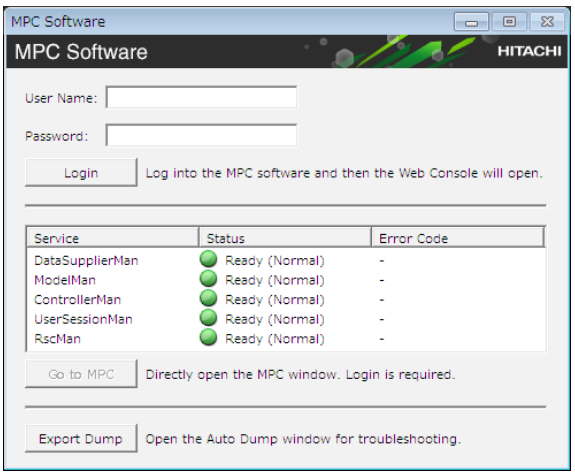


NOTE: If you press the [Cancel] button in the window, the “MPC” window cannot be opened. Perform it again from “1.8.1.1 Open the Window”.

Copyright © 2015, 2017, Hitachi, Ltd.

1.8.1.2 Starting the Maintenance PC Window Only

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



1. Login
   Enter a user name and password in the “MPC Software” window and click the [Login] button.

   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 “1.12 Troubleshooting of Web Console” 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.

1.8.1.3 Close the Window

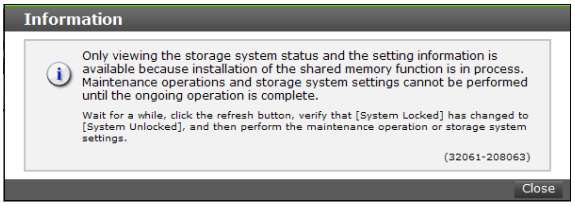
In the [View Mode], select the tool [Execute] - [Exit].

Copyright © 2015, 2017, Hitachi, Ltd.

1.8.2 Maintenance Utility Window

A maintenance function window accessed by service personnel and users is called Maintenance Utility. The following shows how to start the “Maintenance Utility” window.

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.



1.8.2.1 Starting the Web Console Window

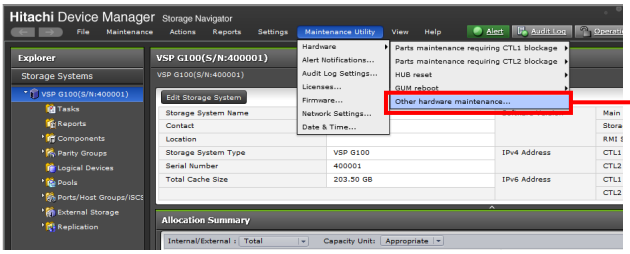
NOTICE: Do not use the Web browser menu.
If you use the browser menu ([Back], [Forward]) or shortcut keys and function keys, you are logged out of Maintenance Utility forcibly and the settings that are operated in the window are discarded. To use Maintenance Utility again, close the Web browser window,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

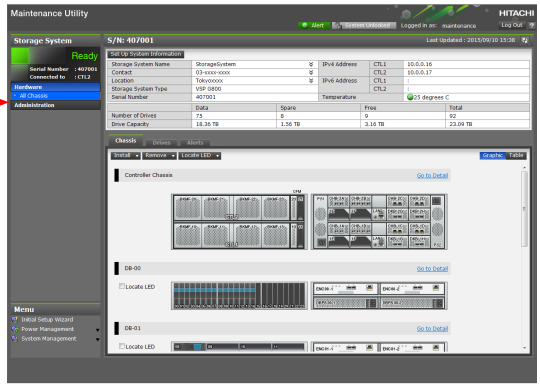
Copyright © 2015, 2017, Hitachi, Ltd.

NOTICE: 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.



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





1.8.2.2 Starting the MPC Window

NOTICE:	Do not use the Web browser menu. 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.

Click the [Maintenance Utility] button in the "MPC" window.

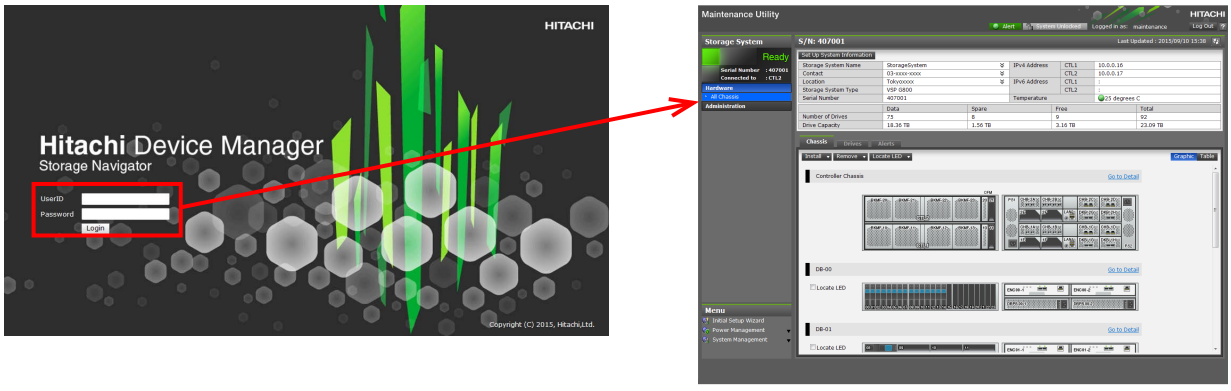
NOTE: When the "MPC" window is not running, see "1.8.1 Maintenance PC Window" and "1.8.1.2 Starting the Maintenance PC Window Only".

1.8.2.3 Starting the Browser

NOTE: When starting Maintenance Utility from the browser, the following restrictions are applied.

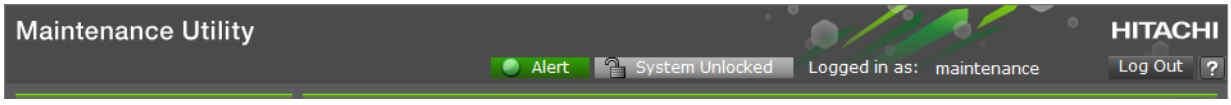
- Update Firmware
  - Firmware cannot be updated.
    Be sure to start Maintenance Utility following the procedure of "1.8.2.1 Starting the Web Console Window" and update the firmware.
- Replacing Parts
  - If multiple failures occur or the special (exceptional) work is performed in accordance with factory instructions, you cannot replace the parts. Be sure to start Maintenance Utility following the procedure of "1.8.2.1 Starting the Web Console Window" and replace the parts.
  - If multiple failures do not occur at the same time, you can replace the parts. After the replacement, however, collect dumps following "3.27 Acquiring System Dumps" (supported in the firmware version 83-02-01-x0/xx or later).

Enter the IP address of CTL1/CTL2 described on the icon in the "Storage Device List" window directly into the address bar of the browser.
A login window is displayed. Enter the Storage System/user name/password to start.



1.8.2.4 Close the Window

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



Copyright © 2015, 2017, Hitachi, Ltd.

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.

1.8.2.5 Basic Framework

Consists of three areas, “Header Area”, “Navigation Area” and “Application Area”.

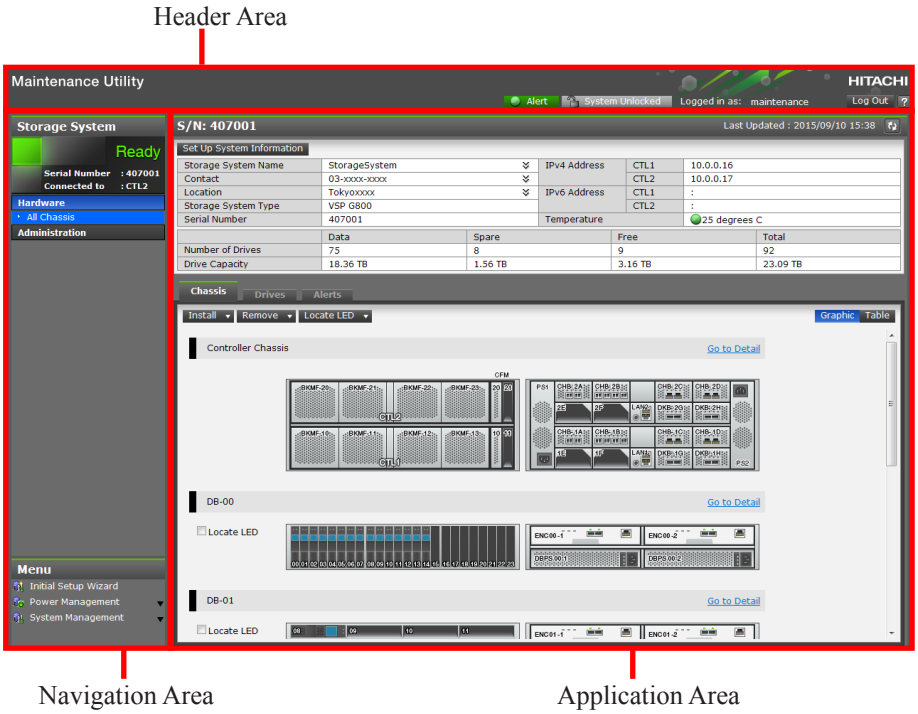


Table 1-6 Window Configuration

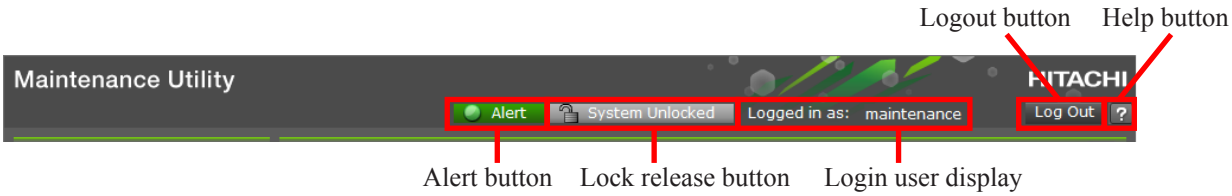
Area	Description
Header Area	The common information (such as alert display/system lock display/user name) is displayed always.
Navigation Area	Display system management menus.
Application Area	Perform information display and setting related to the system.

Copyright © 2015, 2017, Hitachi, Ltd.

1.8.2.6 Header Area Configuration

The following describes the common header area configuration in the main window.

• When the Firmware version is 83-02-01-x0/xx or later



• When the Firmware version is less than 83-02-01-x0/xx

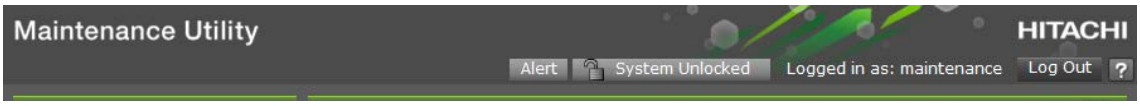


Table 1-7 Header Area Configuration

Window Item	Description
Alert button	• 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 1-9) in the navigation area.
Lock release button	• 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.(*1) 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.

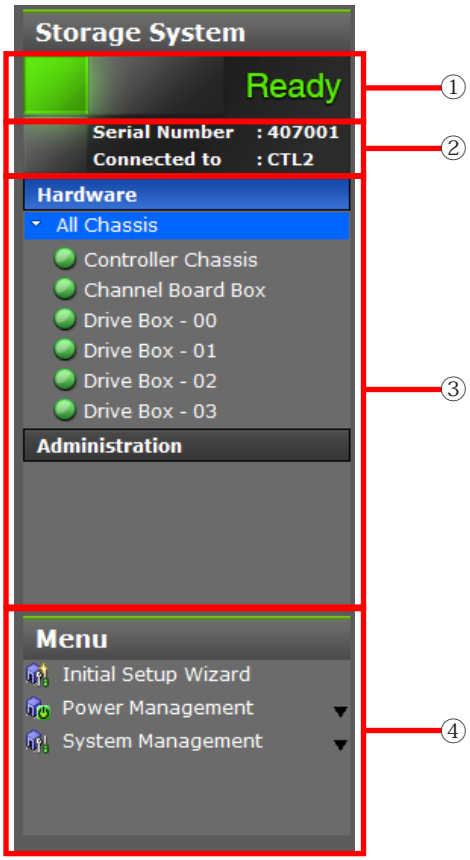
*1: This is displayed when the firmware version is 83-03-01-x0/xx or later.

Copyright © 2015, 2017, Hitachi, Ltd.

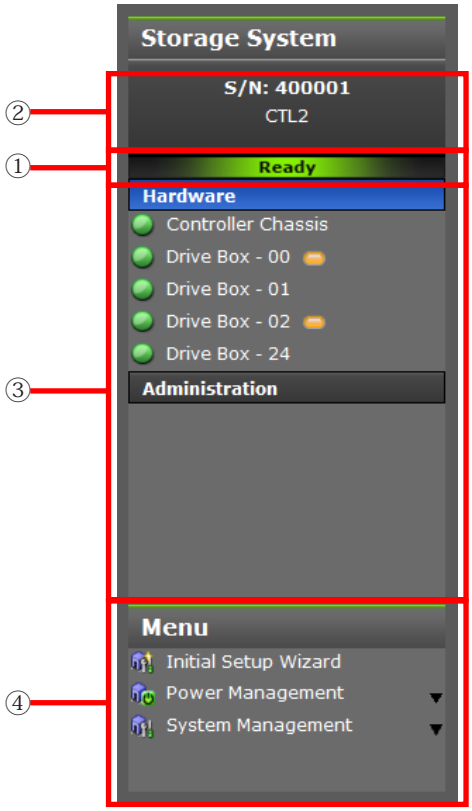
1.8.2.7 Navigation Area Configuration

The following describes the navigation area configuration.

- When the Firmware version is 83-02-01-x0/xx or later



- When the Firmware version is less than 83-02-01-x0/xx



① :Storage System Status
② :Storage System Information
③ :Display Item Selection Panel
④ :Operation Menu Panel

Table 1-8 Navigation Area Configuration

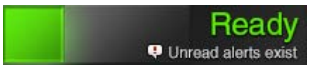
Window Item	Description
Storage System information	• Display a serial number in the first row. • Display the currently connecting CTL number in the second row. • Clicking this area displays the Storage System information (Main window) (Refer to "1.8.2.1 Starting the Web Console Window") in the application area.
Storage System status	Display a Storage System status image. (Refer to Table 1-9)
Display item selection panel	• 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.

Copyright © 2015, 2017, Hitachi, Ltd.

Table 1-9 Storage System Status

NOTE: See "3.22 Alert Display Related to FRU (Field Replacement Unit)" for the status of each part.

- When the Firmware version is 83-02-01-x0/xx or later

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)			–

Copyright © 2015, 2017, Hitachi, Ltd.

- When the Firmware version is less than 83-02-01-x0/xx

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)			-

Copyright © 2015, 2017, Hitachi, Ltd.

1.8.2.8 Application Area Configuration

The following describes the common application area configuration in the main window.

• When the Firmware version is 83-03-01-x0/xx or later



• When the Firmware version is less than 83-03-01-x0/xx



Table 1-10 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 (*1)	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.

*1: This is displayed when the firmware version is 83-03-01-x0/xx or later.

Copyright © 2015, 2017, Hitachi, Ltd.

1.8.3 NAS Manager Window

1.8.3.1 Starting the Window

To start the “NAS Manager” window, enter URL from the Web browser of the Maintenance PC.
See “6.1 Logging into/Logging out NAS Manager” for the procedure.

1.8.3.2 Closing the Window

Click the “Sign Out” button in the upper right of the “NAS Manager” window to close the window.

Copyright © 2015, 2017, Hitachi, Ltd.

1.8.4 BALI (Console) Window

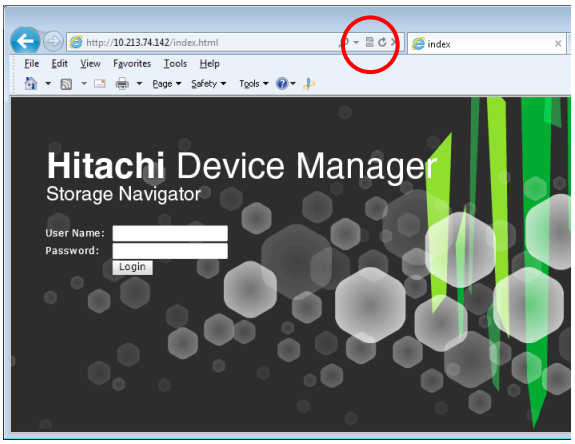
1.8.4.1 Starting the Window

To start the “BALI (Console)” window, connect to the communication software corresponding to ssh2 to log in. See “7.2 Logging into Node” for the procedure

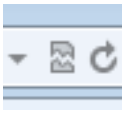
1.8.5 Setting the Browser Compatibility Display to OFF

This section describes the setting method in the Internet Explorer.

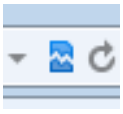
1. Change the compatibility button on the side of the browser address bar to the OFF status.
   When the Internet Explorer version is less than 11, the button is not displayed. Go to Step 2.



OFF status

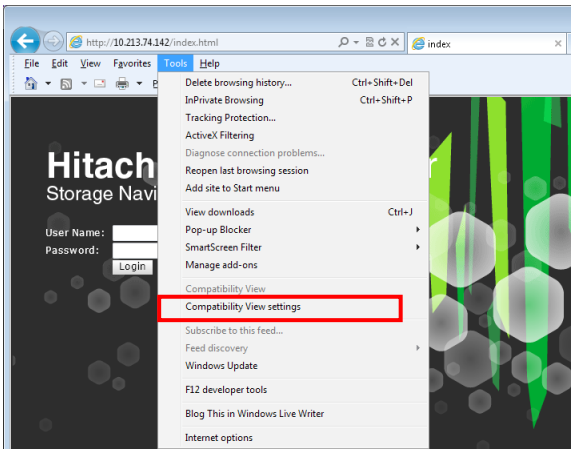


ON status



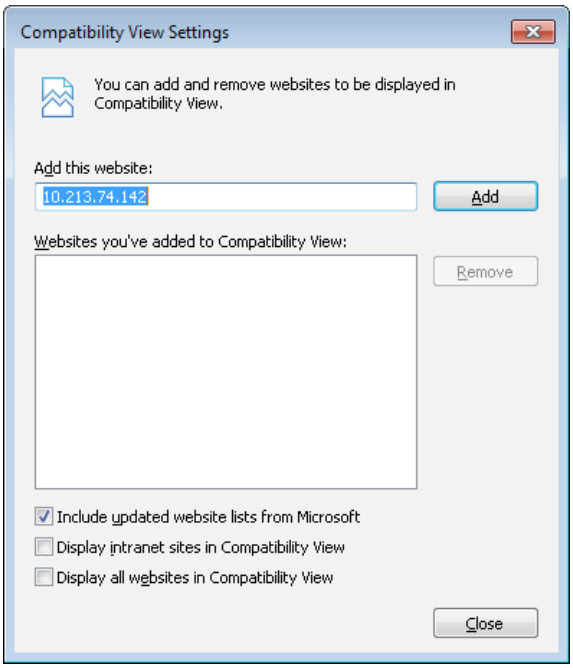
2. Display the compatibility view button.

   (1) Click [Tools] – [Compatibility View settings].



Copyright © 2015, 2017, Hitachi, Ltd.

(2) Uncheck [Display intranet sites in Compatibility view] and [Display all websites in Compatibility View].



(3) Return to Step 1 and set the compatibility view to the OFF status.

Copyright © 2015, 2017, Hitachi, Ltd.

1.9 Check the Version of Third Party Software

Can Check the the version third party software (Apache, Openssl, Jetty, JRE, Perl).
How to check the version that is installed in Maintenance PC, refer to “<Maintenance PC installed directory>\OSS\OSS_Version.txt”.

Copyright © 2015, 2017, Hitachi, Ltd.

1.10 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.
The Storage Navigator services can be stopped and started by the Maintenance PC software of the firmware version 83-04-41-x0/xx or later. 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, MAPPAppServer, MAPPWebServer, and MAPPRestAPIServer that run as the Windows services.

1.10.1 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.

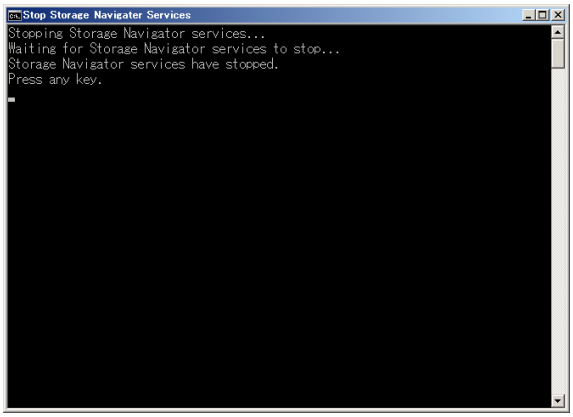
NOTICE:
- Make sure that the maintenance work is not performed before stopping the Storage Navigator services.
- Do not perform any other operations until the procedure for stopping the Storage Navigator services is completed.
- When you perform the following procedure, the Command Prompt window opens. 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 "1.6.2.3 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.

Copyright © 2015, 2017, Hitachi, Ltd.

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 “1.10.2 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. 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, MAPPAppServer, APPWebServer, and MAPPRestAPIServer 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.
201	A service that does not respond to the service stop request is detected.	
202	Other errors are detected.	
300	The software of the Maintenance PC is wrong.	Restart the Maintenance PC. Then, re-install the Maintenance PC software by following the procedure in “1.5 Maintenance PC Initial Installation/Update Installation”.

Copyright © 2015, 2017, Hitachi, Ltd.

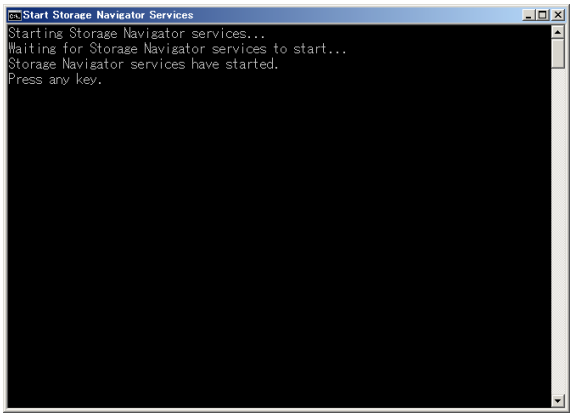
1.10.2 Starting the Storage Navigator Services

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 “1.6.2.2 Starting Web Console”.
   If the service of the Storage System cannot be started, see “1.11 Troubleshooting of Storage Device List”.

Copyright © 2015, 2017, Hitachi, Ltd.

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. Make sure that the services are started by performing the following procedure. 1. From the Windows start menu, select [Control Panel]-[Administrative Tools]-[Services]. 2. Check that the status of DKCMan, MAPPAppServer, APPWebServer, and MAPPRestAPIServer 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.
201	A service that does not respond to the service start request is detected.	
202	Other errors are detected.	
300	The software of the Maintenance PC is wrong.	Re-install the Maintenance PC software by following the procedure in “1.5 Maintenance PC Initial Installation/Update Installation”.

Copyright © 2015, 2017, Hitachi, Ltd.

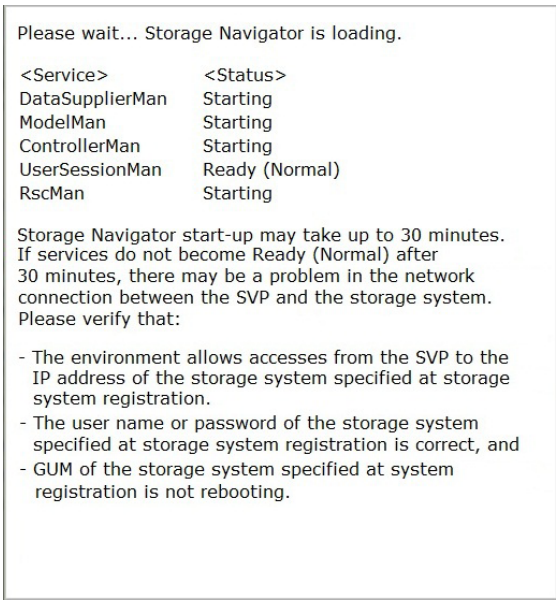
1.11 Troubleshooting of Storage Device List

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 occured 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 occured 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 occured 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] again.
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] again.

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

No	Failure	Recovery action
6.	After starting Web Console, the following window is displayed and you cannot log in.  Please wait... Storage Navigator is loading. <Service> <Status> DataSupplierMan Starting ModelMan Starting ControllerMan Starting UserSessionMan Ready (Normal) RscMan Starting Storage Navigator start-up may take up to 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: - 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.	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. Then, restart the Maintenance PC that you use. If no other Maintenance PCs are connected, reboot GUM from Maintenance Utility. Reboot GUM in CTL1 and CTL2 one by one. (Refer to the "3.18 Reboot GUM" for the reboot method.) Then, restart the Maintenance PC that you use. 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.
7.	When the Storage Device List is started, the (21041 006005) error occured and the Storage Device List cannot be started.	Failed to connect to the Supervisor serviece (DKCMan/MAPPAppServer/MAPPWebServer). 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: 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. 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].
8.	When clicking the Storage System icon, the (21041 006002) error occurs and the Web Console cannot be started.	The default browser is not set. Set the default browser on the setting screen of the browser which is installed on the Maintenance PC, and try again.

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(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.	A customer might have changed the password. Check the password, enter a correct username and password, and try to log in again. 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". 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.

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

1.12 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 versions of Apache and Maintenance PC may mismatch. Uninstall Apache and install it again. Refer to the installation procedure of Apache in the "1.5.4 Maintenance PC Software Installation" for the installation procedure.	
		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.	

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(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.	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”. 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. 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]. 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.	

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(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”	It may be that an application signed with expired certificate. Do the exception setting with following steps. 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. - <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)> If [Security Warning - HTTP Location] was displayed, Click [Continue] button. 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. • From the [Advanced] tab, select (CL) [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	Other administrative clients might be setting Storage Navigator. Check that all the setting windows of Storage Navigator are closed, and then operate Web Console again. In the case other than the above, restart the Maintenance PC. After that, operate Web Console.	

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

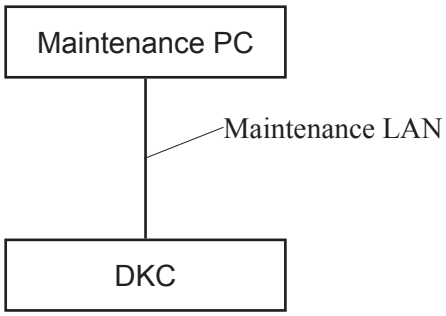
(Continued from preceding page)

	Failure	Recovery action	Remarks
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.	
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 "1.8.1.1 Open the Window".	
13	An error occurred during the operation in the "Web Console" window. • 20121-107022	An unsupported locale might be set in the Maintenance PC. Check whether a supported locale is set in the Maintenance PC. For the locale setting, refer to Hitachi Virtual Storage Platform G200, F400/G400, F600/G600, F800/G800 User Guide.	

*1: If the trouble is not solved in spite of it, collect a dump and restart the Maintenance PC. Refer to "5.2 Dump".

Copyright © 2015, 2017, Hitachi, Ltd.

Please make sure that the cable connections are correct.



Copyright © 2015, 2017, Hitachi, Ltd.

1.13 Troubleshooting of Maintenance Utility

Description	Failure	Recovery Action
Network failures Login failures	• The network cannot connect to Maintenance Utility. • The 32061-204002 error occurs while operating Maintenance Utility. • The network cannot log into the Maintenance Utility.	Check that the LAN cable is not removed. If it is removed, connect the cable, and then restart the operation. If it cannot recover, perform the following. 1. When logging in, log out once and operate it again after closing the browser. 2. 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. 3. If it cannot be recovered yet, see "3.41 Recovery Procedure when a GUM Failure Occurs (SIM = aff1xx)" in the TROUBLESHOOTING SECTION to recover.
	• The network cannot connect to Maintenance Utility when starting it on Web Console.	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. 
	• Login for Maintenance Utility is not available even if 30 minutes elapse after the progress reaches 99%.	See TROUBLESHOOTING SECTION "3.41 Recovery Procedure when a GUM Failure Occurs (SIM = aff1xx)" and restore the failure.

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

Description	Failure	Recovery Action
Network failures Login failures	• The network cannot connect to Maintenance Utility. • The actual IP address and the IP address displayed in the Maintenance Utility window do not match.	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. 1. 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". 2. If it cannot be recovered yet, see "3.41 Recovery Procedure when a GUM Failure Occurs (SIM = aff1xx)" in the TROUBLESHOOTING SECTION to recover.
JavaScript security troubleshooting	• 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.	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. 1. Open [Tool] – [Internet Options] in the Internet Explorer and select the [Security] tab. 2. Select [Reliable Site]、and then select [Site (S)]. 3. Uncheck [All Sites in This Zone Require Confirmation (https:) by Servers (S)]. 4. Enter the IP address of CTL1 into [Add This Web Site to Zone (D)] and click [Add] and select [Close]. 5. Add the IP address of CTL2 in the same way. 6. When returning to the "Internet Option" window, select [OK] to close the window.
Compatibility display	• Contents displayed in the "Maintenance Utility" window are corrupted. • A specific window is not displayed. • Clicking the button has no response.	Exclude Maintenance Utility from the compatibility display target. See "1.8.5 Setting the Browser Compatibility Display to OFF" for the setting method.

*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)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

Description	Failure	Recovery Action
Browser Cache clearing	• 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. 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. 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)

Copyright © 2015, 2017, Hitachi, Ltd.

(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"	It may be that an application signed with expired certificate. Do the exception setting with following steps. 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. - <http://(CTL1 address)> - <http://(CTL2 address)> - <https://(CTL1 address)> - <https://(CTL2 address)> - <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)> If [Security Warning - HTTP Location] was displayed, Click [Continue] button. 4. If the installed Java version is Java 1.7.0_55 or later or Java 1.8.0_5 or later, perform the following setting, too. • From the [Advanced] tab, select (CL) [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.	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. Open the Windows Task Manager and see "Commit" of "System" in the Performance tab to check the free space of the memory.

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

Description	Failure	Recovery Action
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.	GUM is rebooted. See "3.18 Reboot GUM" for the reboot method.
The update firmware window cannot be displayed.	Either of the following errors occurs when you try to start the update firmware window. • A message showing that this page cannot be displayed appears on the browser. • An application error is displayed.	If the error occurs during "1.6.2 Procedures for Connecting to the Storage System", terminate the tool, and then perform "1.6.2 Procedures for Connecting to the Storage System" again. If the error occurs during the firmware update on Maintenance Utility, close the error window, and then update the firmware again.

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

Description	Failure	Recovery Action
The download failed in the backup of the audit log export or the user account information.	The following error occurs when backing up the audit log export or the user account information. • The error window "Maintenance Utility cannot be started." is displayed in the Web browser.	This phenomenon might occur when an unsupported browser is used. See "1.1 Specifications for the Maintenance PC" and use a browser of the supported version.
The displayed description in the Maintenance Utility window is distorted.	• A specific window is not displayed. • Clicking the button has no response.	Exclude the Maintenance Utility window from the compatibility display target. In the Internet Explorer, check the [Compatibility View] on the address bar, and turn OFF the compatibility view. [Compatibility View] is not appeared (less than IE11): 1. Select [Tools] – [Compatibility View Settings]. 2. Clear the "Display intranet sites in Compatibility View" and the "Display all websites in Compatibility View" check box. 3. 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".	1. If the internal network is changed from the default value and also "5.3 Automatic Configuration Definition Mode (System Configuration Initialization)" or "5.1 New Installation (Offline Configuration Definition, All Firmwares)" in FIRMWARE SECTION has been performed, set the default value (126.255.0.15/4.15) referring to "3.6 Network Setting". 2. If the conditions 1 are not satisfied, perform the following procedure. • 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 the to the SIM.

Copyright © 2015, 2017, Hitachi, Ltd.

1.14 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.

Copyright © 2015, 2017, Hitachi, Ltd.

2. Local Setting of Maintenance PC

2.1 Before using Web Console

Java and IP address settings are required for connecting an Maintenance PC to the Storage System.
Refer to “System Administrator Guide” for the specification of the commonness part of Web Console for the operation and conventions.

Copyright © 2015, 2017, Hitachi, Ltd.

2.2 Check of Configuring Web Console Over a Firewall

Set the following TCP/IP port numbers to be used when the Maintenance PC communicates with the Storage System.

- FTP (File Transfer Protocol): 20, 21 (TCP)
- HTTP (Hypertext Transfer Protocol): 80 (TCP)
- SNMP (Simple Network Management Protocol): 161 (UDP)
- HTTPs (Hypertext Transfer Protocol over Secure Socket Layer): 443 (TCP)
- RMI (Remote Method Invocation): 1099 (TCP)
- RMI: 51099 (TCP)
- RMI: 51100-51355 (TCP)

*1: When the SVP software version is 83-03-01-xx/00 or later, unused port numbers are automatically allocated from the described range at the time of the storage system registration and a firewall is also set. The allocated ports numbers are used when starting the storage system.
When the SVP software version is less than 83-03-01-xx/00, 51100 is used.

NOTE: Set a firewall to be able to use these port numbers when connecting the Maintenance PC and the Storage System exceeding the firewall.
Note that 80, 443, 1099, 51099 and 51100 are set at the time of the setup.

Some products have security software supporting the firewall function. To install such software, set the necessary ports to be available.

2.3 Internal Communication Ports Used by the Maintenance PC

The Maintenance PC uses the following port numbers in internal communication.

Item	SVP software version	
	83-03-01-xx/00 or later	Less than 83-03-01-xx/00
Port number	8080	8080
	48081-48336 (*1)	8081
	48411-48666	8211
	9210	9210
	11099	11099

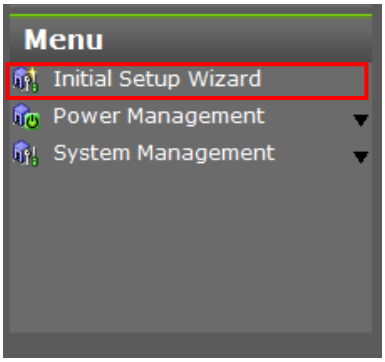
*1: Unused port numbers are automatically used in the described range when the Storage System starts.

NOTE: When the port numbers duplicate with the port numbers used by other applications, the Maintenance PC does not operate correctly.
Change the port numbers used by other applications or disable those applications so that the port numbers do not duplicate.
To check if the Storage System has properly started up, see TROUBLESHOOTING SECTION “3.28.1.5 Background Service Log” to check the background service logs.

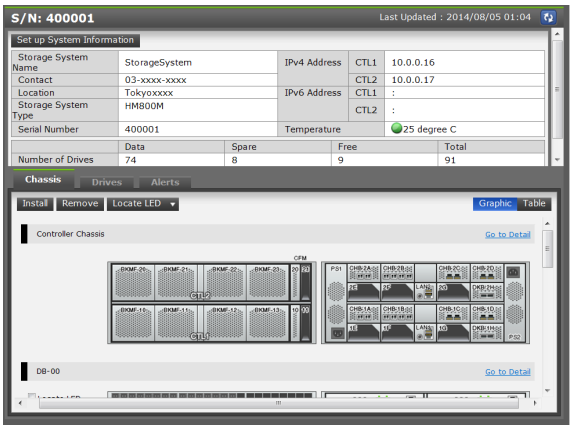
Copyright © 2015, 2017, Hitachi, Ltd.

2.4 Initial Setting Wizard

1. Display the initial setting window
   (1) Click the [Initial Setup Wizard] button from [Menu] at the left lower of the window.



   (2) The “Initial Setup” window is displayed.



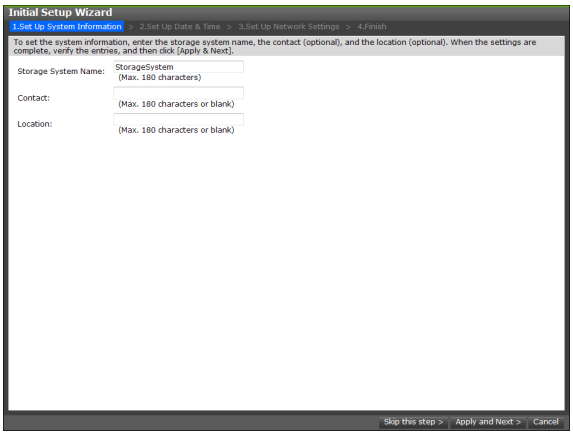
Copyright © 2015, 2017, Hitachi, Ltd.

2. Setting Storage System information
   The “1. Set Up System Information” window is displayed. Enter the system information (system name/ address/installation position).

NOTICE: If the system information (Storage System name, contact and installation location) is set by NAS Manager, the set contents are also reflected in the Storage System.

Such information is used when using the alert notice function by SNMP.
After the input, select the [Apply and Next] button.

NOTE: Clicking the [Apply and Next] button confirms the input description. Even if you click the [Cancel] button at the end of the wizard, you cannot cancel the setting of this window.



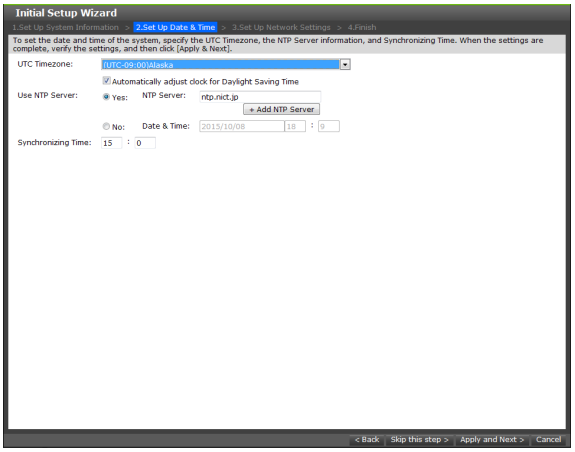
Item	Input Description
Storage System Name	Set a name of the Storage System. You can enter a maximum of 180 alphanumeric characters except for some symbols (\ , / ; : * ? ” < > | & % ^). Do not enter a blank for the first or last character. If you change this item, the Storage System name of [SNMP] Tab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

Copyright © 2015, 2017, Hitachi, Ltd.

3. Time setting
   The “2. Set Up Date & Time” window is displayed. Set a time.
   After the setup, select the [Apply and Next] button.

   NOTE: To use this function, an NTP server should exist in the same LAN as the Storage System.
   If the time setting fails, check the NTP server IP address and the use port setting and reset them. Furthermore, another factors may be on the NTP server side.

   NOTE: Clicking the [Apply and Next] button confirms the input description. Even if you click the [Cancel] button at the end of the wizard, you cannot cancel the setting of this window.



   NOTE: When the Firmware version is less than 83-02-01-x0/xx, the “Automatically adjust clock for Daylight Saving Time” is not displayed.

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. • 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.
	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.

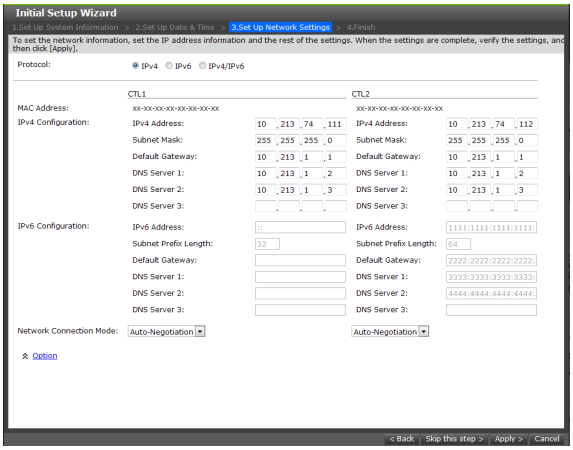
4. Setting a network

> **⚠ 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.

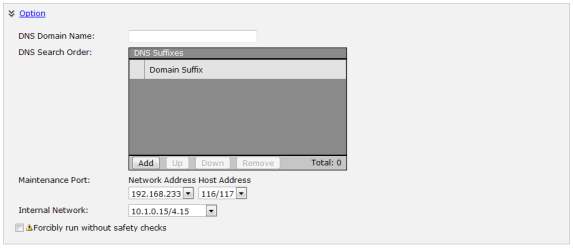
The “3. Set Up Network Settings” window is displayed. Set up a network.
After the setup, select the [Apply] button.

NOTE: Even if you click the [Cancel] button, you cannot cancel the setting of the previous window.

[When the Firmware version is 83-02-01-x0/xx or more]

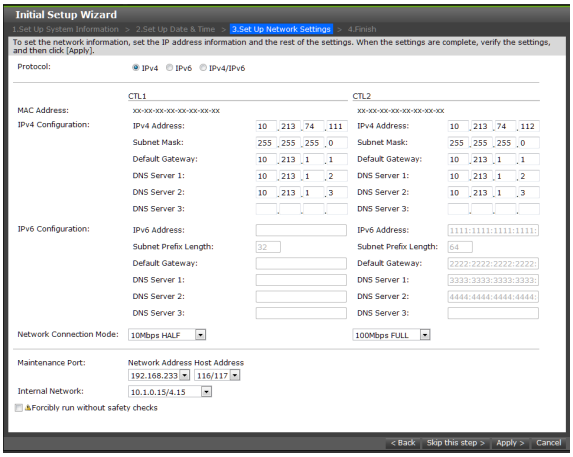


Clicking Option displays the following window.



Copyright © 2015, 2017, Hitachi, Ltd.

[When the Firmware version is less than 83-01-04-x0/xx]



Item		Input Description
Protocol		Selects the network protocol. • [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. • 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.

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

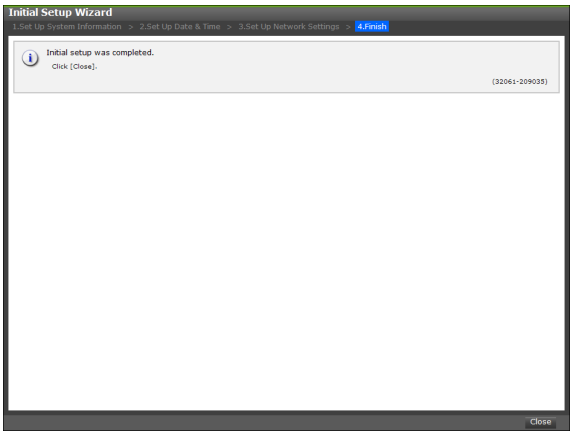
(Continued from preceding page)

Item		Input Description
Option		
	DNS Domain Name	Enters a domain name. • 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. • 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. (*1)

*1: When adding NAS modules, change the internal network from the global IP address (126.255.... or 192.169....) to the private IP address (other than the above global IP address. The recommended default is 10.251....). See “13.1 IP Addresses of Maintenance Ports and Internal Network” for the details.

Copyright © 2015, 2017, Hitachi, Ltd.

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



6. Window Display
   GUM may need to restart depending on the edit content of the network setting.
   When GUM needs to restart due to the setting, go to Step (1). If not, go to Step (2).

   (1) When GUM needs to restart
   (a) Restart GUM automatically.
   (b) The logout window is displayed. Click the [X] button to close the window.
   Wait until GUM starts up.

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

   (2) When GUM does not need to restart
   Return to the main window (Step 1.).

7. When changing the IP address, change the IP address of the Storage Device List.
   Refer to “1.6.5 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.

8. When changing the IP address of the maintenance port, change the IP address of the Maintenance PC.
   Refer to “1.3.1 IP Address Setting Method of Maintenance PC” for the detail.

Copyright © 2015, 2017, Hitachi, Ltd.

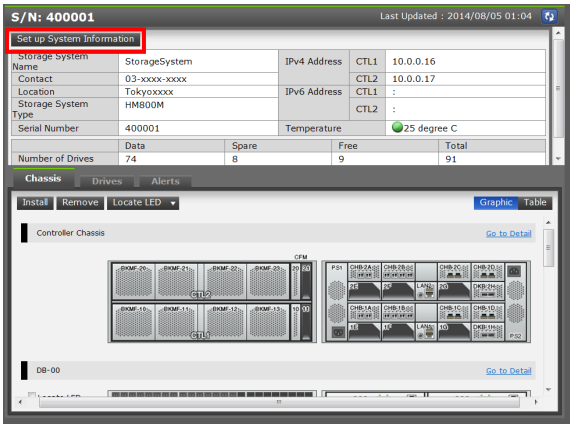
3. Storage System Maintenance Function

3.1 Network Setting [Start Separate Action]

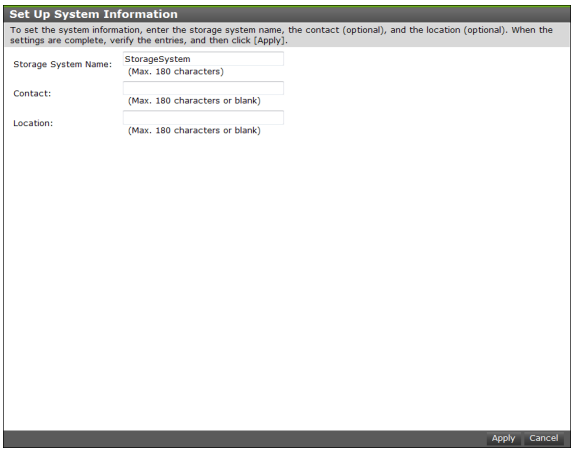
This is a window to register the system information (system name/address/installation position). Such information is used when using the alert notice function by SNMP.

NOTICE:	If the system information (Storage System name, contact and installation location) is set by NAS Manager, the set contents are also reflected in the Storage System.

1. Click the [Set Up System Information] button in the “Maintenance Utility” window.



2. 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.

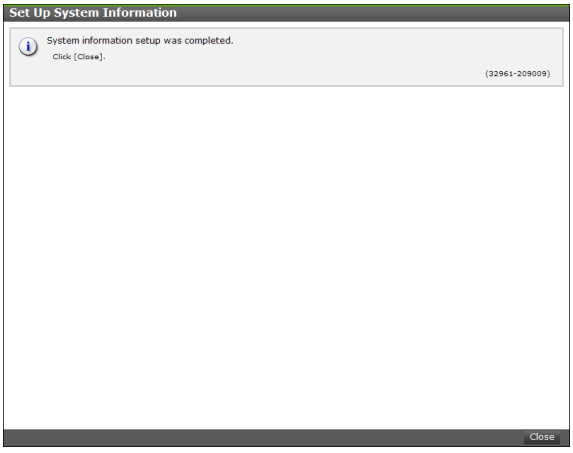
(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(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.

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

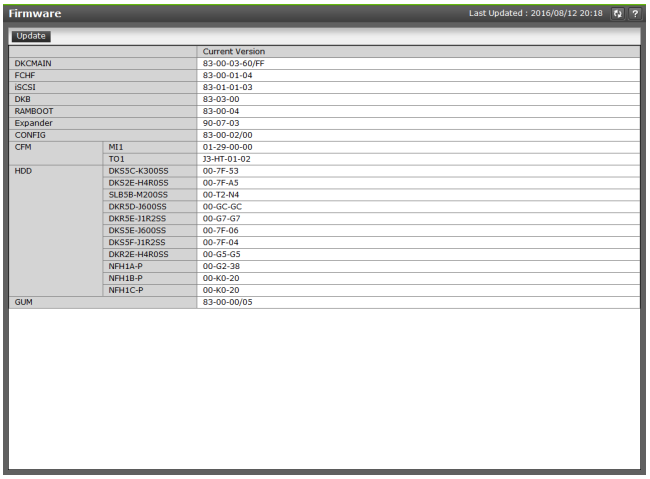


Copyright © 2015, 2017, Hitachi, Ltd.

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”.

Copyright © 2015, 2017, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2015, 2017, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2015, 2017, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2015, 2017, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2015, 2017, Hitachi, Ltd.

This page is for editorial purpose only.

Copyright © 2015, 2017, Hitachi, Ltd.

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.

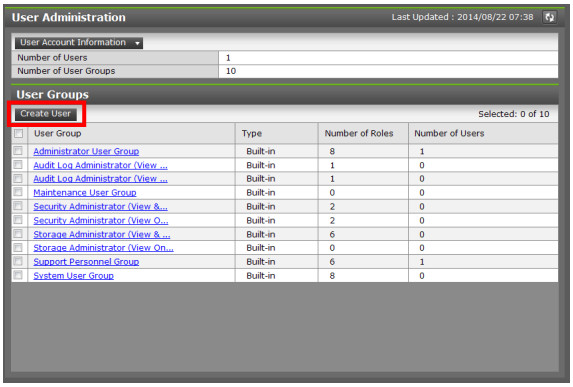
To change the availability of using each operation window of Maintenance Utility, register the user in the user group which has an appropriate role (authority).
You can control the availability of using each operation window of Maintenance Utility in accordance with the role given to the user group. For the role required for each operation window, see "3.3.6 Roles to be Required for the Operation Window of Maintenance Utility".

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.

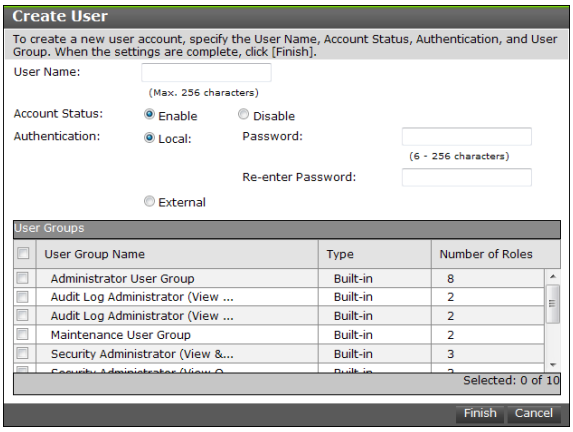
1. In the "Maintenance Utility" window, select [Administration] - [User Administration].

2. Click the [Create User] button of the "User Groups" window.



Copyright © 2015, 2017, Hitachi, Ltd.

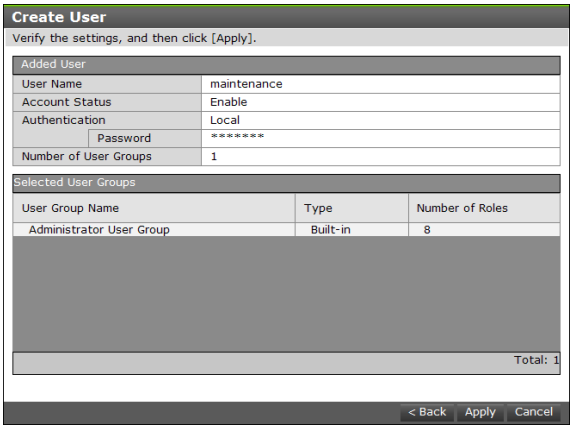
3. Create a new user account. Specify the User name, Account Status, Authentication and User Group. Click the [Finish] button.



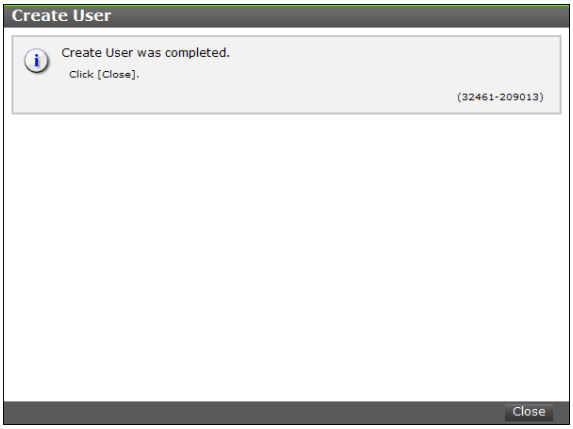
Item	Description
User Name	Enter the user name to be created. • When NAS Modules are not installed You can use up to 256 one-byte alphanumeric characters and the following symbols. (! # $ %& ' * + - . / = ? @ ^ _ ` { | } ~) • When NAS Modules are installed and you log into the NAS platform You can use up to 20 one-byte alphanumeric characters and the following symbols. (- . _) NOTE: Do not specify a user name using only “.” or “..”. Also, do not specify a user name starting with “-”. If you specify these user names, you will not be able to log into the NAS platform.
Account Status	Select whether to enable or disable the account. If the account is disabled, you will not be able to log into Web Console and the NAS platform.
Authentication	Select [Local] to authenticate the user by Web Console only without using the authentication server and to log into the NAS platform. • [Local]: Does not use authentication server. Uses a dedicated password for Web Console. • [External]: Uses authentication server. See “System Administrator Guide” for the details of the user management using the authentication server.
User Group	The user who logs into the NAS platform must belong to built-in Administrator User Group at least. (*1) See “System Administrator Guide” for the details of the built-in groups.

*1: For the firmware version less than 83-04-01-x0/xx, the user must belong to both built-in Administrator User Group and built-in Support Personnel Group at least.

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



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



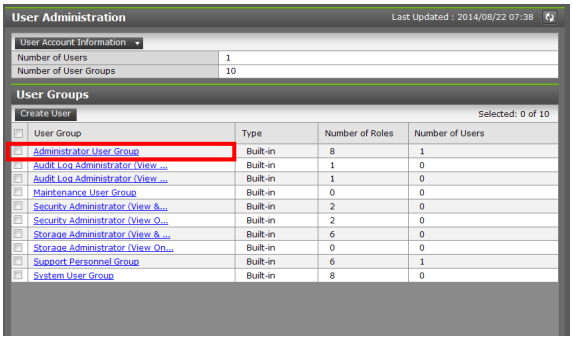
Copyright © 2015, 2017, Hitachi, Ltd.

3.3.2 Disabling User Accounts

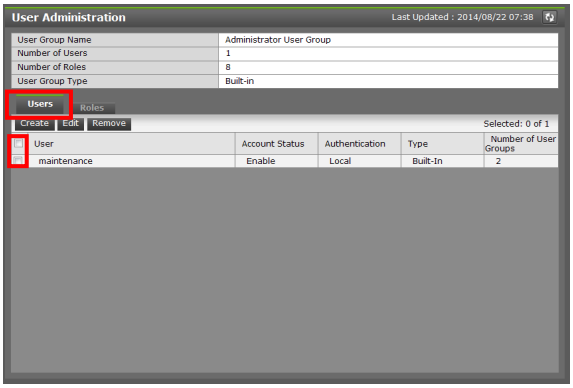
NOTICE:
- Log into an account that is different from the user whose account that you want to disable (you cannot disable the current login user account).
- To disable the user account specified by the registered storage system in the Storage Device List window, click Stop Service of the registered storage 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 "1.6.8 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.



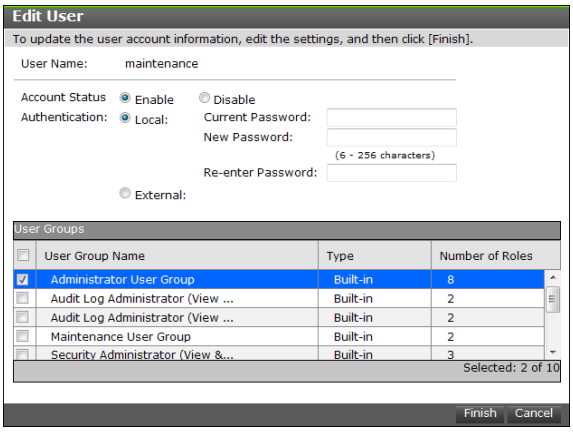
3. Click the [Users] tab. Select the user that you want to disable.



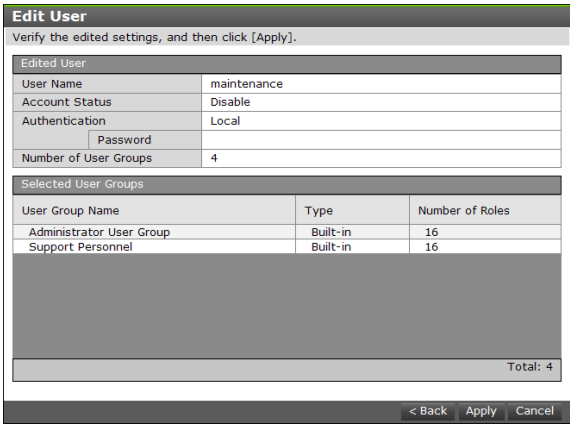
4. Click the [Edit] button.

Copyright © 2015, 2017, Hitachi, Ltd.

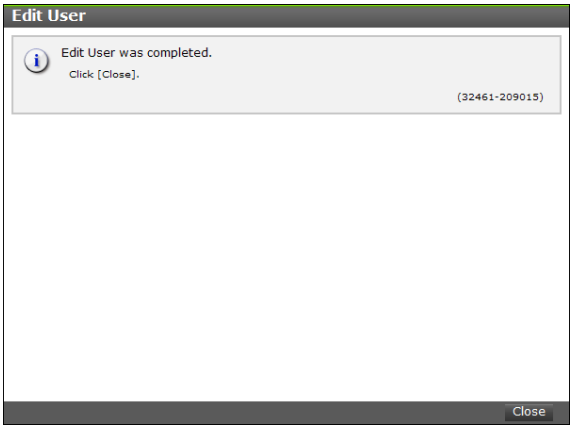
5. Select [Disable] from [Account Status] and click the [Finish] button.



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



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



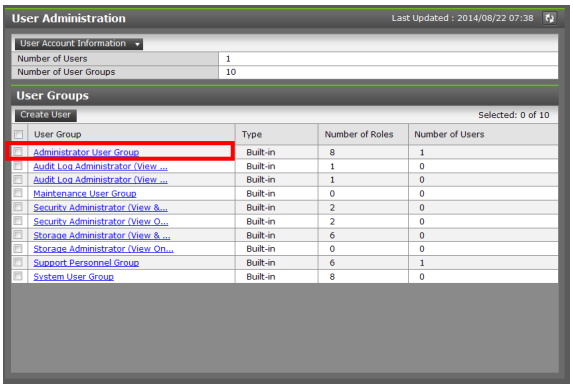
Copyright © 2015, 2017, Hitachi, Ltd.

3.3.3 Changing User Account Authentication

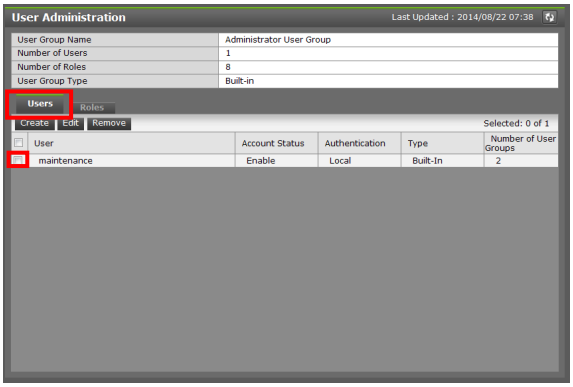
How to change the user account authentication and the password is described.

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.

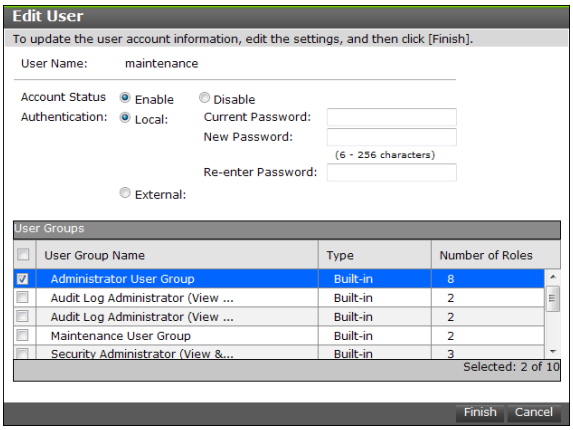


4. Click the [Edit] button.

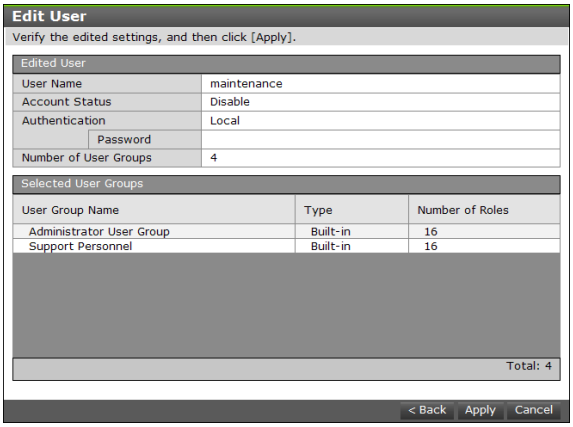
Copyright © 2015, 2017, Hitachi, Ltd.

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 “1.6.8 Incorrect display errors”.

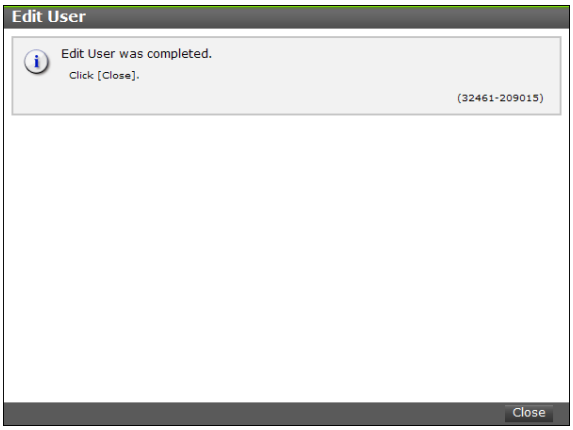


6. Confirm the settings. Click the [Apply] button.



Copyright © 2015, 2017, Hitachi, Ltd.

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



Copyright © 2015, 2017, Hitachi, Ltd.

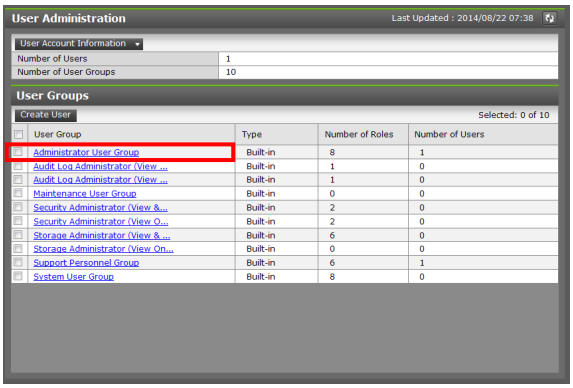
3.3.4 Removing User Accounts

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.

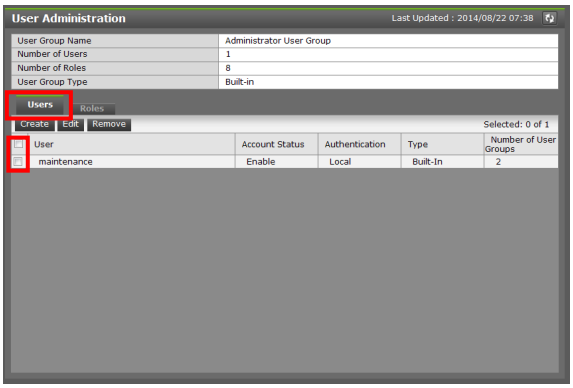
NOTICE:	To delete the user account specified by the registered storage system in the Storage Device List window, click Stop Service of the registered storage system. After deletion, click Edit to set an enabled user account. When the user account was disabled without performing Stop Service, Refer to "1.6.8 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.



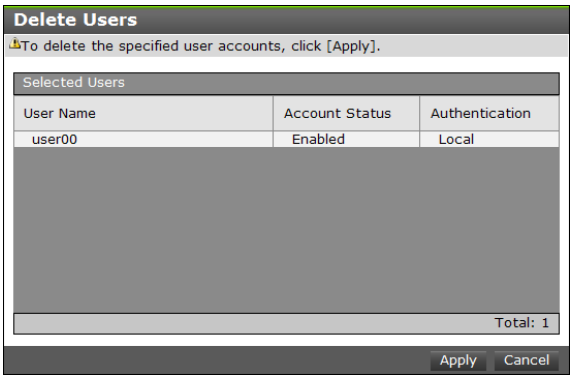
3. Click the [Users] tab. Select the user that you want to remove.



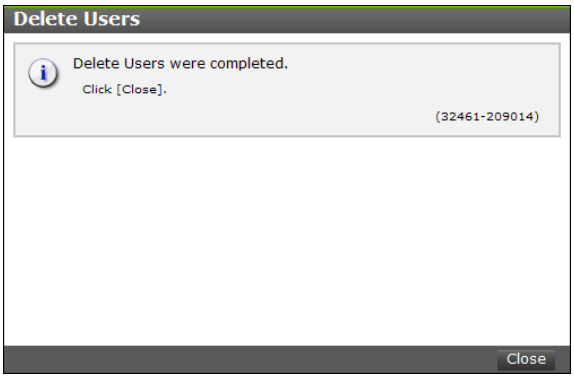
4. Click the [Remove] button.

Copyright © 2015, 2017, Hitachi, Ltd.

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.



Copyright © 2015, 2017, Hitachi, Ltd.

3.3.5 User Account Information

3.3.5.1 Backup User Accounts

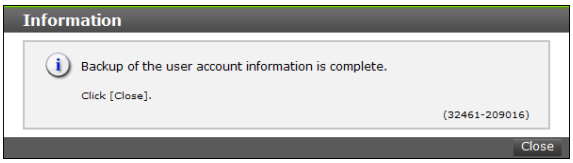
1. In the "Maintenance Utility" window, select [Administration] - [User Administration].

> **NOTICE:** When all the following conditions are met, perform Backup of the user account information again.
> - NAS Modules are installed.
> - The current firmware version is 83-03-24-x0/xx or later.
> - The user account information has been backed up with the firmware version less than 83-03-24-x0/xx.
>
> If you do, login to NAS Manager might fail. In that case, remove the user account and create one again (see to "3.3 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

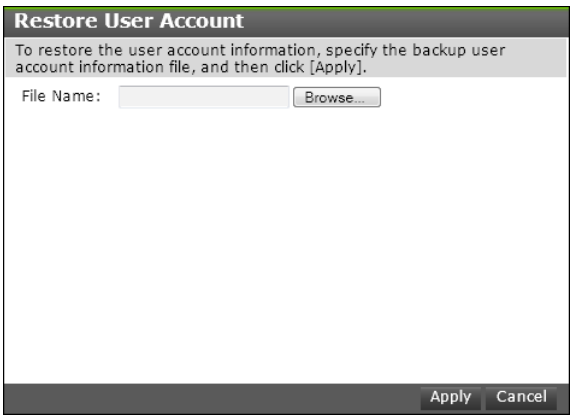
1. In the "Maintenance Utility" window, select [Administration] - [User Administration].

> **NOTICE:** If the current firmware version is 83-03-24-x0/xx or later when the Storage System is used with NAS Modules installed, do not use the user account information file backed up with the firmware version less than 83-03-24-x0/xx for restoring. Use a user account information file backed up with the firmware version 83-03-24-x0/xx or later.

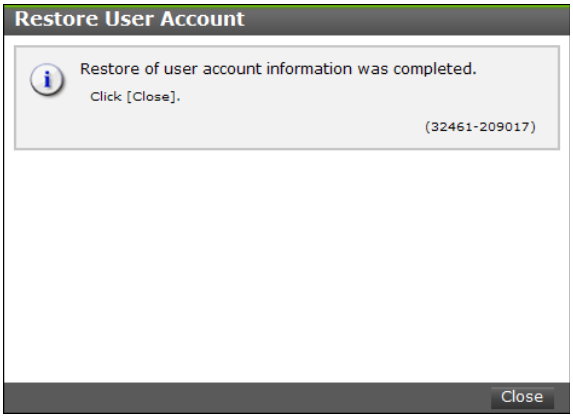
2. Select [User Account Information]-[Restore]. The "Restore User Account" window is displayed.

Copyright © 2015, 2017, Hitachi, Ltd.

3. Specify file names to be restored and click the [Apply] button.



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



Copyright © 2015, 2017, Hitachi, Ltd.

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”.

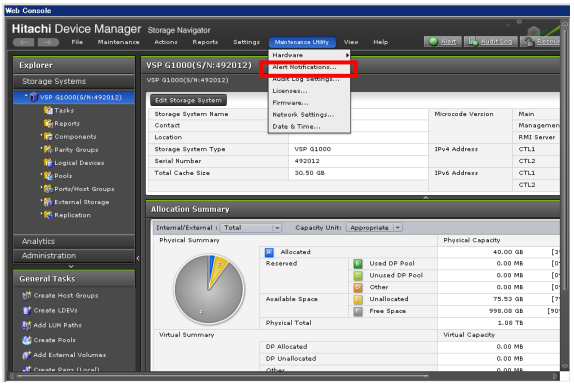
Maintenance Utility operation item	Required role name
Initial Setting Wizard	Storage Administrator (Initial Configuration)
Set Up System Information	Storage Administrator (Initial Configuration)
Firmware	Support Personnel or User Maintenance
User Administration	Security Administrator (View & Modify)
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)
Install NAS Unified Firmware	Support Personnel
Remove NAS Unified Firmware	Support Personnel
System Dump Download	No role is required.
Administration Menu	–
Power Management	–
System Management	–
Resetting GUM	–

Copyright © 2015, 2017, Hitachi, Ltd.

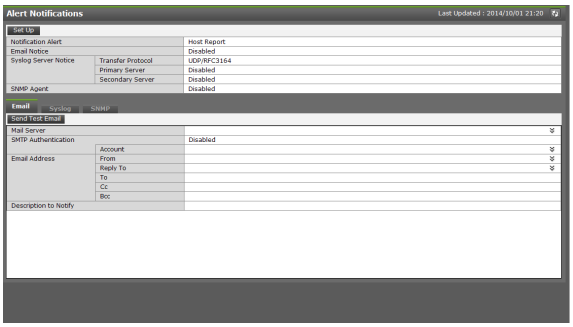
3.4 Alert Notifications

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.

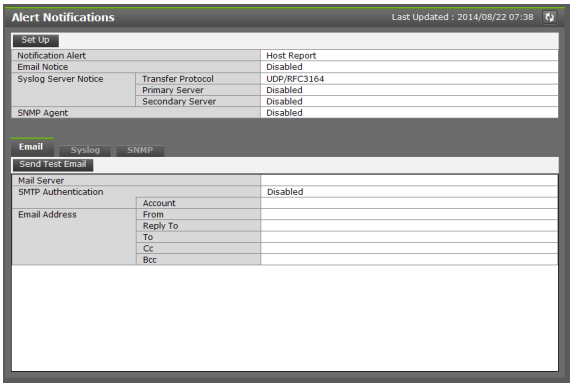
1. Starting “Alert Notifications” window
   (1) Start the Web Console referring to “1.6 Connecting to the Storage System”.
   (2) In the “Web Console” window, select [Maintenance Utility] - [Alert Notifications...]. The current installed firmware version is displayed.



2. The “Alert Notifications” window is displayed.
   [When the Firmware version is 83-01-04-x0/xx or more]



   [When the Firmware version is less than 83-01-04-x0/xx]



Copyright © 2015, 2017, Hitachi, Ltd.

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.

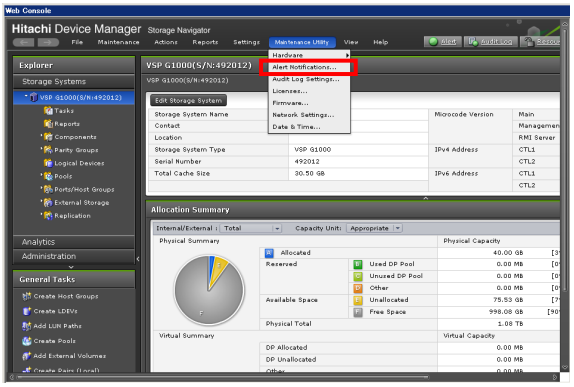
NOTICE:	If the settings (email server, transmission source email address and transmission destination email address) for notifying NAS failures by email are performed by NAS Manager, the set contents are also reflected in the Storage System.

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.

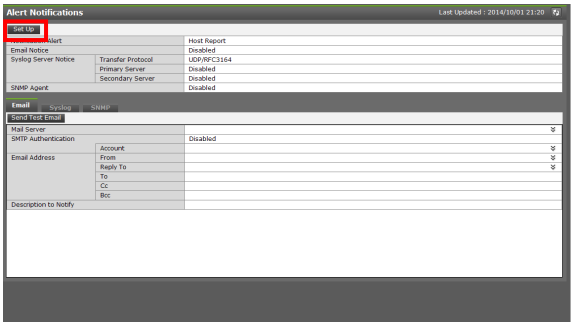
3.4.1.2 Procedure

1. In the “Web Console” window, select [Maintenance Utility] - [Alert Notifications...].

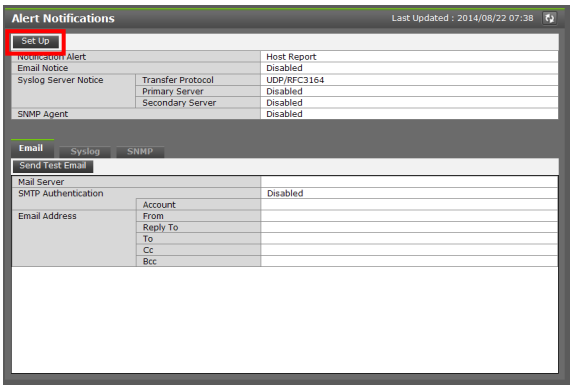


Copyright © 2015, 2017, Hitachi, Ltd.

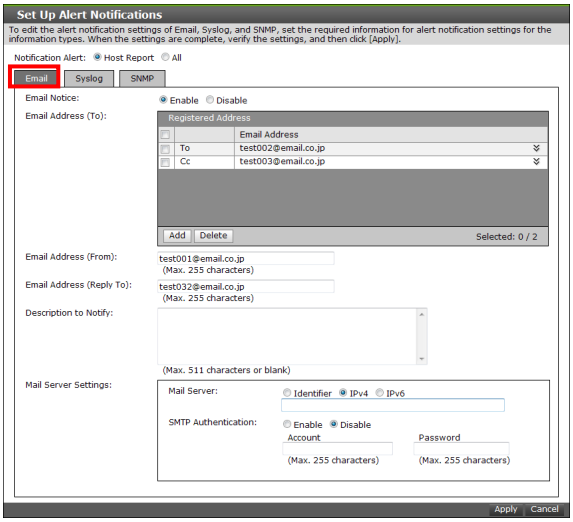
2. In the “Alert Notifications” window, click [Set Up].
   [When the Firmware version is 83-01-04-x0/xx or more]



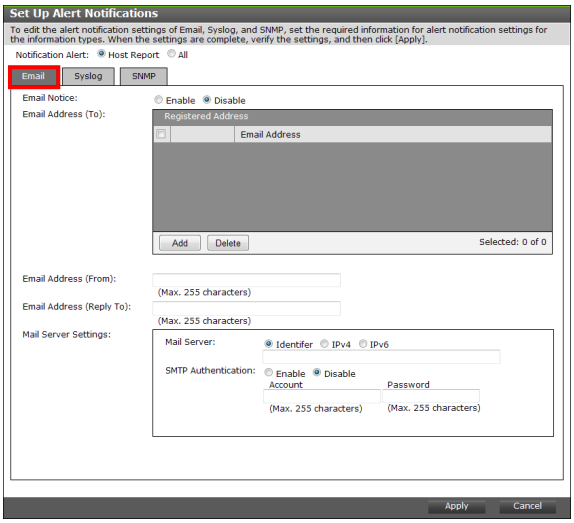
[When the Firmware version is less than 83-01-04-x0/xx]



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.
   [When the Firmware version is 83-01-04-x0/xx or more]



[When the Firmware version is less than 83-01-04-x0/xx]



Item	Description
Notification Alert	Selects a target SIM for notifying alerts. • [Host Report]: Reports the alert to only the SIMs that report to the host. • [All]: Reports the alert to all SIMs. The target SIM for notifying alerts is common for Email, Syslog, and SNMP.
Email Notice	Selects whether to notify the service information message (SIM) • [Enable]: Notifies the service information message (SIM) by email. • [Disable]: Does not notify the service information message (SIM) by email.

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

Item	Description
Email Address (To)	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. • [Email Address]: Displays the mail address.
Email Address (From)	Specifies an email address of the sender to notify the service information message (SIM). Enter up to 255 alphanumeric characters (ASCII codes) and symbols: (! # $ % & ` + - * / ‘ ^ { } _ . @ ~ = ?). If selected [Enable] at [Email Notice], you must set up this item.
Email Address (Reply to)	Specifies a Reply-To address of email. If you specify this address, replies from the email receivers will be sent to this address. If you omit this address, replies from the email receivers will be sent to Mail Address (From). Enter up to 255 alphanumeric characters (ASCII codes) and symbols: (! # $ % & ` + - * / ‘ ^ { } _ . @ ~ = ?).
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 feel 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. • [Identifier]: To specify a host name, select Identifier and enter up to 255 (When the firmware version is less than 83-03-21-x0/xx : 63) alphanumeric characters (ASCII codes) and symbols: (! $ % - . @ _ ` ~). • [IPv4]: To set an IPv4 address, select IPv4 and enter four integers in the range of 0 to 255 (for example, XXX.XXX.XXX.XXX, where X is a number). • [IPv6]:To set an IPv6 address, select IPv6 and enter eight hexadecimal alphanumeric in the range of 0 to FFFF. An abbreviated style of IPv6 address can also be specified. (for example, YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY:YYYY, where Y is a hexadecimal digit). If selected [Enable] at [Email Notice], you must set up this item.
Mail Server Settings-SMTP Authentication	Select whether to use the SMTP authentication. • [Enable]: Uses the SMTP authentication. • [Disable]: Does not use the SMTP authentication. If selected [Enable], you must enter [Account] and [Password]. Enter up to 255 alphanumeric characters (ASCII codes) and symbols: (! $ % - . @ _ ` ~).

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

Copyright © 2015, 2017, Hitachi, Ltd.

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]

Copyright © 2015, 2017, Hitachi, Ltd.

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 : 7fffff
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.

Copyright © 2015, 2017, Hitachi, Ltd.

3.4.2 Setting up Syslog Notification

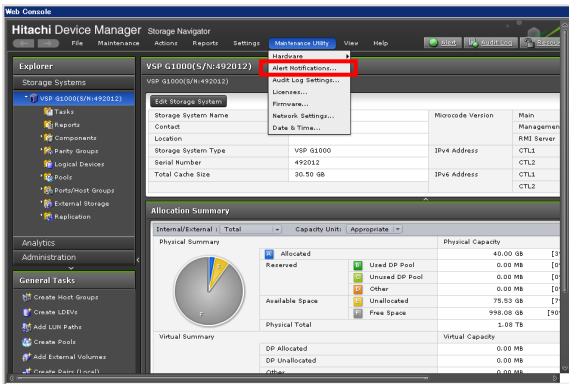
You can set the required information to notify in Syslog format when storage system failures occur.

3.4.2.1 Prerequisites

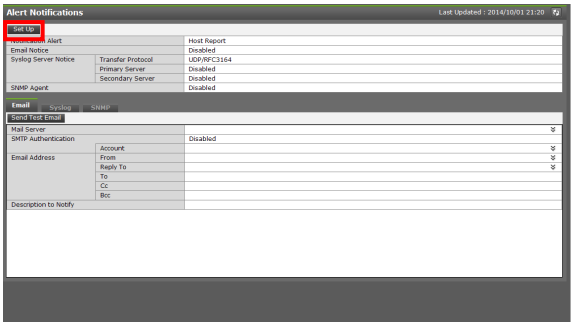
- You must have a server that supports Syslogs.
- If a firewall is used, a port must be opened to transfer Syslogs.

3.4.2.2 Procedure

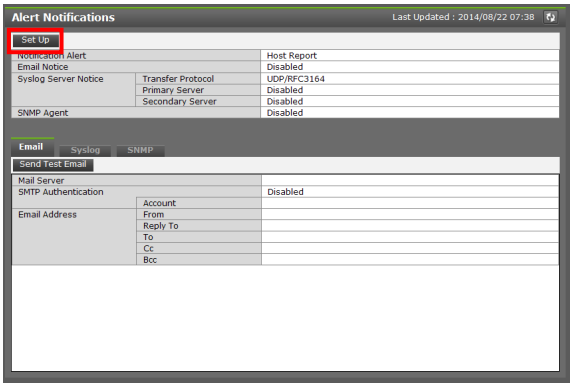
1. Starting “Alert Notifications” window.
   (1) Start the Web Console referring to “1.6 Connecting to the Storage System”.
   (2) In the “Web Console” window, select [Maintenance Utility] - [Alert Notifications...]. The current installed firmware version is displayed.



2. In the “Alert Notifications” window, click [Set Up].
   [When the Firmware version is 83-01-21-x0/xx or more]

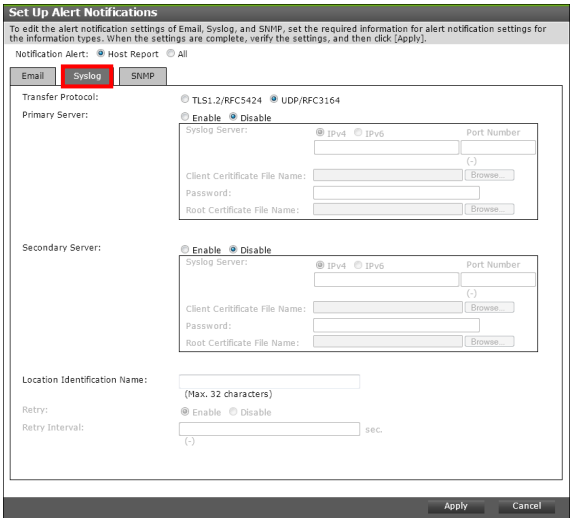


   [When the Firmware version is less than 83-01-21-x0/xx]



Copyright © 2015, 2017, Hitachi, Ltd.

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

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

Item	Description
Primary Server-Client Certificate File Name	Specifies a certificate file. Click [Browse], and then specify a certificate file. You must set this item only when [New Syslog Protocol (TLS1.2/ RFCS5424)] is selected at [Transfer Protocol] and when [Enable] is selected at [Primary Server]. • Be sure to set it when changing the items of the certificate from inactive to active. • After applying the setting, if the certificate is not set (blank) when applying the setting again, the previously updated certificate is used.
Primary Server-Password	Enters a password for the client certificate. Up to 128 characters can be entered for the password. Allowed characters are alphanumeric characters and symbols: ! # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~. Specifies this item only when [Client Certificate File Name] is specified.
Primary Server- Root Certificate File Name	Specifies a certificate file. Click [Browse], and then specify a certificate file. You must set this item only when [New Syslog Protocol (TLS1.2/ RFCS5424)] is selected at [Transfer Protocol] and when [Enable] is selected at [Primary Server]. • Be sure to set it when changing the items of the certificate from inactive to active. • After applying the setting, if the certificate is not set (blank) when applying the setting again, the previously updated certificate is used.
Secondary Server	Selects whether to use an alternative server (secondary server) to the Syslog server. • [Enable]: Notifies the service information message (SIM) to the secondary server in Syslog format . • [Disable]: Does not notify the service information message (SIM) to the secondary server in Syslog format.
Secondary Server-Syslog Server	Specifies an IP address of a server you want to set as a secondary server. The restriction for the available values is the same as that of [Primary Server-Syslog Server].
Secondary Server-Port Number	Specifies a port number to be used on the secondary server. Specifies this item only when [Enable] is selected at [Secondary Server].
Secondary Server-Client Certificate FileName	Specifies a certificate file. Click [Browse], and then specify a certificate file. This item is settable only when [New Syslog Protocol (TLS1.2/ RFCS5424)] is selected at [Transfer Protocol] and when [Enable] is selected at [Primary Server]. • Be sure to set it when changing the items of the certificate from inactive to active. • After applying the setting, if the certificate is not set (blank) when applying the setting again, the previously updated certificate is used.

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(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/ RFCS5424)]) is selected at [Transfer Protocol] and when [Enable] is selected at [Primary Server]. • Be sure to set it when changing the items of the certificate from inactive to active. • After applying the setting, if the certificate is not set (blank) when applying the setting again, the previously updated certificate is used.
Location Identification Name	Specifies an arbitrary name for the storage system that transfers the service information message (SIM) to the Syslog servers, so that you can identify the storage system. Enter 32 characters at the maximum. Allowed characters are alphanumeric characters and symbols: ! " # $ % & ' ( ) * + - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~. A comma (,). Be sure to set it only when [Primary Server] or [Secondary Server] is [Enable].
Retry	Displays the Retry setting. • [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/ RFCS5424)] 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/ RFCS5424)] 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.

Copyright © 2015, 2017, Hitachi, Ltd.

10. Specify the client certificate file, password, and root certificate file name. Specify this item only when [New Syslog Protocol (TLS1.2/ RFCS5424)] 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/ RFCS5424)] is selected at [Transfer Protocol].

13. Click [Apply].

Copyright © 2015, 2017, Hitachi, Ltd.

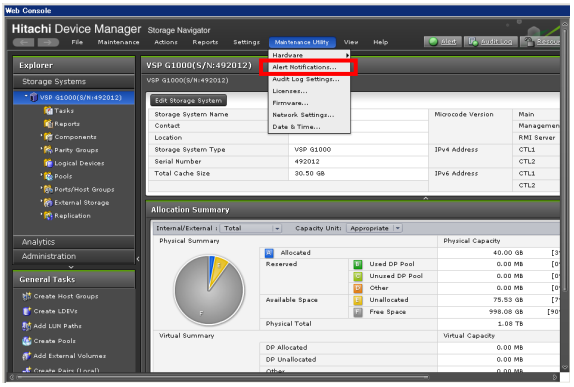
3.4.3 Setting up SNMP Notification

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

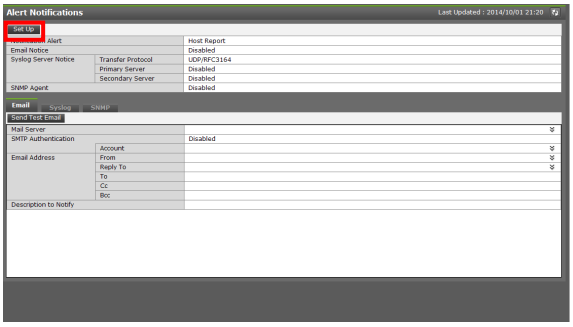
NOTICE:	If the settings (trap notification destination IP address and trap notification destination community) for notifying NAS failures by SNMP are performed by NAS Manager, the set contents are also reflected in the Storage System.

3.4.3.1 Procedure

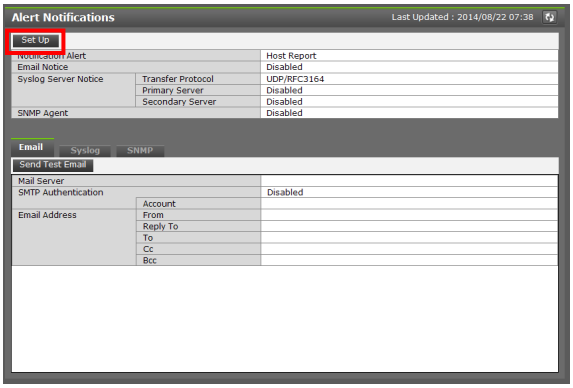
1. Starting "Alert Notifications" window.
   (1) Start the Web Console referring to "1.6 Connecting to the Storage System".
   (2) In the "Web Console" window, select [Maintenance Utility] - [Alert Notifications...]. The current installed firmware version is displayed.



2. In the "Alert Notifications" window, click [Set Up].
   [When the Firmware version is 83-01-04-x0/xx or more]

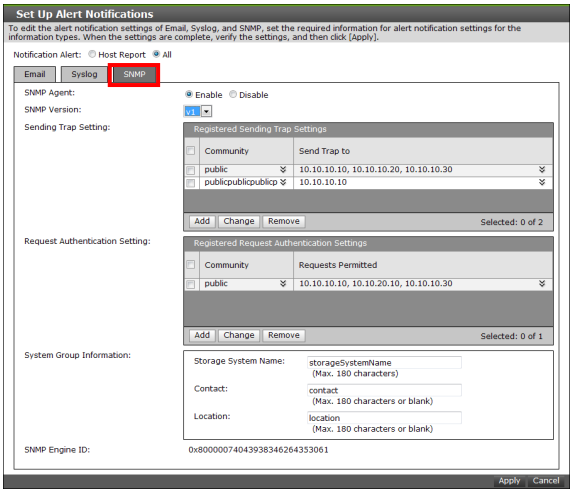


   [When the Firmware version is less than 83-01-04-x0/xx]

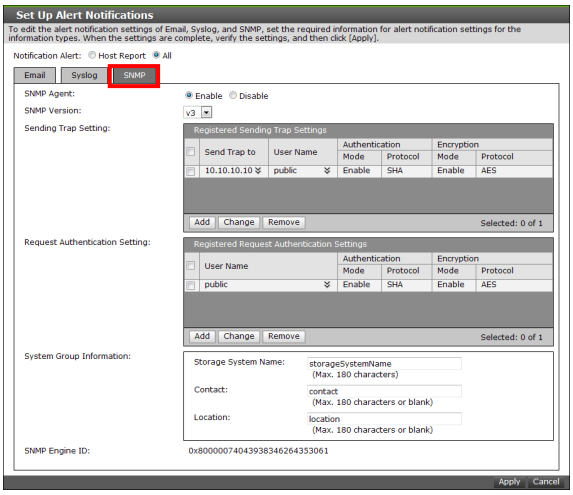


Copyright © 2015, 2017, Hitachi, Ltd.

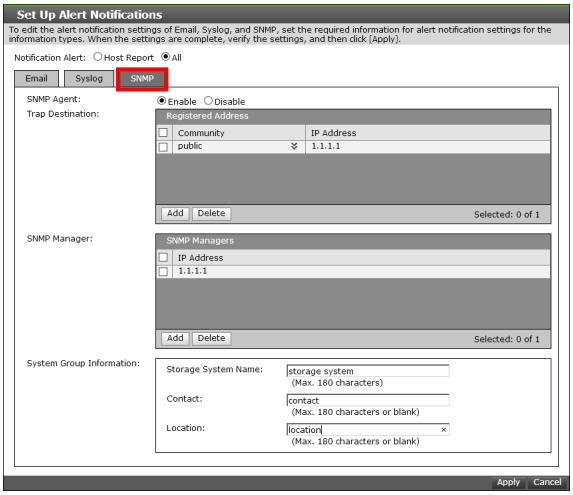
3. The “Set Up Alert Notifications” window appears. Click the [SNMP] tab.
   Set the transmission information of the SNMP which notifies storage system failures.
   [When the firmware version is 83-01-21-x0/xx or more and selecting v1 or v2c for the SNMP version]



[When the firmware version is 83-01-21-x0/xx or more and selecting v3 for the SNMP version]



[When the Firmware version is less than 83-01-21-x0/xx]



Copyright © 2015, 2017, Hitachi, Ltd.

Item	Description
Notification Alert	Selects a target SIM for notifying alerts. • [Host Report]: Reports the alert to only the SIMs that report to the host. • [All]: Reports the alert to all SIMs. The target SIM for notifying alerts is common for Email, Syslog, and SNMP.
SNMP Agent	Selects whether to use the SNMP agent. • [Enable]: Notifies the service information message (SIM) by SNMP trap and accept GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST (*1). • [Disable]: Does not notify the service information message (SIM) by SNMP trap and does not accept GET REQUEST, GETNEXT REQUEST, and GETBULK REQUEST (*1).
SNMP Version (*3)(*4)	Selecting the SNMP Protocol version.
Trap Destination (*2) or Sending Trap Setting (*3)(*4)	[IP Address](*2) Displays the IP address of the SNMP manager that reports the SNMP trap. [Community](*2)(*3) Displays the community name accepting the SNMP trap report [Send Trap to](*3)(*4) Displays the IP address that reports the SNMP trap. [User Name](*4) Displays the user name used for the SNMP trap report. [Authentication] - [Mode](*4) Displays whether the authentication by the password is enabled. [Authentication] - [Protocol](*4) When the authentication by the password is enabled, displays the authentication method. [Encryption] - [Mode](*4) Displays whether the encryption is enabled. [Encryption] - [Protocol](*4) When the encryption is enabled, displays the encryption method. For the settings, see “3.4.3.2 Adding SNMP Trap Notification Destinations”.

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

Item	Description
SNMP Manager (*2) or Request Authentication Setting (*3) (*4)	[IP Address](*2) Displays the IP address of the SNMP manager that accepts GET REQUEST and GETNEXT REQUEST. [Community](*3) Displays the community name that accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST (*1). [Requests Permitted](*3) Displays the IP address that accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST (*1). [User Name](*4) Displays the user name that accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST. [Authentication] - [Mode] (*4) Displays whether the authentication by the password is enabled. [Authentication] - [Protocol] (*4) When the authentication by the password is enabled, displays the authentication method. [Encryption] - [Mode] (*4) Displays whether the encryption is enabled. [Encryption] - [Protocol] (*4) When the encryption is enabled, displays the encryption method. For the settings, see “3.4.3.3 Adding the Request Permission Setting that Accepts GET REQUEST and GETNEXT REQUEST”.
System Group Information-Storage System Name (*5)	Specifies the name of the storage system. Enter up to 180 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? ” < > | & % ^). Do not enter a blank for the first or last character. This is an indispensable input item. If you change this item, the storage system name in the “Storage System” window of Web Console and Maintenance Utility is also changed.
System Group Information-Contact (*5)	Specifies the contact information such as administrator’s name and telephone number. Enter up to 180 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? ” < > | & % ^). Do not enter a blank for the first or last character. If you change this item, the contact in the “Storage System” window of Web Console and Maintenance Utility is also changed.
System Group Information-Location (*5)	Specifies the installation location of the connected storage system. Enter up to 180 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? ” < > | & % ^). Do not enter a blank for the first or last character. If you change this item, the location in the “Storage System” window of Web Console and Maintenance Utility is also changed.

Copyright © 2015, 2017, Hitachi, Ltd.

*1: GETBULK REQUEST is supported only when the firmware version 83-01-21-x0/xx or later and SNMP version is v2c or v3.
*2: This item is displayed when the firmware version is earlier than 83-01-21-x0/xx.
*3: This item is displayed when the firmware version is 83-01-21-x0/xx or later and selecting v1 or v2c for the SNMP version.
*4: This item is displayed when the firmware version is 83-01-21-x0/xx or later and selecting v3 for the SNMP version.
*5: If the system information (Storage System name, contact and installation location) is set by NAS Manager, the set contents are also reflected in the Storage System.

4. Confirm the settings. Click [Apply].

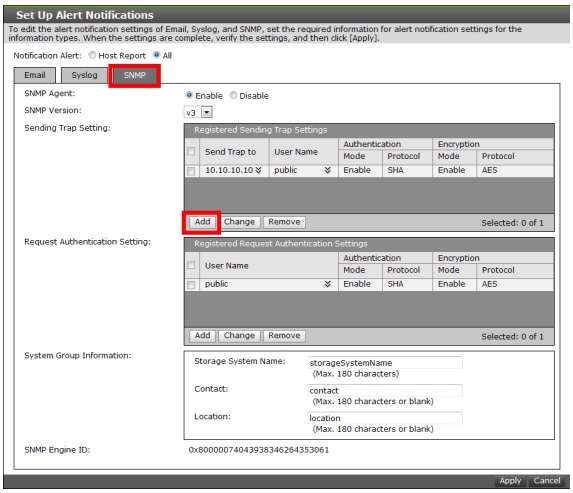
Copyright © 2015, 2017, Hitachi, Ltd.

3.4.3.2 Adding SNMP Trap Notification Destinations

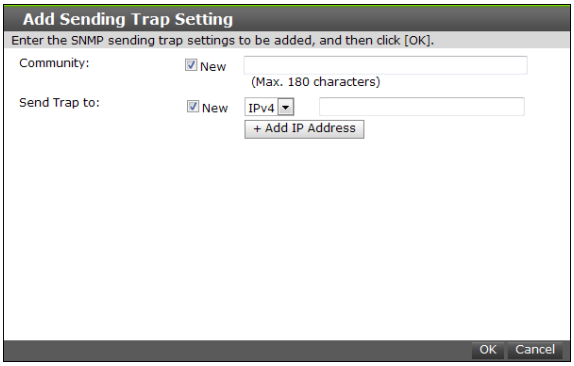
The following procedure describes how to add information of SNMP trap notification destinations used for trap transmission.

- When the Firmware version is 83-01-21-x0/xx or more : "1. When the Firmware version is 83-01-21-x0/xx or more."
- When the Firmware version is less than 83-01-21-x0/xx : "2. When the Firmware version is less than 83-01-21-x0/xx."

1. When the Firmware version is 83-01-21-x0/xx or more.
   (1) In the "Set Up Alert Notifications" window, click the [SNMP] tab.Under the [Sending Trap Setting], click the [Add] button.



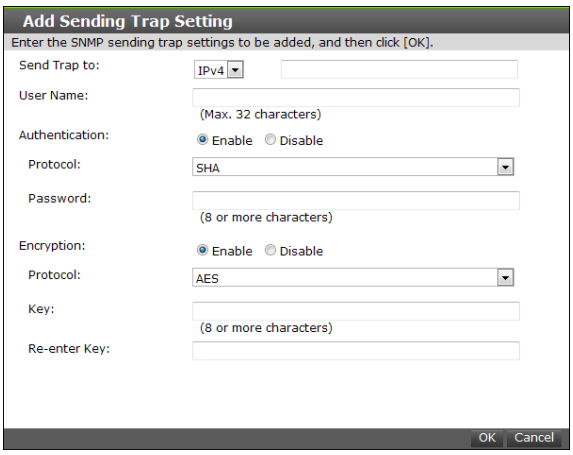
   (2) The "Add Sending Trap Setting" window appears.
   [When selecting v1 or v2c as the SNMP version]



Item	Description
Community	The community name used for the SNMP trap report is displayed. Enter up to 180 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? " < > | & % ^ '). Do not enter a blank for the first or last character.
Send Trap to	Newly enter or select the IP address that reports the SNMP trap. • [+ Add IP Address] Add IP addresses. You can add up to 32 IP addresses.

Copyright © 2015, 2017, Hitachi, Ltd.

[When selecting v3 as the SNMP version]



Item	Description
Send Trap to	Enter the IP address that reports the SNMP trap.
User Name (*1)	Enter the user name used for the SNMP trap report. Enter up to 32 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? ” < > | & % ^). Do not enter a blank for the first or last character.
Authentication	Select whether to enable or disable the authentication by the password. • [Enabled]: Enable the authentication by the password. • [Disabled]: Disable the authentication by the password.
Authentication - Protocol	When enabling the authentication by the password, select the authentication method (SHA or MD5).
Authentication - Password	When enabling the authentication by the password, enter the password. The password should be between eight and 64 characters.
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.
Encryption - Re-enter Key	Re-enter the key entered by [Key].

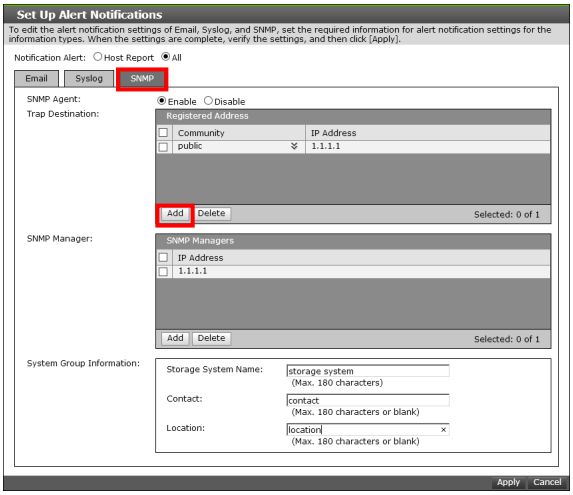
*1: When using the set user name for [Sending Trap Settings] or [Request Authentication Settings], enter the same details as those set by the user in the following items. If you enter different details, the trap might not be sent correctly.
- Authentication
- Authentication - Protocol
- Authentication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

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

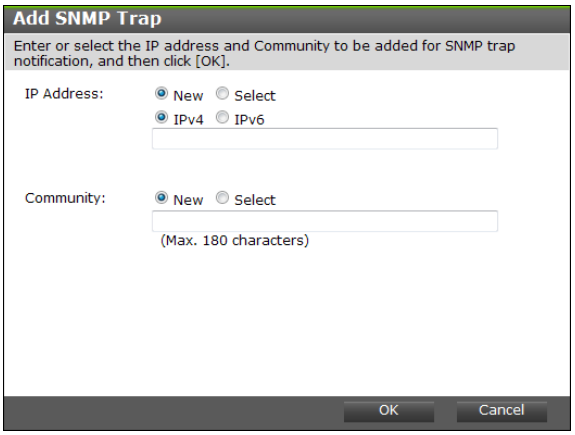
(4) Confirm the settings. Click the [Apply] button.

Copyright © 2015, 2017, Hitachi, Ltd.

2. When the Firmware version is less than 83-01-21-x0/xx.
   (1) In the "Set Up Alert Notifications" window, click the [SNMP] tab.Under the [Trap Destination], click the [Add] button.



   (2) The "Add SNMP Trap" window appears. Enter or select the IP address and Community to be added for SNMP trap notification.



Item	Description
IP Address	Selects whether to enter the new IP address or select the IP address. • [New]: Enter the new IP address. • [Select]: Selects the IP address. Selects [IPv4] or [IPv6] for the version of the IP address version.
Community	Selects whether to enter the new community or select the community. • [New]: Enter the new community. Enter up to 180 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? " < > | & % ^ '). Do not enter a blank for the first or last character. • [Select]: Selects the community. The added community is also used as a community to accept GET REQUEST and GETNEXT REQUEST.

(3) Click the [OK] button.
The combination of the entered community and the IP address is added to [Trap Destination].

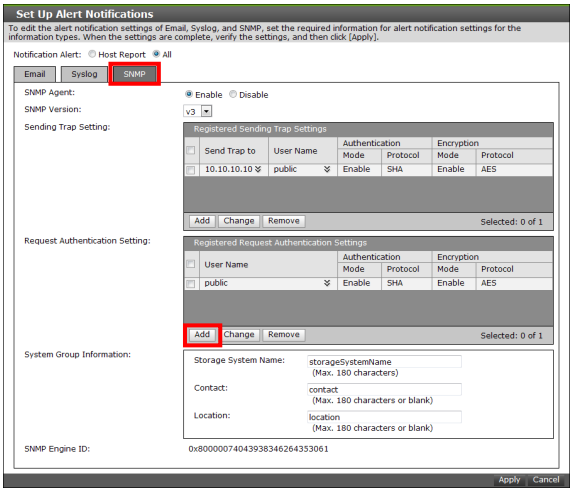
(4) Confirm the settings. Click the [Apply] button.

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.

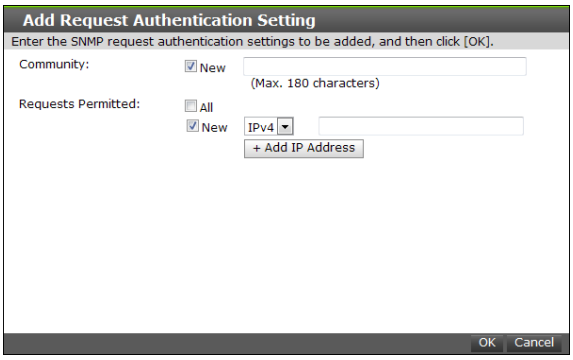
- When the Firmware version is 83-01-21-x0/xx or more : "1. When the Firmware version is 83-01-21-x0/xx or more."
- When the Firmware version is less than 83-01-21-x0/xx : "2. When the Firmware version is less than 83-01-21-x0/xx."

1. When the Firmware version is 83-01-21-x0/xx or more.
   (1) In the "Set Up Alert Notifications" window, click the [SNMP] tab.Under the [Request Authentication Setting], click the [Add] button.



Copyright © 2015, 2017, Hitachi, Ltd.

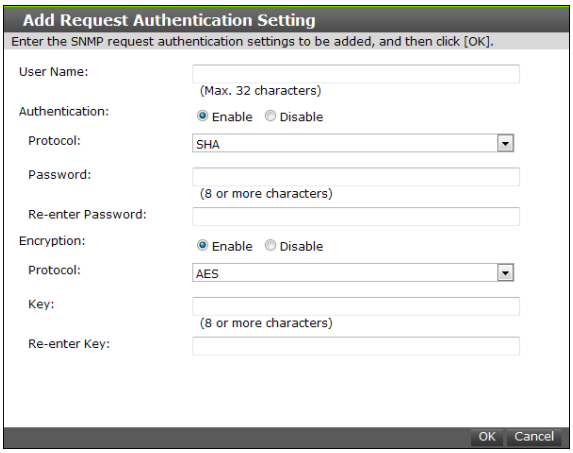
(2) The “Add Request Authentication Setting” window appears.
[When selecting v1 or v2c as the SNMP version]



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

Copyright © 2015, 2017, Hitachi, Ltd.

[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.
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.
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

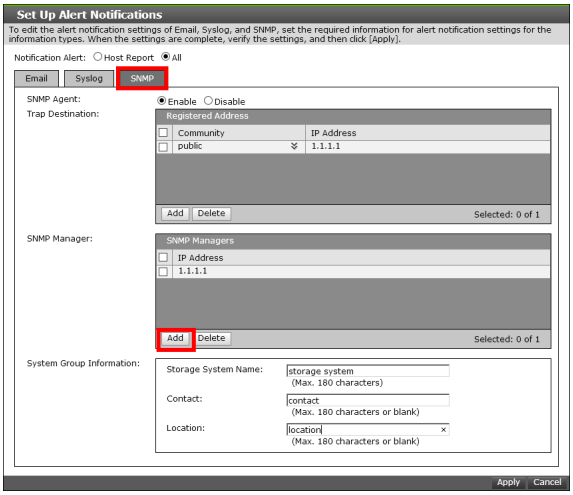
Copyright © 2015, 2017, Hitachi, Ltd.

(3) Click the [OK] button.
The entered information is added to [Request Authentication Setting] in the "Set Up Alert Notifications" window.

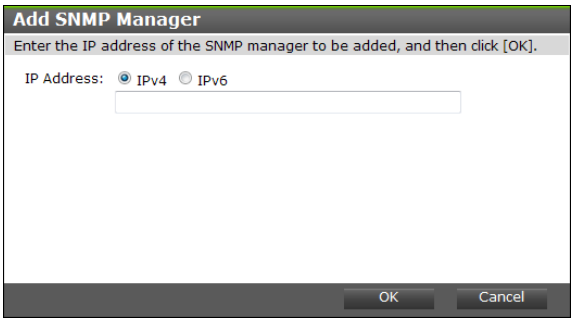
(4) Confirm the settings. Click the [Apply] button.

2. When the Firmware version is less than 83-01-21-x0/xx.

(1) In the "Set Up Alert Notifications" window, click the [SNMP] tab.Under the [SNMP Managers], click the [Add] button.



(2) The "Add SNMP Manager" window appears.Under the [IP Address], select the version of the IP address, and enter the IP address of the SNMP Manager.



NOTICE:	Any IP address that has all values set to zero (0) cannot be specified for IPv4 and IPv6. The IPv6 address is specified by entering eight hexadecimal numbers that are separated by colons (:) using a maximum of 4 digits from zero (0) to FFFF inclusive. The default form of the IPv6 address can be specified.

(3) Click the [OK] button.
The entered IP address is added to the [IP Address] in the [SNMP Managers].

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

Copyright © 2015, 2017, Hitachi, Ltd.

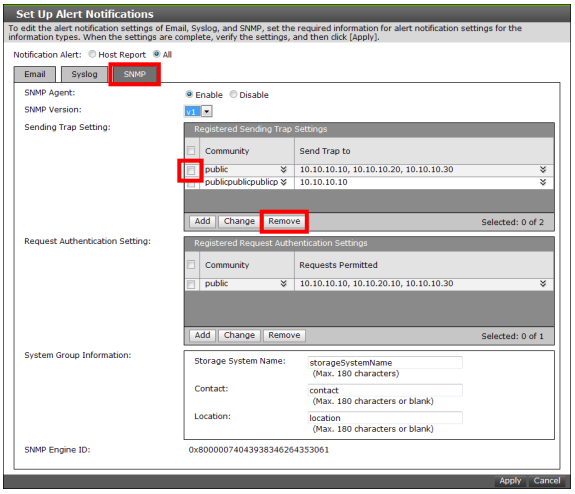
3.4.3.4 Deleting the SNMP Trap Notification

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

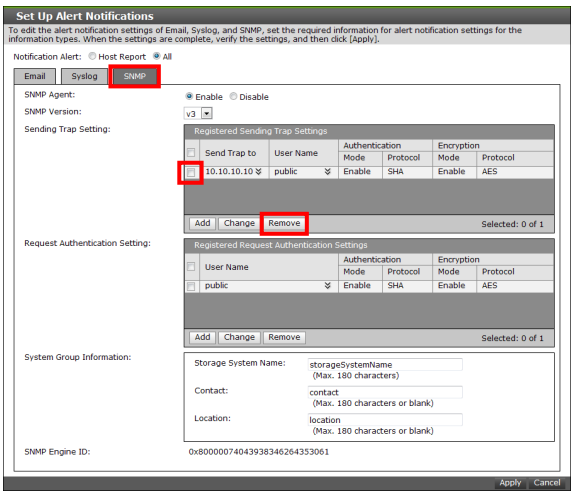
NOTICE:	When the firmware version is 83-01-21-x0/xx or more, the community registered in [Trap Destination] is also used as the community which accepts GET REQUEST and GETNEXT REQUEST. When deleting all communities which accept GET REQUEST and GETNEXT REQUEST, the target communities cannot accept GET REQUEST and GETNEXT REQUEST. Therefore, it is necessary to add communities again.

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] ([Trap Notification Destination] in the case of 83-01-21-x0/xx or earlier) and click [Delete].
   The selected community/user names are deleted.

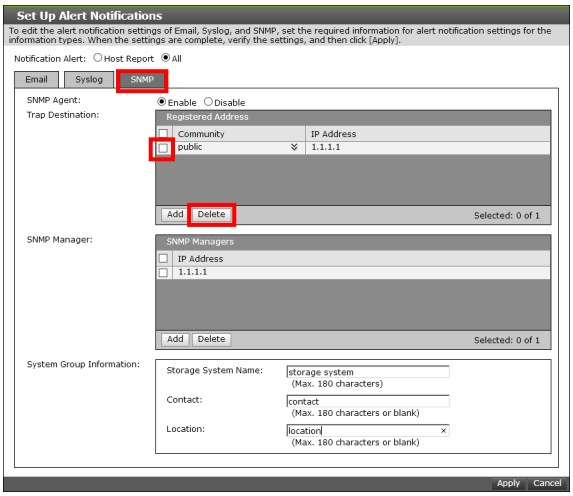
   [When the firmware version is 83-01-21-x0/xx or more and selecting v1 or v2c for the SNMP version]



   [When the firmware version is 83-01-21-x0/xx or more and selecting v3 for the SNMP version]



[When the firmware version is 83-01-21-x0/xx or more]



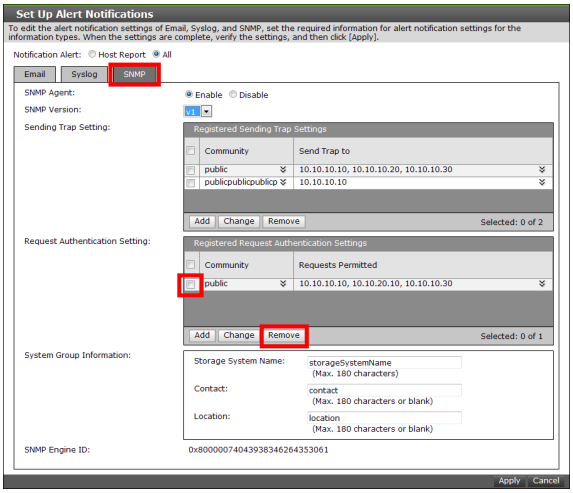
2. Confirm the settings. Click [Apply].

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.

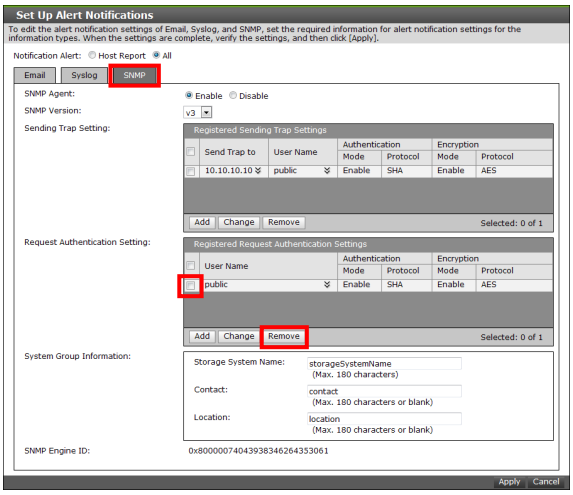
1. In the “Set Up Alert Notifications” window, Click the [SNMP] tab.
   Select one or more rows to be deleted in [Request Authentication Setting] ([SNMP Manager] in the case of 83-01-21-x0/xx or earlier) and click [Delete].
   The selected rows are deleted.

   [When the firmware version is 83-01-21-x0/xx or more and selecting v1 or v2c for the SNMP version]

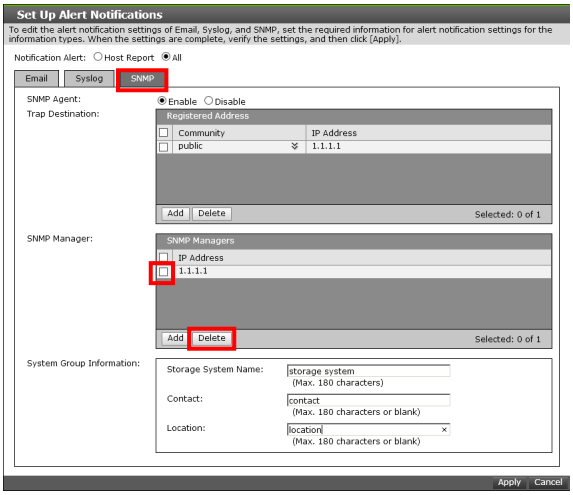


Copyright © 2015, 2017, Hitachi, Ltd.

[When the firmware version is 83-01-21-x0/xx or more and selecting v3 for the SNMP version]



[When the firmware version is 83-01-21-x0/xx or more]



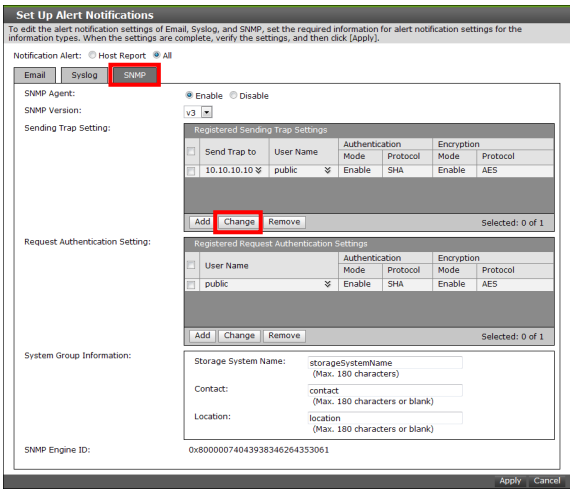
2. Confirm the settings. Click [Apply].

Copyright © 2015, 2017, Hitachi, Ltd.

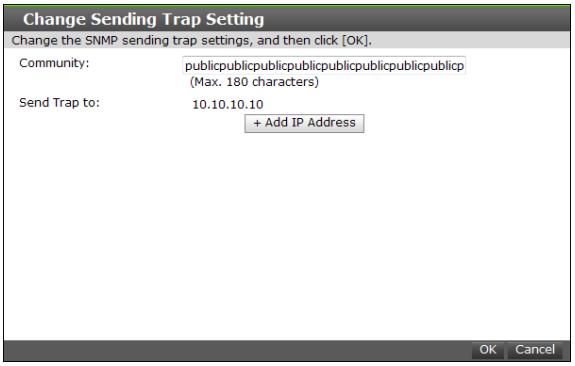
3.4.3.6 Changing the Sending Trap Settings

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.



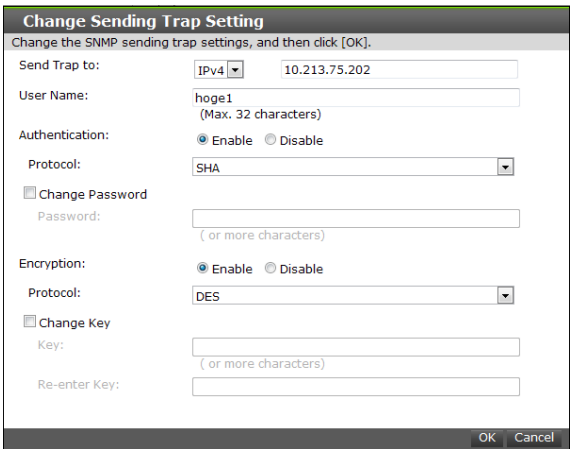
2. The "Change Sending Trap Setting" window appears.
   [When selecting v1 or v2c as the SNMP version]



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

Copyright © 2015, 2017, Hitachi, Ltd.

[When selecting v3 as the SNMP version]



Item	Description
Send Trap to	Enter the IP address that reports the SNMP trap.
User Name (*1)	Enter the user name used for the SNMP trap report. Enter up to 32 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? ” < > | & % ^). Do not enter a blank for the first or last character.
Authentication	Select whether to enable or disable the authentication by the password. • [Enabled]: Enable the authentication by the password. • [Disabled]: Disable the authentication by the password. The columns of [Authentication] and [Encryption] are displayed only when selecting [Enabled].
Authentication - Protocol	When enabling the authentication by the password, select the authentication method (SHA or MD5).
Authentication - Change Password	The column of [Password] is displayed only when checking the checkbox of [Change Password].
Authentication - Password	When enabling the authentication by the password, enter the password. The password should be between eight and 64 characters.
Encryption	Select whether to enable or disable the encryption. • [Enabled]: Enable the encryption. • [Disabled]: Disable the encryption. The column of [Encryption] is displayed only when selecting [Enabled].
Encryption - Protocol	When enabling the encryption, select the encryption method (AES or DES).
Encryption - change Key	The columns of [Key] and [Re-enter Key] are displayed only when checking the checkbox of [Change Key].
Encryption - Key	When enabling the encryption, enter the key. The key should be between eight and 64 characters.
Encryption - Re-enter Key	Re-enter the key entered by [Key].

Copyright © 2015, 2017, Hitachi, Ltd.

*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.

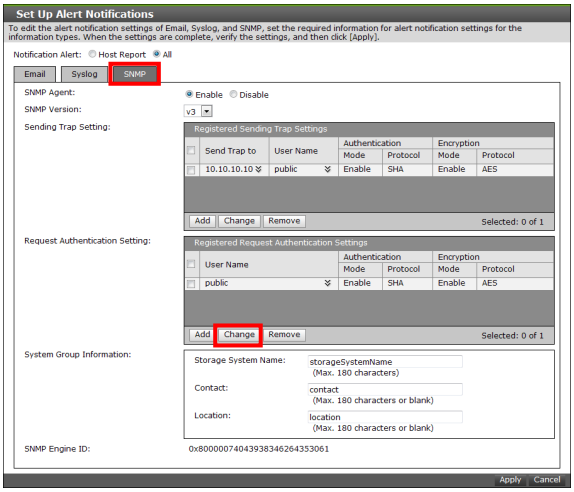
4. Confirm the settings. Click the [Apply] button.

Copyright © 2015, 2017, Hitachi, Ltd.

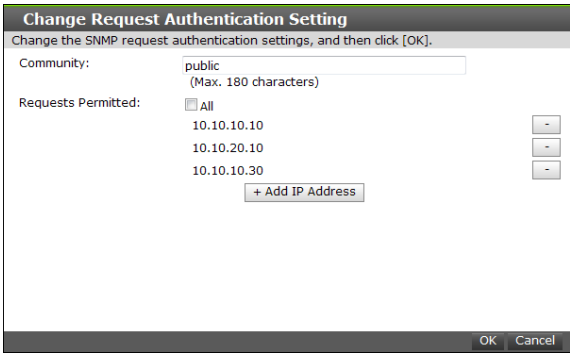
3.4.3.7 Changing the Request Permission Setting

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.



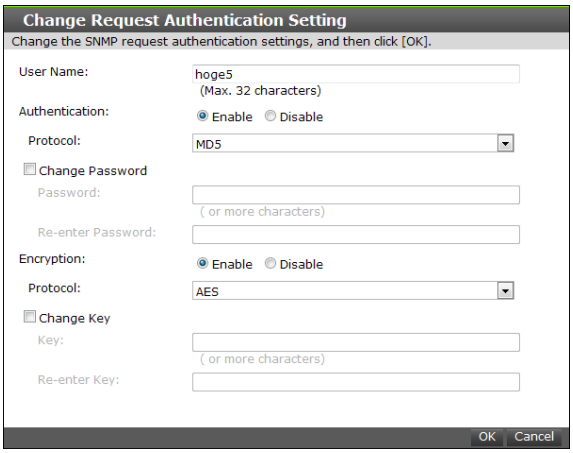
2. The "Change Request Authentication Setting" window appears.
[When selecting v1 or v2c as the SNMP version]



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

Copyright © 2015, 2017, Hitachi, Ltd.

[When selecting v3 as the SNMP version]



Item	Description
User Name (*1)	Enter the user name who accepts GET REQUEST, GETNEXT REQUEST and GETBULK REQUEST. Enter up to 32 alphanumeric characters (ASCII codes), except for some symbols (\ , / ; : * ? ” < > | & % ^). Do not enter a blank for the first or last character.
Authentication	Select whether to enable or disable the authentication by the password. • [Enabled]: Enable the authentication by the password. • [Disabled]: Disable the authentication by the password. The columns of [Authentication] and [Encryption] are displayed only when selecting [Enabled].
Authentication - Protocol	When enabling the authentication by the password, select the authentication method (SHA or MD5).
Authentication - Change Password	The column of [Password] is displayed only when checking the checkbox of [Change Password].
Authentication - Password	When enabling the authentication by the password, enter the password. The password should be between eight and 64 characters.
Authentication - Re-enter Password	Re-enter the password entered in [Password].
Encryption	Select whether to enable or disable the encryption. • [Enabled]: Enable the encryption. • [Disabled]: Disable the encryption. The column of [Encryption] is displayed only when selecting [Enabled].
Encryption - Protocol	When enabling the encryption, select the encryption method (AES or DES).
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.
Encryption - Re-enter Key	Re-enter the key entered by [Key].

Copyright © 2015, 2017, Hitachi, Ltd.

*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.

Copyright © 2015, 2017, Hitachi, Ltd.

3.4.3.8 Performing the Trap Report Test

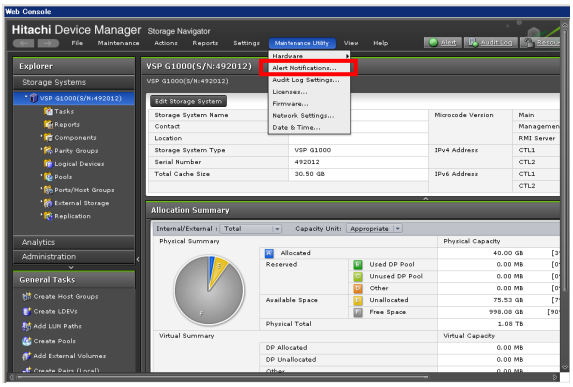
Performing this operation issues the SNMP trap for test (reference code: 7fffff) to the trap sending destination.

Prerequisites

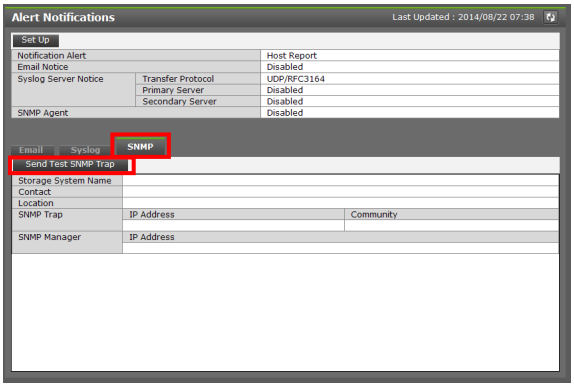
- The trap sending destination should be set completely in the “Set Up Alert Notifications” window.

Procedure

1. Starting “Alert Notifications” window.
   (1) Start the Web Console referring to “1.6 Connecting to the Storage System”.
   (2) In the “Web Console” window, select [Maintenance Utility] - [Alert Notifications...]. The current installed firmware version is displayed.



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



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

Copyright © 2015, 2017, Hitachi, Ltd.

3.5 Time Setting

This is a window to set the system time.

NOTICE:	If the date, the time, the time zone and the NTP server are set by NAS Manager, the set contents are also reflected in the Storage System.

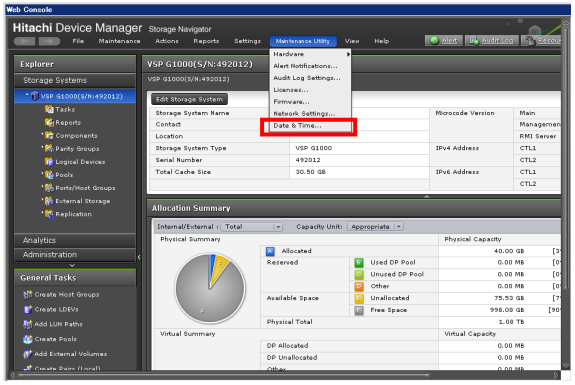
3.5.1 Setting Synchronization Information

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
   (1) When starting Maintenance Utility from the browser
      (a) Refer to "1.8.2.3 Starting the Browser" to start Maintenance Utility.
      (b) In the "Maintenance Utility" window, select [Administration] - [Date & Time].
   (2) When starting Maintenance Utility from Web Console
      (a) Start the Web Console referring to "1.6 Connecting to the Storage System".
      (b) In the "Web Console" window, select [Maintenance Utility] - [Date & Time...]. The current installed firmware version is displayed.

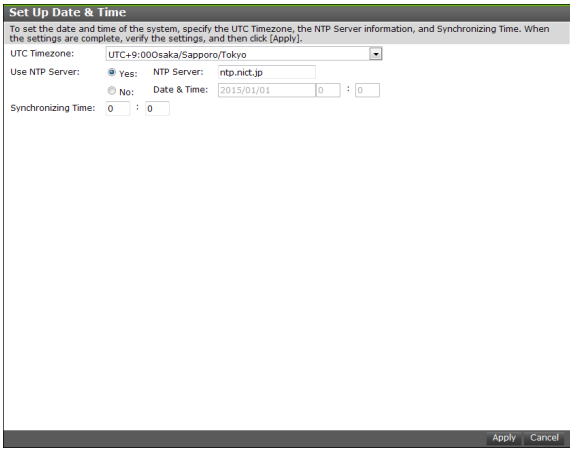


Copyright © 2015, 2017, Hitachi, Ltd.

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.



NOTE: When the Firmware version is less than 83-02-01-x0/xx, the "Automatically adjust clock for Daylight Saving Time" is not displayed.

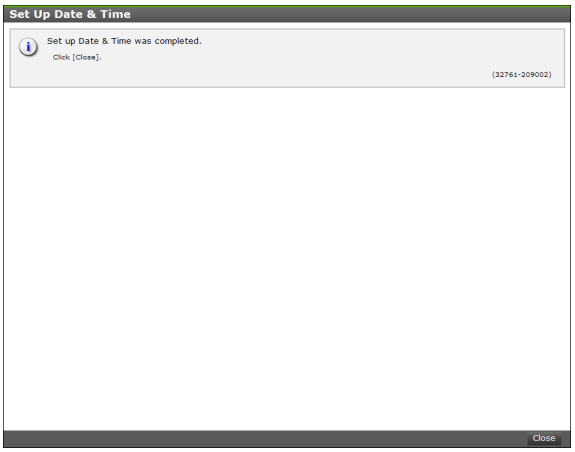
Item	Input Description
UTC Timezone	Select an area of the Universal Time Coordinated
Automatically adjust clock for Daylight Saving Time	Select whether to adjust the daylight-saving time automatically. Displayed only when the UTC time zone applies the daylight-saving time.

(To be continued)

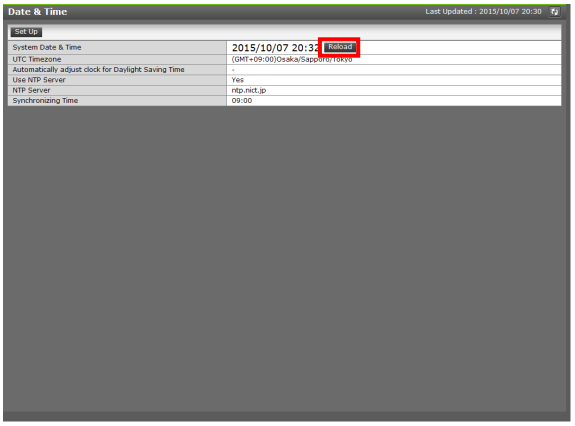
(Continued from preceding page)

Item		Input Description
Use NTP Server		Check the use of the NTP server
	Yes: NTP Server	Enter an IP address or a server name. • 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.
	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.



Copyright © 2015, 2017, Hitachi, Ltd.

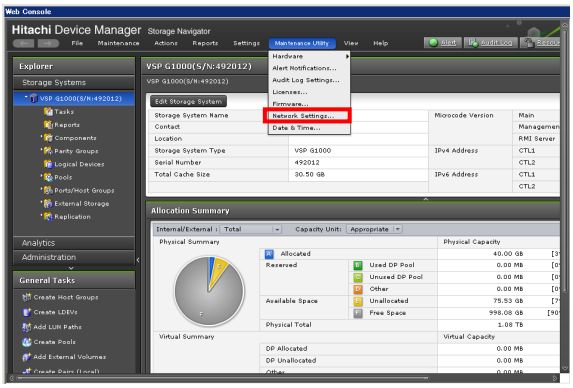
3.6 Network Setting

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.

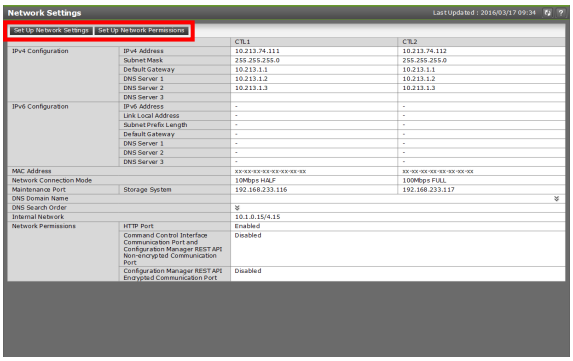
NOTICE:	If the DNS servers, the DNS domain name and the domain search order are set by NAS Manager, the set contents are also reflected in the Storage System.

3.6.1 Network Setting

1. Starting “Network setting” window
   (1) When starting Maintenance Utility from the browser
      (a) Refer to “1.8.2.3 Starting the Browser” to start Maintenance Utility.
      (b) In the “Maintenance Utility” window, select [Administration] - [Network setting].
   (2) When starting Maintenance Utility from Web Console
      (a) Start the Web Console referring to “1.6 Connecting to the Storage System”.
      (b) In the “Web Console” window, select [Maintenance Utility] - [Network setting...]. The current installed firmware version is displayed.



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.



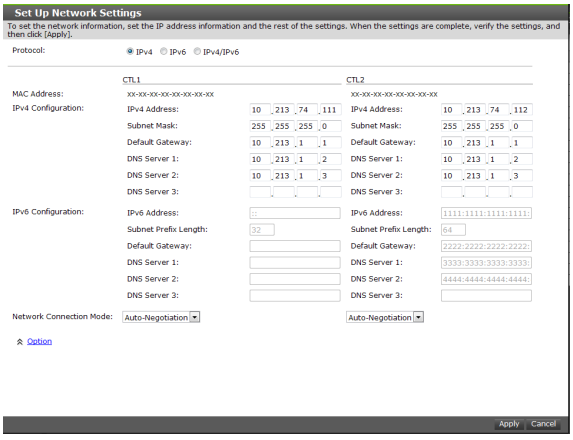
Copyright © 2015, 2017, Hitachi, Ltd.

3. Advanced setting of network

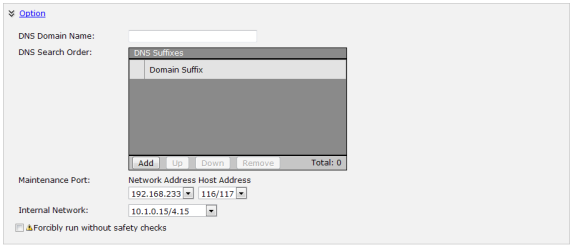
⚠ CAUTION

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.

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



Clicking Option displays the following window.



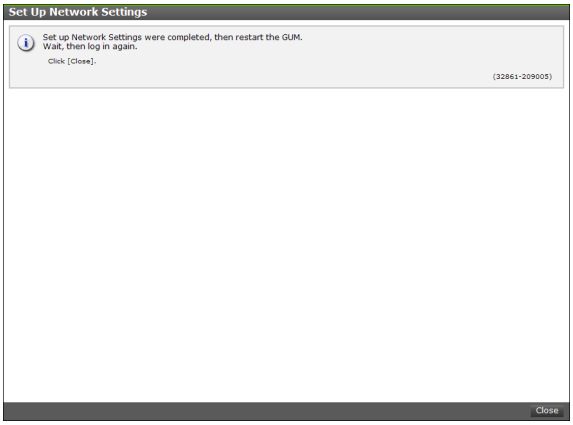
Copyright © 2015, 2017, Hitachi, Ltd.

Item		Input Description
Protocol		Selects the network protocol. • [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. • 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. • 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. • 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. (*1)

Copyright © 2015, 2017, Hitachi, Ltd.

*1: When adding NAS modules, change the internal network from the global IP address (126.255.... or 192.169....) to the private IP address (other than the above global IP address. The recommended default is 10.251....). See "13.1 IP Addresses of Maintenance Ports and Internal Network" for the details.

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 "1.6.5 Changing Storage System Information and Updating Software of Web Console" for the detail.

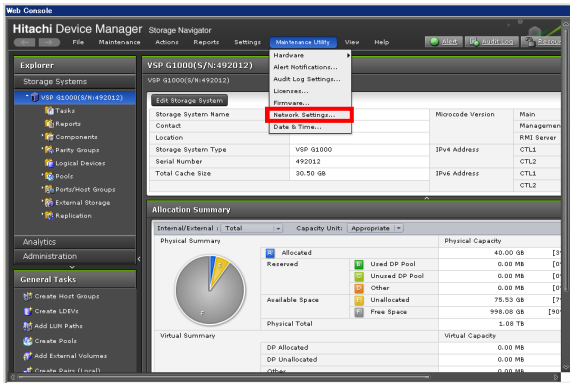
NOTE: If you change the IP address of the Maintenance PC before changing the IP address of Storage Device List, you cannot edit the setting of Storage Device List.

7. When changing the IP address of the maintenance port, change the IP address of the Maintenance PC.
Refer to "1.3.1 IP Address Setting Method of Maintenance PC" for the detail.

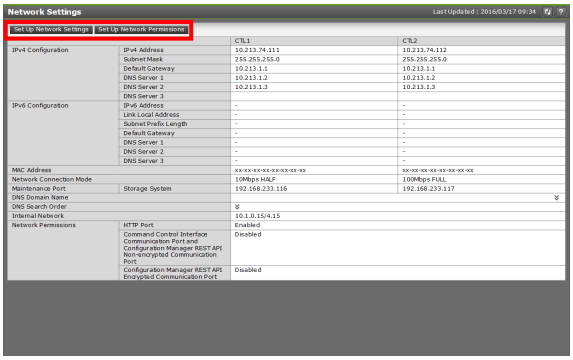
Copyright © 2015, 2017, Hitachi, Ltd.

3.6.2 Network Permissions

1. Starting “Network setting” window
   (1) When starting Maintenance Utility from the browser
      (a) Refer to “1.8.2.3 Starting the Browser” to start Maintenance Utility.
      (b) In the “Maintenance Utility” window, select [Administration] - [Network setting].
   (2) When starting Maintenance Utility from Web Console
      (a) Start the Web Console referring to “1.6 Connecting to the Storage System”.
      (b) In the “Web Console” window, select [Maintenance Utility] - [Network setting...]. The current installed firmware version is displayed.

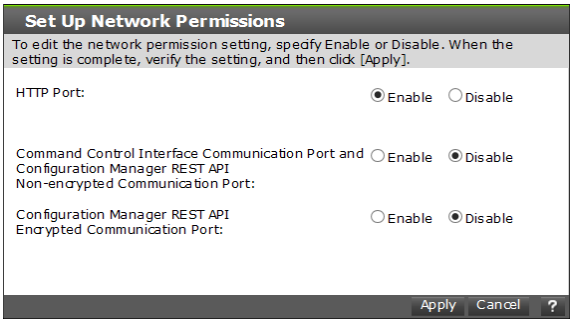


2. Network setting
   - Click the [Set Up Network Settings] button for setting the network detail. Go to “3.6.1 Network Setting” Step 3.
   - Click the [Set Up Network Permissions] button for setting the network permission. Go to Step 3.



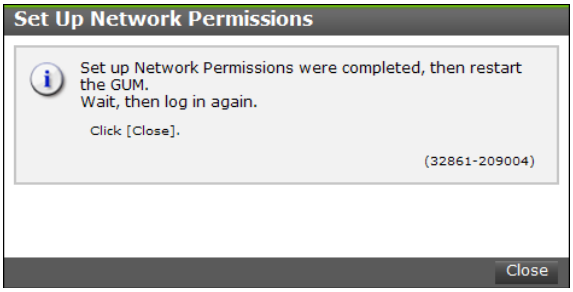
Copyright © 2015, 2017, Hitachi, Ltd.

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 Configuration Manager REST API Non-encrypted Communication Port	Enable	Enable the Command Control Interface Communication Port and Configuration Manager REST API Non-encrypted Communication Port.
	Disable	Disable the Command Control Interface Communication Port and Configuration Manager REST API Non-encrypted Communication Port.
Configuration Manager REST API Encrypted Communication Port	Enable	Enable the Configuration Manager REST API Encrypted Communication Port.
	Disable	Disable the Configuration Manager REST API Encrypted Communication Port.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

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.

NOTICE: The program product can be installed by NAS Manager. Although NAS Manager supports the installation by the license key file, it does not support the program product installation by entering the license key.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

3.7.2 Software Packaging

1. VSP G200, G400, G600, G800
   The following table shows the software included for each software bundle.

Software bundle	Software
Hitachi Storage Virtualization Operating System (SVOS)	Open Volume Management
	LUN Manager (*1)
	Performance Monitor
	Server Priority Manager (*2)
	HDvM/Device Manager - Storage Navigator
	SNMP Agent
	Data Retention Utility
	Volume Shredder
	JAVA API
	SMI-S Provider
	Dynamic Provisioning (*3)
	Universal Volume Manager
	Virtual Partition Manager
	Resource Partition Manager
Hitachi Remote Replication	TrueCopy (*4)
	Universal Replicator (*5)
Hitachi Local Replication	ShadowImage (*4)
	Thin Image (*6)
Hitachi Data Mobility	Dynamic Tiering (*7)
	Volume Migration V2
	active flash (*8)
Hitachi Encryption Key (*9)	Encryption License Key
Hitachi Remote Replication Extended (*12)	Remote Replication Extended (*10) (*12)
nondisruptive migration	nondisruptive migration
global-active device	global-active device (*11)
—	dedupe and compression

*1: Includes LUN security function
*2: To use Server Priority Manager, you need to install the Performance Monitor.
*3: For VSP G400, VSP G600, and VSP G800, you need to estimate the total pool capacity.
*4: For VSP G800, you need to estimate the normal volume. If you are using Dynamic Provisioning or Dynamic Tiering or active flash V-VOL for P-VOL or S-VOL, license capacity is calculated by using the capacity of pages allocated to the V-VOL (capacity which the pool uses).
*5: To use Universal Replicator, you need to install TrueCopy. For VSP G800, you need to estimate the normal volume. For the normal volume, if you are using Dynamic Provisioning or Dynamic Tiering or active flash V-VOL for P-VOL or S-VOL, license capacity is calculated by using the capacity of pages allocated to the V-VOL (capacity which the pool uses).
*6: To use Thin Image, you need to install Dynamic Provisioning. For VSP G800, you need to estimate the combined capacity of normal volume and total pool capacity. For the normal volume, if you are using Dynamic Provisioning or Dynamic Tiering or active flash V-VOL for P-VOL or S-VOL, license capacity is calculated by using the capacity of pages allocated to the V-VOL (capacity which the pool uses).

Copyright © 2015, 2017, Hitachi, Ltd.

*7: To use Dynamic Tiering, you need to install Dynamic Provisioning. For VSP G800 you need to estimate the total pool capacity.
*8: To use active flash, you need to install Dynamic Provisioning and Dynamic Tiering. For VSP G800 you need to estimate the total pool capacity.
*9: Supported for VSP G400, VSP G600, and VSP G800. Supported for VSP G200 in the firmware version 83-03-01-x0/xx or later.
*10: The installation of Universal Replicator is also necessary to use Remote Replication Extended.
*11: For the normal volume, if you are using Dynamic Provisioning or Dynamic Tiering or active flash V-VOL for P-VOL or S-VOL, license capacity is calculated by using the capacity of pages allocated to the V-VOL (capacity which the pool uses).
*12: The name of "Hitachi Disaster Recovery Extended" or "Disaster Recovery Extended" are applied when the firmware version is less than 83-03-21-x0/xx.

NOTICE:	Before using Volume Migration, contact Hitachi Data Systems customer support.

NOTICE:	A model upgrade license is required when upgrading from VSP G400 to VSP G600.

NOTICE:	All Flash Array is the license key required for VSP F400, VSP F600 and VSP F800.

NOTICE:	If you purchase Virtual Storage Platform G200 or Virtual Storage Platform G600, Model upgrade license is already installed.

NOTICE:	"dedupe and compression" is the license required for using the Capacity Saving function. To use "dedupe and compression", you need to install Dynamic Provisioning.

Copyright © 2015, 2017, Hitachi, Ltd.

2. VSP F400, F600, F800
   The following table shows the software included for each software bundle.

Software bundle	Software
Hitachi Storage Virtualization Operating System (SVOS)	Open Volume Management
	LUN Manager (*1)
	Performance Monitor
	Server Priority Manager (*2)
	HDvM/Storage Navigator
	SNMP Agent
	Data Retention Utility
	JAVA API
	Dynamic Provisioning (*3)
	SMI-S Provider
	Resource Partition Manager
	ShadowImage (*4)
	Thin Image (*6)
Hitachi Remote Replication	TrueCopy (*4)
	Universal Replicator (*5)
Hitachi Encryption Key	Encryption License Key
Hitachi Remote Replication Extended (*8)	Remote Replication Extended (*7) (*8)
global-active device	global-active device (*9)(*10)

*1: Includes LUN security function
*2: To use Server Priority Manager, you need to install the Performance Monitor.
*3: For VSP F400, VSP F600, and VSP F800, you need to estimate the total pool capacity.
*4: For VSP F800, you need to estimate the normal volume. If you are using Dynamic Provisioning V-VOL for P-VOL or S-VOL, license capacity is calculated by using the capacity of pages allocated to the V-VOL (capacity which the pool uses).
*5: To use Universal Replicator, you need to install TrueCopy. For VSP F800, you need to estimate the normal volume. For the normal volume, if you are using Dynamic Provisioning V-VOL for P-VOL or S-VOL, license capacity is calculated by using the capacity of pages allocated to the V-VOL (capacity which the pool uses).
*6: To use Thin Image, you need to install Dynamic Provisioning. For VSP F800, you need to estimate the combined capacity of normal volume and total pool capacity. For the normal volume, if you are using Dynamic Provisioning V-VOL for P-VOL or S-VOL, license capacity is calculated by using the capacity of pages allocated to the V-VOL (capacity which the pool uses).
*7: To use Remote Replication Extended, you need to install Universal Replicator.
*8: The name of “Hitachi Disaster Recovery Extended” or “Disaster Recovery Extended” are applied when the firmware version is less than 83-03-21-x0/xx.
*9: When the firmware version is 83-04-20-x0/xx or later.
*10: For the normal volume, if you are using Dynamic Provisioning V-VOL for P-VOL or S-VOL, license capacity is calculated by using the capacity of pages allocated to the V-VOL (capacity which the pool uses).

Copyright © 2015, 2017, Hitachi, Ltd.

NOTICE:
- All Flash Array is the license key required for VSP F400, VSP F600 and VSP F800.
- If you purchase Virtual Storage Platform F600, Model upgrade license is already installed.

NOTICE: "dedupe and compression" is the license required for using the Capacity Saving function.
To use "dedupe and compression", you need to install Dynamic Provisioning.

Copyright © 2015, 2017, Hitachi, Ltd.

3.7.3 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.
Based on what licensed capacity is calculated differs depending on program products.

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

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

Copyright © 2015, 2017, Hitachi, Ltd.

The following table lists the software and licensed capacity.

1. VSP G200, G400, G600, G800

Software bundle	Licensed capacity		
	VSP G200	VSP G400/VSP G600	VSP G800
Hitachi Storage Virtualization Operating System (SVOS)	Unlimited capacity	Implementation capacity	Implementation capacity
Hitachi Remote Replication	Unlimited capacity	Implementation capacity	Used capacity
Hitachi Local Replication	Unlimited capacity	Implementation capacity	Used capacity
Hitachi Command Suite Data Mobility	Unlimited capacity	Implementation capacity	Used capacity
Hitachi Encryption Key	Unlimited capacity (*1)	Unlimited capacity	Unlimited capacity
Hitachi Remote Replication Extended (*2)	Unlimited capacity	Unlimited capacity	Unlimited capacity
nondisruptive migration	Unlimited capacity	Unlimited capacity	Unlimited capacity
global-active device	Unlimited capacity	Implementation capacity	Used capacity
dedupe and compression	Unlimited capacity	Unlimited capacity	Unlimited capacity
All Flash Array	Unlimited capacity	Unlimited capacity	Unlimited capacity

*1: When the firmware version is 83-03-01-x0/xx or later.
*2: The name of “Hitachi Disaster Recovery Extended” is applied when the firmware version is less than 83-03-21-x0/xx.

2. VSP F400, F600, F800

Software bundle	Licensed capacity
Hitachi Storage Virtualization Operating System (SVOS)	Unlimited capacity
Hitachi Remote Replication	Unlimited capacity
Hitachi Encryption Key	Unlimited capacity
Hitachi Remote Replication Extended (*1)	Unlimited capacity
Hitachi Performance Analytics	Unlimited capacity
Hitachi Volume Migration	Unlimited capacity
global-active device (*2)	VSP F400, F600, F800: Implementation capacity

*1: The name of “Hitachi Disaster Recovery Extended” is applied when the firmware version is less than 83-03-21-x0/xx.
*2: When the firmware version is 83-04-20-x0/xx or later.

Copyright © 2015, 2017, Hitachi, Ltd.

3.7.4 Calculating Licensed Capacity

After checking the licensed capacity applied to the program product, calculate the licensed key.

NOTE: When you calculate the volume capacity, round the value up to the second decimal place.

3.7.4.1 Calculating Capacity for a Normal Volume (LDEV)

You can calculate the licensed capacity for a normal volume by volume capacity and the number of volumes. For example, when volume capacity is 60 GB and the number of volumes is 512, the licensed capacity is at least 30 TB.

Item	Value
Volume emulation type	OPEN-V
Volume capacity (GB)	60
Number of volumes	512
Total capacity of all the volumes	60 GB × 512 = 30,720 GB 30,720 GB / 1,024 = 30 TB
Licensed capacity	At least 30 TB

3.7.4.2 Calculating Licensed Capacity for an External Volume Mapped to the Storage System

Use the following equation to calculate the licensed capacity for an external volume:
External Volume Capacity (KB) = Volume Capacity (number of blocks) × 512 (bytes) / 1,024

3.7.4.3 Calculating Pool Capacity

- The licensed capacity of Dynamic Provisioning is calculated using the total capacity of the Dynamic Provisioning pool.
- If you use Dynamic Provisioning V-VOLs as P-VOLs or S-VOLs of ShadowImage/TrueCopy/Universal Replicator, the license capacity of ShadowImage/TrueCopy/Universal Replicator is calculated using the page capacity allocated to the Dynamic Provisioning V-VOLs (that is, used pool capacity).

For more information on calculating pool capacity, refer to the “Provisioning Guide”.

3.7.4.4 Implementation Capacity of the Parity Group whose Accelerated Compression Setting is Enabled

For the implementation capacity of the parity groups whose Accelerated Compression setting is enabled, compare between the total capacity of the LDEVs created in the parity group and the physical capacity, and then add the lower capacity of the two.

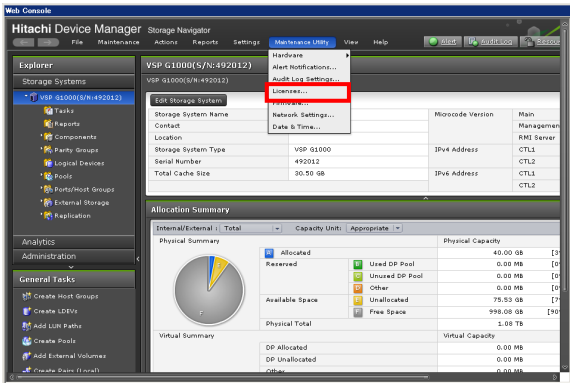
Total capacity of LDEVs in the parity group	Physical capacity	Implementation capacity to be added
12 TB	20 TB	12 TB
24 TB	20 TB	20 TB

Copyright © 2015, 2017, Hitachi, Ltd.

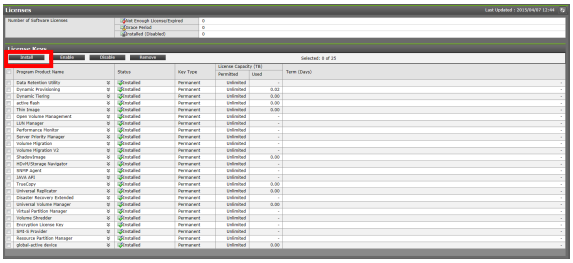
3.7.5 Installing Software Using a License Key Code

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

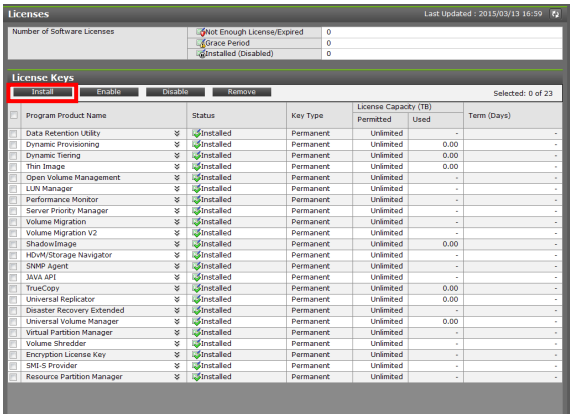
1. Starting “Licenses” window
   (1) When starting Maintenance Utility from the browser
      (a) Refer to “1.8.2.3 Starting the Browser” to start Maintenance Utility.
      (b) In the “Maintenance Utility” window, select [Administration] - [Licenses].
   (2) When starting Maintenance Utility from Web Console
      (a) Start the Web Console referring to “1.6 Connecting to the Storage System”.
      (b) In the “Web Console” window, select [Maintenance Utility] - [Licenses...]. The current installed firmware version is displayed.



2. The “Licenses” window is displayed. Click the [Install] button.
   [When the Firmware version is 83-01-21-x0/xx or more]



   [When the Firmware version is less than 83-01-21-x0/xx]



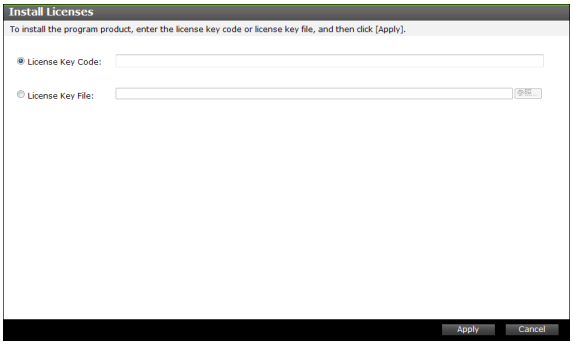
Copyright © 2015, 2017, Hitachi, Ltd.

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

Copyright © 2015, 2017, Hitachi, Ltd.

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

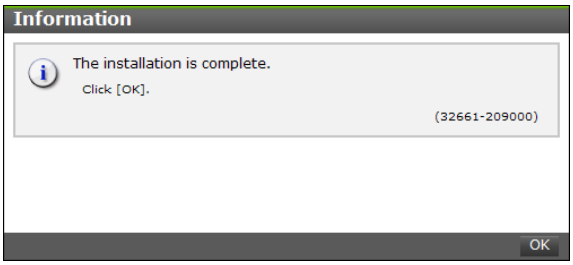
4. Click the [Apply] button.



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 license key file name can be up to 200 alphanumeric characters but cannot include the following symbols: " \ ; : , * ? < > | / . 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.

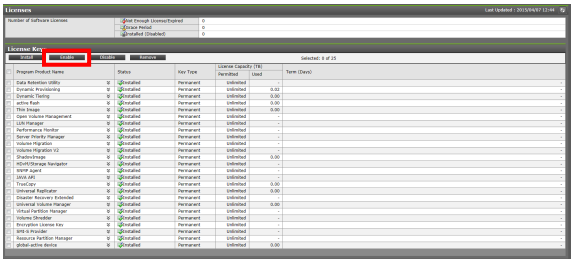
Copyright © 2015, 2017, Hitachi, Ltd.

3.7.6 Enabling a License

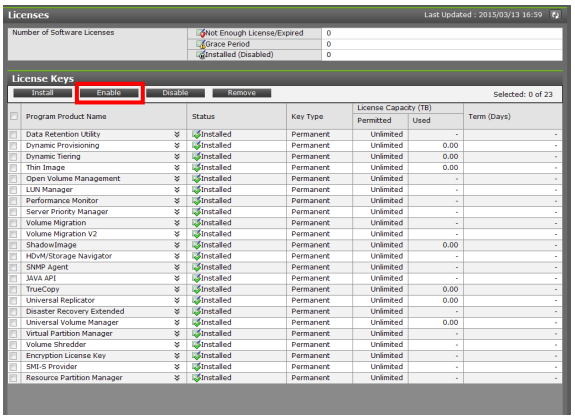
You can enable a license that is in the disabled status.

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

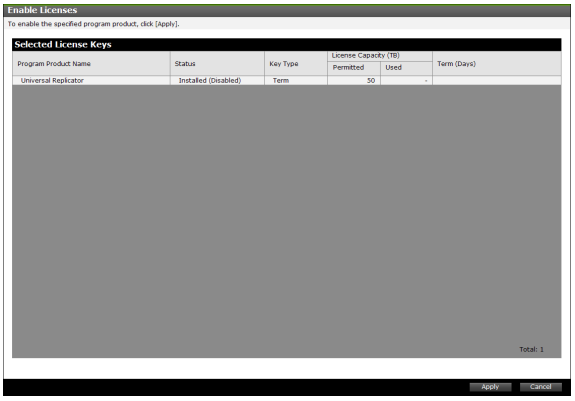
2. Click the [Enable] button in the “License Keys” window.
   [When the Firmware version is 83-01-21-x0/xx or more]



   [When the Firmware version is less than 83-01-21-x0/xx]

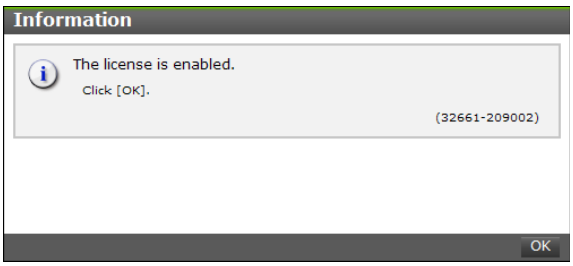


3. Confirm the settings. Click the [Apply] button.



Copyright © 2015, 2017, Hitachi, Ltd.

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



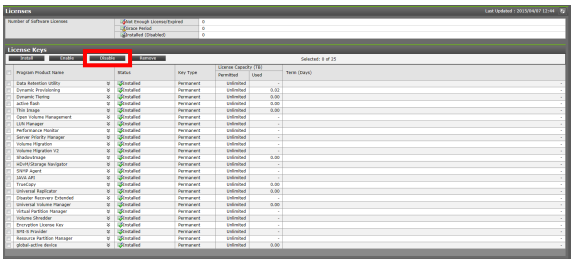
Copyright © 2015, 2017, Hitachi, Ltd.

3.7.7 Disabling a License

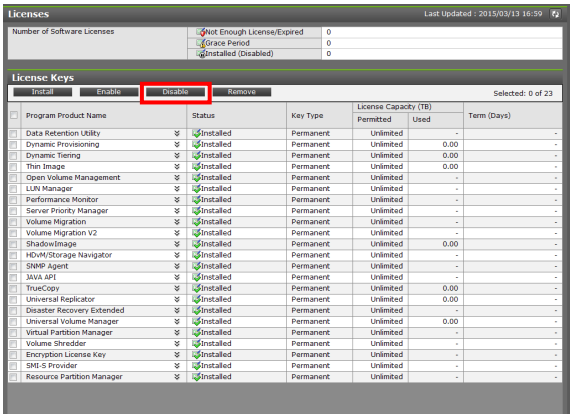
You can disable a license that is in the enabled status.

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

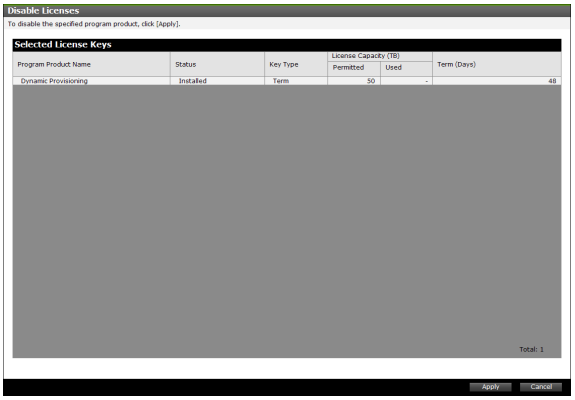
2. Click the [Disable] button in the “License Keys” window.
   [When the Firmware version is 83-01-21-x0/xx or more]



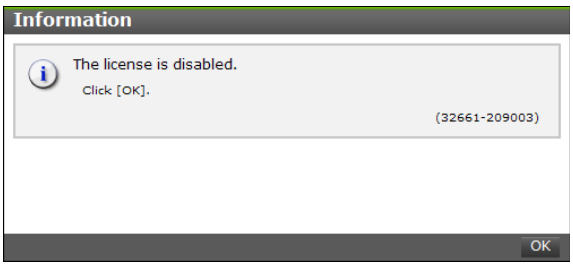
   [When the Firmware version is less than 83-01-21-x0/xx]



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



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



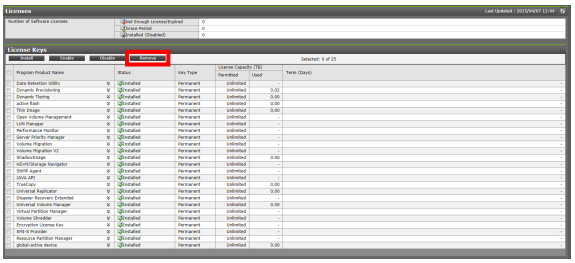
Copyright © 2015, 2017, Hitachi, Ltd.

3.7.8 Removing Program Product

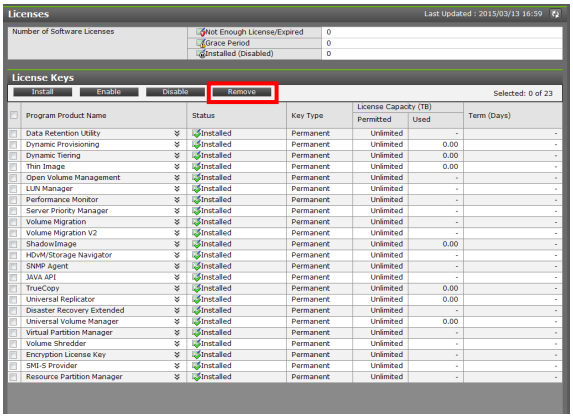
The following procedure describes to remove the program product.

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

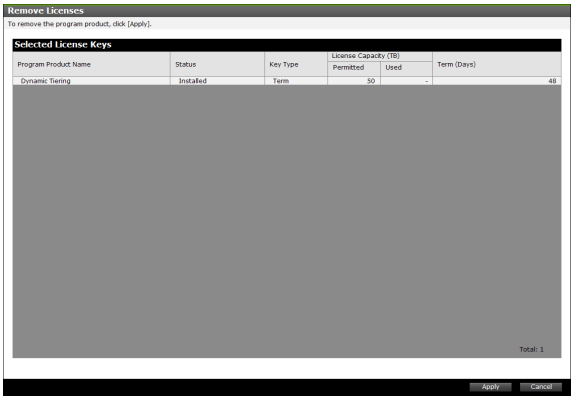
2. Click the [Remove] button in the “License Keys” window.
   [When the Firmware version is 83-01-21-x0/xx or more]



   [When the Firmware version is less than 83-01-21-x0/xx]

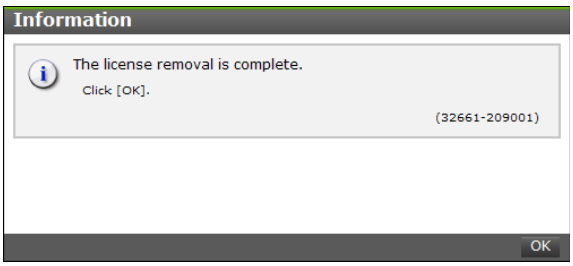


3. Confirm the settings. Click the [Apply] button.



Copyright © 2015, 2017, Hitachi, Ltd.

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

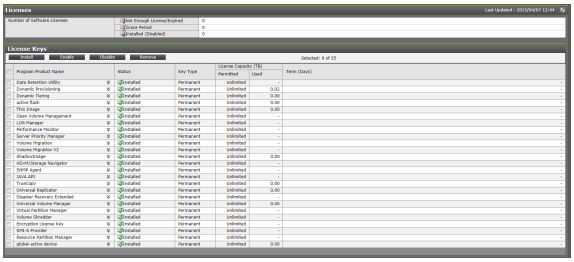


Copyright © 2015, 2017, Hitachi, Ltd.

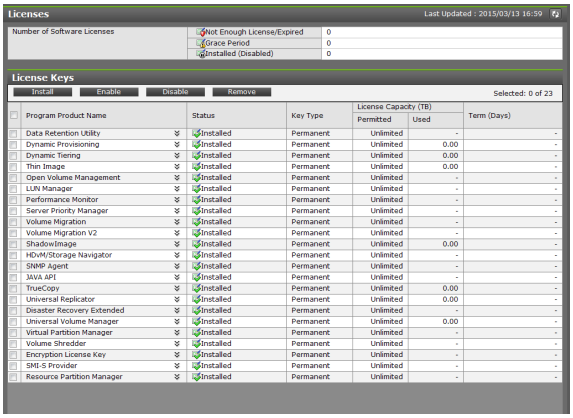
3.7.9 Verifying License

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

[When the Firmware version is 83-01-21-x0/xx or more]



[When the Firmware version is less than 83-01-21-x0/xx]



Copyright © 2015, 2017, Hitachi, Ltd.

3.7.9.1 Examples of the displayed window

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

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

Copyright © 2015, 2017, Hitachi, Ltd.

3.7.10 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.

Copyright © 2015, 2017, Hitachi, Ltd.

3.7.11 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.

Copyright © 2015, 2017, Hitachi, Ltd.

3.7.12 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”.

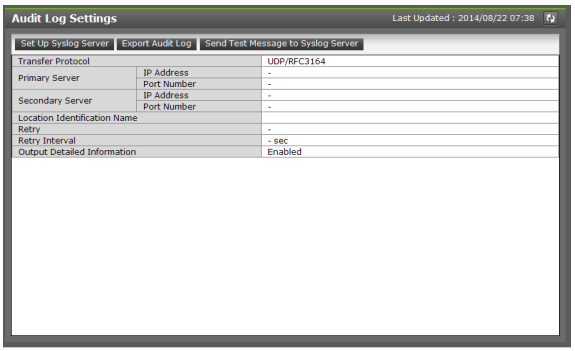
Copyright © 2015, 2017, Hitachi, Ltd.

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. • 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. • [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/ RFCS5424) is selected at Transfer Protocol.
Retry Interval	Displays the Retry interval. Displays this item only when New Syslog Protocol (TLS1.2/RFCS5424) is selected at Transfer Protocol and Retry is Enabled.
Output Detailed Information	Displays the output detailed information setting. • [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.

Copyright © 2015, 2017, Hitachi, Ltd.

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

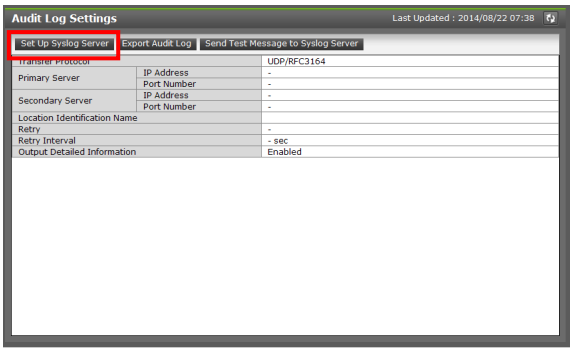
- You must have Audit Log Administrator (View & Modify) role to configure Syslog server settings.
- Make sure the storage system is connected to Syslog servers on a LAN.
- Make sure the Syslog servers are configured so as to transfer audit logs to the Syslog servers.
- The Syslog server certificate and 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

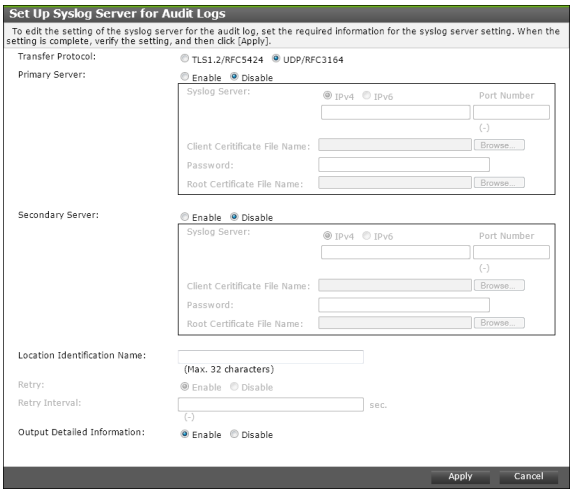
1. In the “Maintenance Utility” window, select [Administration] - [Audit Log Settings].

2. Click [Set Up Syslog Server] in the “Audit Log Settings” window.



Copyright © 2015, 2017, Hitachi, Ltd.

3. Set up the Syslog server settings.



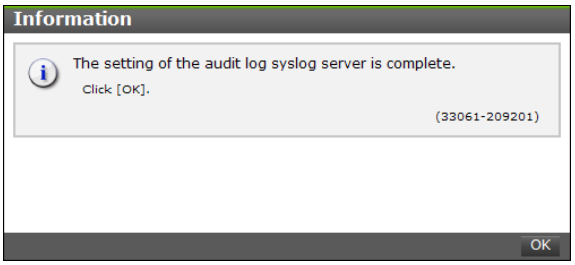
Item	Description
Transfer Protocol	Selects a protocol to transfer the audit log. • New Syslog Protocol (TLS1.2/RFC5424) • Old Syslog Protocol (UDP/RFC3164)
Primary Server	Selects whether to use the Syslog server. • [Enable] : Transfers the audit log to the Syslog server. • [Disable] : Do not transfer the audit log to the Syslog server.
Primary Server-Syslog Server	Specifies an IP address of a server you want to set as a Syslog server. • 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	Enters a port number to be used at the Syslog server.
Primary Server-Client Certificate File Name	Specifies a certificate file. Click Browse, and then specify a certificate file. This item is settable only when [TLS1.2/RFC5424] is selected at [Transfer Protocol]. • 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	Specifies a password for the client certificate. Up to 128 characters can be entered for the password. Allowed characters are alphanumeric characters and symbols: ! # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~. Specifies this item only when Client Certificate File Name is specified.

Copyright © 2015, 2017, Hitachi, Ltd.

Item	Description
Primary Server-Root Certificate File Name	Specifies a certificate file. Click Browse, and then specify a certificate file. This item is settable only when [TLS1.2/RFC5424] is selected at [Transfer Protocol]. • Be sure to set it when changing the items of the certificate from inactive to active. • After applying the setting, if the certificate is not set (blank) when applying the setting again, the previously updated certificate is used.
Secondary Server	Selects whether to use an alternative server (secondary server) to the Syslog server. • [Enable] : Transfers the audit log to the secondary server. • [Disable] : Does not transfer the audit log to the secondary server.
Secondary Server-Syslog Server	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.
Secondary Server-Port Number	Specifies a port number to be used on the secondary server.
Secondary Server-Client Certificate File Name	Specifies a certificate file. Click Browse, and then specify a certificate file. This item is settable only when [TLS1.2/RFC5424] is selected at [Transfer Protocol]. • Be sure to set it when changing the items of the certificate from inactive to active. • After applying the setting, if the certificate is not set (blank) when applying the setting again, the previously updated certificate is used.
Secondary Server-Password	Specifies a password for the client certificate. Up to 128 characters password can be entered. The restriction for the available values is the same as that of Primary Server-Server Setting.
Secondary Server-Root Certificate File Name	Specifies a certificate file. Click Browse, and then specify a certificate file. This item is settable only when [TLS1.2/RFC5424] is selected at [Transfer Protocol]. • 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 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].
Retry	Selects whether to retry when the connection to the Syslog server fails. • [Enable] : Retry when the connection to the Syslog server fails. • [Disable] : Does not retry when the connection to the Syslog server fails. Specifies this item only when New Syslog Protocol (TLS1.2/ RFCS5424) is selected at Transfer Protocol.
Retry Interval	Specifies the retry interval when the communication with the Syslog server fails in the range of 1 to 60 seconds. The default is 1 second. Specifies this item only when New Syslog Protocol (TLS1.2/ RFCS5424) is selected at Transfer Protocol.
Output Detailed Information	Selects whether to transfer the detailed information of the audit log to the Syslog server. • [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.

Copyright © 2015, 2017, Hitachi, Ltd.

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
     (Specy this item only when New Syslog Protocol (TLS1.2/ RFCS5424) 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/ RFCS5424) 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/ RFCS5424) 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.



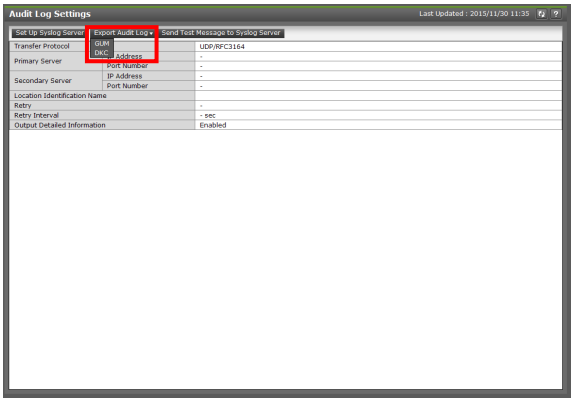
Copyright © 2015, 2017, Hitachi, Ltd.

3.8.3 Exporting Audit Log

3.8.3.1 Exporting Audit Log (Maintenance Utility)

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. If [GUM] or [DKC] is selected, another white window is displayed. If the certificate is invalid at the time of the https connection, the security confirmation window is displayed.
   If the security confirmation window is displayed, select "Continue to this website (not recommended)".
   Do not close the white window or the security confirmation window until the download is completed.

4. 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.

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

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

Copyright © 2015, 2017, Hitachi, Ltd.

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. • The time of downloading files depends on the network speed.

8. Confirm the completion of the download.

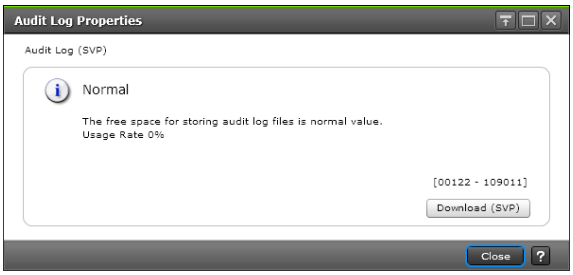
NOTICE:	Close the white window or the security confirmation window manually.

Copyright © 2015, 2017, Hitachi, Ltd.

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: • 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.

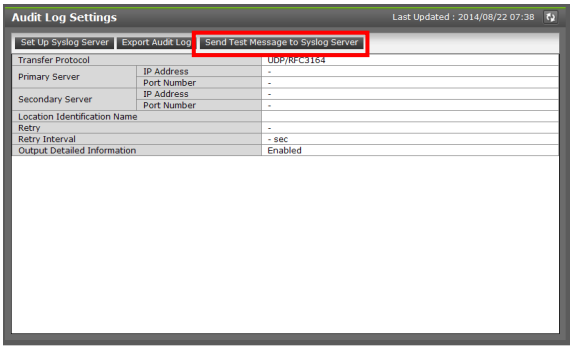
6. Click the [Close] button.

Copyright © 2015, 2017, Hitachi, Ltd.

3.8.4 Sending a Test Message to the Syslog Server

1. In the "Maintenance Utility" window, select [Administration] - [Audit Log Settings].

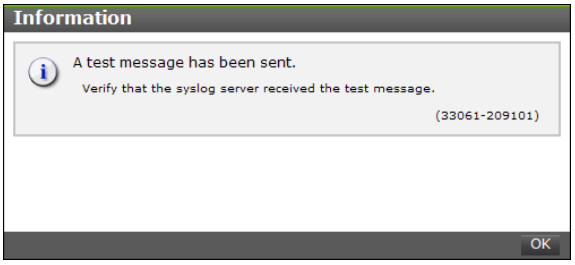
2. Click [Send Test Message to Syslog Server] in the "Audit Log Settings" window.



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.



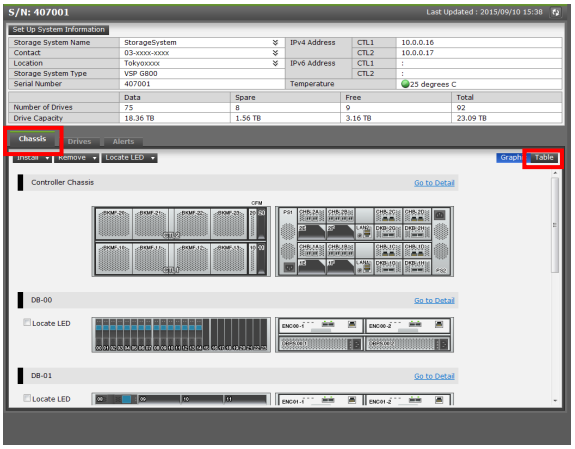
Copyright © 2015, 2017, Hitachi, Ltd.

3.9 Turn on/off Locate LEDs

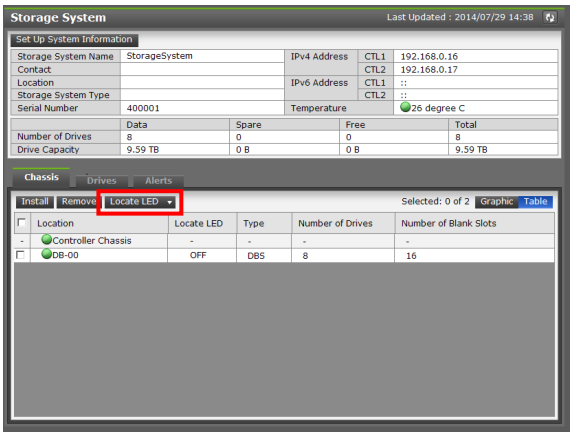
This is a window to turn on/off the LEDs located on the front and rear of the Drive Box.

3.9.1 Trun on Locate LED

1. Table display of Drive Box
   Select the [Table] switch from the [Chassis] tab in the main window.

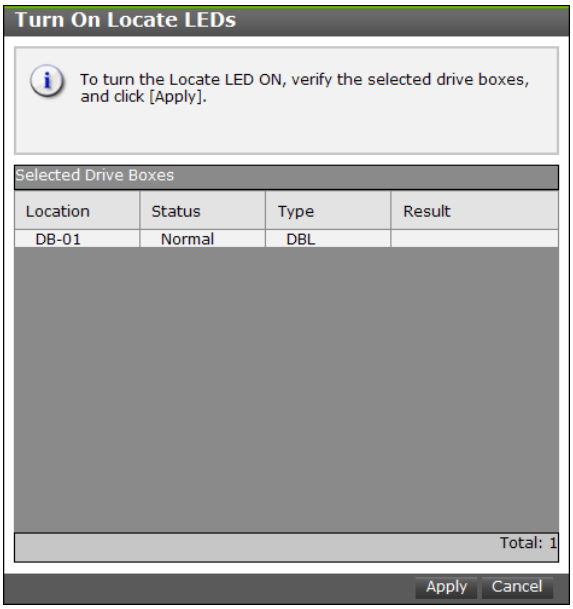


2. Select (multiple) DBs from the list
   Select a DB to change and select [Turn on] from the [Locate LED] menu. (Multiple selection possible)

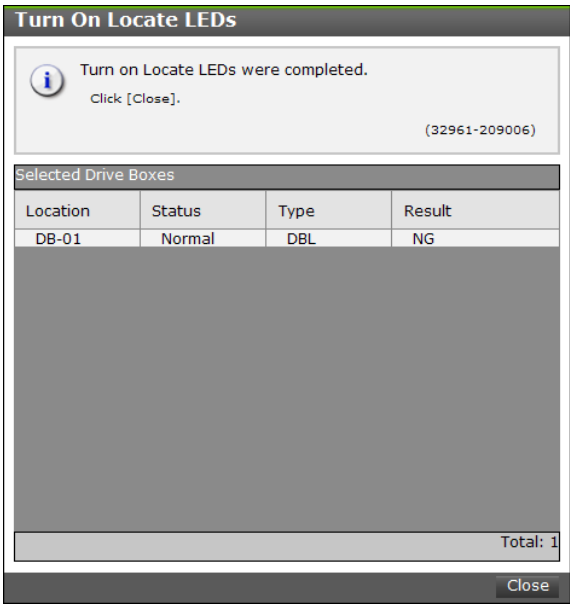


Copyright © 2015, 2017, Hitachi, Ltd.

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



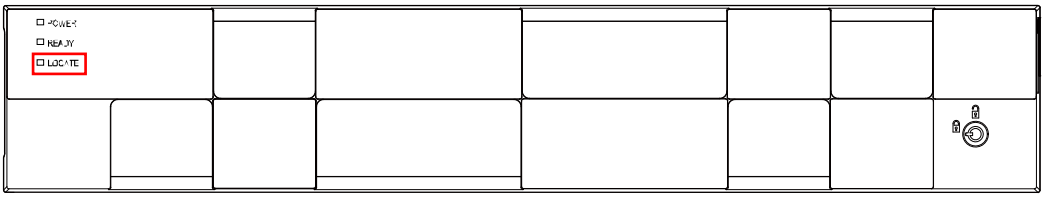
4. A message is displayed. Click the [Close] button.



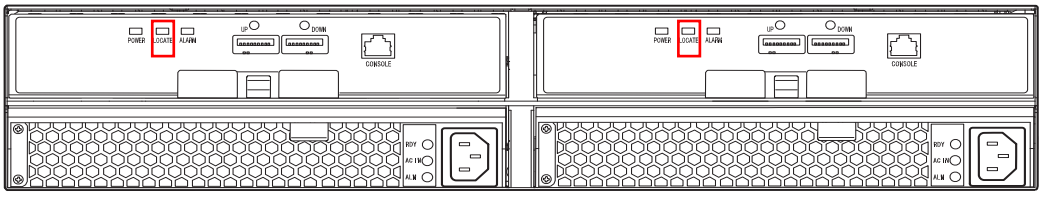
Copyright © 2015, 2017, Hitachi, Ltd.

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

DBS/DBL

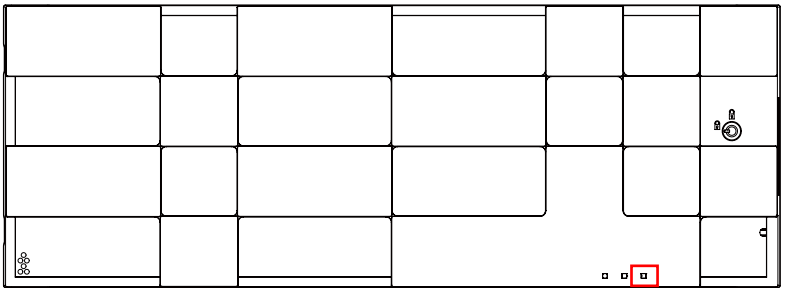


DBL/DBS Front Bezel

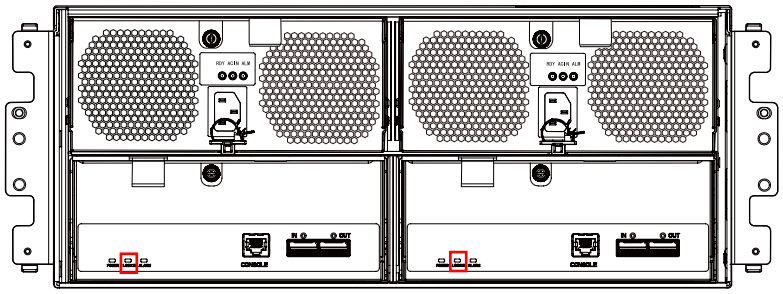


Rear view of DBS/DBL

DB60



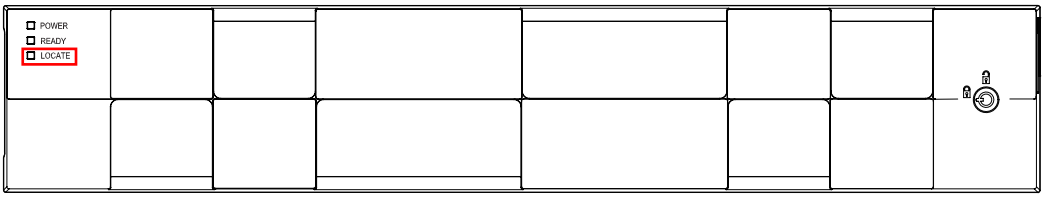
Front view of DB60



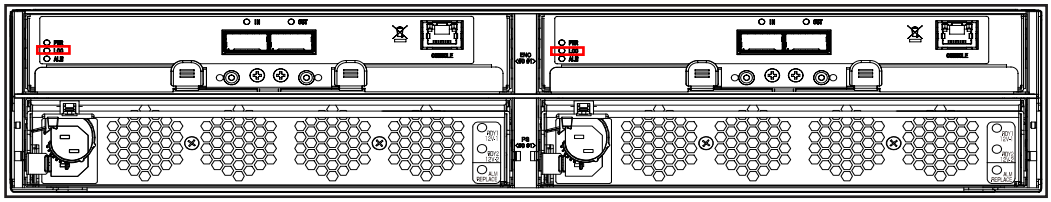
Rear view of DB60

Copyright © 2015, 2017, Hitachi, Ltd.

DBF



DBF Front Bezel

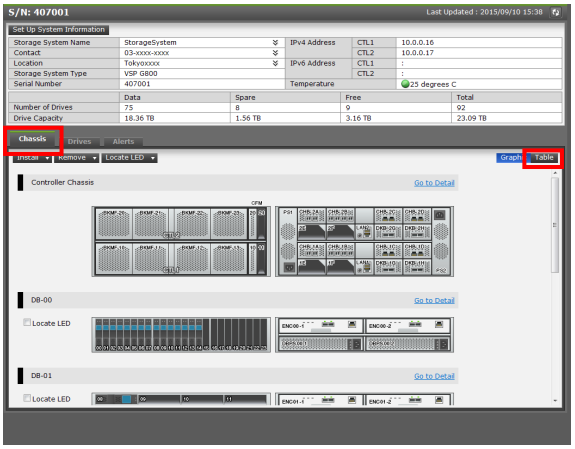


Rear view of DBF

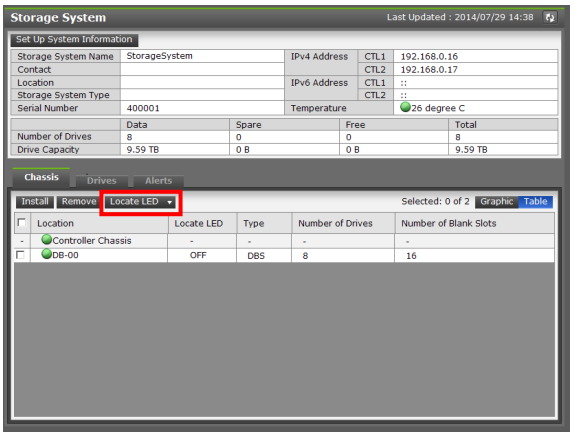
Copyright © 2015, 2017, Hitachi, Ltd.

3.9.2 Trun off Locate LED

1. Table display of Drive Box
   Select the [Table] switch from the [Chassis] tab in the main window.

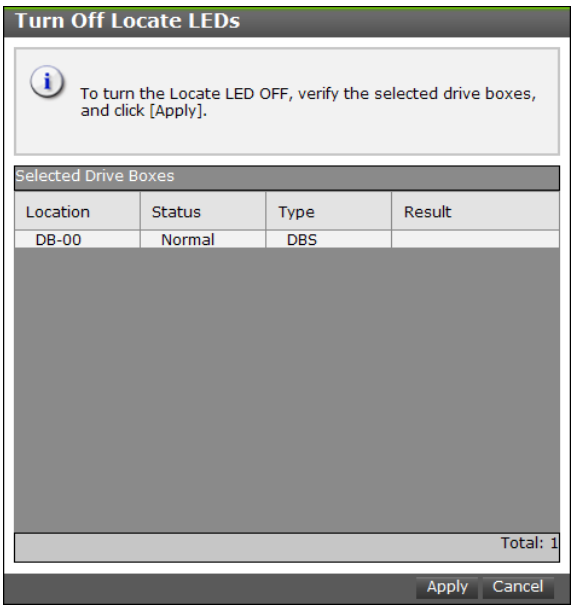


2. Select (multiple) DBs from the list
   Select a DB to change and select [Turn off] from the [Locate LED] menu. (Multiple selection possible)

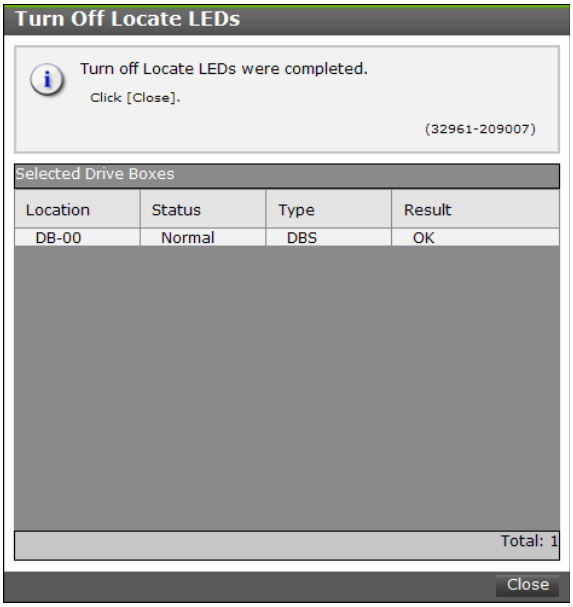


Copyright © 2015, 2017, Hitachi, Ltd.

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



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



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

Copyright © 2015, 2017, Hitachi, Ltd.

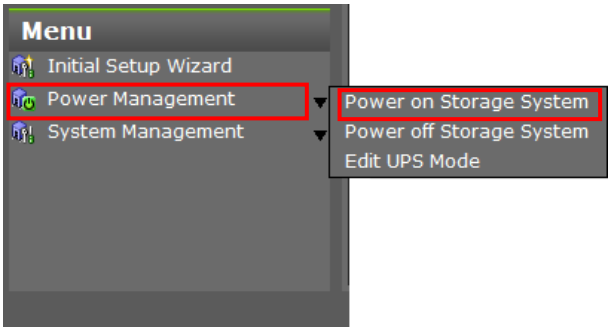
3.10 Power on Storage System

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

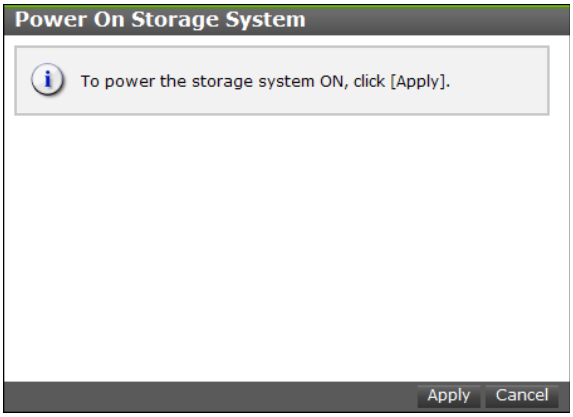
NOTE: If you turn off the Storage System by the main switch, you cannot turn on the Storage System from the power management menu.

1. Operation menu panel
   Select [Power on Storage System] from [Power Management].

   NOTE: The location number is displayed in the “Maintenance Utility” window for the firmware version 83-01-21-x0/xx or more.

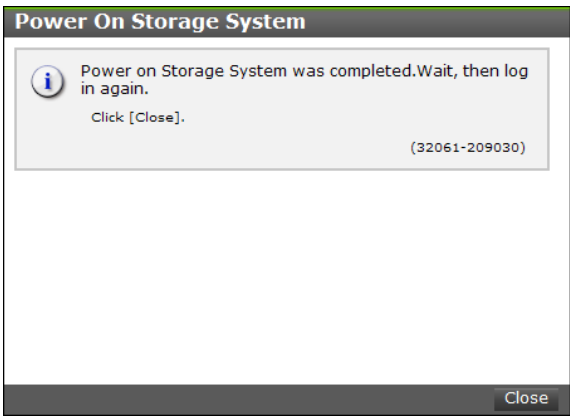


2. Click the [Apply] button.



Copyright © 2015, 2017, Hitachi, Ltd.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

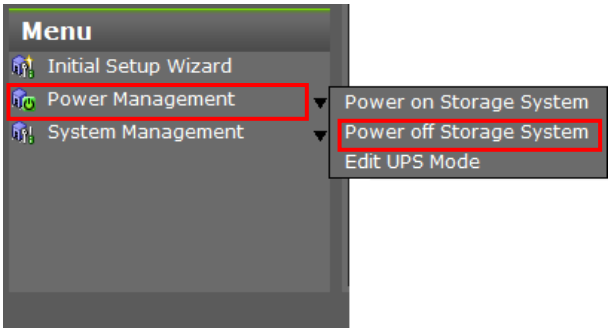
3.11 Power off Storage System

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].

   NOTE: The location number is displayed in the “Maintenance Utility” window for the firmware version 83-01-21-x0/xx or more.



2. Click the [Apply] button.



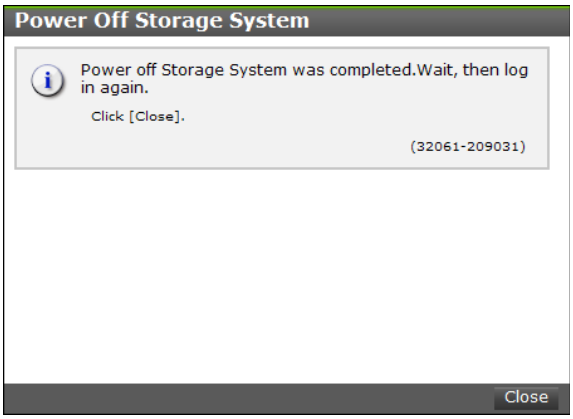
Copyright © 2015, 2017, Hitachi, Ltd.

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 password and 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.



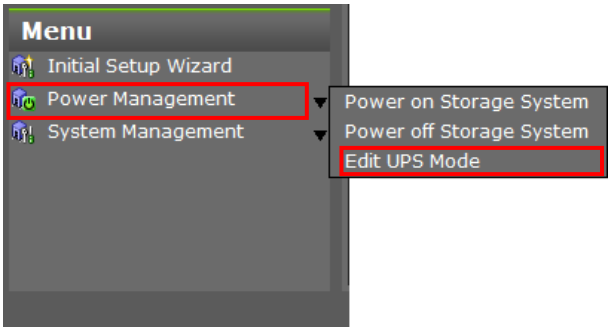
Copyright © 2015, 2017, Hitachi, Ltd.

3.12 Edit UPS Mode

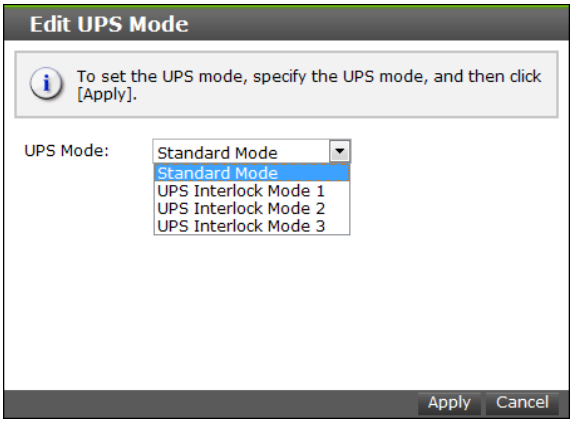
This is a window to change the UPS mode (UPS connection setting).

1. Operation menu panel
   Select [Edit UPS Mode] from [Power Management].

   NOTE: The location number is displayed in the “Maintenance Utility” window for the firmware version 83-01-21-x0/xx or more.



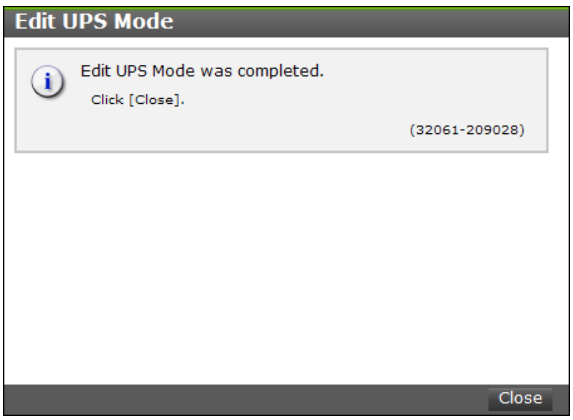
2. Select [UPS Interlock Mode] from the [UPS Mode] pull-down menu and click the [Apply] button.



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.

Copyright © 2015, 2017, Hitachi, Ltd.

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.)

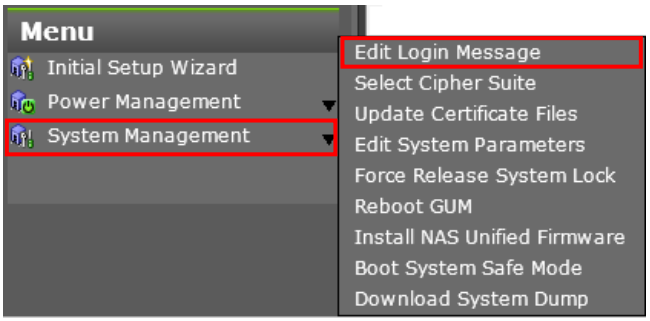
(1) Turn off the main switch.
Check that the READY LED (green) goes out.
(2) Remove two power cables from the Controller Chassis.
(3) After waiting for about 30 seconds, install two power cables in the Controller Chassis.
(4) When interlocking with the UPS, turn on the output of the UPS.
(5) Turn on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

Copyright © 2015, 2017, Hitachi, Ltd.

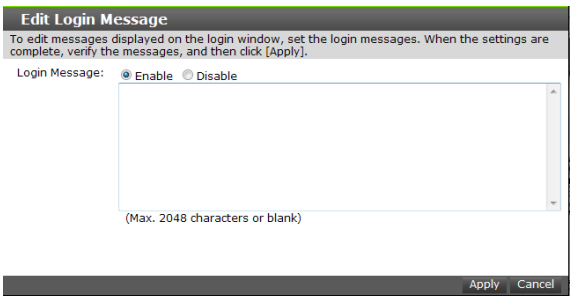
3.13 Edit Login Message

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.

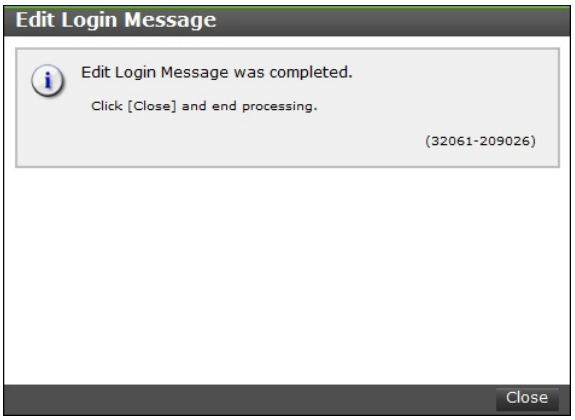


NOTE: When the Firmware version is less than 83-02-01-x0/xx, the “Enable” and “Disable” is not displayed.

Item	Description
Selecting login message display	Select whether to enable or disable the login message display. • [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. • A line feed is counted as one character. • Character decoration is not allowed. Enter simple text information. • You can enter up to 2048 alphanumeric characters. A blank is also allowed.

Copyright © 2015, 2017, Hitachi, Ltd.

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

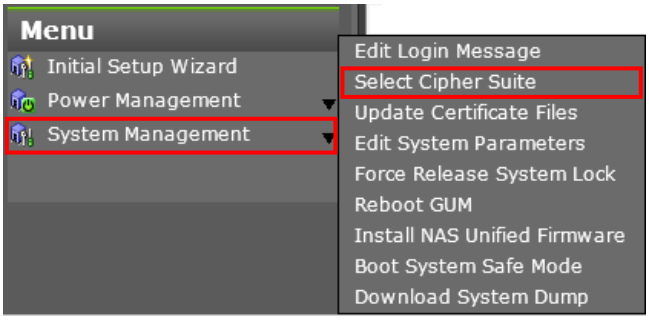


Copyright © 2015, 2017, Hitachi, Ltd.

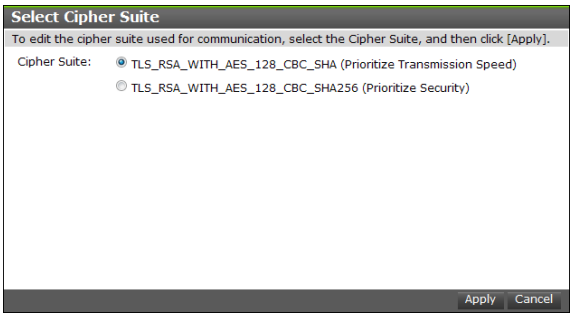
3.14 Select Cipher Suite

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

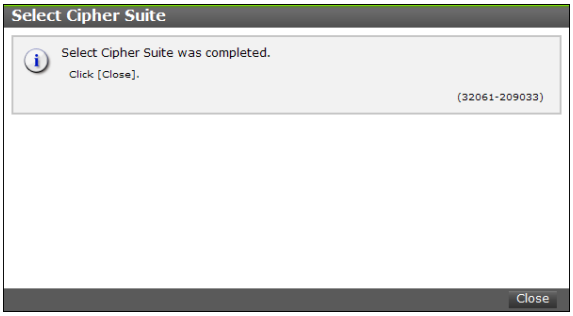
1. Operation menu panel
   Select [Select Cipher Suite] from [System Management].



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



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



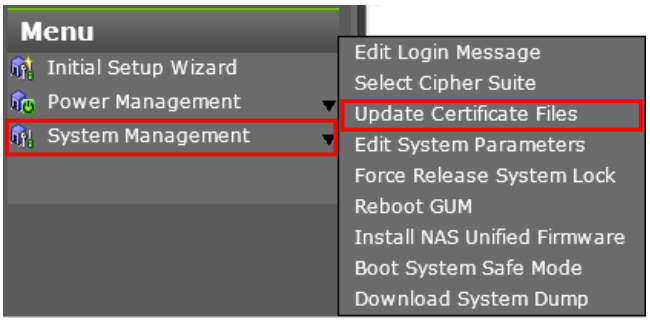
Copyright © 2015, 2017, Hitachi, Ltd.

3.15 Update Certificate Files

This is a window to update the certificate used for the communication (a communication for management between the SVP and the CTL) with the CTL.

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.



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.

Copyright © 2015, 2017, Hitachi, Ltd.

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.

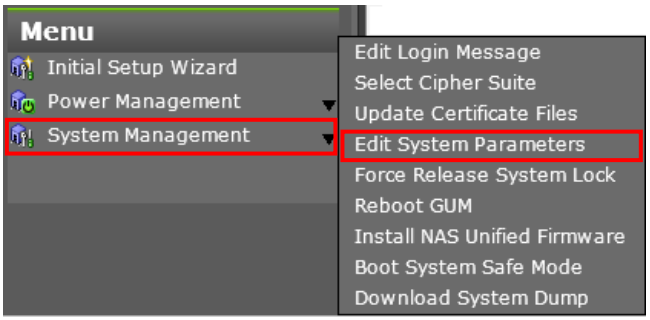
Copyright © 2015, 2017, Hitachi, Ltd.

3.16 Edit System Parameters

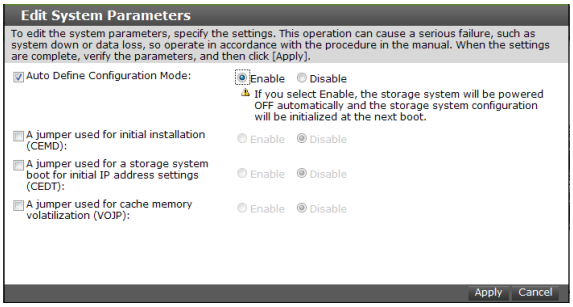
This is a window used for initial installation of the Storage System and volatilization start. This window is displayed only when starting the “Maintenance Utility” window in the following procedures.

- 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.

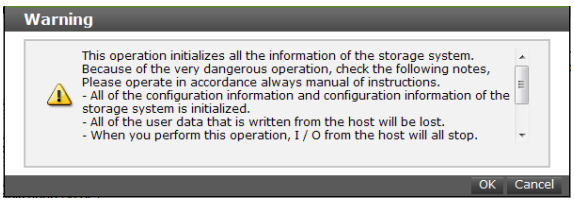


Menu	Description
Auto Define Configuration Mode	Auto Define Configuration Mode Selecting Enable powers off the Storage System automatically and initializes the system configuration at the next start.
A jumper used for initial installation (CEMD)	A jumper used for initial installation
A jumper used for 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.

Copyright © 2015, 2017, Hitachi, Ltd.

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

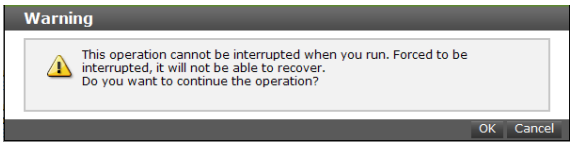


4. Displaying the Password entry window

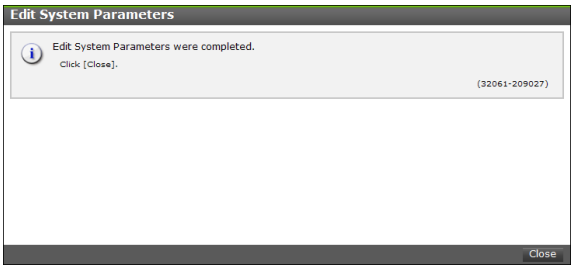
> **⚠ CAUTION**
>
> This operation may cause a serious error such as a system down or a data loss. Confirm the appropriateness of the operation, and then input of the password.

Enter the password and 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.

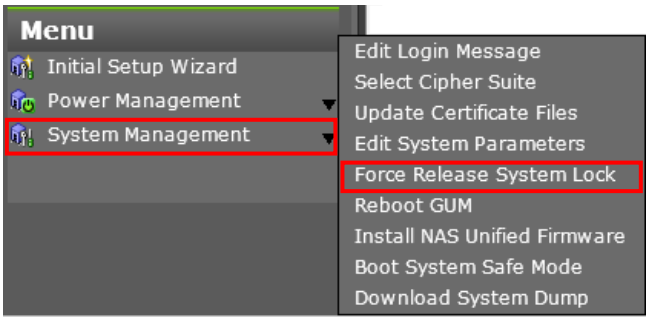


Copyright © 2015, 2017, Hitachi, Ltd.

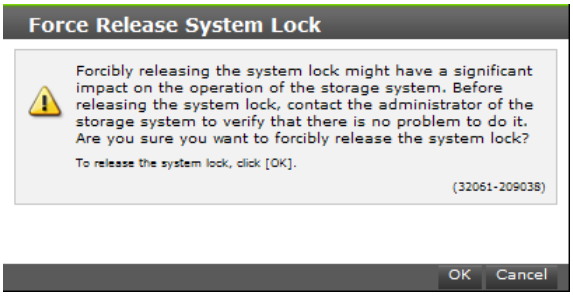
3.17 Force Release System Lock

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

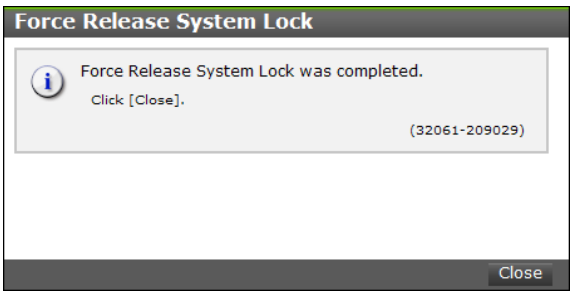
⚠ CAUTION

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 password and click the [OK] button.

Copyright © 2015, 2017, Hitachi, Ltd.

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



Copyright © 2015, 2017, Hitachi, Ltd.

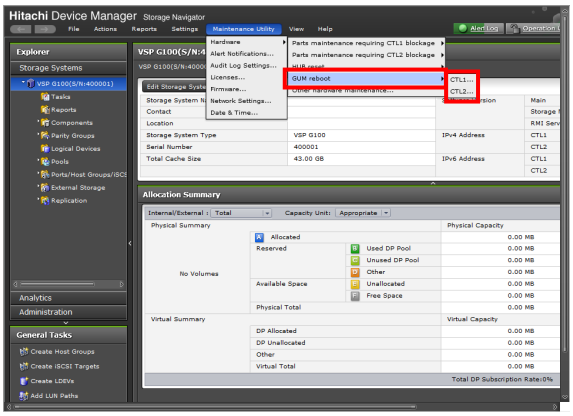
3.18 Reboot GUM

This is a window to restart the connected GUM.
This function is operated by service personnel.

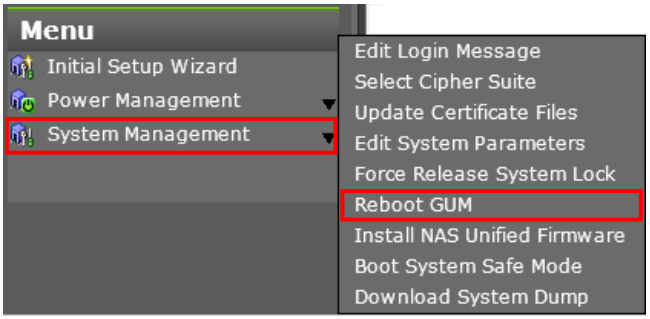
NOTE:
- To reboot GUM of the both controllers, perform the following procedure.
  1. Log into the Maintenance Utility of CTL1 and reboot GUM.
  2. Wait for about five minutes.
  3. Confirm that you can log into the Maintenance Utility of CTL1.
     (If you cannot login, wait for one to two minutes and 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".
- When NAS Modules are installed in the Storage System and the NAS Unified Firmware status that can be viewed in the "Maintenance Utility" window is Active, if GUM is rebooted, the NAS Unified Firmware status is temporarily displayed as Active (Not Redundant).
  The status returns to Active before the login to the Maintenance Utility of the Controller in which GUM is rebooted is confirmed.

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 "1.2 Attachment / Removal Procedure of Maintenance PC".

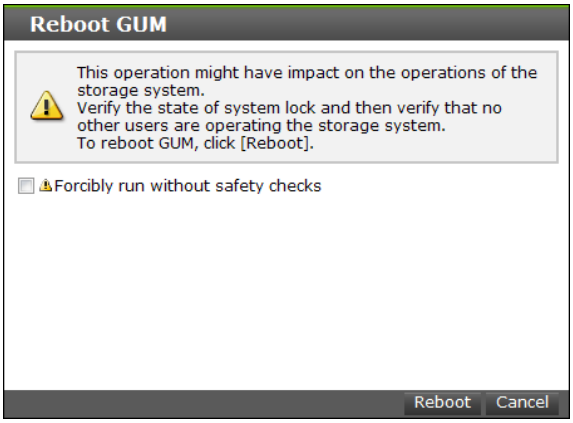
2. Starting Maintenance Utility
   (1) See [When updating software separately] (MPC01-249F) of "1.6.2 Procedures for Connecting to the Storage System" and start Web Console.
   (2) Selecting the toolbar [Maintenance Utility] – [Hardware] – [GUM reboot] – [CTL1...] or [CTL2...] in the "Web Console" window displays the "Maintenance Utility" window.



3. Operation menu panel
   Select [Reboot GUM] from [System Management].



4. Click the [Reboot] button.



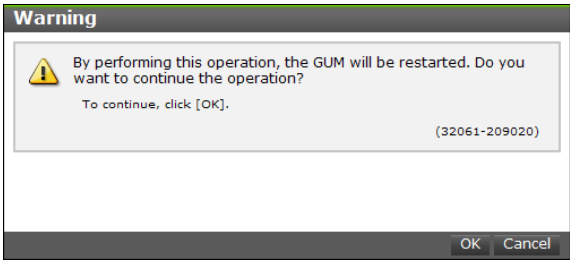
Copyright © 2015, 2017, Hitachi, Ltd.

5. Displaying the Password entry window

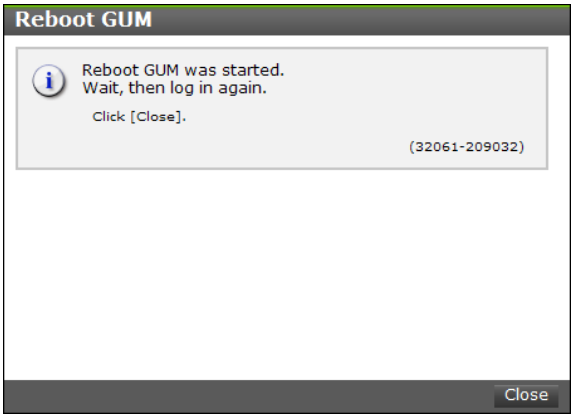
> **⚠ CAUTION**
>
> The Storage System operation might be affected. Confirm the appropriateness of the operation, and then input of the password.

Enter the password and click the [OK] button.

6. 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.

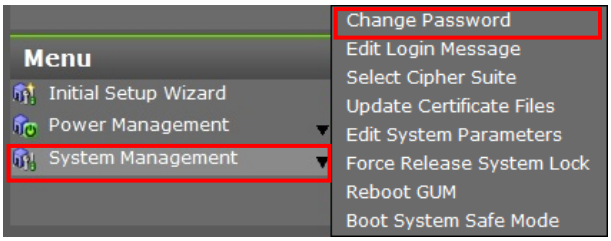
Copyright © 2015, 2017, Hitachi, Ltd.

3.19 Change Password

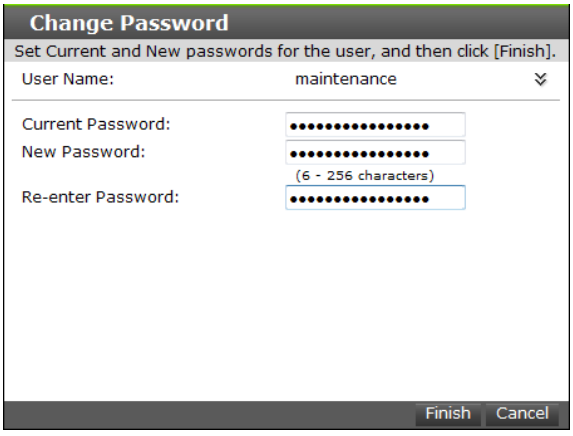
This is a window to change the messages displayed in the login window.
This window is displayed only when specifying the IP address of the CTL on the browser and logging into the Maintenance Utility.

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 "1.6.8 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].

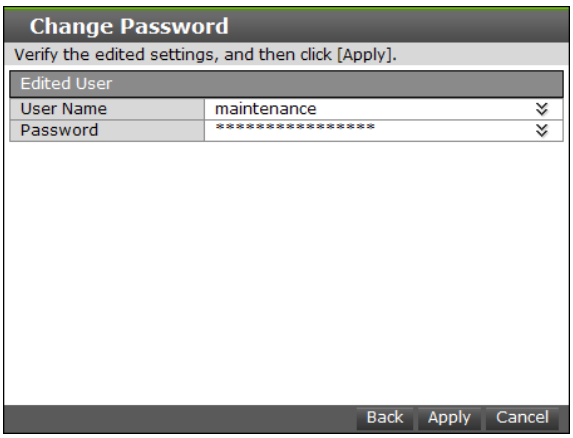


2. Enter the current password and a new password, and then click the [Finish] button.

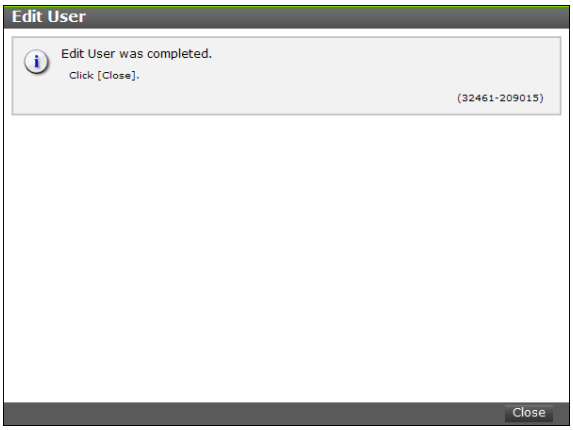


Copyright © 2015, 2017, Hitachi, Ltd.

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



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



Copyright © 2015, 2017, Hitachi, Ltd.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

This page is for editorial purpose only.

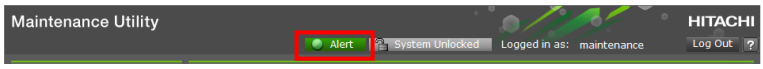
Copyright © 2015, 2017, Hitachi, Ltd.

3.21 Alert Display

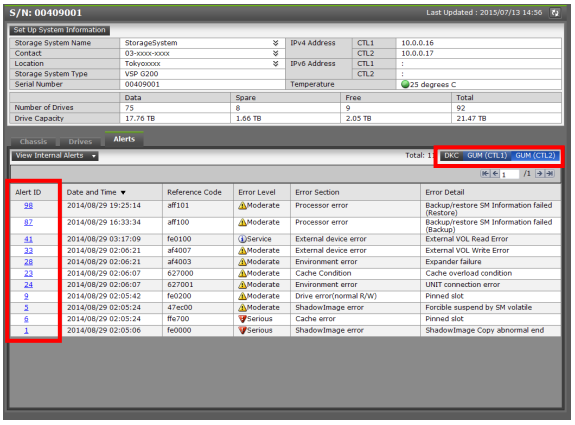
You can check “Alert” described in this section by referring to “[2] SIM Log ” of “5.3.1 Log Indication” and “Internal Alert” by “[1] SSB Log”.

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 1-9 for the Storage System status.

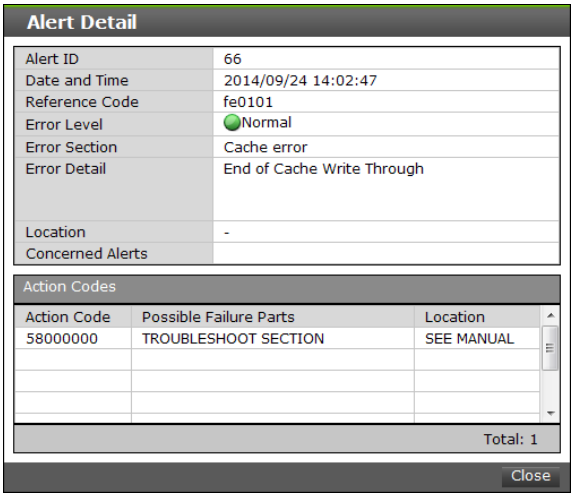
1. Clicking the [Alert] button displays the [Alerts] tab.



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.

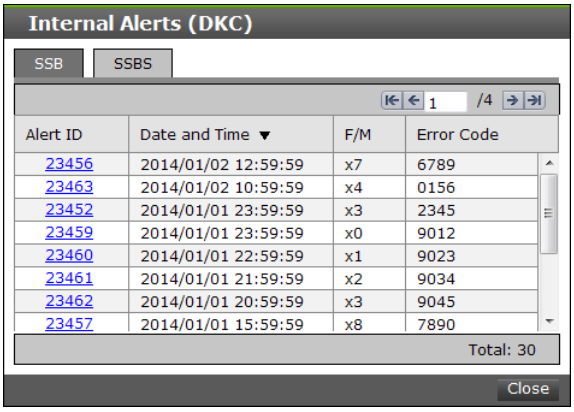


3. Clicking the character string of the alert ID displays the “Alert Detail” window.
Check the alert contents.

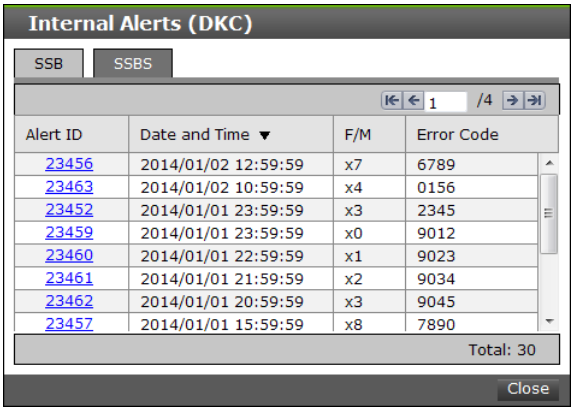


4. <Check of Internal Alerts>
Select [Internal Alerts (DKC)] and [Internal Alerts (GUM)] from the [Refer to Internal Alert] pull-down menu of the [Alert] tab. See SIM RC SECTION (SIMRC00-00) for the details of the displayed content.

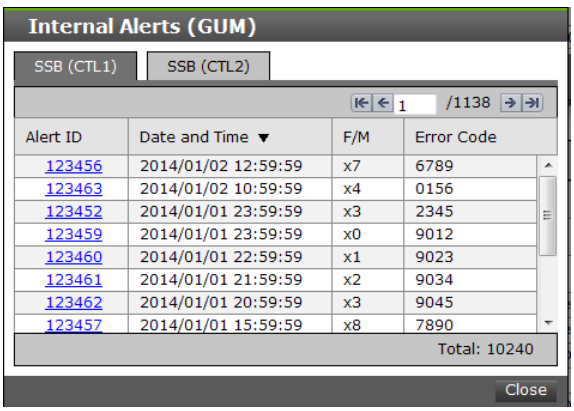
[Internal Alerts (DKC)]
[SSB] tab



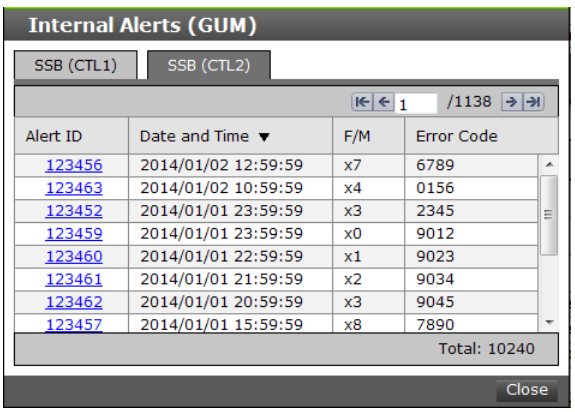
[SSBS] tab



[Internal Alerts (GUM)]
[SSB(CTL1)] tab

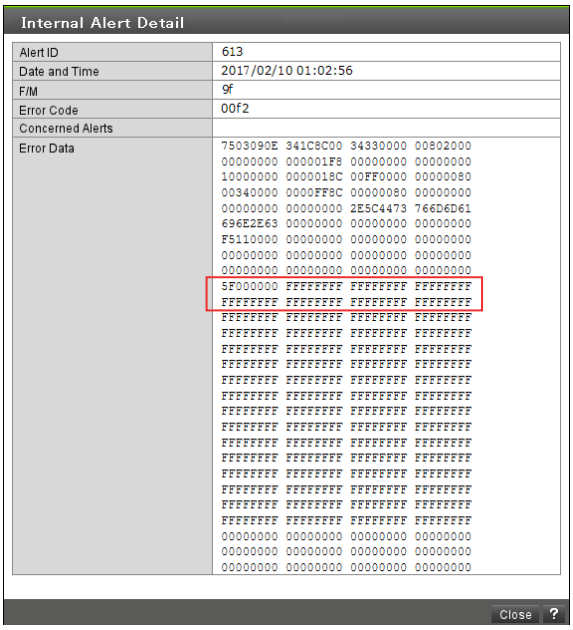


[SSB(CTL2)] tab



Copyright © 2015, 2017, Hitachi, Ltd.

5. <Check of Internal Alert Detail>
   In the [Internal Alerts (DKC)] window or the [Internal Alerts (GUM)] window, click a character string 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.



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.

Copyright © 2015, 2017, Hitachi, Ltd.

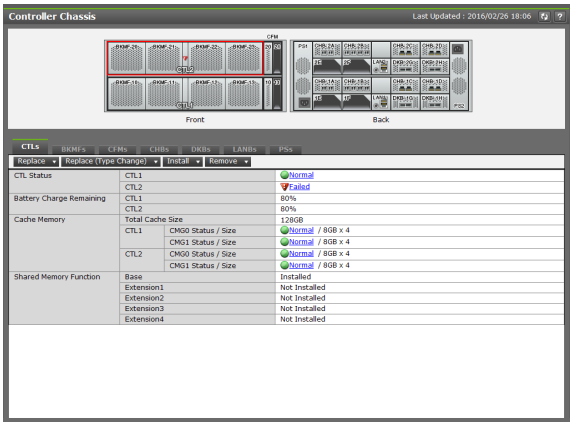
3.22 Alert Display Related to FRU (Field Replacement Unit)

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 alert window.

1. Click [Status] of the hardware from the hardware menu in the "Maintenance Utility" window.

   NOTE: The location number is displayed in the "Maintenance Utility" window for the firmware version 83-01-21-x0/xx or more.

- In case of Controller Chassis



- A display method of the "Related Alerts" window per hardware is as follows.

[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]
		[CFMs] tab	[Status]
		[PSs] tab	[Status]
Drive Box	Drive Box window	[Drives] tab	[Status]
		[ENCs] tab	[Status]
		[PSs] tab	[Status]

*1: If [SFP Status] is clicked, the "Small Form-factor Pluggable" window is displayed. If [SFP Status] is clicked again, the "related alert" window is displayed.

Copyright © 2015, 2017, Hitachi, Ltd.

[In case of CBLM2/CBLM3]

Part	Main window	Tab	Status
Controller Chassis	Controller Chassis window	[CTLs] tab	[CTL Status]
			[CMG0 Status], [CMG1 Status]
		[BKFMs] tab	[BKMFs Status]
			[Battery]-[Status]
		[CFMs] tab	[Status]
		[CHBs] tab	[Status]
			[SFP Status] (*1)
			Cache Memory Status (NAS Module)] (*2)(*3)
		[DKBs] tab	[Status]
		[LANBs] tab	[Status]
		[PSs] tab	[Status]
Drive Box	Drive Box window	[Drives] tab	[Status]
		[ENCs] tab	[Status]
		[PSs] tab	[Status]
NAS Module (*2)	Main window - NAS Module Status window		[Unified Hypervisor]
			[Hypervisor Network Module]
			[NAS Unified Firmware]

*1: If [SFP Status] is clicked, the “Small Form-factor Pluggable” window is displayed.
If [SFP Status] is clicked again, the “Related Alerts” window is displayed.

*2: This is displayed when the firmware for NAS Modules is installed.

*3: If [Cache Memory Status (NAS Module)] is clicked, the “NAS Module Cache Memory” window is displayed.
If [NAS Module Cache Memory Status] is clicked again, the “Related Alerts” window is displayed.

Copyright © 2015, 2017, Hitachi, Ltd.

[In case of CBLH]

Part	Main window	Tab	Status
Controller Chassis	Controller Chassis window	[CTLs] tab	[CTL Status]
			[CMG0 Status], [CMG1 Status]
		[BKFMs] tab	[BKMFs Status]
			[Battery]-[Status]
		[CFMs] tab	[Status]
		[CHBs] tab	[Status]
			[SFP Status] (*1)
			Cache Memory Status (NAS Module)] (*2)(*3)
		[PECBs] tab	[Status]
		[DKBs] tab	[Status]
		[LANBs] tab	[Status]
		[PSs] tab	[Status]
Drive Box	Drive Box window	[Drives] tab	[Status]
		[ENCs] tab	[Status]
		[PSs] tab	[Status]
Channel Board Box	Channel Board Box window	[CHBs] tab	[Status]
			[SFP Status] (*1)
		[SWPKs] tab	[Status]
		[FANs] tab	[Status]
		[PCPs] tab	[Status]
		[PSs] tab	[Status]
NAS Module (*2)	Main window - NAS Module Status window		[Unified Hypervisor]
			[Hypervisor Network Module]
			[NAS Unified Firmware]

*1: If [SFP Status] is clicked, the “Small Form-factor Pluggable” window is displayed.
If [SFP Status] is clicked again, the “Related Alerts” window is displayed.

*2: This is displayed when the firmware for NAS Modules is installed.

*3: If [Cache Memory Status (NAS Module)] is clicked, the “NAS Module Cache Memory” window is displayed.
If [NAS Module Cache Memory Status] is clicked again, the “related alert” window is displayed.

Copyright © 2015, 2017, Hitachi, Ltd.

- The followings are displayed in [Status].

[Status]	Description	Parts frame color	Status icon
Normal	This indicates normal status. But the latest status might not be reflected due to failures of other related parts. If failures in other related parts are notified, the latest status is reflected by replacing the failed parts.	-	
Warning	• 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.	Amber	
	[NAS Module Status-limited] Any of the following failures occurs. • NAS Module hardware fails. • NAS Module related software has trouble. • Warning is displayed by being involved in other parts failures. The status changes to Active by replacing other parts.	None	
Failed	The parts are broken.	Red	
	[Drive Status-limited] • 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.		
	[Hypervisor Network Module Status-limited] Failures occur in Hypervisor Network Module.	None	
Failed (NAS Unified Firmware)	[NAS Unified Firmware Status-limited] Failures occur in NAS Unified Firmware.	None	
Failed (Hardware)	[Unified Hypervisor Status-limited] Unified Hypervisor is blocked due to hardware factors.	None	
Failed (Software)	[Unified Hypervisor Status-limited] Unified Hypervisor is blocked due to software factors.	None	
Failed (Service)	[NAS Unified Firmware Status-limited] Failures occur in the file storage function of NAS Unified Firmware.	None	
Failed (Unknown)	[Unified Hypervisor Status-limited] Unified Hypervisor is blocked.	None	

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

[Status]	Description	Parts frame color	Status icon
Blocked	Only parts needed the blockage instruction by using Maintenance Utility are displayed, and the parts are in an exchangeable status.	Red	
Not fix	[SFP Status-limited] The classification is in an undetermined status.	Amber	
Warning (Port n failed)	[Drive Status-limited] The drive port is in a failure status. n: Failure drive port number	Amber	
Copying n % (TYPE to 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: “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	
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	

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

[Status]	Description	Parts frame color	Status icon
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	
Installing	[NAS Unified Firmware Status-limited] NAS Unified Firmware is being installed.	None	
?	[NAS Module Status-limited] Unified Hypervisor is not starting up.	None	
Active	[NAS Module Status-limited] This indicates normal status.	None	
	[Unified Hypervisor Status-limited] Unified Hypervisor started completely.		
	[Hypervisor Network Module Status-limited] Hypervisor Network Module operates normally.		
	[NAS Unified Firmware Status-limited] NAS Unified Firmware is normal.		
Active (Not Redundant)	[NAS Unified Firmware Status-limited] NAS Unified Firmware detected a failure in either cluster.	None	
Active (Warning)	[NAS Unified Firmware Status-limited] NAS Unified Firmware detected trouble in either cluster.	None	
Inactive	[NAS Module Status-limited] No trouble occurs, but start-up is not completed.	None	
Initial	[Unified Hypervisor Status-limited] Unified Hypervisor is initialized.	None	
Failure Processing	[Unified Hypervisor Status-limited] Unified Hypervisor is in the process of blockade.	None	
	[NAS Unified Firmware Status-limited] NAS Unified Firmware is in the process of blockade.		
Failure Processing (Stopped)	[Hypervisor Network Module Status-limited] Hypervisor Network Module stopped.	None	

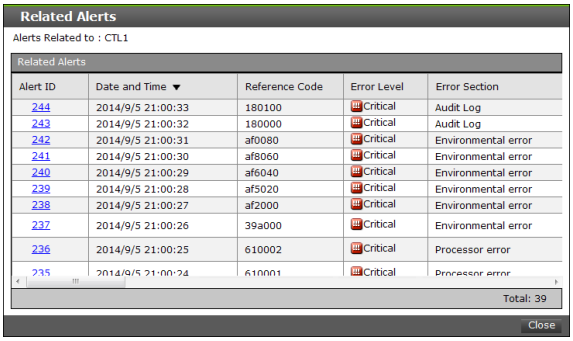
(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

[Status]	Description	Parts frame color	Status icon
Failure Processing (Restarting)	[Hypervisor Network Module Status-limited] Hypervisor Network Module is being reset.	None	
Processing	[NAS Unified Firmware Status-limited] NAS Unified Firmware is in the process of start-up or stopping. (Case 2)	None	
Starting	[Unified Hypervisor Status-limited] Unified Hypervisor is in the process of start-up.	None	
	[NAS Unified Firmware Status-limited] NAS Unified Firmware is starting up. (Case 1)		
Starting (Service)	[NAS Unified Firmware Status-limited] The file storage function of NAS Unified Firmware is starting up.	None	
Starting (NVRAM Restoring)	[NAS Unified Firmware Status-limited] NAS Unified Firmware is loading the configuration definition.	None	
Stopping	[Unified Hypervisor Status-limited] Unified Hypervisor is in the process of stopping.	None	
Stopping (Service)	[NAS Unified Firmware Status-limited] The file storage function of NAS Unified Firmware is in the process of stopping.	None	
Stopped	[Unified Hypervisor Status-limited] Unified Hypervisor stopped.	None	
	[NAS Unified Firmware Status-limited] NAS Unified Firmware stopped.		
Stopped (Service)	[NAS Unified Firmware Status-limited] The file storage function of NAS Unified Firmware stopped.	None	

2. 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.



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]

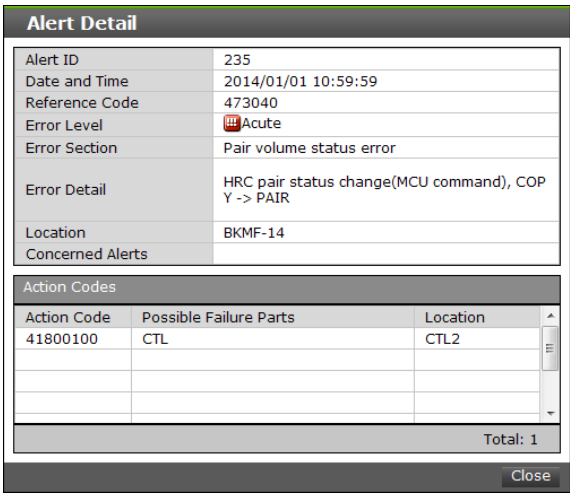
- Only the alerts including the specified parts and the internal parts in the action codes are displayed. (You can check the actions codes in the “Alert Detail” window in Step 3.)
  For example, the alerts of which the action codes are only manual reference are not displayed in the “Related Alerts” window.

- 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.

3. Clicking the character string of the alert ID displays the “Alert Detail” window.

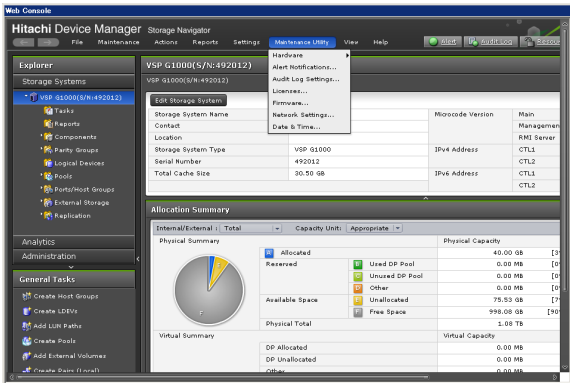


Copyright © 2015, 2017, Hitachi, Ltd.

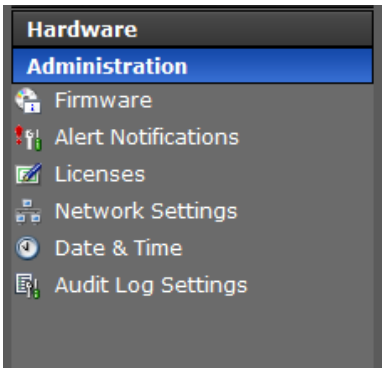
3.23 Management Menu

1. Starting “Maintenance Utility” window
   When starting Maintenance Utility from the browser See “1.8.2.3 Starting the Browser” to start Maintenance Utility.

2. When starting Maintenance Utility from Web Console
   (1) Start the Web Console referring to “1.6 Connecting to the Storage System”.
   (2) In the “Web Console” window, select [Maintenance Utility].



The window can be displayed from the menu location in the “Maintenance Utility” window.



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”.)

Copyright © 2015, 2017, Hitachi, Ltd.

3.24 Power Supply Management

1. Clicking the [Menu] item opens menus.

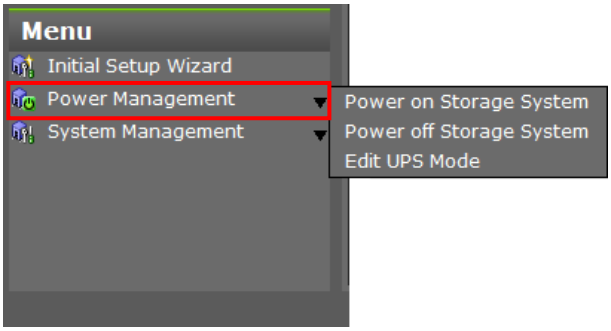


Table 3-1 List of Power Management Menus

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.

Copyright © 2015, 2017, Hitachi, Ltd.

3.25 System Management

Clicking the [Menu] item opens menus.

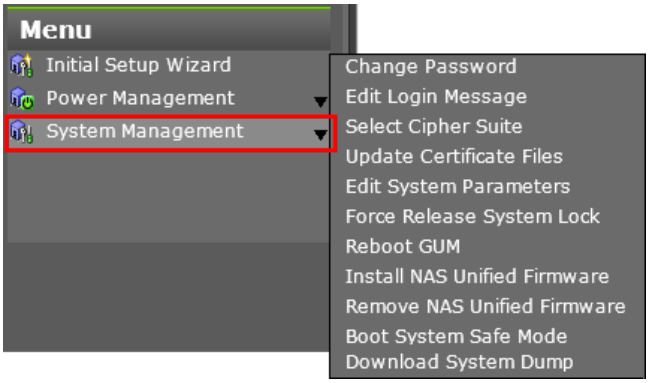


Table 3-2 List of System Management Menus

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
	Install NAS Unified Firmware (*2)	Install NAS Unified Firmware. For the operation procedure, see INSTALLATION SECTION "7.1 New Installation of the NAS Unified Firmware".
	Remove NAS Unified Firmware (*2)	Uninstall of NAS unified firmware. For the operation procedure, see INSTALLATION SECTION "7.2 Removing the NAS Unified Firmware".
	Change Password	Change password
	Boot System Safe Mode (*1)	Switch to System Safe Mode

*1: This item is displayed when the firmware version is 83-03-01-x0/xx or later.

*2: This item is displayed when the firmware version is 83-03-21-x0/xx or later and NAS Modules are installed.

Copyright © 2015, 2017, Hitachi, Ltd.

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.
- When NAS Modules are installed in the Storage System and the NAS Unified Firmware status that can be viewed in the "Maintenance Utility" window is Active, if GUM is reset, the NAS Unified Firmware status is temporarily displayed as Active (Not Redundant).
  The status returns to Active before the login to the Maintenance Utility of the Controller in which GUM is reset is confirmed.

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.

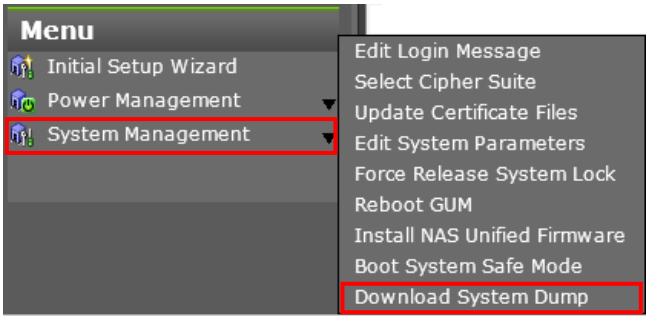
Copyright © 2015, 2017, Hitachi, Ltd.

3.27 Acquiring System Dumps

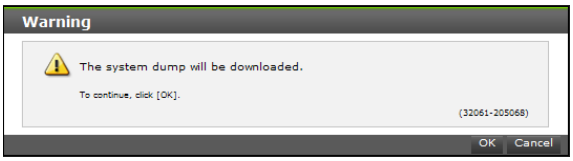
The following procedure describes how to acquire system dumps from Maintenance Utility.
This function is supported in the firmware version 83-02-01-x0/xx or later.

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] from [System Management].



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



3. If [OK] button is clicked, another white window is displayed. If the certificate is invalid at the time of the https connection, the security confirmation window is displayed.
   If the security confirmation window is displayed, select “Continue to this website (not recommended)”.
   Do not close the white window or the security confirmation window until the download is completed.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

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.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

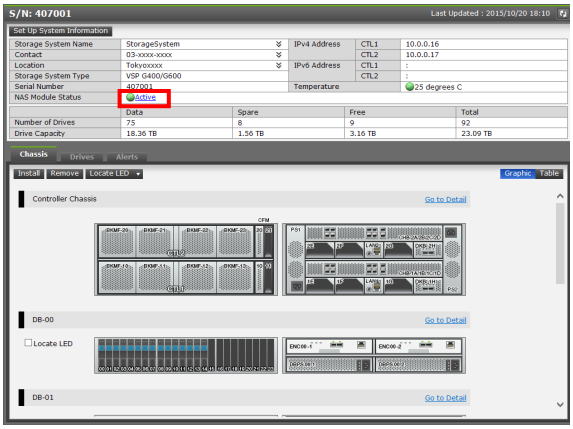
3.28 Confirming the NAS Module Status

This is a window to perform the verifying or setting.

3.28.1 Displaying the NAS Module Status

1. Start Maintenance Utility.

2. Click [NAS Module Status] in the “Main” window.



3. The “NAS Module Status” window is displayed.
For the NAS Module status, see “3.22 Alert Display Related to FRU (Field Replacement Unit)”.

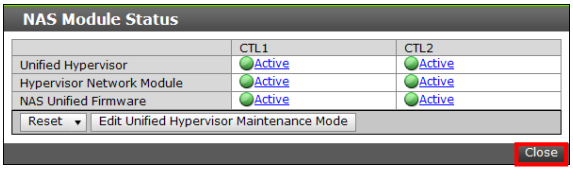


Table 3-3 NAS Module Status Window List

No.	Item	References
1	Unified Hypervisor	“3.28.2 Resetting Unified Hypervisor”
2	Hypervisor Network Module	“3.28.3 Resetting Hypervisor Network Module”
3	NAS Unified Firmware	“3.28.4 Resetting NAS Unified Firmware”
4	Editing Unified Hypervisor Maintenance Mode	“3.28.5 Editing Unified Hypervisor Maintenance Mode”

4. Close the “NAS Module Status” window.
Click the [Close] button.

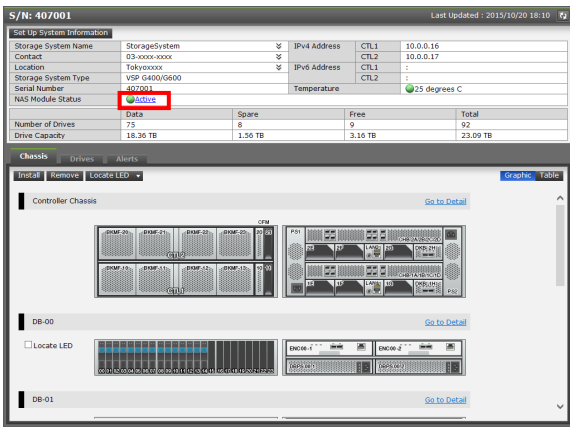
5. Log out to terminate Maintenance Utility.

Copyright © 2015, 2017, Hitachi, Ltd.

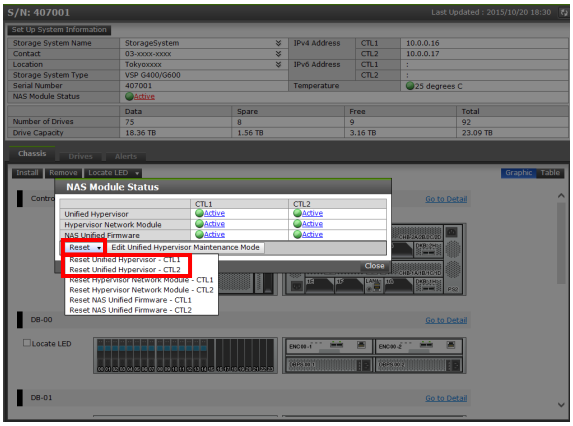
3.28.2 Resetting Unified Hypervisor

1. Start Maintenance Utility.

2. Click [NAS Module Status] in the “Main” window



3. Selecting Reset Unified Hypervisor
   Click the [Reset] button in the “NAS Module Status” window and select [Reset Unified Hypervisor – CTL1] or [Reset Unified Hypervisor – CTL2].



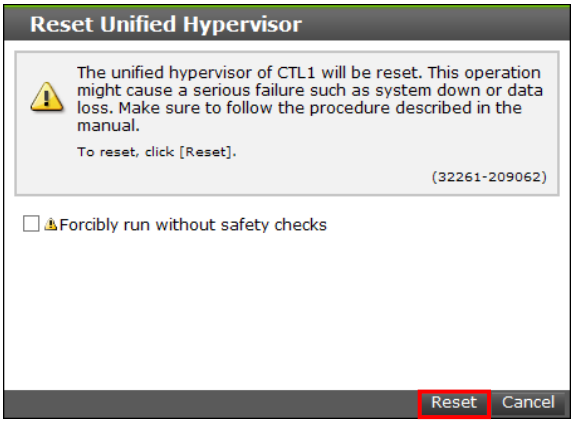
Copyright © 2015, 2017, Hitachi, Ltd.

4. Resetting Unified Hypervisor

⚠ 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.

Click the [Reset] button to reset the Unified Hypervisor.



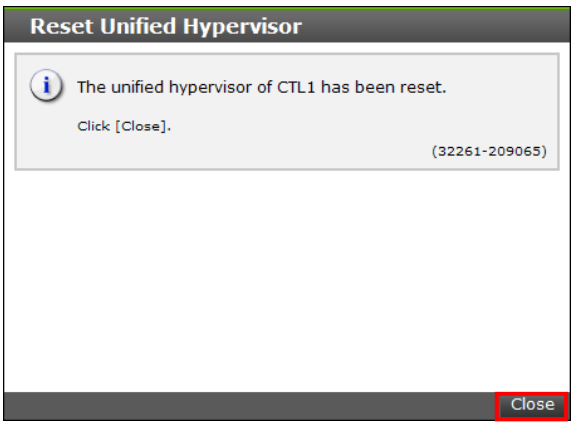
5. Entering the password

⚠ CAUTION

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

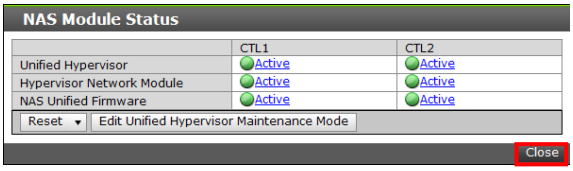
Enter the password and click the [OK] button.

6. Checking Reset Unified Hypervisor
Check the message "The unified hypervisor of CTLx has been reset.", and then click the [Close] button.



Copyright © 2015, 2017, Hitachi, Ltd.

7. Completing Reset Unified Hypervisor
   Click the [Close] button in the “NAS Module Status” window.



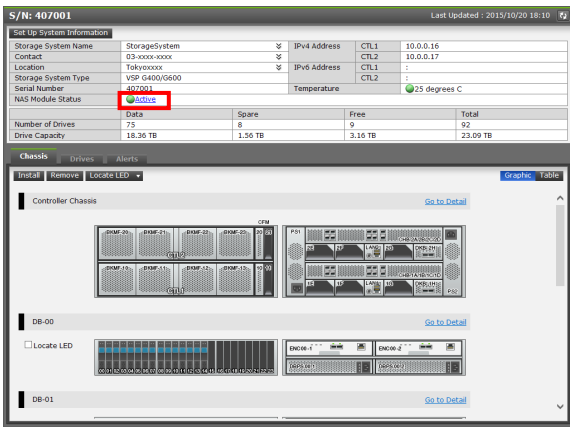
8. Log out to terminate Maintenance Utility.

Copyright © 2015, 2017, Hitachi, Ltd.

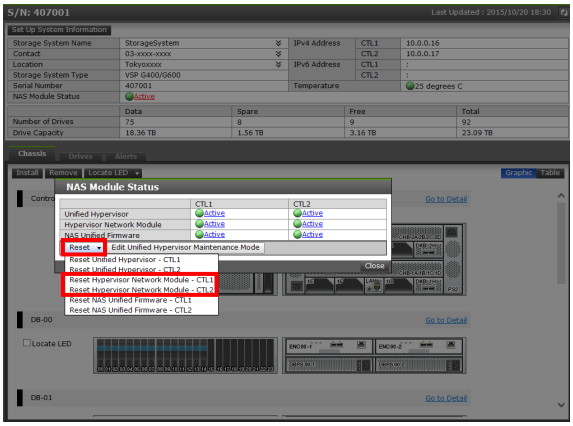
3.28.3 Resetting Hypervisor Network Module

1. Start Maintenance Utility.

2. Click [NAS Module Status] in the “Main” window



3. Selecting Reset Unified Hypervisor
   Click the [Reset] button in the “NAS Module Status” window and select [Reset Hypervisor Network Module – CTL1] or [Reset Hypervisor Network Module – CTL2].

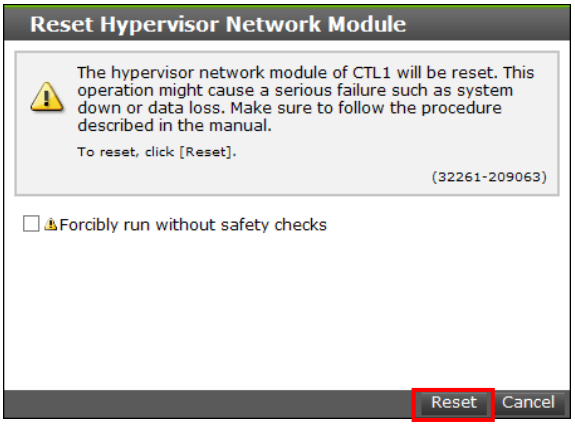


Copyright © 2015, 2017, Hitachi, Ltd.

4. Resetting Hypervisor Network Module

> **⚠ 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.

Click the [Reset] button to reset the Hypervisor Network Module.

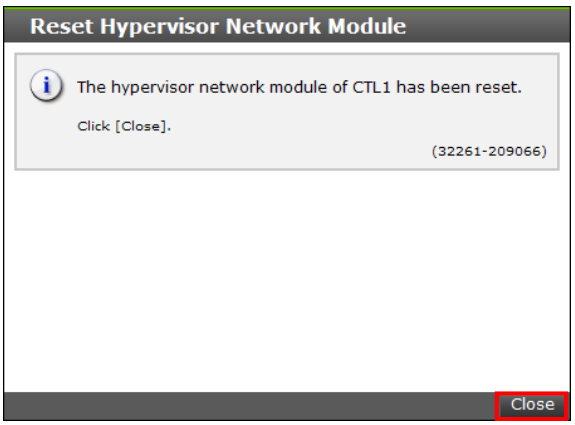


5. Entering the password

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

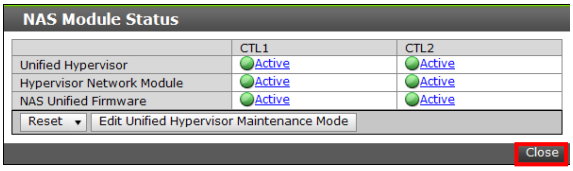
Enter the password and click the [OK] button.

6. Checking Reset Hypervisor Network Module
Check the message "The hypervisor network module of CTLx has been reset.", and then click the [Close] button.



Copyright © 2015, 2017, Hitachi, Ltd.

7. Completing Reset Hypervisor Network Module
   Click the [Close] button in the “NAS Module Status” window.



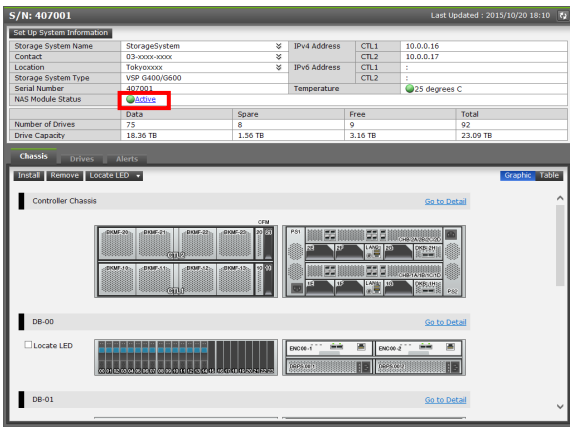
8. Log out to terminate Maintenance Utility.

Copyright © 2015, 2017, Hitachi, Ltd.

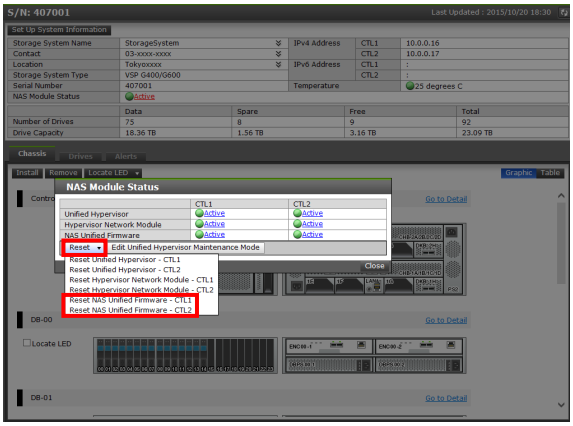
3.28.4 Resetting NAS Unified Firmware

1. Start Maintenance Utility.

2. Click [NAS Module Status] in the “Main” window



3. Selecting Reset NAS Unified Firmware
   Click the [Reset] button in the “NAS Module Status” window and select [Reset NAS Unified Firmware – CTL1] or [Reset NAS Unified Firmware – CTL2].

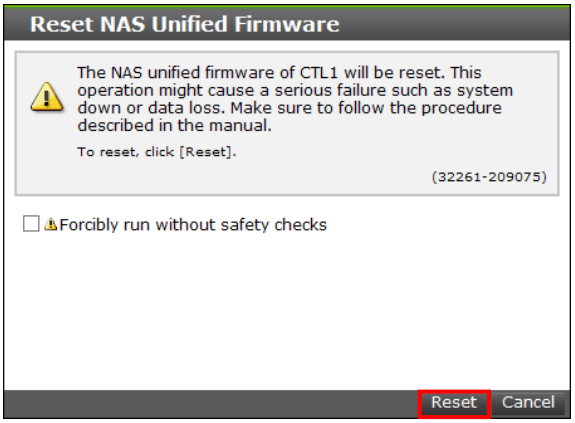


Copyright © 2015, 2017, Hitachi, Ltd.

4. Resetting NAS Unified Firmware

> **⚠ 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.

Click the [Reset] button to reset the NAS Unified Firmware.

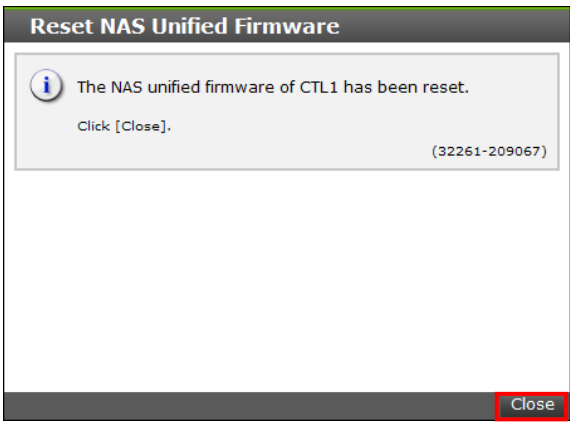


5. Entering the password

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

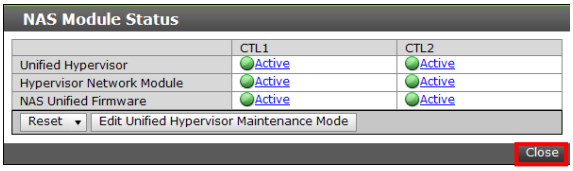
Enter the password and click the [OK] button.

6. Checking Reset NAS Unified Firmware
Check the message "The NAS unified firmware of CTLx has been reset.", and then click the [Close] button.



Copyright © 2015, 2017, Hitachi, Ltd.

7. Completing NAS Unified Firmware
   Click the [Close] button in the “NAS Module Status” window.



8. Log out to terminate Maintenance Utility.

Copyright © 2015, 2017, Hitachi, Ltd.

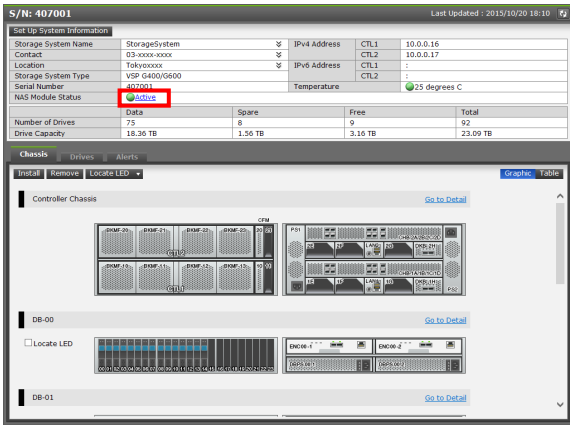
3.28.5 Editing Unified Hypervisor Maintenance Mode

Procedure for enabling or disabling Unified Hypervisor Maintenance Mode.

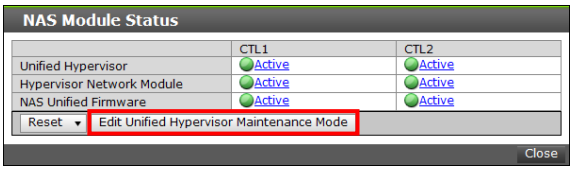
NOTICE: Perform the operation only when the Technical Support Division issues instructions.

1. Start Maintenance Utility.

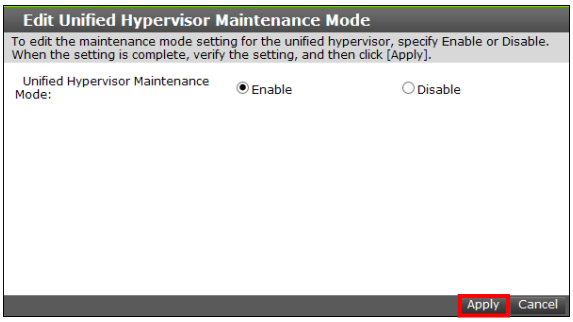
2. Click [NAS Module Status] in the “Main” window



3. Selecting Edit Unified Hypervisor Maintenance Mode
   Click the [Edit Unified Hypervisor Maintenance Mode] button in the “NAS Module Status” window.

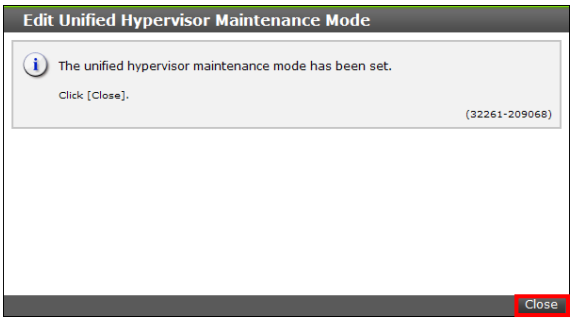


4. Setting Unified Hypervisor Maintenance Mode
   Select [Enable] or [Disable] in the “Edit Unified Hypervisor Maintenance Mode” window and click the [Apply] button.
   - [Enable] : Maintenance Mode is enabled
   - [Disable] : Maintenance Mode is disabled

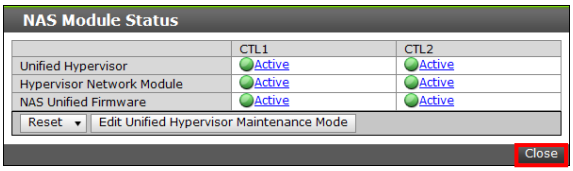


Copyright © 2015, 2017, Hitachi, Ltd.

5. Checking Unified Hypervisor Maintenance Mode
   Check the message “The unified hypervisor maintenance mode has been set.”, and then click the [Close] button.



6. Completing Edit Unified Hypervisor Maintenance Mode
   Click the [Close] button in the “NAS Module Status” window.



7. Log out to terminate Maintenance Utility.

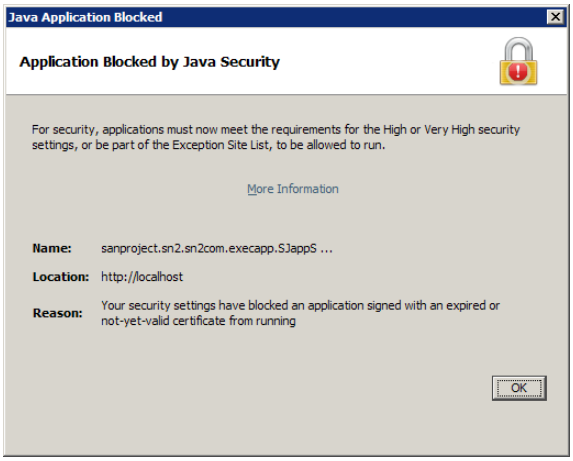
Copyright © 2015, 2017, Hitachi, Ltd.

3.29 Changing Java Security Settings When Electronic Certificate is Expired

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 expiration data is reached, the following window appears.



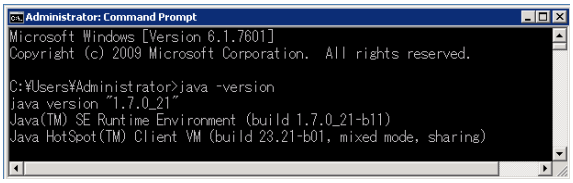
Copyright © 2015, 2017, Hitachi, Ltd.

3.29.1 Confirm Java Version

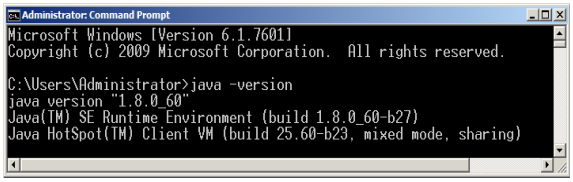
Check the Java version in use.

1. Open the [Command Prompt]
   Select (CL) [Start]-[All Programs]-[Accessories], and launch the Command Prompt.

2. Confirm Java version
   Enter “java -version” and check that the version is Java 1.7.0_55 or later or Java 1.8.0_5 or later.



Eg.: Example: For Java 1.7.0_21



Eg.: Example: For Java 1.8.0_60

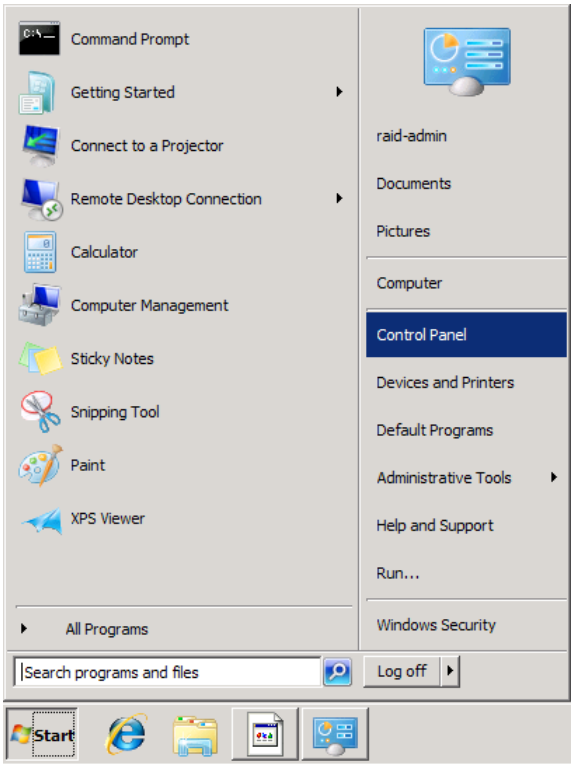
When the version is the version mentioned above, go to “3.29.2 Changing Java Security Settings”.
When the version is not the version mentioned above, end the procedure.

Copyright © 2015, 2017, Hitachi, Ltd.

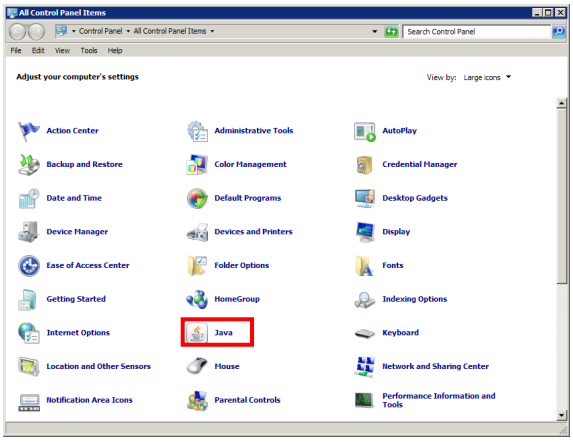
3.29.2 Changing Java Security Settings

Change the settings following the procedure below.

1. Open Control Panel
   Select (CL) [Start]-[Control Panel].

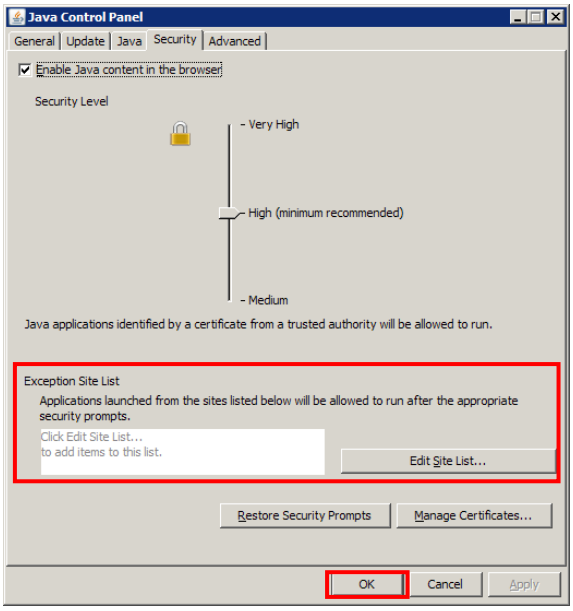


2. Open Java Control Panel
   Select (CL) [Java].



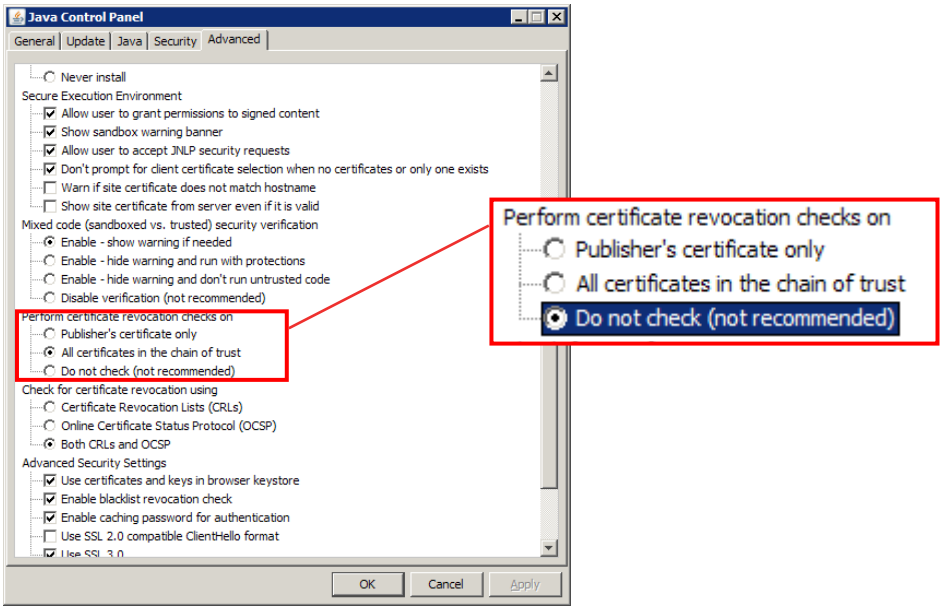
Copyright © 2015, 2017, Hitachi, Ltd.

3. Open the [Security] tab in the Java Control Panel
   Add the following URLs to the “Exception Site List” and select (CL) [OK].
   URLs to be added:
   - http://(IP address of MPC)
   - https://(IP address of MPC)
   - 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://(IP address of 127.0.0.1)
   - https://(IP address of 127.0.0.1)
   - http://(IP address of localhost)
   - https://(IP address of localhost)



Copyright © 2015, 2017, Hitachi, Ltd.

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



5. 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.

Copyright © 2015, 2017, Hitachi, Ltd.

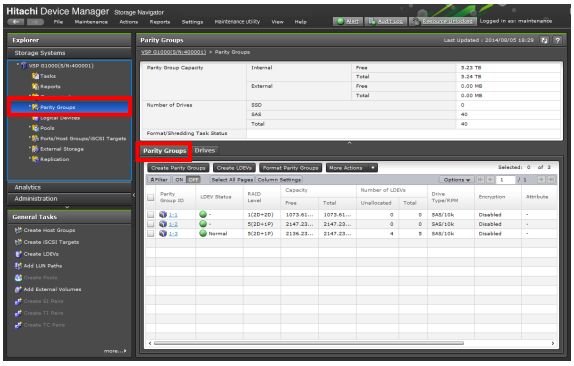
4. Storage System Management Function

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.



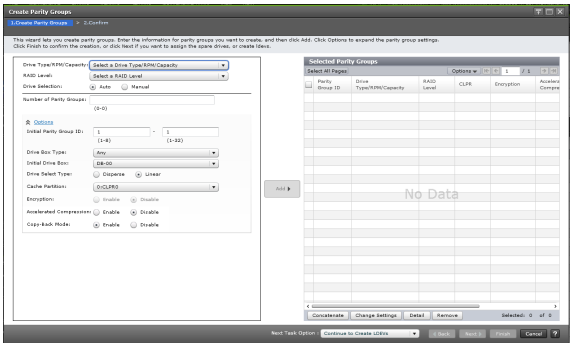
Item	Description
Parity Group ID	Number of the parity groups
LDEV Status	A status of all the devices in the parity group
RAID Level	RAID level specified.
Capacity-Free	Available capacity of the parity group
Capacity-Total	Entire capacity of the parity group
Number of LDEVs-Unallocated	The number of the 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.

Copyright © 2015, 2017, Hitachi, Ltd.

3. 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.



   NOTE: When the Firmware version is less than 83-03-01-x0/xx, the Accelerated Compression is not displayed.

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. • 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 alphanumeric characters, which are fixed characters of the head of the parity group names. Characters are case-sensitive. 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.

Copyright © 2015, 2017, Hitachi, Ltd.

Item	Description
Drive Select Type	This item appears when selected Auto as your drive selection. Select the method for the selecting of drives in a parity group. • Disperse: Selected drives where are located dispersedly. • Linear: Selected drives where are located linearly. This item is not available with VSP G200. In VSP G200, [Linear] is set by default.
Cache Partition	Select a CLPR number which is displayed as ID:CLPR.
Encryption	Specify if encrypted parity groups are created. • Enable: Encrypted parity groups are created. • Disable: Non-encrypted parity groups are created.
Accelerated Compression	Specify if the Accelerated Compression is set to parity groups. (*1) • Enable: The Accelerated Compression is set to parity groups. • Disable: The Accelerated Compression is not set to parity groups.
Copy-Back Mode	Specify if the Copy-Back Mode is set to parity groups. • 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”.

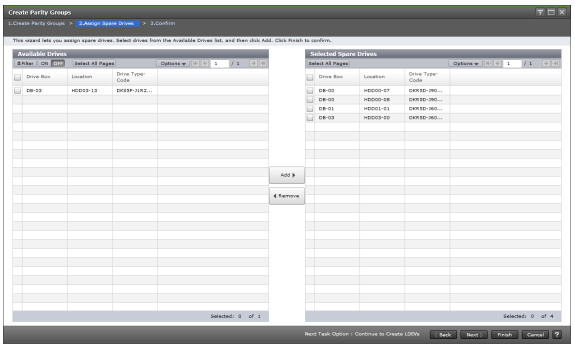
Copyright © 2015, 2017, Hitachi, Ltd.

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.

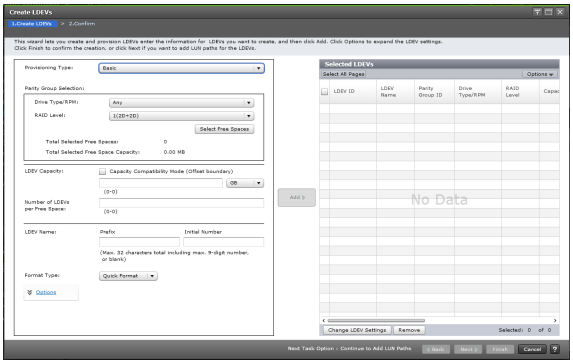


[Available Drives] table and [Selected Spare Drives]

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.

Copyright © 2015, 2017, Hitachi, Ltd.

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.

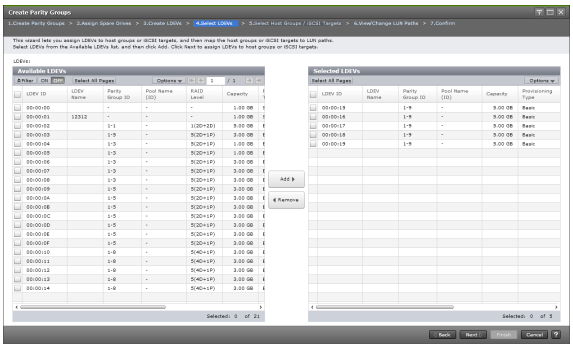
Item	Description
Provisioning Type	Select the type of LDEV. Basic: Internal volume. Dynamic Provisioning: DP-VOL. External: External volume. Snapshot: Thin Image volume. ALU: LDEV of the ALU attribution.
Drive Type/RPM	Select the data drive type and RPM. Any: All types of disk drives and RPMs that can 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.

Copyright © 2015, 2017, Hitachi, Ltd.

Item	Description
LDEV Capacity	• Capacity Compatibility Mode (Offset boundary): If you want to offset the specified LDEV capacity by boundary, set the Capacity Compatibility Mode (Offset boundary) to ON. • Input area: Specify the LDEV capacity to create in a free space, a pool, or an external volume. Detailed calculation of the LDEV capacity differs depending on the specification of the unit. For details, see “Provisioning Guide”.
Number of LDEVs per Free Space, Number of LDEVs, or Number of LDEVs per External Volume	Specify the number of LDEVs to create in a free space, pool, or the external volume.
LDEV Name	LDEV name. Specify the prefix characters and the initial number. • Prefix: A fixed character string. • Initial Number: The initial number of the LDEV name. Specify the initial number according to the examples below. You can specify up to 32 characters total. Example: • 1: Up to 9 numbers are added (1, 2, 3... 9). • 08: Up to 92 numbers are added (08, 09, 10...99). • 23: Up to 77 numbers are added (23, 24, 25...99). • 098: Up to 902 numbers are added (098, 099,100... 999).
Format Type	Specify the format type. This appears when an internal or external volume is used. Quick Format: Quick formatting is the default format type. You cannot select this when the provisioning type is something other than the internal volume. Normal Format: Normal formatting. Parity Group Format: Format the parity group. You can select this when no LDEV exists in the parity group. No Format: Volumes are not formatted.
Initial LDEV ID	Specify the LDEV ID. LDKC is fixed to 00. Default of CU and DEV is 00:00. For creating multiple LDEVs, select the interval of the assigned LDEV ID from the Interval list.
View LDEV IDs	Displays the View LDEV IDs windows.
MP Unit ID	Specify the MP unit you want to assign to the LDEV. You can select an ID from I/F Board 0 to I/F Board 7. If automatic assignment is enabled for one or more MPs, you can also select Auto. If Auto is enabled, the default is Auto. If Auto is disabled, the default is the lowest number of the MP unit.
T10 PI	Sets the T10 PI attribute of the LDEV. [Enabled]: Enables the T10 PI attribute of the LDEV. [Disabled]: Disables the T10 PI attribute of the LDEV. This function is [Provisioning Type] and it can be set when any of [Basic], [DP], and [Snapshot] is selected.

Copyright © 2015, 2017, Hitachi, Ltd.

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 be appear for undefined LDEVs. A hyphen appearing in columns to the right of the LDEV ID and LDEV name (for example, Parity Group ID, Pool Name ID, Capacity, and so on) indicates the LDEV is undefined.
LDEV Name	LDEV names.
Parity Group ID	Parity group identifier where the LDEV belongs.
Pool Name (ID)	Pool name and pool identifier.
RAID level	RAID level specified.
Capacity	Capacity of each LDEV.
Provisioning Type	Provisioning type of each volume. Basic: Internal volume DP: V-VOLs of Dynamic Provisioning External: External volume Snapshot: Thin Image volume ALU: LDEV of the ALU attribution.
Attribute	Attribute of the volume indicating how the LDEV is used. Command Device: Command device Remote Command Device: Remote command device JNL VOL: Journal volume Pool VOL: Pool volume. The number in parentheses shows the pool ID. ALU: LDEV of the ALU attribution. SLU: LDEV of the SLU attribution. NAS Platform (User LU): LDEV in which the NAS user data is stored. This is displayed when the NAS Module is installed. 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.

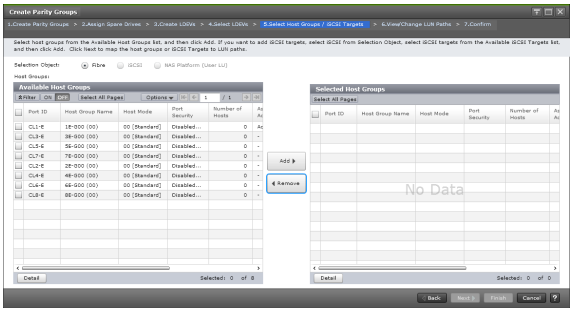
(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(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.

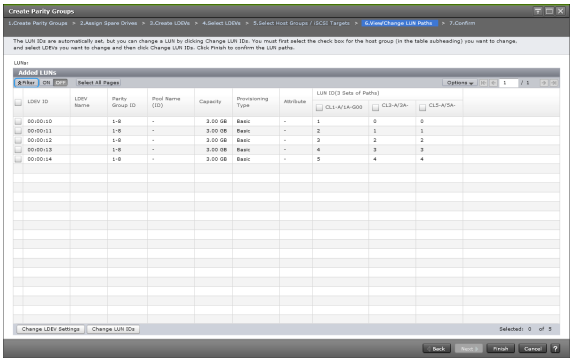


[Available Host Groups] table and [Selected Host Groups] table

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.

Copyright © 2015, 2017, Hitachi, Ltd.

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. NAS Platform (User LU): LDEV in which the NAS user data is stored. This is displayed when the NAS Module is installed. -: 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.

Copyright © 2015, 2017, Hitachi, Ltd.

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.

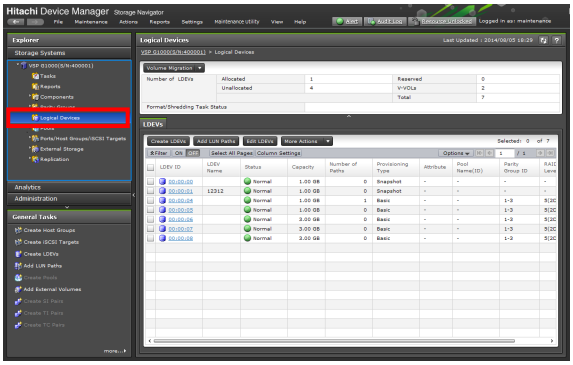
    NOTE: To display the “Task” window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

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

Copyright © 2015, 2017, Hitachi, Ltd.

4.1.2 Verifying LDEVs

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

Copyright © 2015, 2017, Hitachi, Ltd.

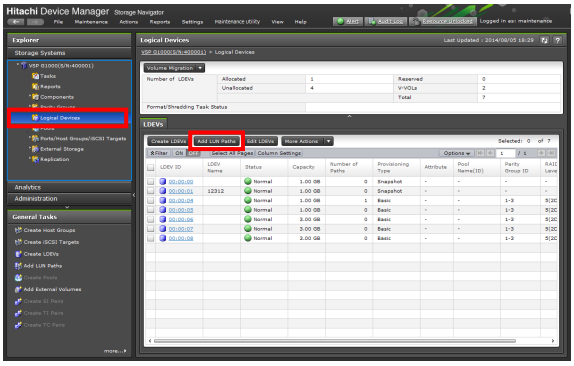
4.1.3 Allocating the Logical Devices of a Storage System to a Host

NOTE: iSCSI in this Chapter indicates iSCSI (optic/copper) of the Channel Board.
(Model name: DW-F800-2HS10B/2HS10S)
Regarding iSCSI for NAS Module, see "File Service Administration Guide".

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.

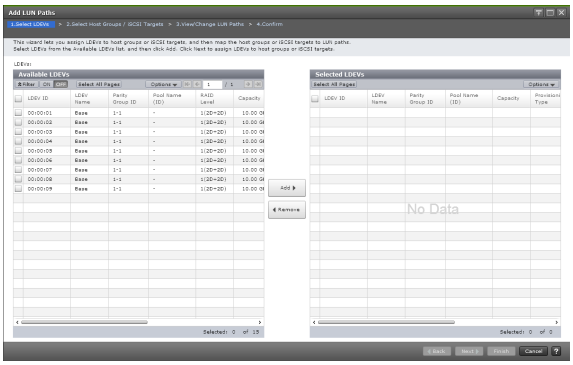
NOTICE:	When the Storage System and the host are connected with the Fibre Channel interface, the logical device of the Storage System cannot be recognized unless the logical device 0 is not created in the Storage System depending on the host. When using this host, create the logical device 0 or map the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



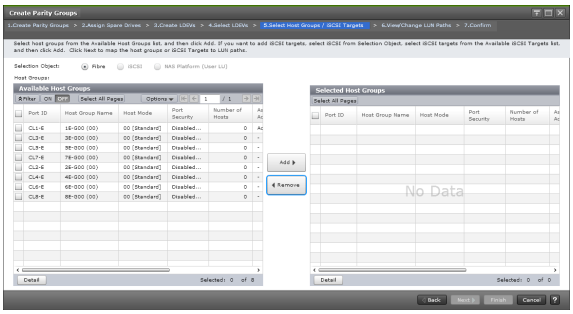
Copyright © 2015, 2017, Hitachi, Ltd.

[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. NAS Platform (User LU): LDEV in which the NAS user data is stored. This is displayed when the NAS Module is installed. -: 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.

Copyright © 2015, 2017, Hitachi, Ltd.

4. The “Add LUN Paths” window appears.
   Select a Fibre, iSCSI or NAS platform (user LU) 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.



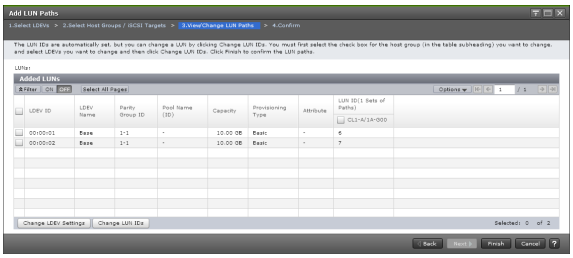
[Available Host Groups] table and [Selected Host Groups] table

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.

Copyright © 2015, 2017, Hitachi, Ltd.

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. NAS Platform (User LU): LDEV in which the NAS user data is stored. This is displayed when the NAS Module is installed. -: 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.

Copyright © 2015, 2017, Hitachi, Ltd.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

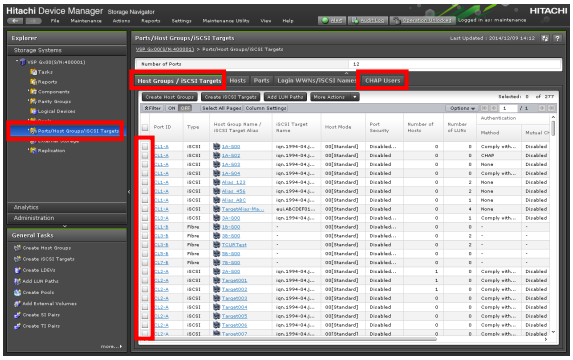
4.1.4 Configuring a Host Group or iSCSI Target

NOTE: iSCSI in this Chapter indicates iSCSI (optic/copper) of the Channel Board.
(Model name: DW-F800-2HS10B/2HS10S)
Regarding iSCSI for NAS Module, see “File Service Administration Guide”.

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 Construct iSCSI Target or Host Group

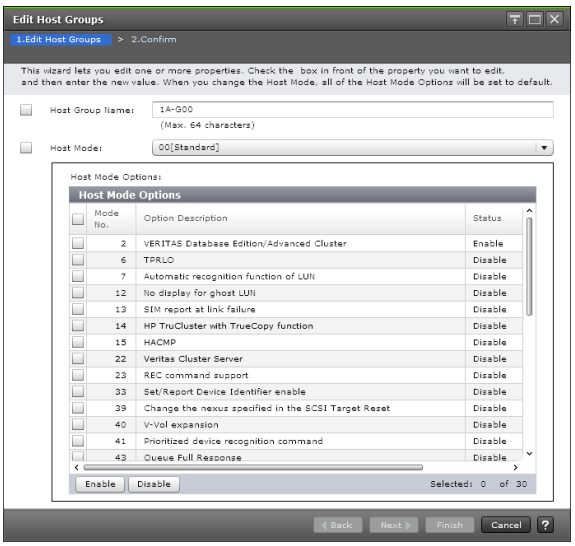
1. Select [Storage Systems]-[Ports/Host Groups/iSCSI Targets]. Click the [Host Groups/iSCSI Targets] tab.



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].

Copyright © 2015, 2017, Hitachi, Ltd.

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



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

Copyright © 2015, 2017, Hitachi, Ltd.

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].

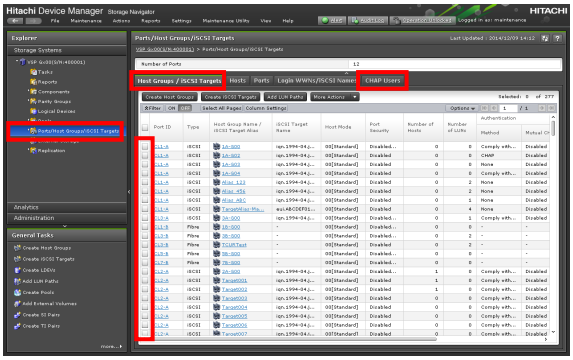
6. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

Copyright © 2015, 2017, Hitachi, Ltd.

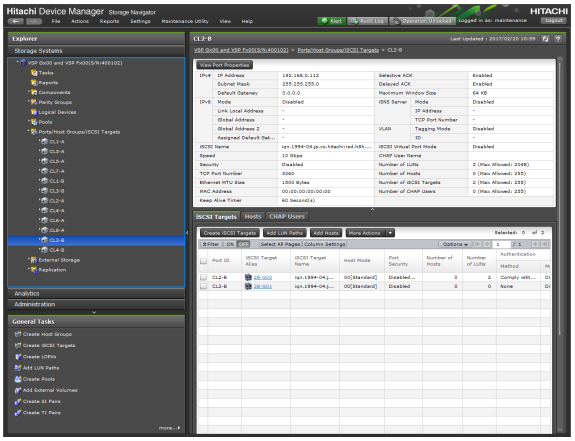
4.1.4.2 Configuring iSCSI Target Information

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.



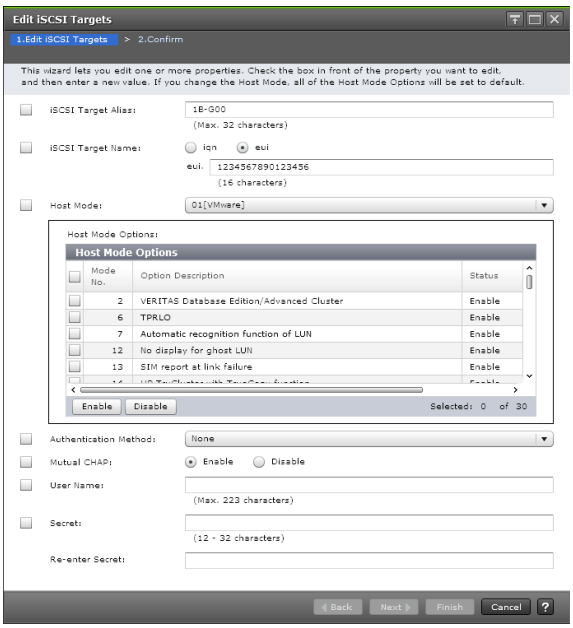
2. Check the [Type] is specified [iSCSI], and then check the check box of the port that you want to edit.



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

Copyright © 2015, 2017, Hitachi, Ltd.

4. 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.
iSCSI Target Name		[ign] or [eui]: Select either format.
		Text box: Enter an iSCSI target name. • The following describes the iqn format. Format: iqn.1994-04.jp.co.hitachi:rsd. Model name.t. Serial number. Port name iSCSI target ID Display example: iqn.1994-04.jp.co.hitachi:rsd.h8s.t.62507. (Port ID) (iSCSI target ID) You can use up to 219 ASCII characters (alphanumeric characters and symbols). However, you cannot use the following symbols. \ / , ; * ? “ < > | • The eui format is described. Format: eui. (OUI6 digits) (Storage System fixed value) (Serial number) (Port name) (iSCSI target ID) Display example: eui.02004567A425678D You can use alphanumeric characters with 16 characters fixed.
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.

Copyright © 2015, 2017, Hitachi, Ltd.

Item	Description
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.

Copyright © 2015, 2017, Hitachi, Ltd.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

4.2 Managing Drives

NOTE: iSCSI in this Chapter indicates iSCSI (optic/copper) of the Channel Board.
(Model name: DW-F800-2HS10B/2HS10S)
Regarding iSCSI for NAS Module, see "File Service Administration Guide".

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.

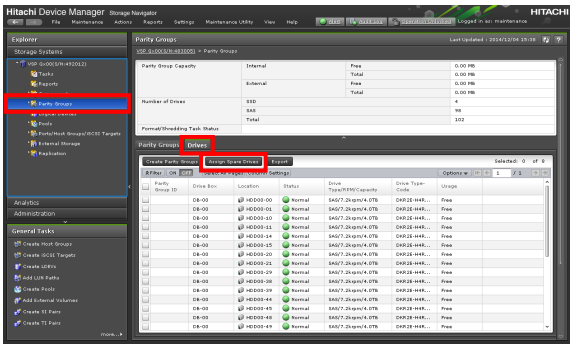
4.2.1.1 Guidelines When Allocating Spare Drives

- 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.
  CBSS/CBSL: 16 spare disks
  CBLM2/CBLM3: 32 spare disks
  CBLH: 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".

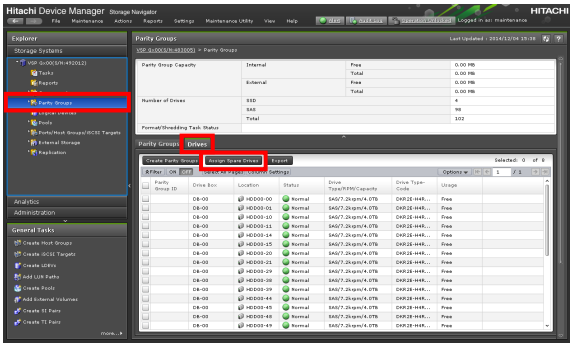


Item	Description
Parity Group ID	Number of the parity groups
Drive Box	Drive Box
Location	Location of the spare drive
Status	A status of the drive
Drive Type/RPM/ Capacity	Displays the drive type, round-per-minute (RPM), and capacity.
Drive type code	Display a drive type code
Usage	Usage of the drive

Copyright © 2015, 2017, Hitachi, Ltd.

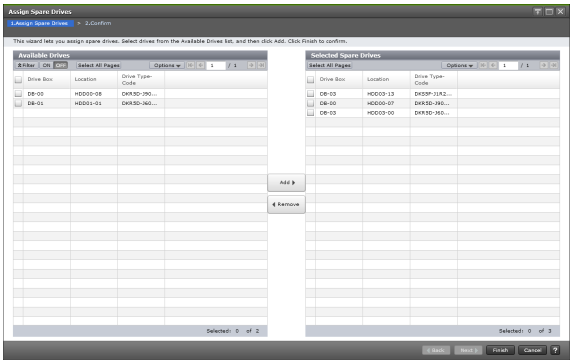
4.2.1.3 Allocating/Deleting Spare Drives

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 assiging 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 drives 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.

Copyright © 2015, 2017, Hitachi, Ltd.

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].

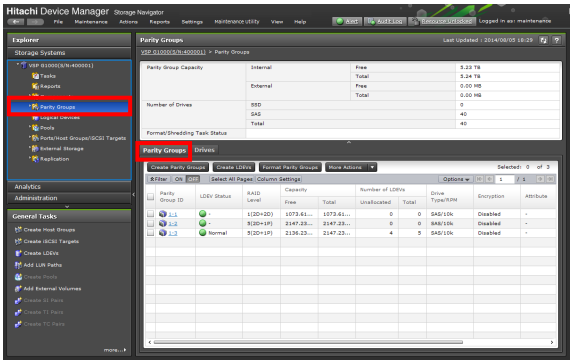
7. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

Copyright © 2015, 2017, Hitachi, Ltd.

4.2.2 Managing Parity Group

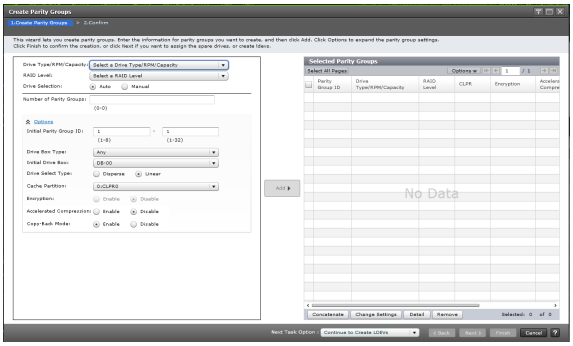
4.2.2.1 Creating Parity Group

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.



NOTE: When the Firmware version is less than 83-03-01-x0/xx, the Accelerated Compression is not displayed.

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.

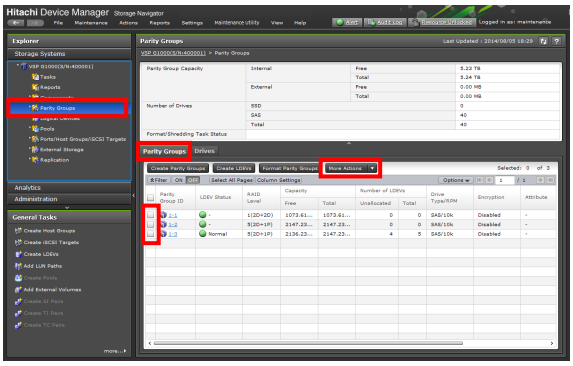
Copyright © 2015, 2017, Hitachi, Ltd.

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.

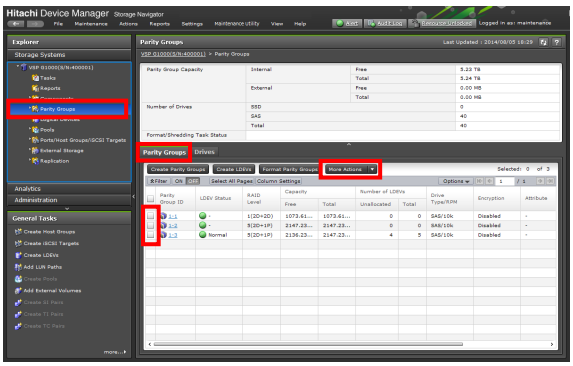


4.2.2.3 Deleting Parity Group

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

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

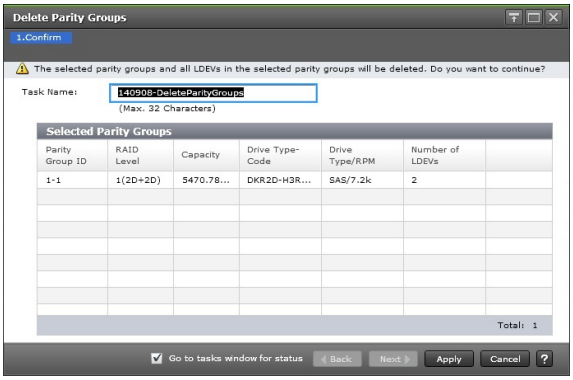
1. Select [Storage Systems]-[Parity Groups]. Click the [Parity Groups] tab.



Copyright © 2015, 2017, Hitachi, Ltd.

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].

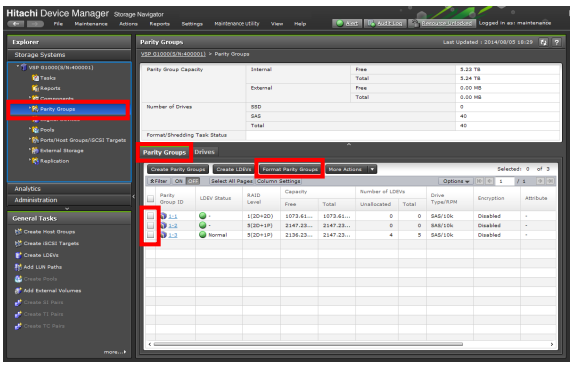
6. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

Copyright © 2015, 2017, Hitachi, Ltd.

4.2.2.4 Formatting Parity Group

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

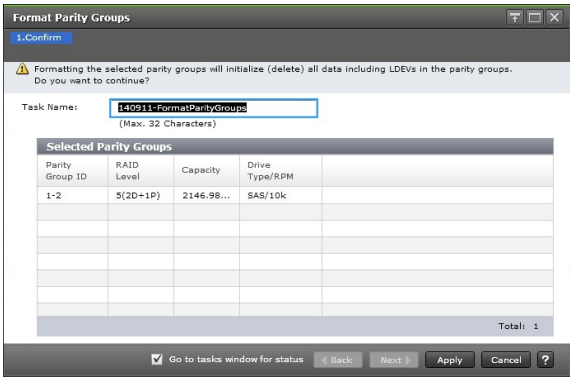
1. To format all LDEVs in the [Parity Groups], select the [Parity Groups].



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].



Copyright © 2015, 2017, Hitachi, Ltd.

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.

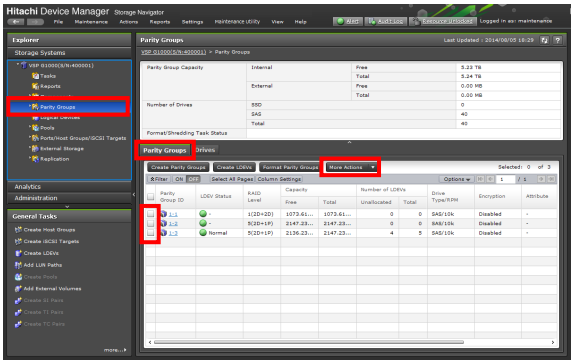
   NOTE: To display the “Task” window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

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

Copyright © 2015, 2017, Hitachi, Ltd.

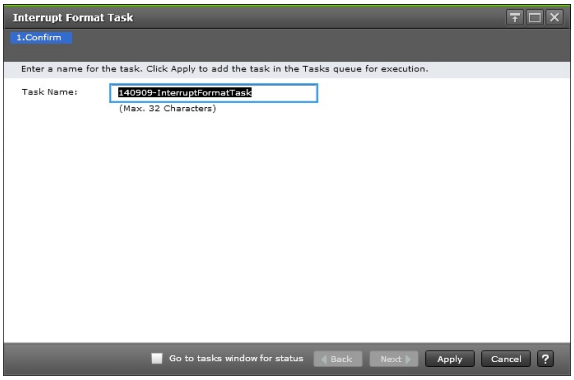
4.2.2.5 Interrupting Parity Group Format Task

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.

Copyright © 2015, 2017, Hitachi, Ltd.

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

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”.

Copyright © 2015, 2017, Hitachi, Ltd.

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

Copyright © 2015, 2017, Hitachi, Ltd.

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	Quick Format can be performed on multiple parity groups simultaneously. The number of those parity groups depends on the total of parity group entries. The number of entries is an indicator for controlling the number of parity groups on which Quick Format can be performed. The number of parity group entries depends on the drive capacity configuring each parity group. The number of entries for parity groups is as follows. • Parity group configured with drives of 8 TB or less: 1 entry • Parity group configured with drives of more than 8 TB: 2 entries The maximum number of entries on which Quick Format can be performed is as follows. • VSP G200: 18 entries • VSP G400, G600; VSP F400, F600: 36 entries • VSP G800; VSP F800: 72 entries The number of volumes on which Quick Format can be performed is not limited.
Concurrent Quick Format operations	Additional Quick Format can be executed during Quick Format execution. In this case, the total number of entries during Quick Format and those to be added is limited to the maximum number of entries per model.
Preliminary processing	At the beginning of the Quick Format operation, Web Console performs preliminary processing to generate management information. If a volume is undergoing preliminary processing, the Web Console main window shows the status of the volume as Preparing Quick Format. While preliminary processing is in progress, hosts cannot perform I/O access to the volume.

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from the preceding page)

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

Copyright © 2015, 2017, Hitachi, Ltd.

4.2.3.5 Formatting a Specific LDEV

This procedure performs Normal formatting on the volume.

CAUTION

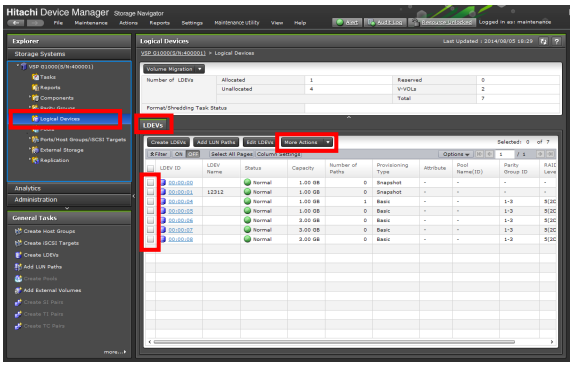
When a specified logical device is formatted, the user data within the specified logical device is lost. When incorrectly specifying a logical device, click Cancel and redo processing by selecting a logical device to be reformatted.

CAUTION

If the corresponding LDEV attribute is NAS Platform (System LU), proceed with the procedure in accordance with the guidance from the Technical Support Division.

NOTE: If the corresponding LDEV exists in the resource group for NAS Module (NAS_Platform_System_RSG), see "4.8.2 Removing LDEVs from Resource Group" to delete the LDEV from the resource group for NAS Module.

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

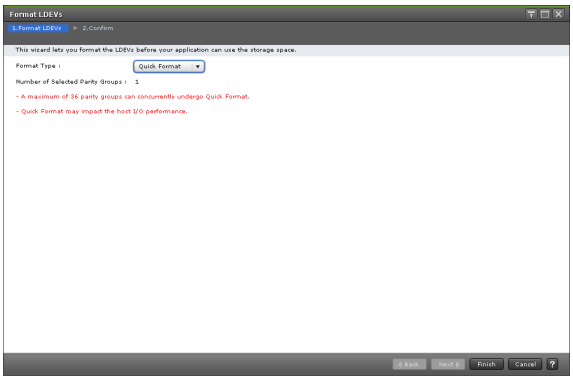


2. Select and block the LDEV to be formatted.
   See Blocking LDEV on "4.4.1 Blocking LDEVs" for blocking an internal volume. See the Hitachi Universal Volume Manager User Guide for blocking an external volume.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

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].

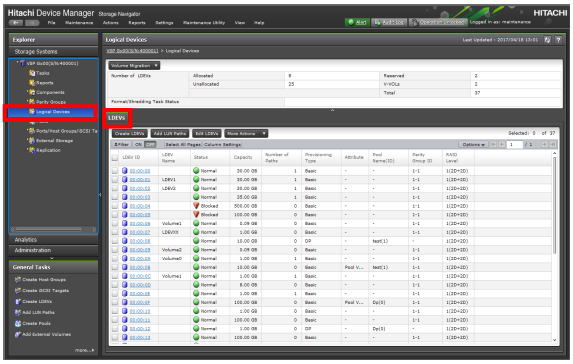
8. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

Copyright © 2015, 2017, Hitachi, Ltd.

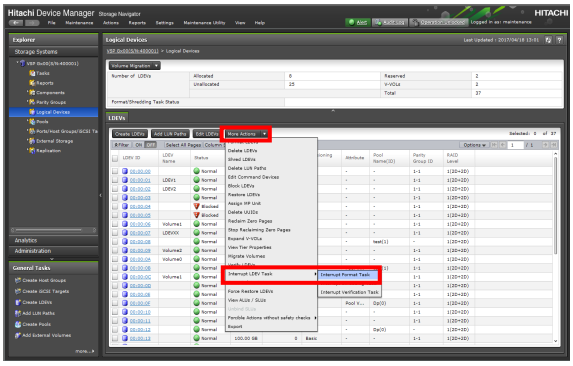
4.2.3.6 Interrupting Format Task

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

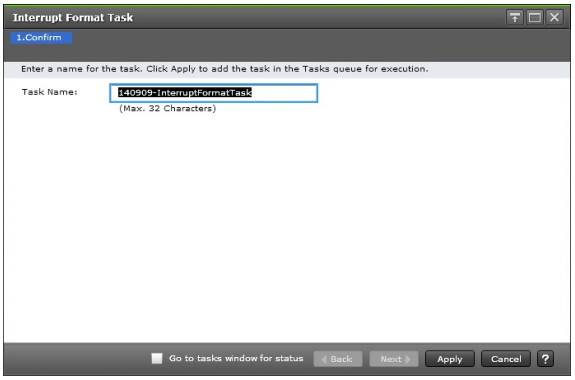
1. Select [Storage Systems]-[Logical Devices]. Click the [LDEVs] tab.



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	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>.

Copyright © 2015, 2017, Hitachi, Ltd.

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].

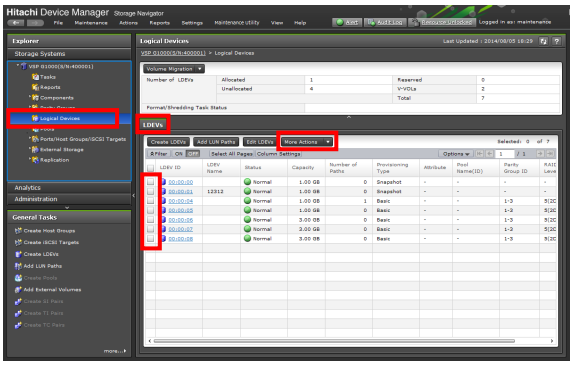
5. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

   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

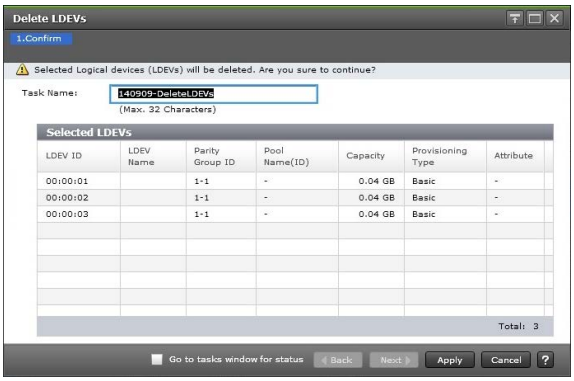
> **⚠ CAUTION**
>
> Deleting logical devices deletes all the data associated with them. Therefore, back up the data associated with logical devices before deleting them..

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



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

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



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

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from the preceding page)

Item	Description
Attribute	Displays the attribute of the LDEV. Command Device: Command device. ALU: LDEV of the ALU attribution. SLU: LDEV of the SLU attribution. NAS Platform (System LU): LDEV in which the system data of the NAS Unified Firmware is stored. This is displayed when the NAS Module is installed. NAS Platform (User LU): LDEV in which the NAS user data is stored. This is displayed when the NAS Module is installed. 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.

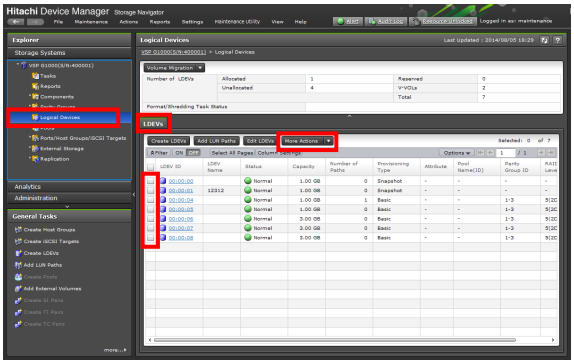
   NOTE: To display the “Task” window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

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

Copyright © 2015, 2017, Hitachi, Ltd.

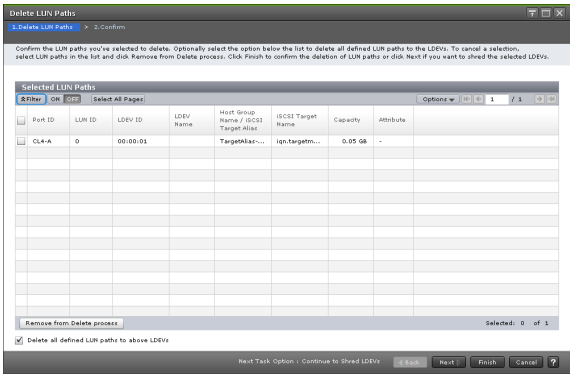
4.2.3.8 Releasing Logical Device Assignments

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. NAS Platform (System LU): LDEV in which the system data of the NAS Unified Firmware is stored. This is displayed when the NAS Module is installed. NAS Platform (User LU): LDEV in which the NAS user data is stored. This is displayed when the NAS Module is installed. -: Volume in which the attribute is not defined.

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(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].

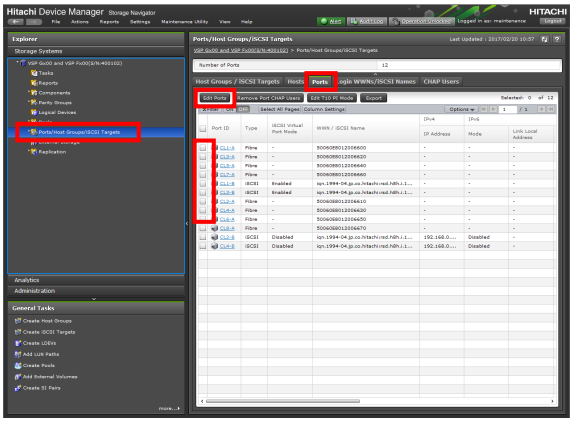
6. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

Copyright © 2015, 2017, Hitachi, Ltd.

4.3 Managing Port

4.3.1 Editing Fibre Channel

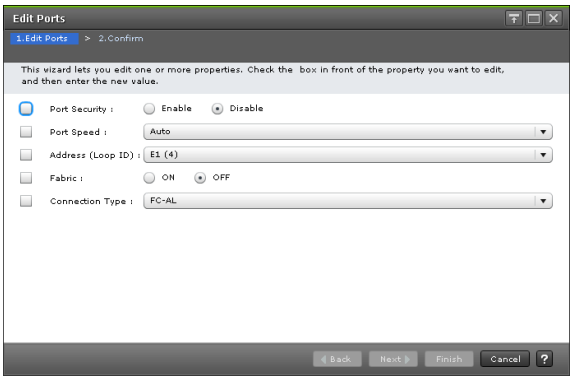
1. Select [Storage Systems]-[Ports/Host Groups/iSCSI Targets]. Click the [Ports] tab.



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.



Copyright © 2015, 2017, Hitachi, Ltd.

Item	Description
Port Security	Select whether LUN security is Enabled or Disabled.
Port Speed	Select the data transfer speed, in Gbps, for the selected Fibre Channel port. If Auto is selected, the storage system automatically sets the data transfer speed to 2, 4, 8, 16 or 32 Gbps. NOTE: If you are using 2-Gbps HBA and switch, set the transfer speed of the CHB (FC) (Fibre Channel adapter) port as 2 Gbps. If you are using 4-Gbps HBA and switch, set the transfer speed of the CHB (FC) port as 4 Gbps. If you are using 8-Gbps HBA and switch, set the transfer speed of the CHB (FC) port as 8 Gbps. If you are using 16-Gbps HBA and switch, set the transfer speed of the CHB (FC) port as 16-Gbps. If the Auto Negotiation setting is required, the linkup may become improper at server restart. Check a channel lamp, and if it is blinking, remove and re-insert the cable to perform the signal synchronization and linkup. If you are using 32-Gbps HBA and switch, set the transfer speed of the CHB (FC) port as 32 Gbps. When the transfer speed of the CHB (FC) port is set to Auto, the data might not be transferred at the maximum speed depending on the connected device. Confirm the transfer speed appearing in Speed in the Ports list when you start up the storage system, HBA, or switch. When the transfer speed is not the maximum speed, select the maximum speed from the list on the right or remove and reinsert the cable.
Address (Loop ID)	Select the address of the selected port.
Fabric	Select whether a fabric switch is set to ON or OFF.
Connection Type	Select the topology. • FC-AL: Fibre Channel arbitrated loop • P-to-P (point-to-point). NOTE: Some fabric switches require that you specify point-to-point topology. If you enable a fabric switch, check the documentation for the fabric switch to determine whether your switch requires point-to-point topology.

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

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

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

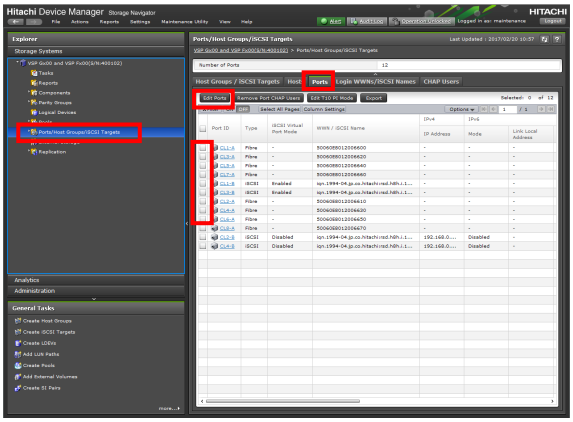
7. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

Copyright © 2015, 2017, Hitachi, Ltd.

4.3.2 Editing iSCSI

NOTE: iSCSI in this Chapter indicates iSCSI (optic/copper) of the Channel Board.
(Model name: DW-F800-2HS10B/2HS10S)
Regarding iSCSI for NAS Module, see "File Service Administration Guide".

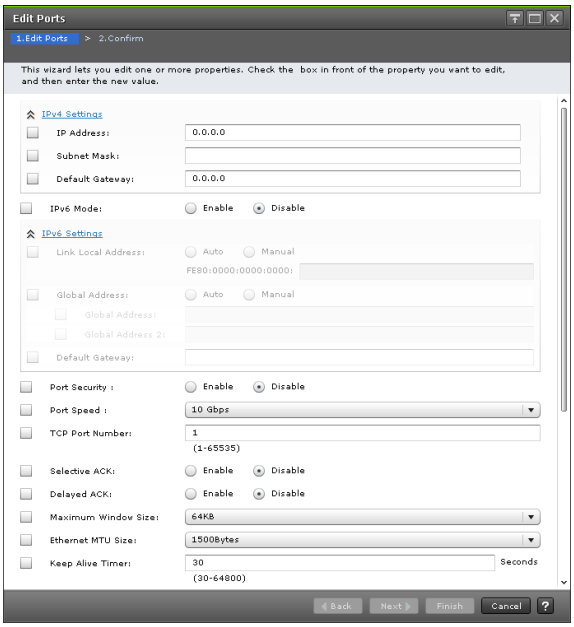
1. Select [Storage Systems]-[Ports/Host Groups/iSCSI Targets]. Click the [Ports] tab.



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.



Copyright © 2015, 2017, Hitachi, Ltd.

Information Setting Area (When Selecting iSCSI)

Item	Description
IPv4 settings (*1)	Set the information corresponding to IPv4. • [IP Address]: Enter an IP address. Note that, when selecting multiple ports, you cannot enter the IP address. • [Subnet Mask]: Enter a subnet mask. • [Default Gateway]: Enter a default gateway.
IPv6 mode (*1)	Set this to enable IPv6. • [Enable]: Enable the IPv6 mode. In this case, you can set each item of [Set IPv6]. • [Disable]: Disable the IPv6 mode.
IPv6 settings (*1)	Set the information corresponding to IPv6. • [Link Local Address]: Set a link local address. • [Auto]: Set a link local address automatically. • [Manual]: Set a link local address manually. Enter the address into the text box. • [Global Address]: Select the setting method of a global address from Auto or Manual. • [Auto]: Set a global address automatically. • [Manual]: Set a global address manually. • [Global Address]: When [Manual] is selected, enter an address into the global address 1. This item is a must for [Manual]. • [Global Address 2]: When [Manual] is selected, enter an address into the global address 2. This item is optional. • [Default Gateway]: Enter an address into the default gateway.
Port Security	Set the LUN security of the port. • [Enable]: Enable the LUN security of the port. • [Disable]: Disable the LUN security of the port.
Port Speed	Select the data transfer speed of the port. The unit is Gbps (Gigabit per second). Auto, 10 Gbps and 1 Gbps are selectable for Copper. Optic is fixed to 10 Gbps. When selecting [Auto], the transfer speed is set to 1 Gbps or 10 Gbps automatically by the Storage System. (*2)
TCP Port Number (*1)	Set a TCP port number.
Selective ACK (*1)	Set a selective ACK • [Enable]: Enable the selective ACK • [Disable]: Disable the selective ACK
Delayed ACK (*1)	Set a delayed ACK • [Enable]: Enable the delayed ACK. • [Disable]: Disable the delayed ACK.
Maximum Window Size (*1)	Set a maximum window size. The settable value is 64 KB, 128 KB, 256 KB, 512 KB or 1024 KB.
Ethernet MTU Size (*1)	Set an Ethernet MTU size. The settable value is 1500 bytes, 4500 bytes or 9000 bytes.

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(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.

*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].

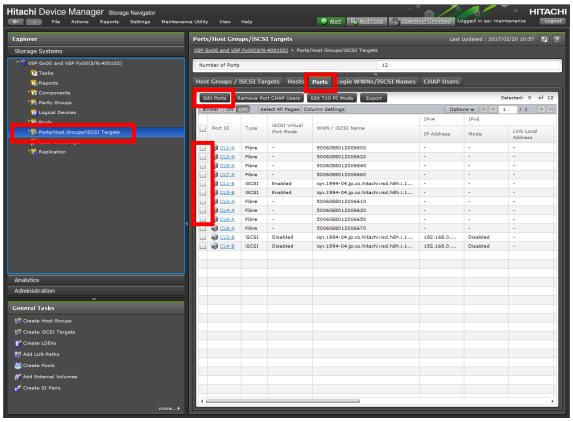
7. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

Copyright © 2015, 2017, Hitachi, Ltd.

4.3.3 Deleting Host Group Information

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

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

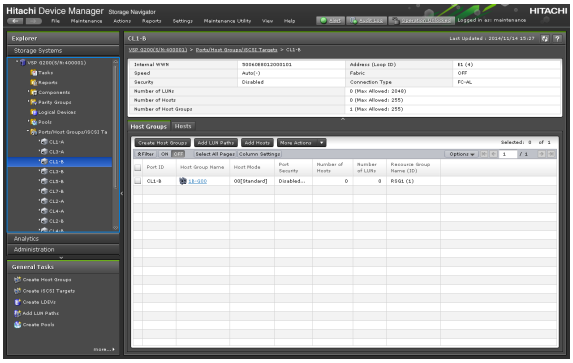


2. Check that any of [Fibre]/[NAS Platform (User LU)]/[NAS Platform (System LU)] is specified for [Type], and then click the port name that you want to edit.

3. The selected port window opens.

4. Click the [Host Groups] tab.

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



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

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

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

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

Copyright © 2015, 2017, Hitachi, Ltd.

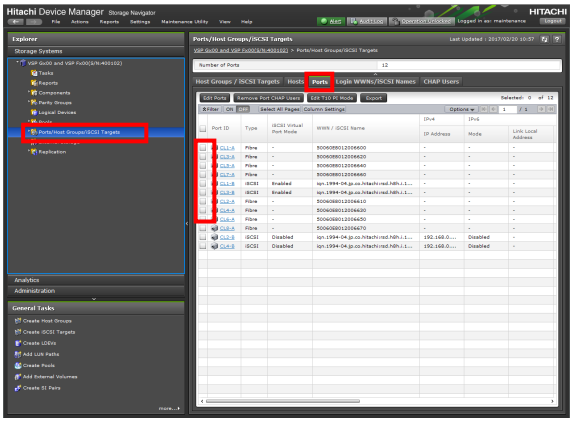
4.3.4 Deleting iSCSI Target Information

NOTE: iSCSI in this Chapter indicates iSCSI (optic/copper) of the Channel Board.
(Model name: DW-F800-2HS10B/2HS10S)
Regarding iSCSI for NAS Module, see "File Service Administration Guide".

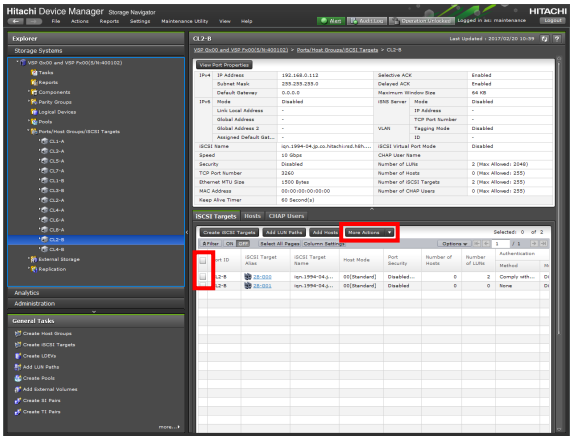
After you define target information for the iSCSI ports on your Storage System, use the following procedure to initialize the target information.

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.

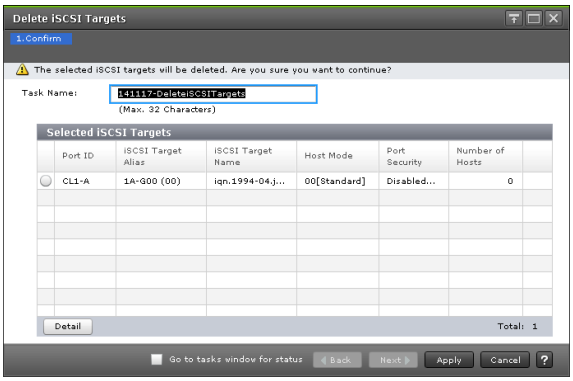
   NOTE: Check the [Type] is specified "iSCSI".



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].



3. 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.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

4.3.5 Using CHAP Authentication with iSCSI Ports

NOTE: iSCSI in this Chapter indicates iSCSI (optic/copper) of the Channel Board.
(Model name: DW-F800-2HS10B/2HS10S)
Regarding iSCSI for NAS Module, see "File Service Administration Guide".

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.

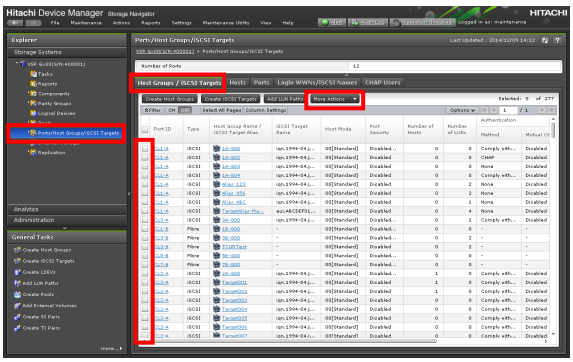
NOTICE:	If you enable CHAP authentication on the Storage System, configure it on the host server as well using the iSCSI initiator. If you replace an HBA in an attached host, change the iSCSI Name setting in CHAP. If changing the MTU size, make the change in the Storage System and at the switch/host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

Copyright © 2015, 2017, Hitachi, Ltd.

4.3.5.1 Configuring One-Way CHAP

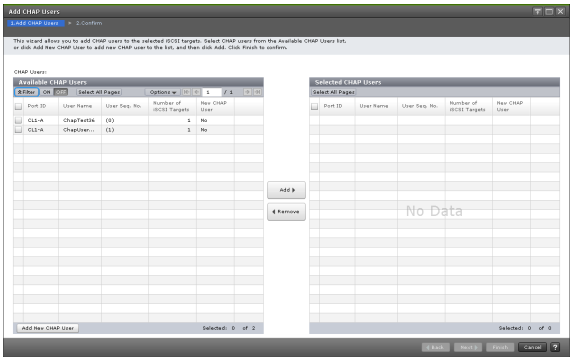
To set up one-way CHAP on the Storage System:

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.



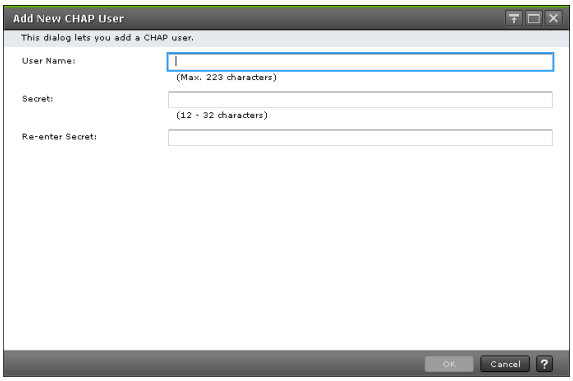
4. Click the [Finish] button.

Copyright © 2015, 2017, Hitachi, Ltd.

[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.

Copyright © 2015, 2017, Hitachi, Ltd.

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].

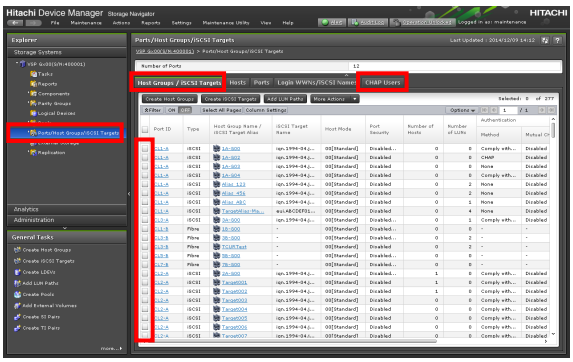
7. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

Copyright © 2015, 2017, Hitachi, Ltd.

4.3.5.2 Changing One-Way CHAP Settings

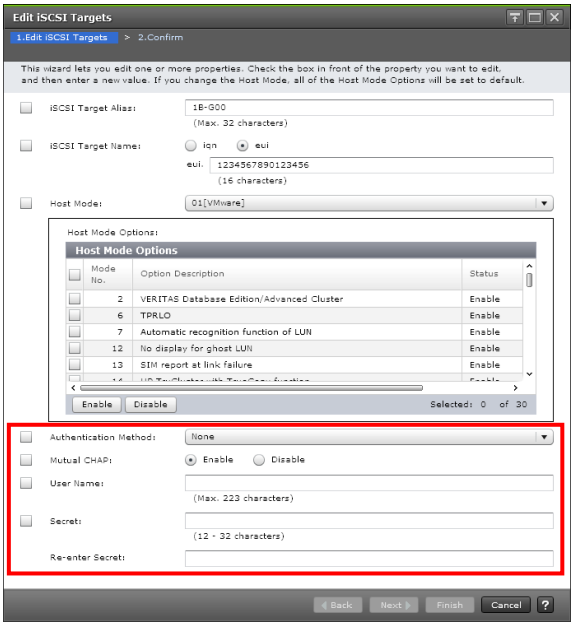
You can set the authentication mode in the “Edit iSCSI Targets” window.

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.



Copyright © 2015, 2017, Hitachi, Ltd.

Item		Description
iSCSI Target Alias		Display an iSCSI target alias.
iSCSI Target Name		[ign] or [eui]: Select either format.
		Text box: Enter an iSCSI target name. • The following describes the iqn format. Format: iqn.1994-04.jp.co.hitachi:rsd. Model name.t. Serial number. Port name iSCSI target ID Display example: iqn.1994-04.jp.co.hitachi:rsd.h8s.t.62507. (Port ID) (iSCSI target ID) You can use up to 219 ASCII characters (alphanumeric characters and symbols). However, you cannot use the following symbols. \ / , ; * ? " < > | • The eui format is described. Format: eui. (OUI6 digits) (Storage System fixed value) (Serial number) (Port name) (iSCSI target ID) Display example: eui.02004567A425678D You can use alphanumeric characters with 16 characters fixed.
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.

Copyright © 2015, 2017, Hitachi, Ltd.

Item	Description
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.

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.

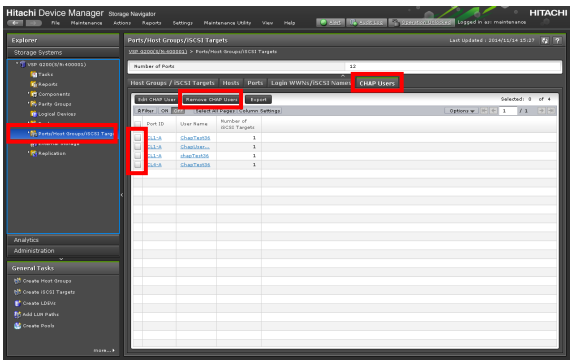
   NOTE: To display the “Task” window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

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

Copyright © 2015, 2017, Hitachi, Ltd.

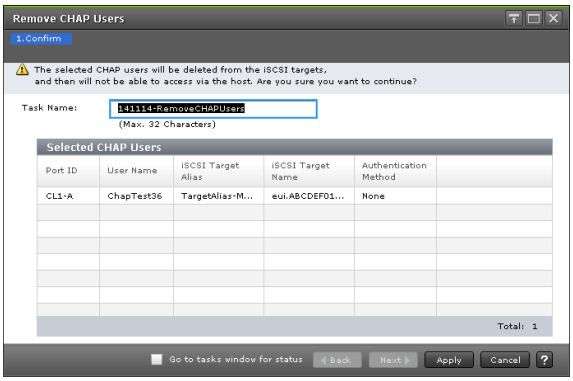
4.3.5.3 Deleting a One-Way CHAP User

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.

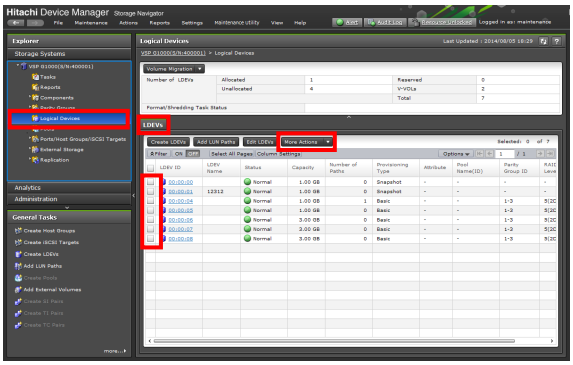
Copyright © 2015, 2017, Hitachi, Ltd.

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.



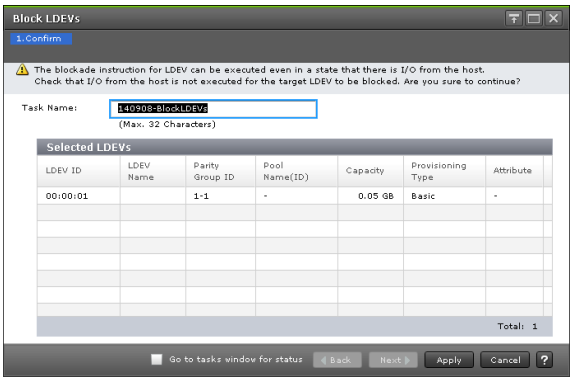
2. If [Blocked] does not appear in the [Status] column, you can use the following steps to block the LDEV. If [Blocked] does appear in the column, you can skip the remaining steps.

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

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

Copyright © 2015, 2017, Hitachi, Ltd.

5. 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.

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.

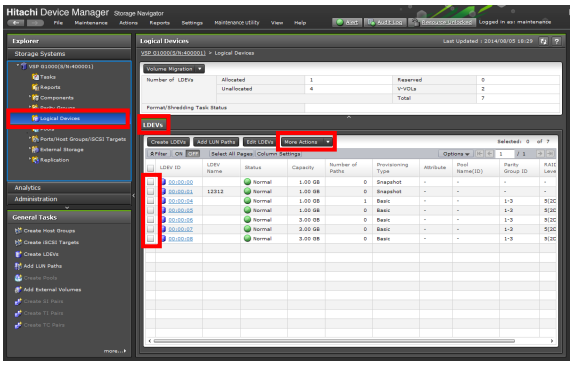
Copyright © 2015, 2017, Hitachi, Ltd.

4.4.2 Restoring Blocked LDEVs

⚠ CAUTION

If the corresponding LDEV attribute is NAS Platform (System LU), proceed with the procedure in accordance with the guidance from the Technical Support Division.

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



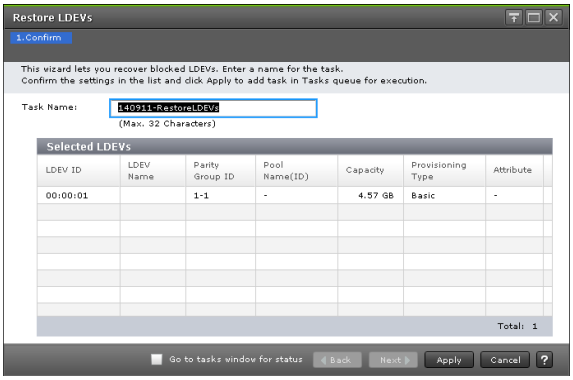
2. If [Blocked] appears in the [Status] column, you can use the following steps to restore the LDEV.
   If [Blocked] does not appear in the column, you can skip the remaining steps.

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

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

Copyright © 2015, 2017, Hitachi, Ltd.

5. 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.



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. NAS Platform (System LU): LDEV in which the system data of the NAS Unified Firmware is stored. This is displayed when the NAS Module is installed. NAS Platform (User LU): LDEV in which the NAS user data is stored. This is displayed when the NAS Module is installed. Hyphen (-): Volume in which the attribute is not defined.

Copyright © 2015, 2017, Hitachi, Ltd.

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].

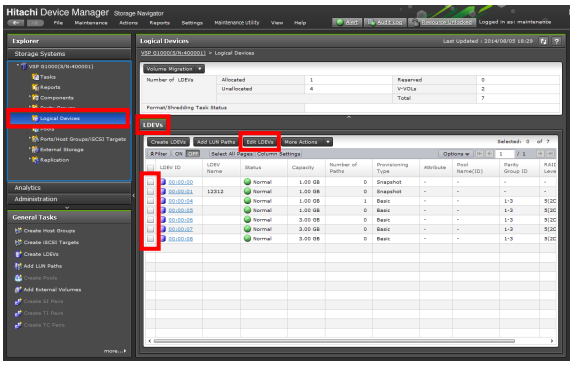
7. Check the operation result in the “Task” window. Before execution, you can suspend or cancel the task in the “Task” window.

Copyright © 2015, 2017, Hitachi, Ltd.

4.4.3 Editing an LDEV Name

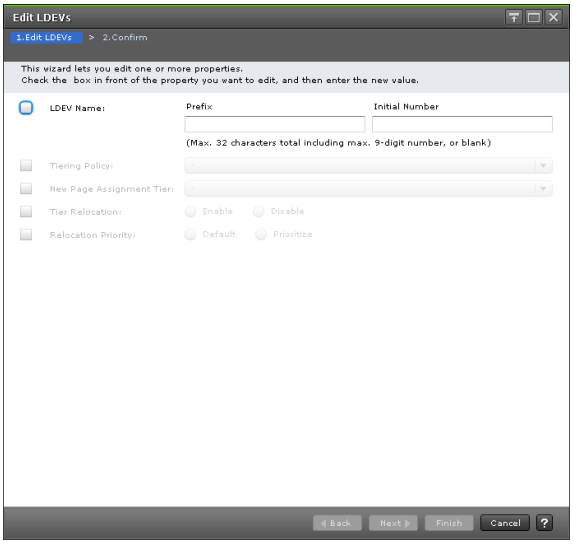
You can edit the name of a registered internal volume.
For information about editing a registered external volume, see Hitachi Universal Volume Manager User Guide.

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.



Copyright © 2015, 2017, Hitachi, Ltd.

Item	Description
LDEV Name	Specify the LDEV name, using up to 32 characters. • Prefix: Fixed character string. • Initial Number: Initial number. Specify the initial number according to these examples. Example: - 1: Up to 9 numbers are added (1, 2, 3 ... 9) - 08: Up to 92 numbers are added (08, 09, 10 ...99) - 23: Up to 77 numbers are added (23, 24, 25 ...99) - 098: Up to 902 numbers are added (098, 099, 100 ... 999)
Tiering Policy	Specify the tiering policy for the LDEV. For details about the setting. You can specify this function only when the V-VOLs using Dynamic Tiering/active flash are available. See “Provisioning Guide”.
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: • 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.

Copyright © 2015, 2017, Hitachi, Ltd.

4.4.4 Force Restore LDEVs

Prerequisites

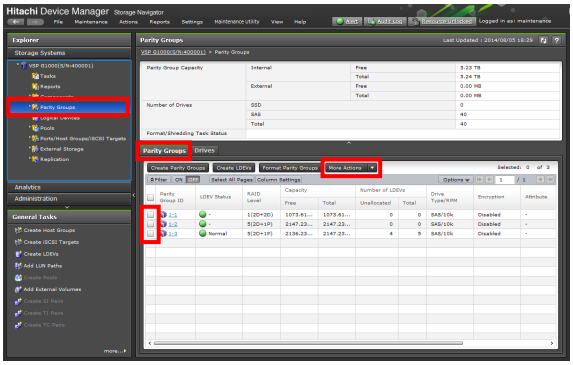
LDEVs to be restored forcibly should be blocked.

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

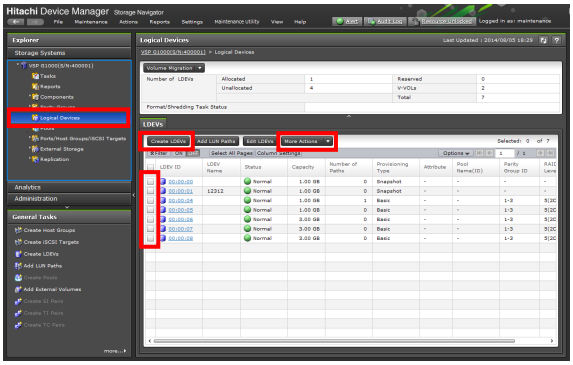
> **CAUTION**
>
> If the corresponding LDEV attribute is NAS Platform (System LU), proceed with the procedure in accordance with the guidance from the Technical Support Division.

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.



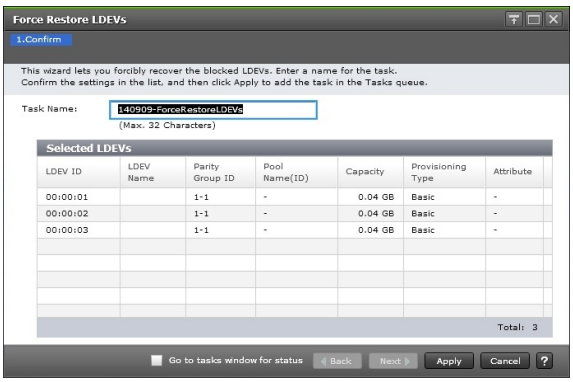
   (2) When forcibly restoring each LDEV.
   Select [Logical Device] from the [Storage System] tree and display the [LDEV] tab. Select the heck box of the LDEV.



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

Copyright © 2015, 2017, Hitachi, Ltd.

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



[Selected LDEVs]

Item	Description
LDEV ID	LDEV indentifier, 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. NAS Platform (System LU): LDEV in which the system data of the NAS Unified Firmware is stored. This is displayed when the NAS Module is installed. NAS Platform (User LU): LDEV in which the NAS user data is stored. This is displayed when the NAS Module is installed. [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.

Copyright © 2015, 2017, Hitachi, Ltd.

4.5 WebConsole Operation

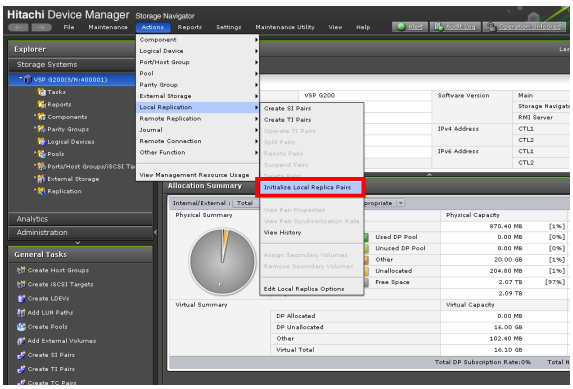
Web Console and Storage Navigator have the common window display and operation. Refer to the “System Administrator Guide” for the details.

Copyright © 2015, 2017, Hitachi, Ltd.

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.

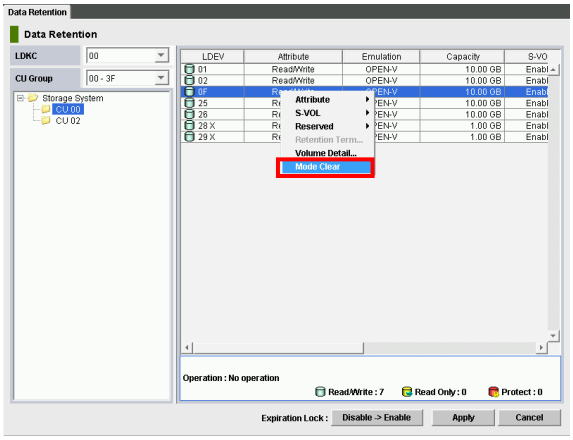
NOTE 1: Initializing local replica pairs cancels not only the pairs created by ShadowImage but the pairs created by Volume Migration and Thin Image.

NOTE 2: Perform the operation only when the Technical Support Division issues instructions.

Copyright © 2015, 2017, Hitachi, Ltd.

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”.

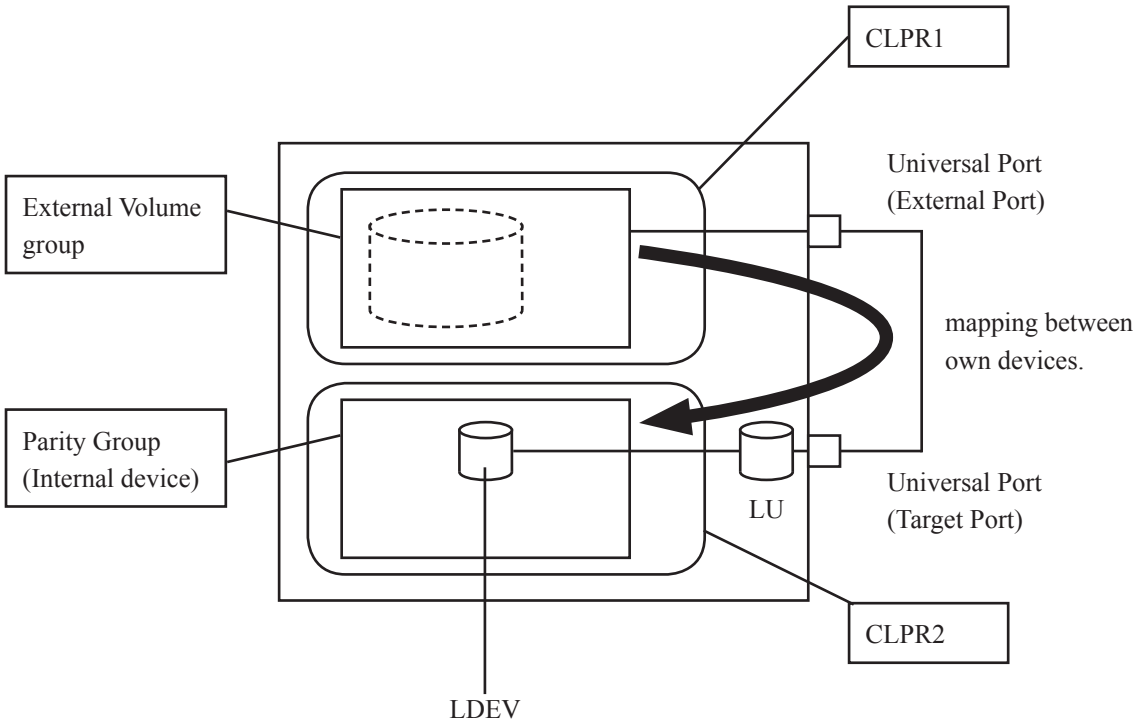
Copyright © 2015, 2017, Hitachi, Ltd.

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

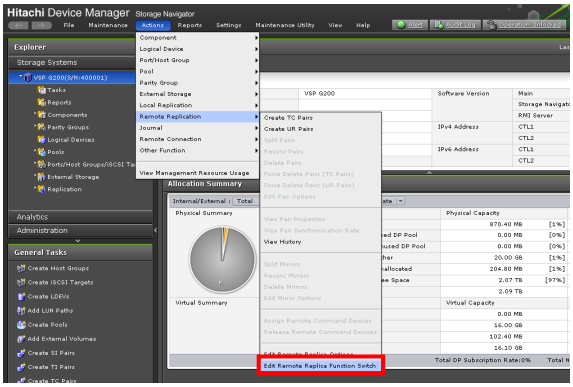


Copyright © 2015, 2017, Hitachi, Ltd.

4.5.4 Remote Replication

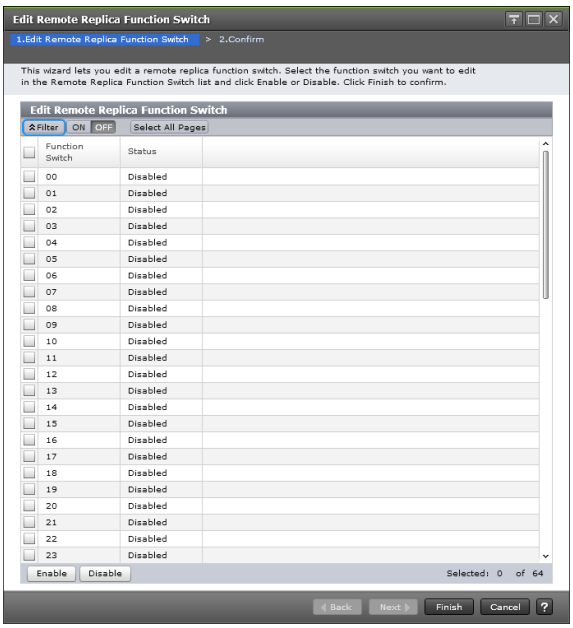
4.5.4.1 Remote Replica Function Switch

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.



Copyright © 2015, 2017, Hitachi, Ltd.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

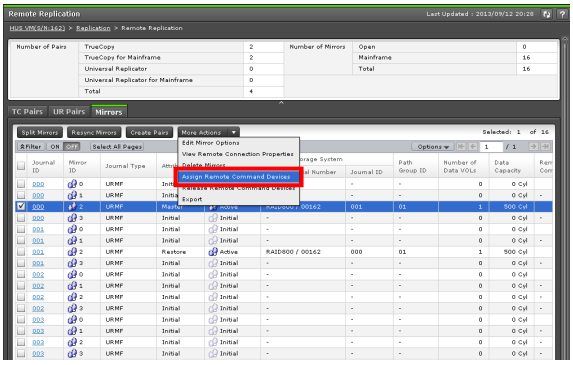
2. Remote Replica Function Switch
   The function allocated in each switch is as follows.

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. • 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.
41	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 #41 and #42.
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 #41 and #42.
43	In the function of switch #17 or switch #41 and #42, the path is blocked even if the number of path is less than that is set by minimum path.

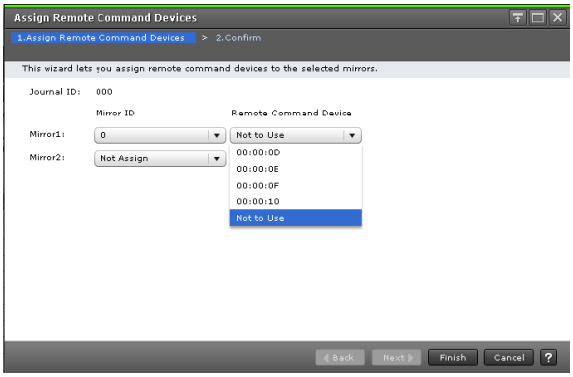
Copyright © 2015, 2017, Hitachi, Ltd.

4.5.4.2 Assign Remote Command Devices Window

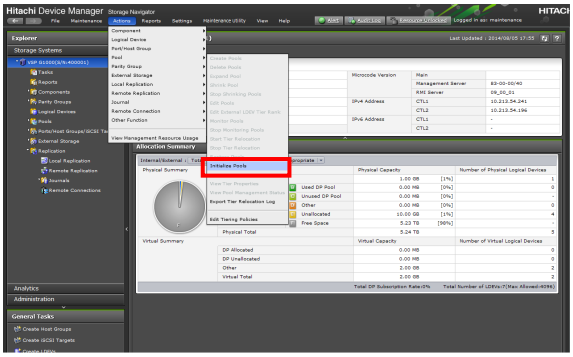
Click [Mirrors] at the application area of “Remote Replication” window.
Click mirrors in Initial, Active, Halt or Stopped state.
Click [Assign Remote Command Devices] to activate “Assign Remote Command Devices” window. (When mirrors other than above state are selected, the operation fails.)
Remote Command 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.

Copyright © 2015, 2017, Hitachi, Ltd.

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.

NOTE6: Perform the operation only when it is directed by the Technical Support Division.

Copyright © 2015, 2017, Hitachi, Ltd.

4.5.6 Performance Monitor

When using Performance Monitor in the Maintenance PC, perform the performance monitor function by reference to "5. The configuration when monitoring" of "1.2.1 Attachment Procedure of Maintenance PC".

NOTICE: The exclusive control is not applied to between Performance Monitor operating on the SVP and on the Maintenance PC. Therefore, be careful of the following items when using Performance Monitor in the Maintenance PC.

- Do not use Performance Monitor in the SVP and the Maintenance PC simultaneously (reference only is possible but not recommended from the point of view of operational error suppression).
- If performing the following edit and changes in the Maintenance PC while monitoring by the SVP, the monitor data stored in the SVP is damaged. In this case, set the "Monitoring Switch" window to [Disable] in the SVP. After that, set it to [Enable] to discard the existing monitor data and store new monitor data. See "3. Change the monitoring status" of "8. Monitoring" for changing the monitoring status.
  - Editing the monitoring switch
  - Changing the monitoring interval
  - Changing the monitoring target CU
  - Changing the monitoring target WWN
- When connecting the Maintenance PC to the Controller Chassis in the state that the existing monitor data is stored in the Maintenance PC, the monitor data might not be stored. In that case, set the "Monitoring Switch" window to [Disable] on the Maintenance PC, and then change it to [Enable].

Copyright © 2015, 2017, Hitachi, Ltd.

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.

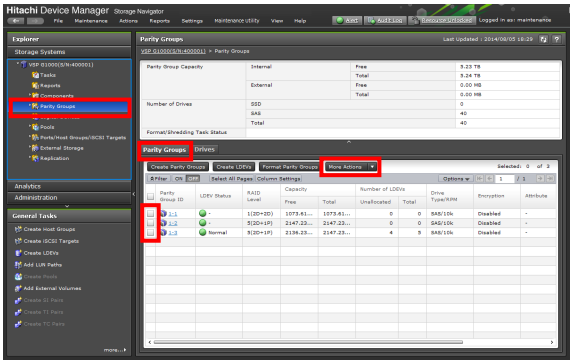
4.6.1 Setting the Copy Back

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.

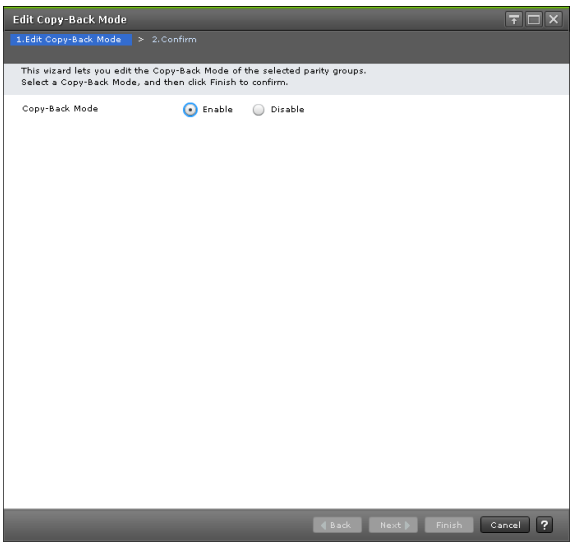


2. Select a target parity group.

3. Click [More Actions] - [Edit Copy-Back Mode].

Copyright © 2015, 2017, Hitachi, Ltd.

4. Select whether to execute the copy back or not in the “Edit Copy-Back Mode” window.



Item		Description
Copy-Back Mode	Enable	Perform the copy back when the failed HDD recovered.
	Disable	Do not perform the copy back when the failed HDD 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.

Copyright © 2015, 2017, Hitachi, Ltd.

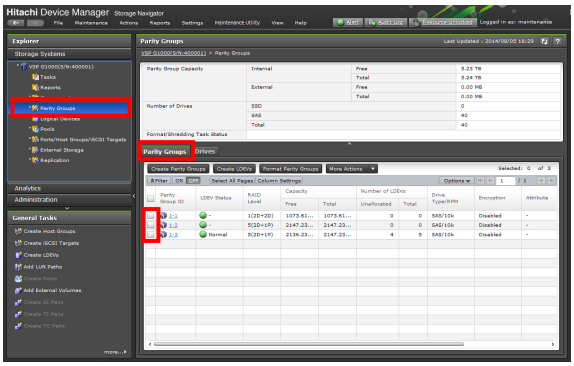
4.7 Verify（Parity Consistency Check）

4.7.1 Executing Verify（Parity Consistency Check）

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

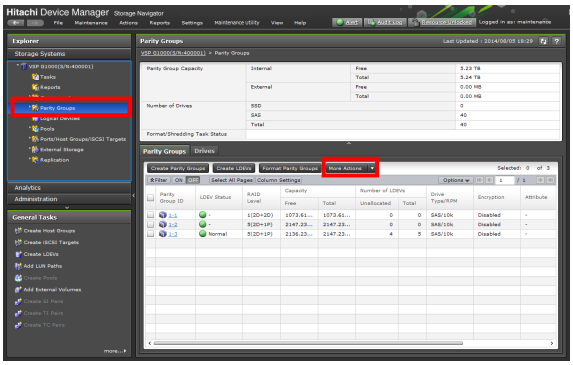
2. Set Verify from the [Parity Group] tab.
   - Select a parity group whose LDEV status is [Normal] or [Quick Format].
   - You can specify two or more parity groups. The number of parity groups you can specify is up to 16.
   - When specifying 17 or more parity groups, a message is displayed. Change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

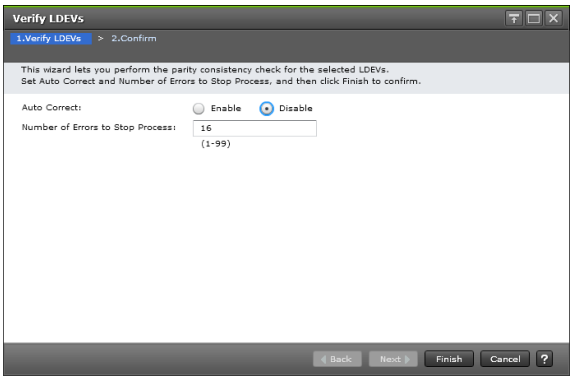


Copyright © 2015, 2017, Hitachi, Ltd.

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



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



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

5. Click the [Finish] button.

Copyright © 2015, 2017, Hitachi, Ltd.

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.

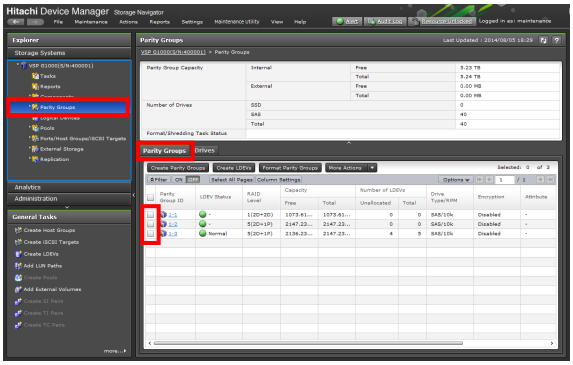
   NOTE: To display the “Task” window automatically after closing the wizard, select [Display Task Window after Clicking “Apply”] in the wizard and click [Apply].

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

Copyright © 2015, 2017, Hitachi, Ltd.

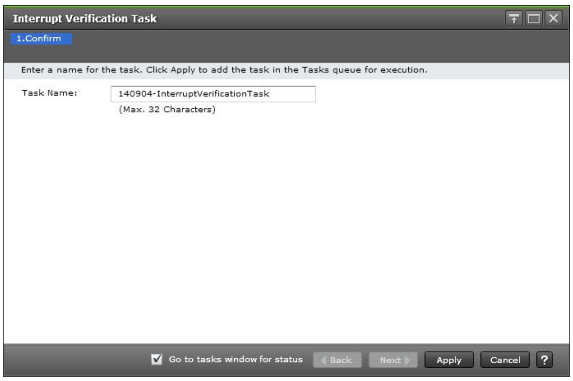
4.7.2 Interrupting Verify

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.

Copyright © 2015, 2017, Hitachi, Ltd.

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”.

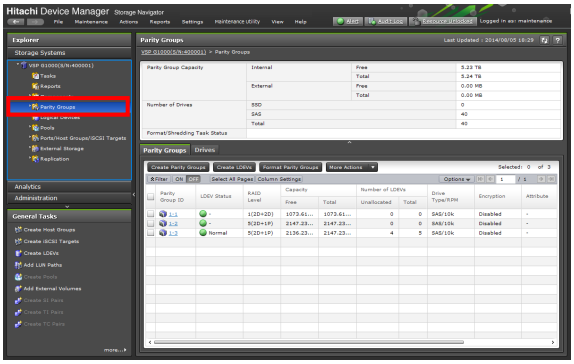
Check the progress in the “LDEV” window : Refer to “4.7.3.2 Checking the Progress in the “LDEV” Window”.

Check the progress with the task : Refer to “4.7.3.3 Checking the Progress in the Task”.

Copyright © 2015, 2017, Hitachi, Ltd.

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

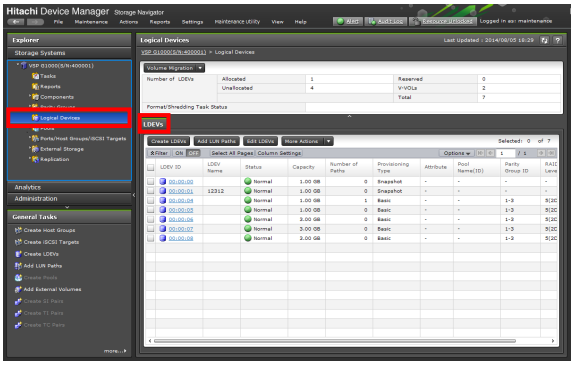
*1: [Free] does not include the capacity of the control information (e.g. control cylinder) used on the Storage System.

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

Copyright © 2015, 2017, Hitachi, Ltd.

4.7.3.2 Checking the Progress in the “LDEV” Window

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

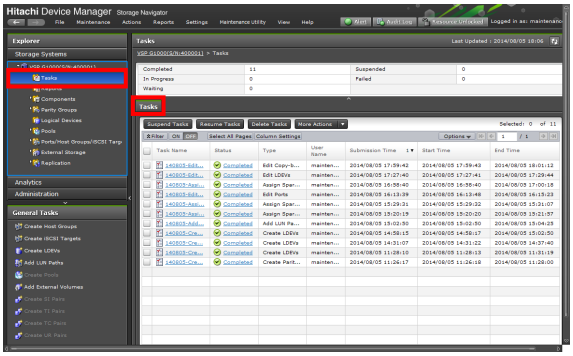


Item	Description
[Number of LDEVs]	Displays the information on the number of LDEVs. • [Defined]: Displays the number of LDEVs of the allocated open systems (excluding virtual VOLs). • [Undefined]: Displays the number of LDEVs of the unallocated open systems (excluding virtual VOLs). • [Reservation]: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

Copyright © 2015, 2017, Hitachi, Ltd.

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. • : 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.

Copyright © 2015, 2017, Hitachi, Ltd.

Item	Description
Auto Delete	Enabled: A task is automatically deleted when the following two events occur: • The task is completed • The number of tasks in the Task list reaches the maximum number the window can display (384) Disabled: Tasks will remain displayed until users delete them. Tasks whose status is Failed are automatically Disabled by the system.
[Suspend Tasks] button	Suspends the selected tasks. They will not be started even if the storage system is ready. Only waiting tasks can be suspended.
[Resume Tasks] button	Resume the selected tasks. The status goes back to waiting.
[Delete Tasks] button	Deletes the selected tasks from the window. • The waiting or suspended tasks will be cancelled. • The failed or aborted tasks can be deleted from the window. • Tasks in progress cannot be deleted. • If the maximum number of tasks displayed on the window is reached when Auto Delete is enabled, execution of a new task will result in automatic deletion of a task starting with the oldest one.
[Disable Auto Delete](*1)	When disabled, the selected task remains in the task list after the task is completed.
[Enable Auto Delete](*1)	When enabled, the selected task is deleted from the Task list when the following two events occur: • The task is completed • The number of tasks in the Task list reaches the maximum number the window can display (384)
[Export](*1)	Window for saving table information to a file.

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

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

Copyright © 2015, 2017, Hitachi, Ltd.

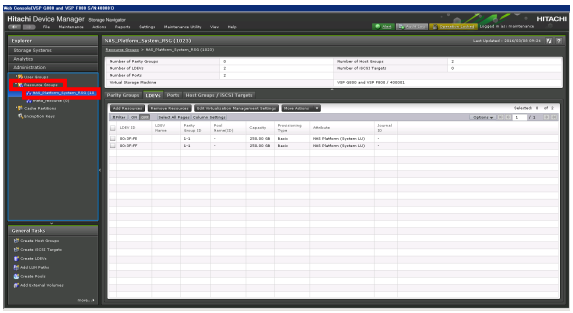
4.8 Managing Resource Group

4.8.1 Adding LDEVs to Resource Group

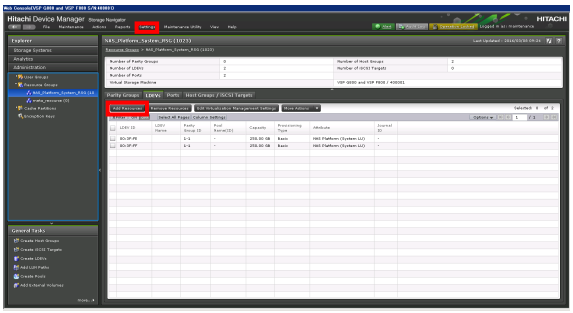
Add arbitrary LDEVs to an arbitrary resource group.

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.

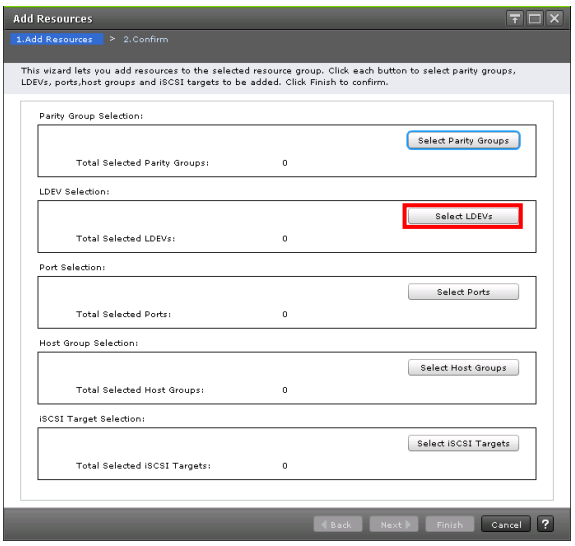


3. Display the “Add Resources” window in either of the following ways.
   - Click [Add Resources].
   - Select [Resource Administration] – [Add Resources] from the [Settings] menu.

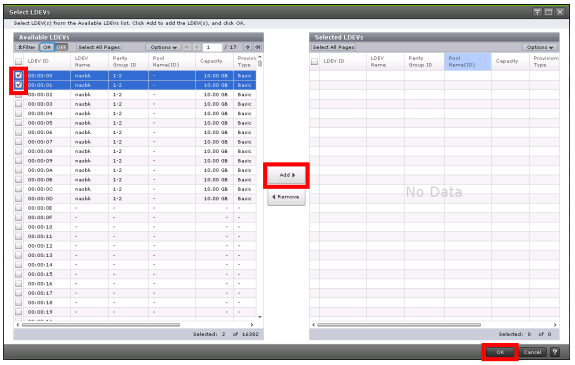


Copyright © 2015, 2017, Hitachi, Ltd.

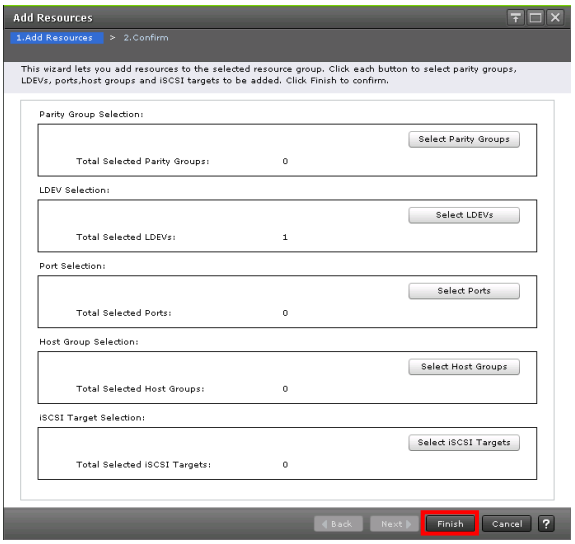
4. The “Add Resources” window is displayed. Click the [Select LDEVs] button.



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.

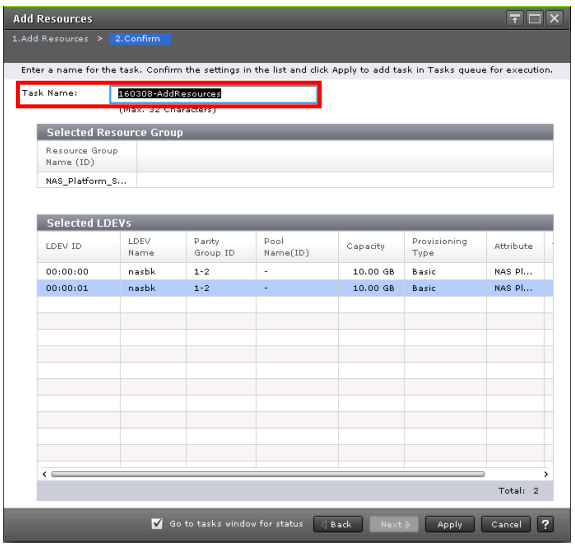


6. Return to the “Add Resources” window. Click the [Finish] button.



Copyright © 2015, 2017, Hitachi, Ltd.

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



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

   NOTE:
   - When adding the LDEVs to the NAS resource group (NAS_Platform_System_RSG), the password entry window is displayed. If the password entry window is displayed, enter the login password and click the [OK] button.
   - 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.

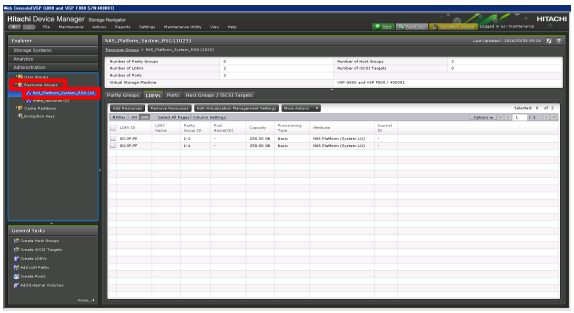
Copyright © 2015, 2017, Hitachi, Ltd.

4.8.2 Removing LDEVs from Resource Group

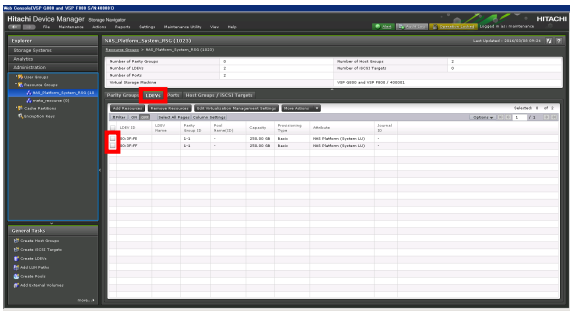
Remove arbitrary LDEVs belonging to an arbitrary resource group.

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

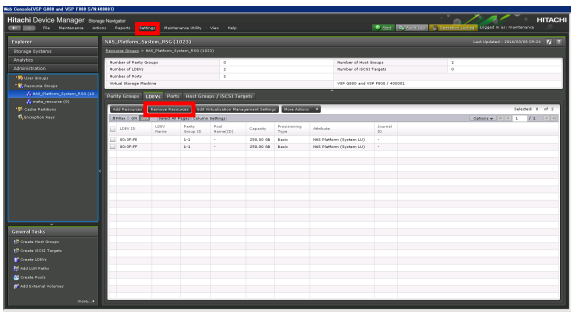
2. Click the resource group name to remove LDEVs under [Resource Groups].
   The individual “Resource Groups” window is displayed.



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

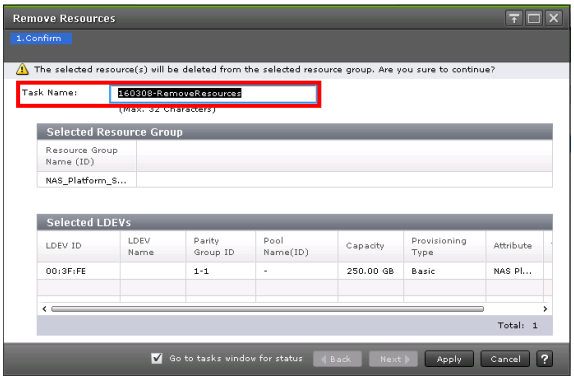


4. Display the “Remove Resources“ window in either of the following ways.
   - Click [Remove Resources].
   - Select [Resource Administration] – [Remove Resources] from the [Settings] menu.



Copyright © 2015, 2017, Hitachi, Ltd.

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



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

NOTE:
- When removing the LDEVs from the NAS resource group (NAS_Platform_System_RSG), the password entry window is displayed. If the password entry window is displayed, enter the login password and click the [OK] button.
- 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.

Copyright © 2015, 2017, Hitachi, Ltd.

5. Maintenance Function of Maintenance PC

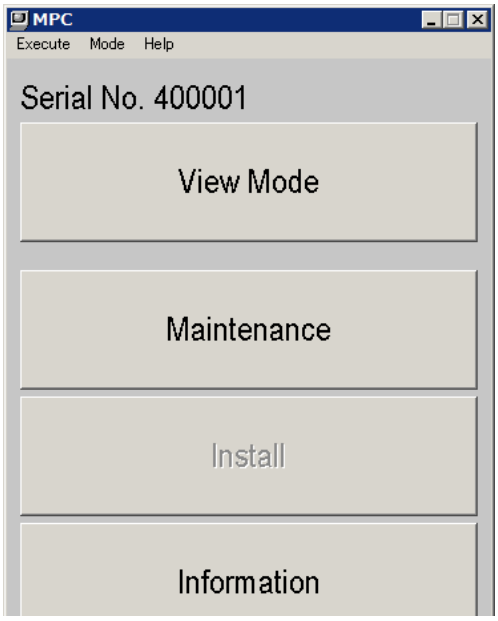
NOTICE: When a failure such as that the information cannot be acquired by the Storage System while operating the maintenance using the Maintenance PC, open the "Maintenance Utility" window and check the Storage System status. When a communication failure has occurred in the Storage System of the CTL 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")

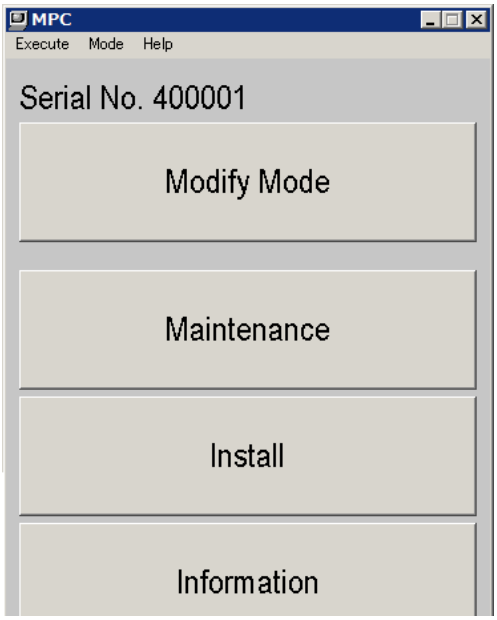
5.1 Mode

1. <View Mode>
In View Mode, referring to the Storage System status is allowed.



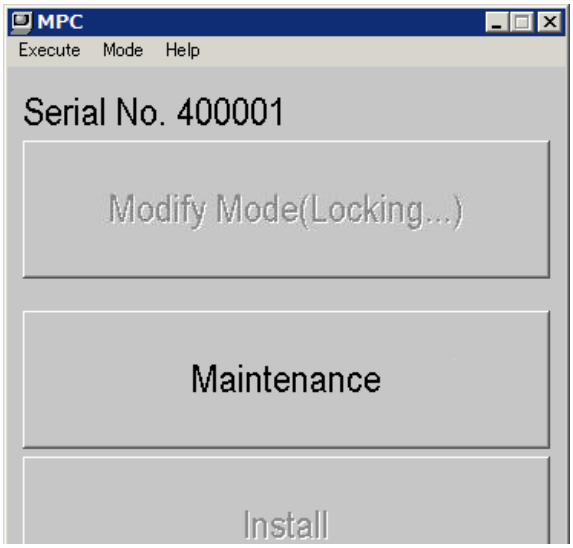
Copyright © 2015, 2017, Hitachi, Ltd.

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.

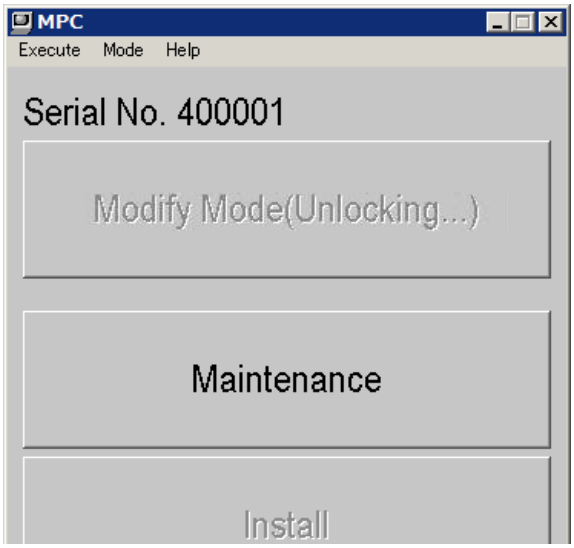


Copyright © 2015, 2017, Hitachi, Ltd.

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)

Copyright © 2015, 2017, Hitachi, Ltd.



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.	-
Create Configuration Backup	MPC05-910
All Configuration Files	MPC05-940
Restore Configuration	FIRM05-200
New Installation	FIRM05-10
Delete Log File	MPC05-370
Diagnosis (LAN Check etc.)	DIAG00-00
Auto Define Configuration	INST06-02-110

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.

Copyright © 2015, 2017, Hitachi, Ltd.

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 System Dumps" for the procedure. System dumps do not have NAS information. Therefore, when NAS Modules are installed in a Storage System, collect NAS dumps together. See "7.3.1 Collecting NAS Dumps Manually" for the procedure.

Collection Method	Description
Auto Dump (*1)	Use Auto Dump unless otherwise instructed by the Technical Support Division. See "[1] Auto Dump" for the procedure.
Exporting Dump (*1)	Use this when the "MPC" window is not displayed or you cannot log into the " MPC Software" window. See "1.8.1.2 Starting the Maintenance PC Window Only" for the procedure.
System Dump (*2)	Use this when no Maintenance PC exists or the Maintenance PC cannot connect to the Storage System. See "3.27 Acquiring System Dumps" for the procedure. System dumps do not have NAS information. Therefore, when NAS Modules are installed in a Storage System, collect NAS dumps together. See "7.3.1 Collecting NAS Dumps Manually" for the procedure.
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". Dump files collected manually do not have NAS information. Therefore, when NAS Modules are installed in a Storage System, collect NAS dumps together. See "7.3.1 Collecting NAS Dumps Manually" for the procedure.

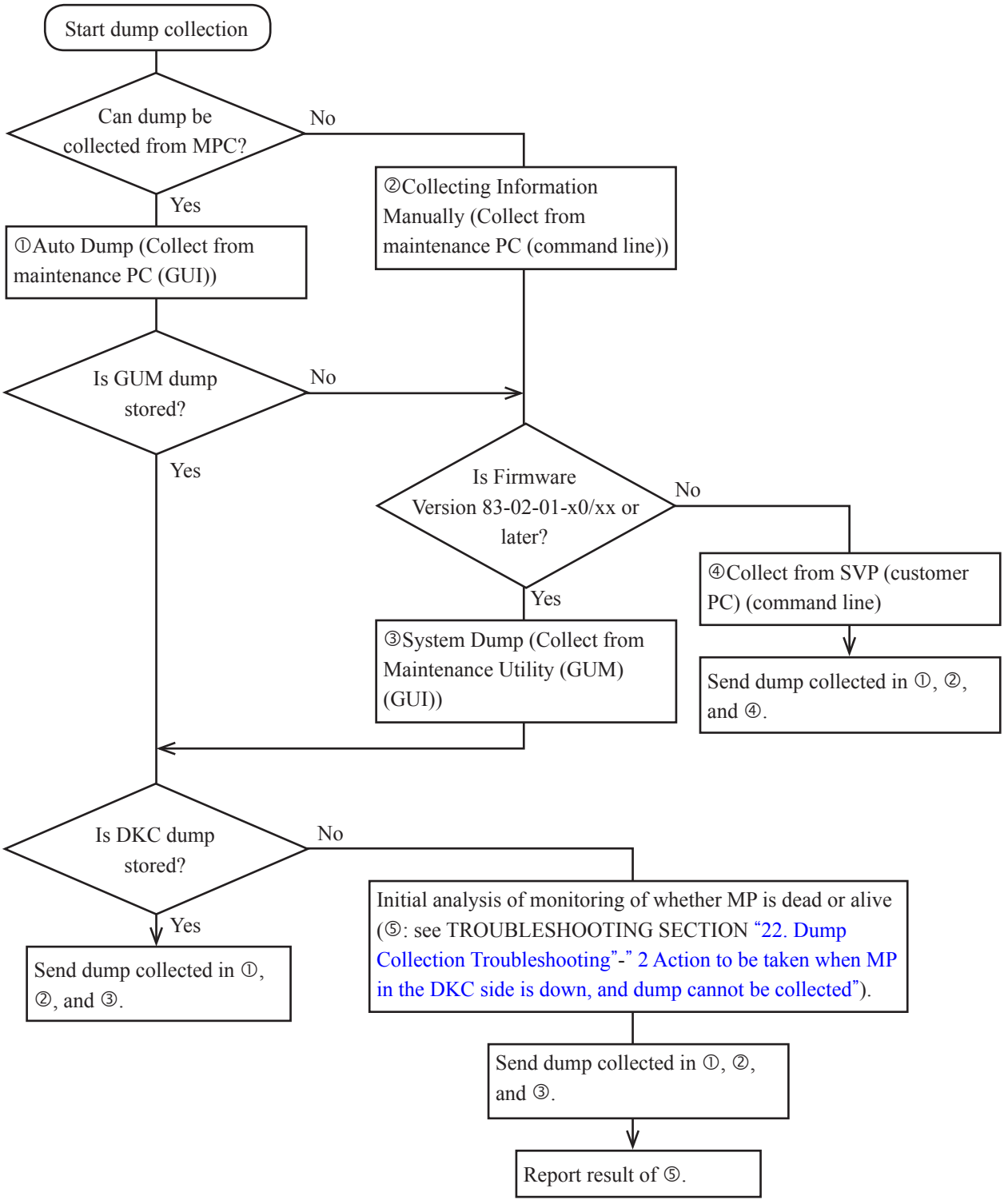
*1: You can collect NAS dumps by Auto Dump or dump export (Rapid, Normal or Detail), but not NAS-OS dumps.

*2: This function is supported in the firmware version 83-02-01 or later.

Copyright © 2015, 2017, Hitachi, Ltd.

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]



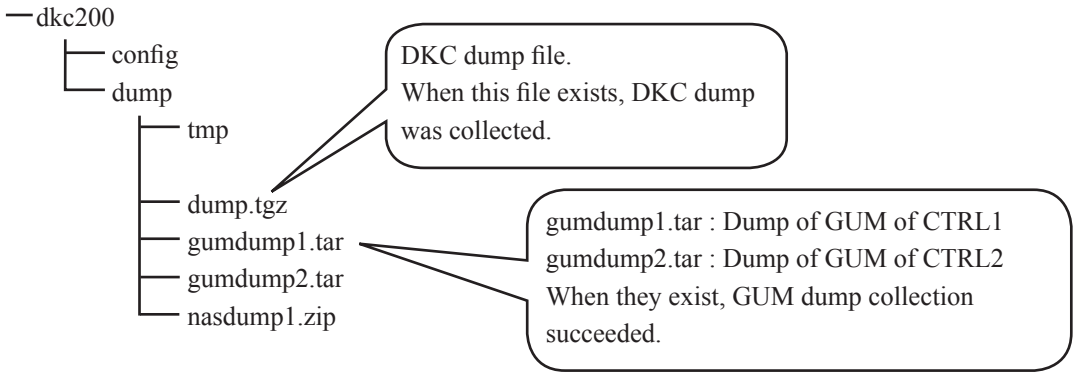
Copyright © 2015, 2017, Hitachi, Ltd.

[How to check if DKC dump and GUM dump are stored]

When dump is collected from SVP, hdcp.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 “22. 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”.
NAS Dump (*1)	See “7.3.1 Collecting NAS Dumps Manually”.
NAS-OS Dump (*1)	See “7.3.2 Collecting NAS-OS Dump”.

*1: This function is supported in the firmware version 83-03-21-x0/xx or later.

Copyright © 2015, 2017, Hitachi, Ltd.

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 Audo Dump is performed while the dump tool is running in the SVP, the acquired dump data might be lost. • Check that the system dump is not performed in Maintenance Utility. If Auto Dump is performed while the system dump is running, the acquired dump data might be lost.

NOTICE:	To run Auto Dump in the NAS Module-installed configuration, the Cache write pending rate needs to be less than or equal to 30%. If the condition is not met, the NAS Unified Firmware might not collect dumps. To check the Cache write pending rate, see "8. Monitoring"

1.

Select [Maintenance Components (General)] from the tool bar [Maintenance] in the "Web Console" window. See "1.2 Attachment / Removal Procedure of Maintenance PC" 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.

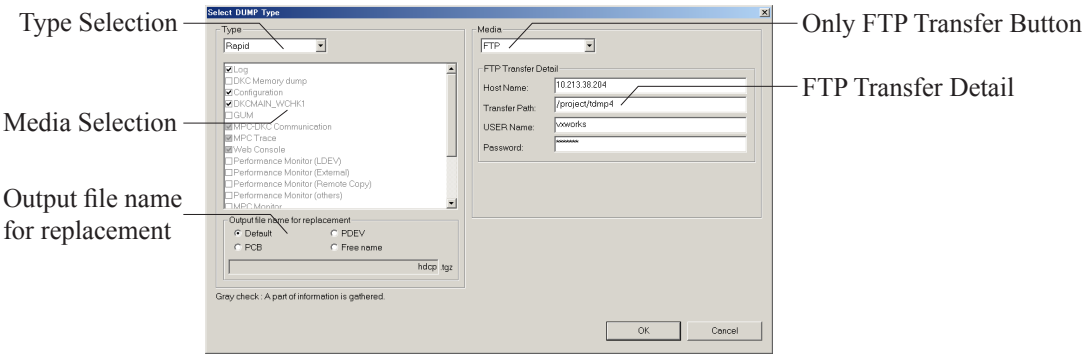
Copyright © 2015, 2017, Hitachi, Ltd.

3.

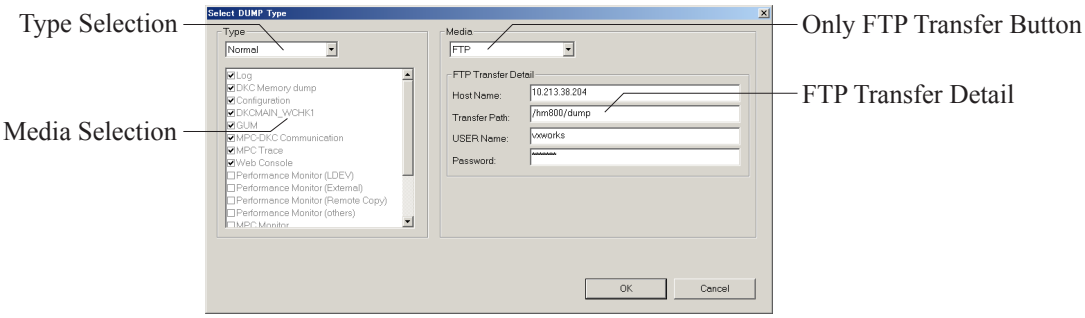
Select a dump type and a medium for output and make settings of the FTP transfer detail and the Client PC output detail, etc., and then click the [OK] button.
To stop the operation, click the [Cancel] button.

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.

- [When the Firmware version is 83-01-21-x0/xx or more]



- [When the Firmware version is less than 83-01-21-x0/xx]



Copyright © 2015, 2017, Hitachi, Ltd.

Table 5-2 Media in the Select Dump Type Window

Menu	Description
Rapid	This dump type is to get log information, Maintenance PC operation history, configuration information, or NAS dump information. Maintenance PC will compress these files automatically. 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.
Normal	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.
Detail	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.
DUMP	The dump of this type selects the processors and gets dumps from them individually.
NAS	The dump of this type collects NAS unified firmware dumps. They are collected from both CL1 and CL2.
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	The dump of this type selects source items from the detailed information items and collects information from them. (Refer to Table 5-3) 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".
No Gather	The dump of this type only outputs "C:\Mapp\wk\83xxxxyyyyyy\dkc200\tmp\", which has already been collected, to a directory set by the FTP transfer destination detail without compressing the data. The dump of this type can collect information only when "C:\Mapp\wk\83xxxxyyyyyy\dkc200\tmp\" exists and FTP is selected as a medium. • xxxx: Model name of DKC • yyyyyy: Serial number
MPC Memory dump	The dump of this type collects MPC Memory dump.

Copyright © 2015, 2017, Hitachi, Ltd.

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\83xxxxyyyyyy\dkc200\tmp\", log information, Maintenance PC registry information • 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
MPC Memory dump	MPC memory dump
NAS dump	NAS Unified Firmware dump of NAS

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 "hdcp.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. • "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. • "xxxxxxxxxxxx_xxxxxxx_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.

Copyright © 2015, 2017, Hitachi, Ltd.

Table 5-5 Media in the Select Dump Type Window

Menu	Description
HDD	Maintenance PC will store the compressed files to HDD. The file name is "C:\Mapp\wk\83xxxxyyyyyy\dkc200\tmp\". If you can transfer the files to your center directly, this type will be useful. • xxxx: Model name of DKC • yyyyyy: Serial number NOTE: Operating the maintenance may delete the compressed data. When performing the maintenance after data collection, transfer the data first. NOTE: When changing the file name setting by the Output file name for replacement, the file name to be output might be different from hdcp.tgz.
FTP	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.

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]

Copyright © 2015, 2017, Hitachi, Ltd.

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).

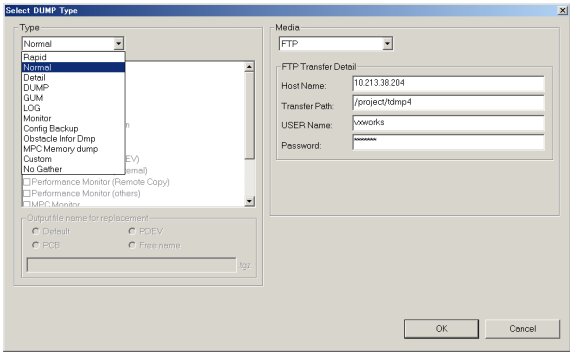
   When selecting “Rapid”, “NAS”, or “Custom” (in case of selecting any of “NAS dump” in the detailed gather items) for a dump type, DUMP is gathered.
   Go to Step (2).

   When selecting “DUMP”, “Log”, or “Custom” (in case of selecting any of “Log”, “DUMP”, and “DKCMAIN_WCHK1” in the detailed gather items) for a dump type, DUMP is gathered.
   Go to Step (3).

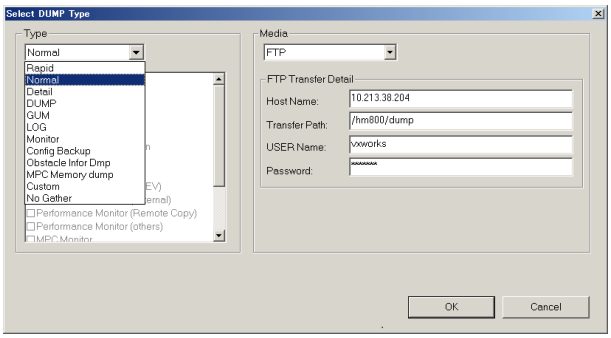
   When selecting “No Gather”, a message, “Do you want to output the already gathered dump information, log information, Maintenance PC operation history and operation information without gather them again?” is displayed. Clicking the [OK] button outputs the gathered ones to the selected media. It is not possible to output to HDD.
   Go to Step (5).

   When selecting other dump types, data is compressed.
   Go to Step (4).

   • [When the Firmware version is 83-01-21-x0/xx or more]



   • [When the Firmware version is less than 83-01-21-x0/xx]

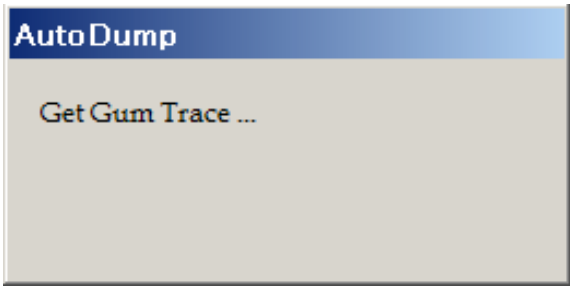


Copyright © 2015, 2017, Hitachi, Ltd.

(1) GUM Gather

The GUM gather GUM progress window is displayed.

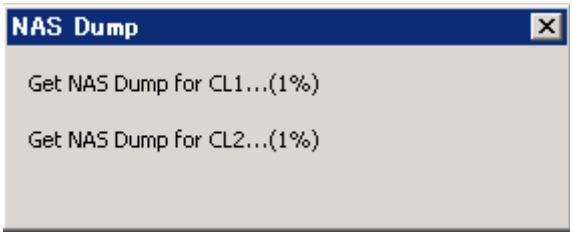
- When selecting “Normal”, “Detail”, or “Custom” (in case of selecting any of “NAS dump” in the detailed gather items), DUMP gather is required.
  Go to Step (2).
- When selecting “Custom” (in case of selecting any of “Log”, “DUMP”, and “DKCMAIN_WCHK1” in the detailed gather items), DUMP gather is required.
  Go to Step (3).
- When selecting “GUM” or “Custom” (in case of selecting none of “Log”, “DUMP”, and “DKCMAIN_WCHK1” in the detailed gather items), DUMP gather is not required.
  Go to Step (4).



(2) NAS Gather

The NAS dump gathering progress window is displayed. Since the NAS dump gathering is performed at the same time as “(3) DUMP Gather”, the progress window might not be displayed.

- When selecting “Rapid”, “Normal”, “Detail”, or “Custom” (in case of selecting any of ““Log”, “DUMP”, and “DKCMAIN_WCHK1” in the detailed gather items) for a dump type, DUMP is gathered.
  Go to Step (3).
- When selecting “Normal”, or “Custom” (in case of selecting none of “Log”, “DUMP”, and “DKCMAIN_WCHK1” in the detailed gathering items), DUMP gathering is not required.
  Go to Step (4).

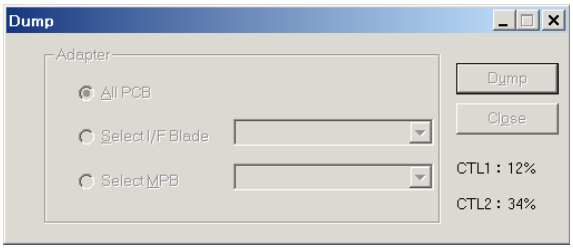


Copyright © 2015, 2017, Hitachi, Ltd.

(3) DUMP Gather

(a) The progress of DUMP gather

A box indicating progress of the dump is displayed.

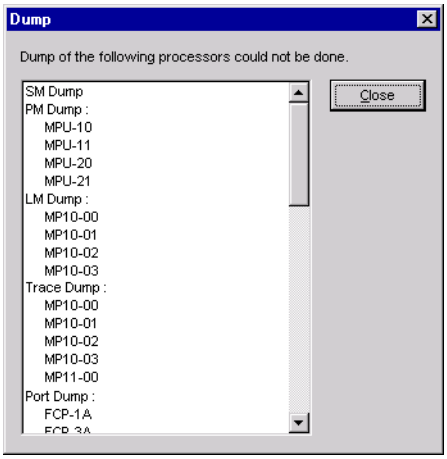


When the dump terminates normally, go to Step (4).

(b) When an error occurs

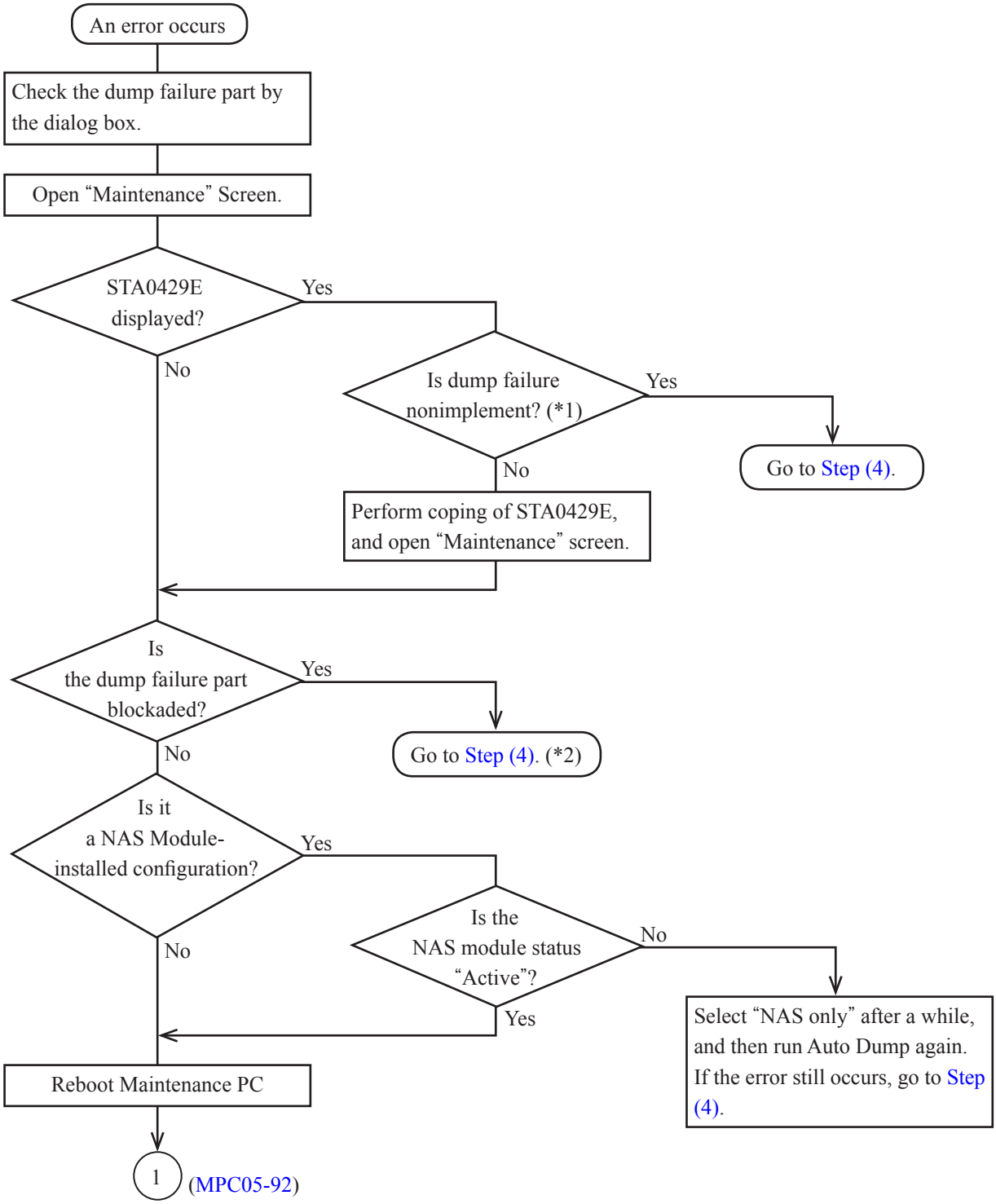
When an error occurs, the following dialog box is displayed.

For the action, retry it in accordance with [Dump Gather Procedure when Errors Occur] (MPC05-91).



Copyright © 2015, 2017, Hitachi, Ltd.

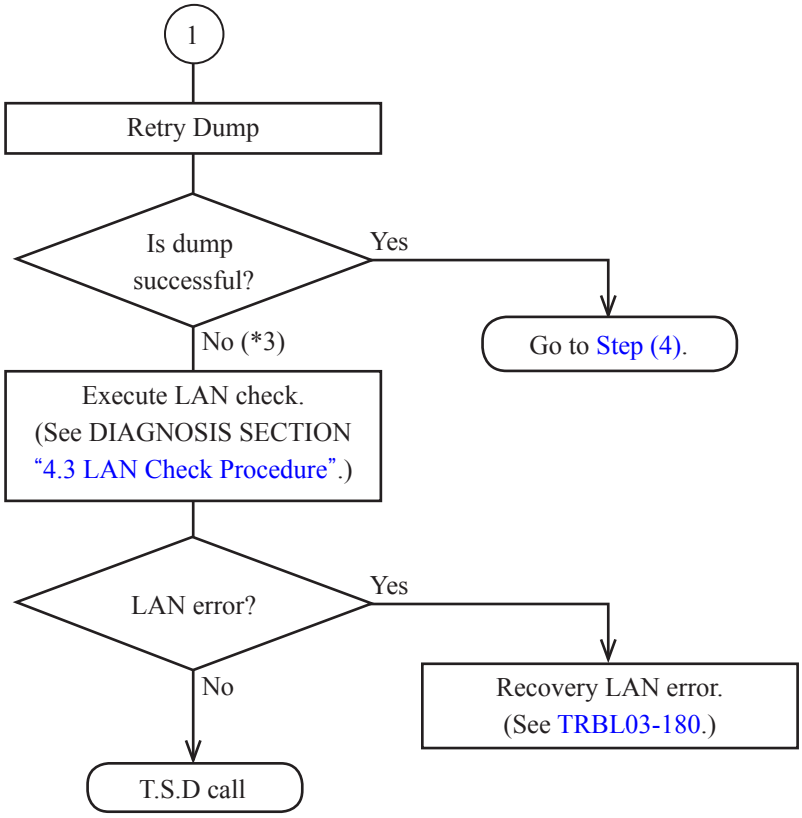
[Dump Gather Procedure when Errors Occur]



*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.

Copyright © 2015, 2017, Hitachi, Ltd.



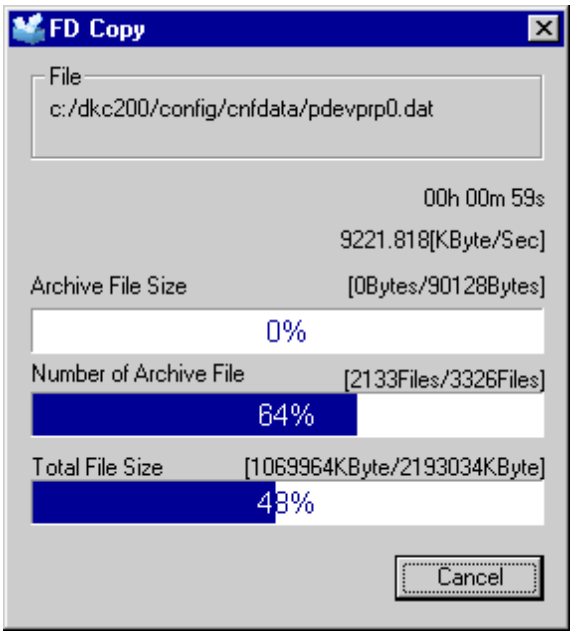
*3: Check the blockaded part by the Maintenance.

Copyright © 2015, 2017, Hitachi, Ltd.

(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.

Copyright © 2015, 2017, Hitachi, Ltd.

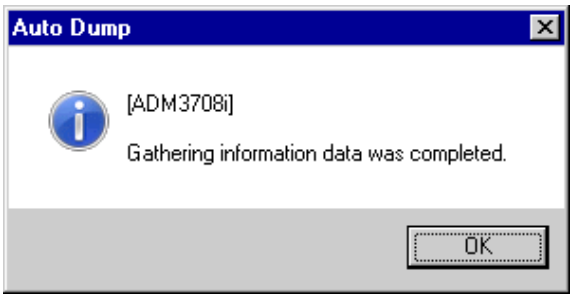
5. Output to a selected medium.
   An output is done to a selected medium

   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.

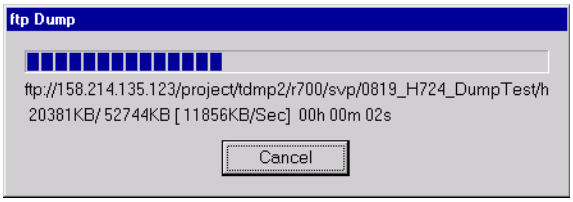


(b) Check that the dump file is stored in the following [Storage Destination].
[Storage Destination]: The dump file is stored under the "C:\Mapp\wk\83xxxx (DKC model name) yyyyyy (serial number) \dkc200\tmp" directory in the Maintenance PC.
The file name follows the setting in Table 5-4. The default name is "hdcp.tgz".

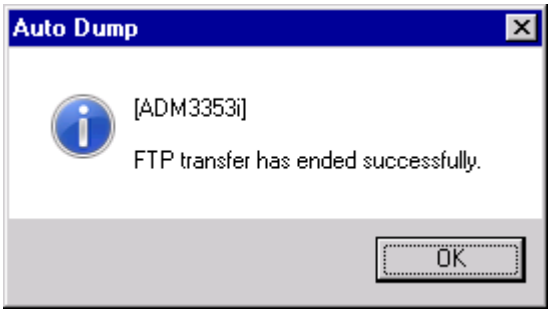
---

(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.



Copyright © 2015, 2017, Hitachi, Ltd.

(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”.

Copyright © 2015, 2017, Hitachi, Ltd.

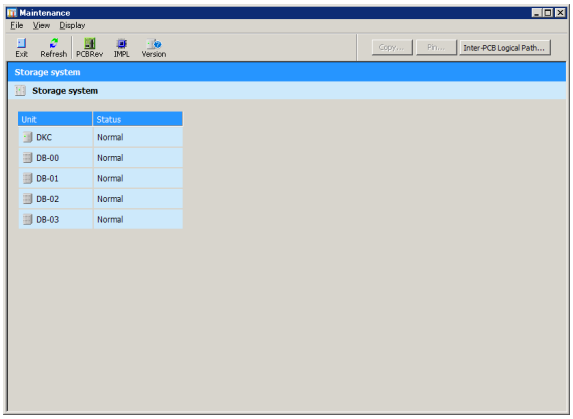
[2] FMD Dump

The FMD Dump is the dump to collect the operational information of FMD and includes the following:

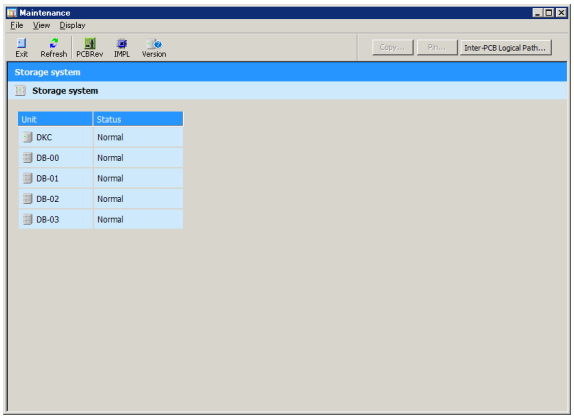
- Information on hardware operation within FMD
- Information on errors within FMD
- Information on endurance of flash memory chip
- Information on performance of FMD
- Trace of firmware operation of FMD

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 “1.2 Attachment / Removal Procedure of Maintenance PC”.

2. <Maintenance window>
   Click the [Maintenance] button, the “Maintenance” window is displayed.

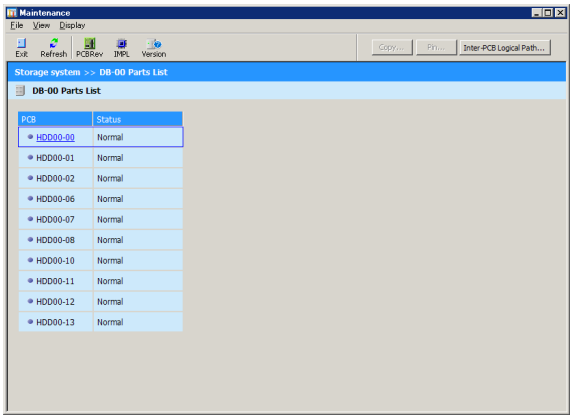


3. <Maintenance window>
   Click the DB information [DB-nn] of the DB which installs the HDD to be replaced in the “Maintenance” window.



Copyright © 2015, 2017, Hitachi, Ltd.

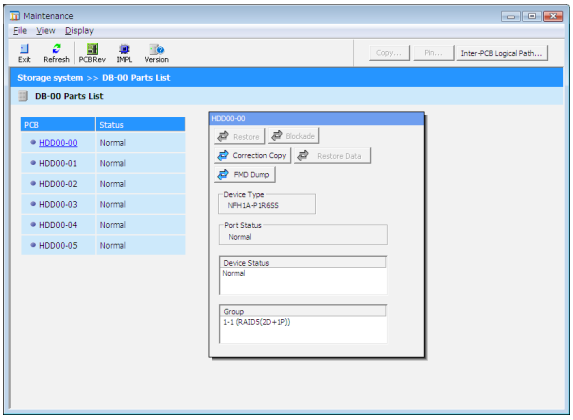
4. <Select HDD>
   Check and click HDDmm-nn to be replaced.



5.
   Make sure that the “Device Status” is [Normal].

   NOTE: Please check that the selected HDD is not formatting (without Quick Format) in the “Logical Device” window.

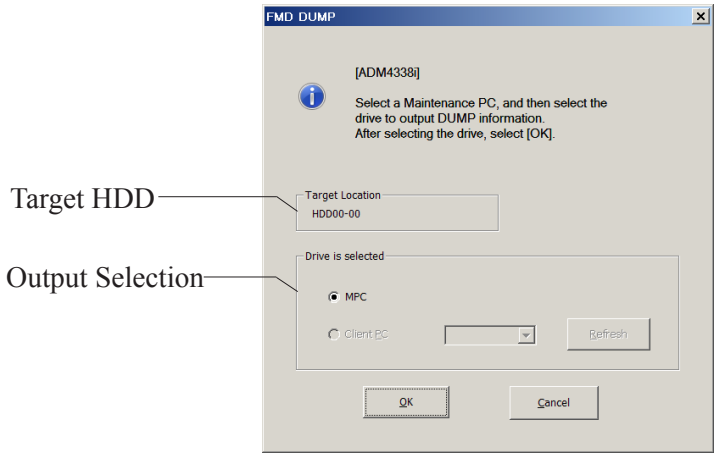
   Click the [FMD Dump] button.



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.

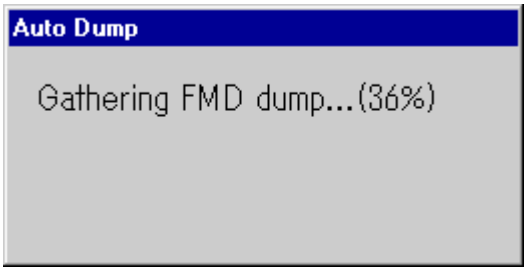


<<Output Detail>>

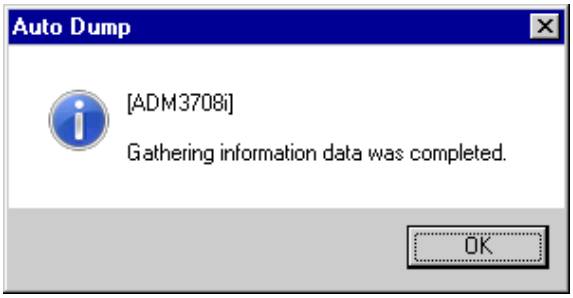
- MPC:
  Dump data is output to “C:\Mapp\wk\83xxxxyyyyyy\DKC200\others” directory of Maintenance PC.

Copyright © 2015, 2017, Hitachi, Ltd.

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 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”.

Copyright © 2015, 2017, Hitachi, Ltd.

[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
- %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*
- %WINDIR%\minidump*.dmp
- 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)

Copyright © 2015, 2017, Hitachi, Ltd.

5.3 Log

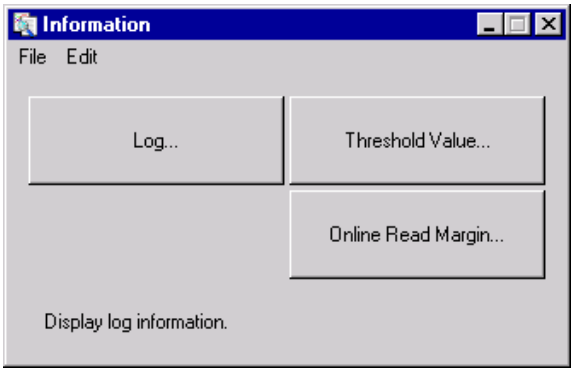
5.3.1 Log Indication

[1] SSB Log ---------- MPC05-180
[2] SIM Log ---------- MPC05-230
[3] Detail Log ---------- MPC05-260
[4] Reset Log ---------- MPC05-280
[5] Power Event Log ---------- MPC05-300
[6] Diagnosis Log ---------- MPC05-310
[7] Copy History Log ---------- MPC05-330
[8] MP# - Location correspondence table ---------- MPC05-350
[9] Port - Location correspondence table ---------- MPC05-360

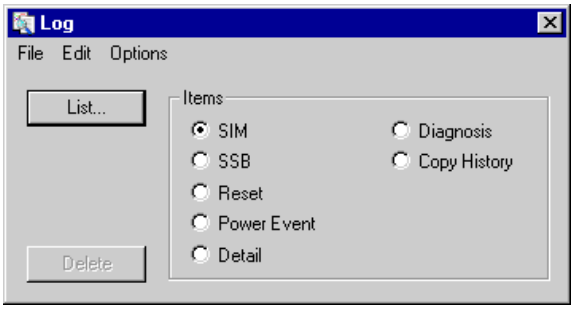
Prerequisite Operation:

1. Click the [Information] button.

2. Click the [Log...] button.



3. The “Log” window is displayed.



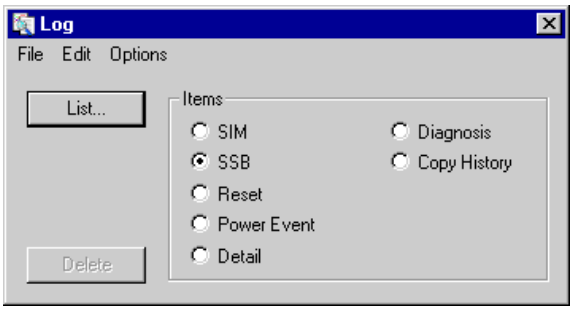
Copyright © 2015, 2017, Hitachi, Ltd.

[1] SSB Log

Display the SSB detected by the DKC, GUM, and Maintenance PC.

1.

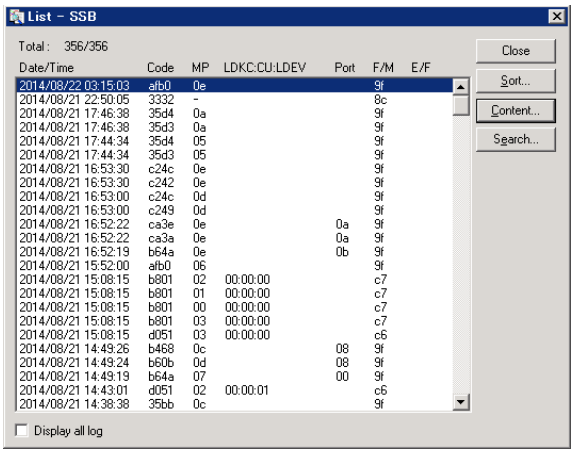
Click the [SSB] button in the “Log”.
Click the [List...] button.



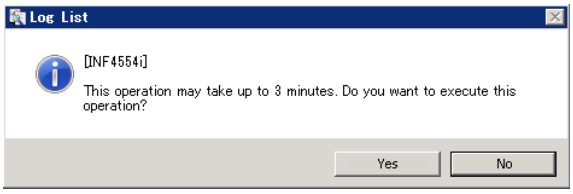
NOTE: When the DKC communication error has occurred, the SSB of the successful acquisition and the SSB stored on the Maintenance PC are displayed.

2.

Select the data to be indicated in the “List-SSB” window and click the [Content...] button.

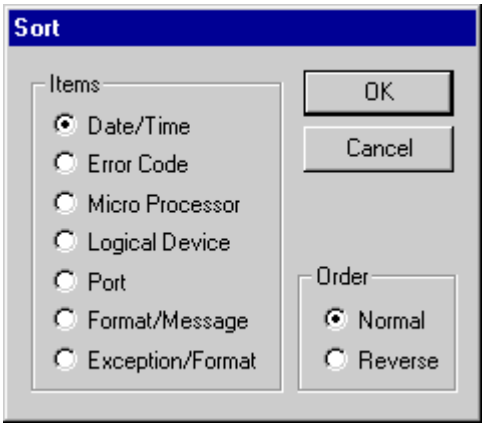


When displaying all the SSBs stored in the DKC, check the [Display all logs] checkbox. After that, click the [Yes] button in the displayed message [4554].



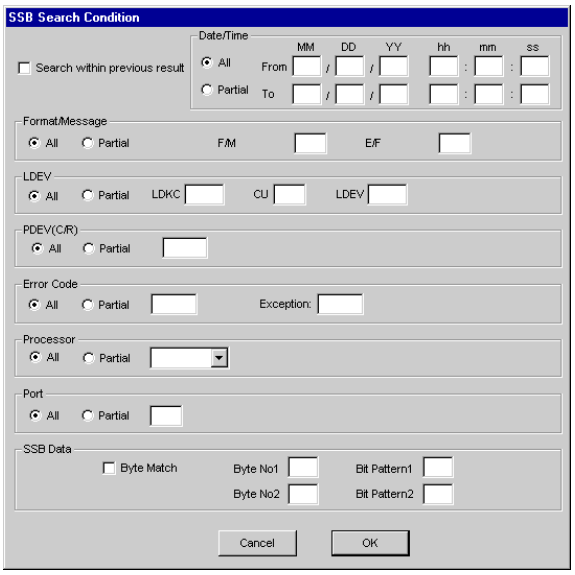
Copyright © 2015, 2017, Hitachi, Ltd.

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.



Copyright © 2015, 2017, Hitachi, Ltd.

(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.(MPC05-360)

(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].

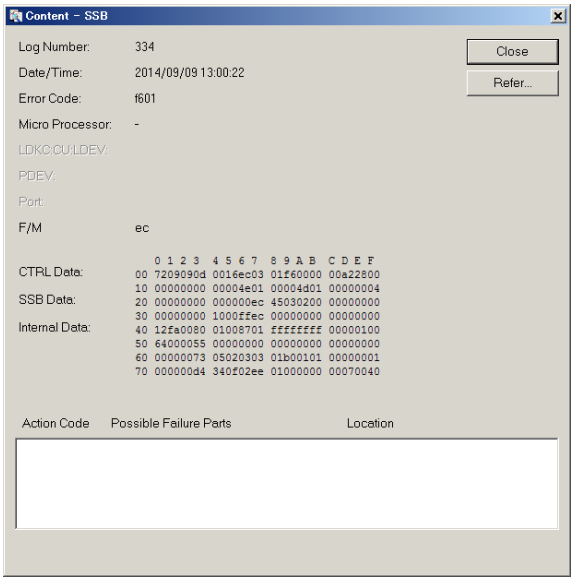
Byte No2 : Enter a position of the byte to search.

Byte Pattern2 : Enter a value to search in a position of the byte specified in [Byte No2].

Copyright © 2015, 2017, Hitachi, Ltd.

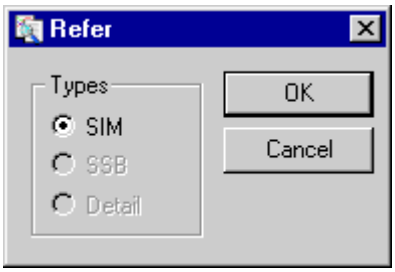
3.

The detailed data is displayed in the “Content-SSB” window.
Click the [Refer...] button in the “Content-SSB” window to display the relative log.



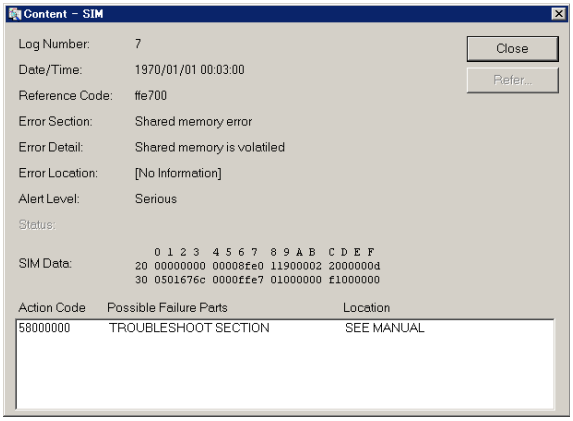
4.

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.)



Copyright © 2015, 2017, Hitachi, Ltd.

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.

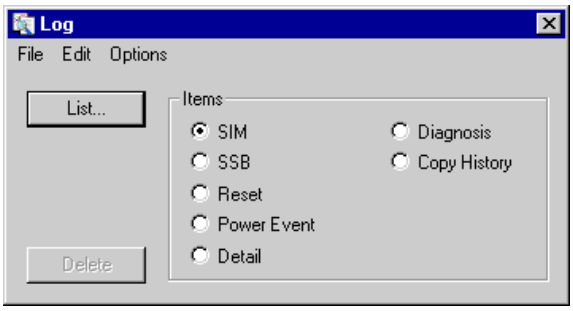
Copyright © 2015, 2017, Hitachi, Ltd.

[2] SIM Log

Display the SIM detected by the DKC and GUM.

1.

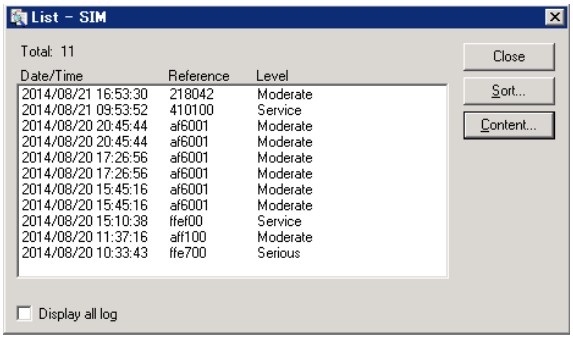
Click the [SIM] button in the “Log” window.
Click the [List...] button.



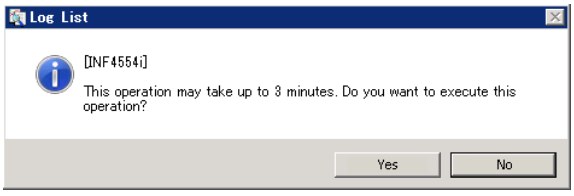
NOTE: When the DKC communication error has occurred, the SIM of the successful acquisition is displayed.

2.

Select the data to be indicated in the “List-SIM” window and click the [Content...] button.

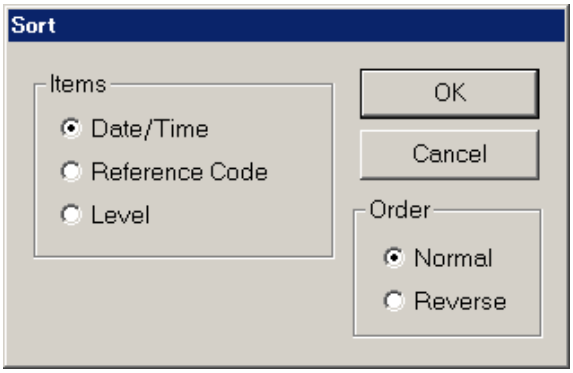


When displaying all the SSBs stored in the DKC, check the [Display all logs] checkbox. After that, click the [Yes] button in the displayed message [4554].



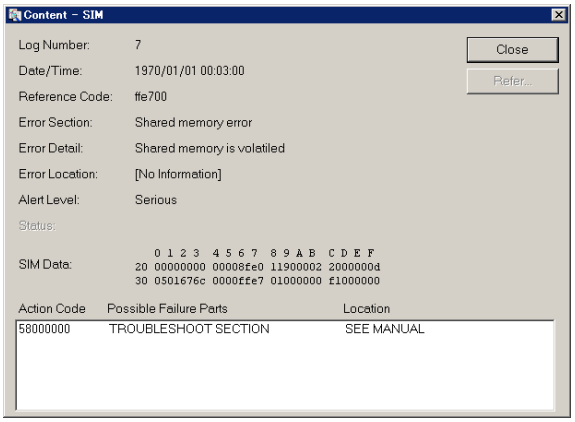
Copyright © 2015, 2017, Hitachi, Ltd.

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.



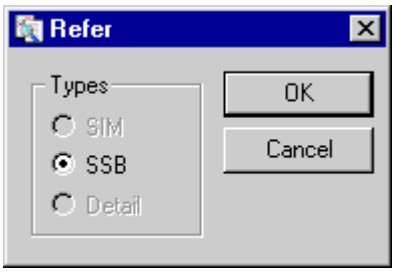
NOTE: In WCHK1 dump and ABEND dump received SIM (RC = 3080x0, 3081x0), the system error code is indicated in the format [yyyy] as in Reference Code 3080x0[yyyy].

NOTE: If Reference Code is 73xxyy or 1400x0, perform the recovery procedure for CTL processor failure/MPC Software failure.
(Refer to TROUBLESHOOTING SECTION “3.10 Recovery Procedure for LAN Error”.)

Copyright © 2015, 2017, Hitachi, Ltd.

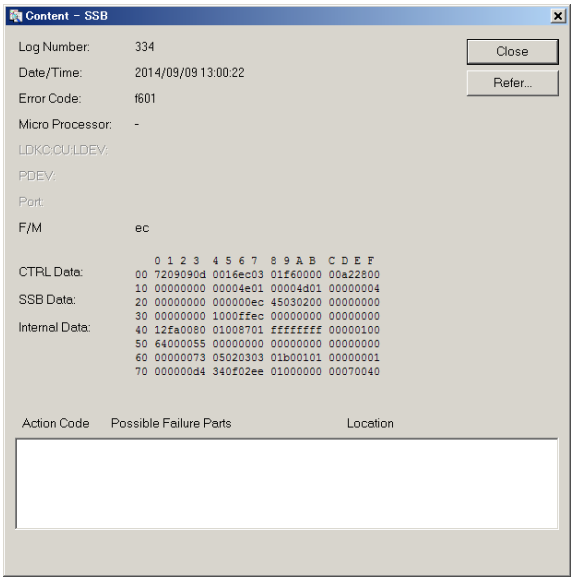
4.

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.

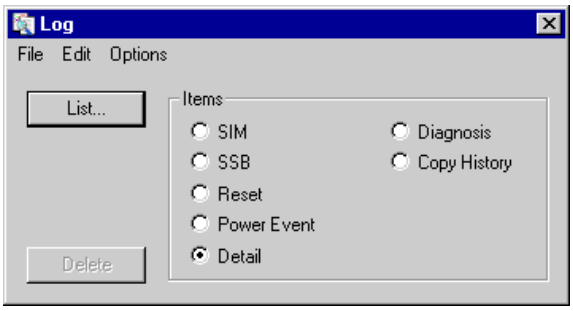
Close the relative log when it is referred to.
Click the [Close] button in the “Content-SSB” window.
Click the [Close] button in the “Content-SIM” window.
Click the [Close] button in the “List-SIM” window.
Close the “Log” window and close the “Information” window.

Copyright © 2015, 2017, Hitachi, Ltd.

[3] Detail Log

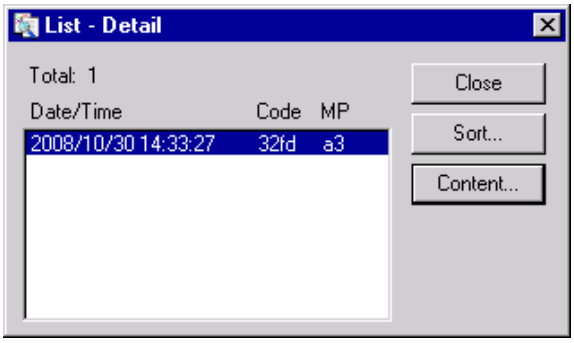
1.

Click the [Detail] button in the “Log” window.
Click the [List...] button.

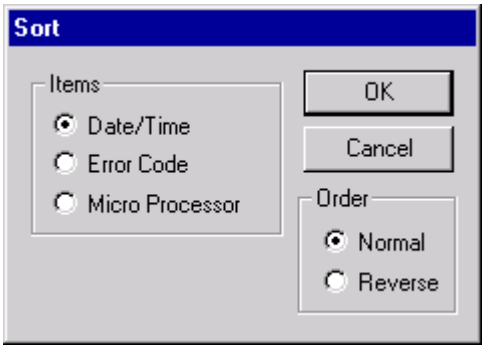


2.

Select the data to be indicated in the “List-Detail” window, and click the [Content...] button.



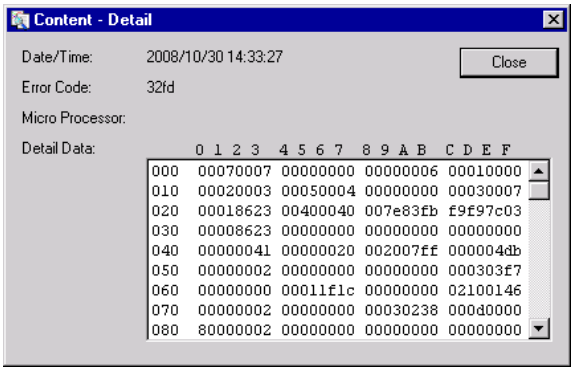
NOTE: To sort and list items, click the [Sort...] button first.
Then select the desired item in the [Items] and [Order] options in the “Sort” window, and click the [OK] button.



Copyright © 2015, 2017, Hitachi, Ltd.

3.

The “Content-Detail” window is displayed.



4.

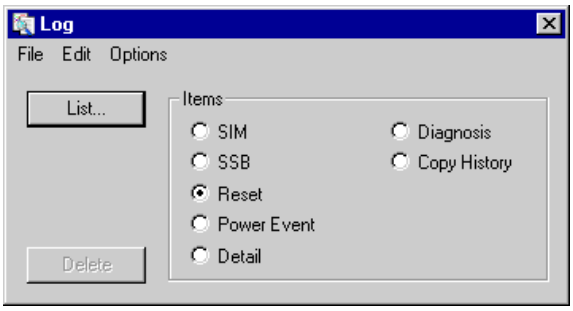
Click the [Close] button in the “Content-Detail” window.
Click the [Close] button in the “List-Detail” window.
Close the “Log” window and close the “Information” window.

Copyright © 2015, 2017, Hitachi, Ltd.

[4] Reset Log

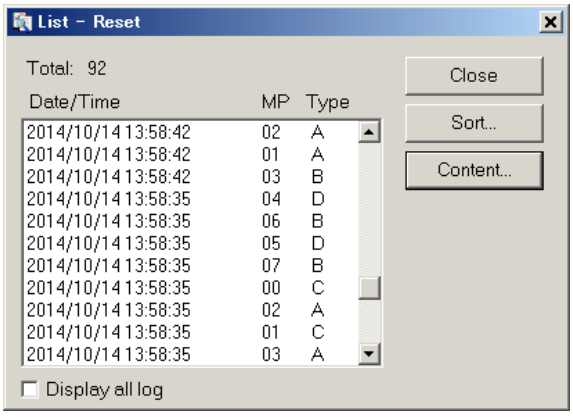
1.

Click the [Reset] button in the “Log” window.
Click the [List...] button.

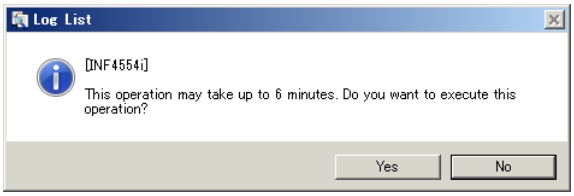


2.

Select the data to be indicated in the “List-Reset” window and click the [Content...] button.

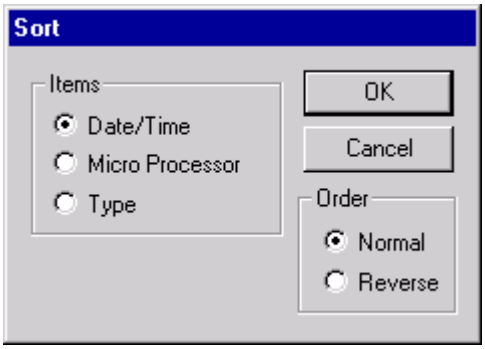


When displaying all the Reset Logs stored in the DKC, check the [Display all log] checkbox. After that, click the [Yes] button in the displayed message [4554].



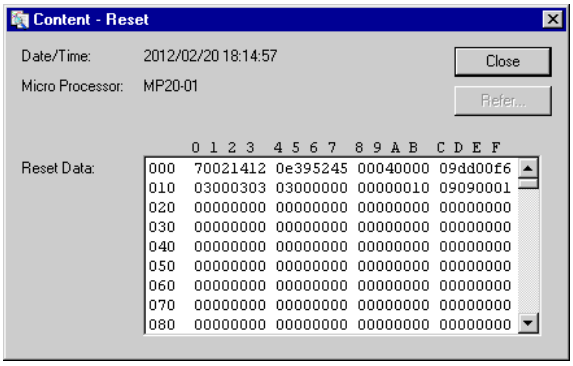
Copyright © 2015, 2017, Hitachi, Ltd.

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.

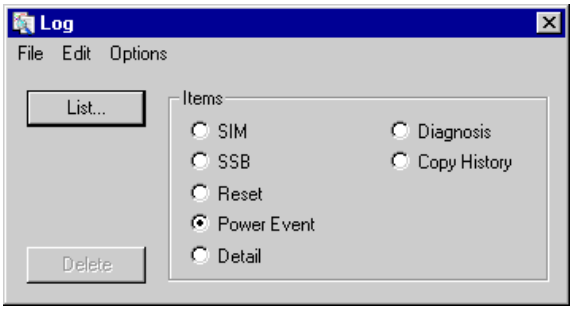
Click the [Close] button in the “Content-Reset” window.
Click the [Close] button in the “List-Reset” window.
Close the “Log” window and close the “Information” window.

Copyright © 2015, 2017, Hitachi, Ltd.

[5] Power Event Log

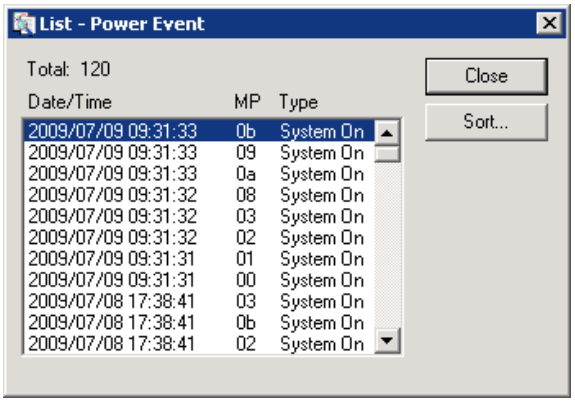
1.

Click the [Power Event] button in the “Log” window.
Click the [List...] button.

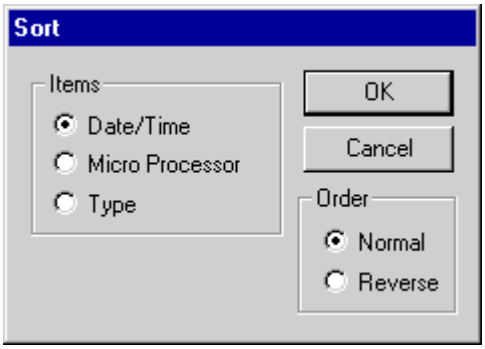


2.

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.

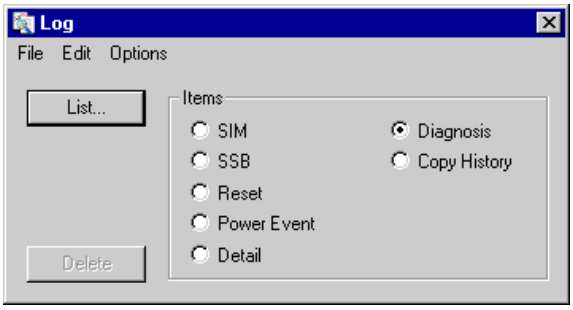
Click the [Close] button in the “List-Power Event” window.
Close the “Log” window and close the “Information” window.

Copyright © 2015, 2017, Hitachi, Ltd.

[6] Diagnosis Log

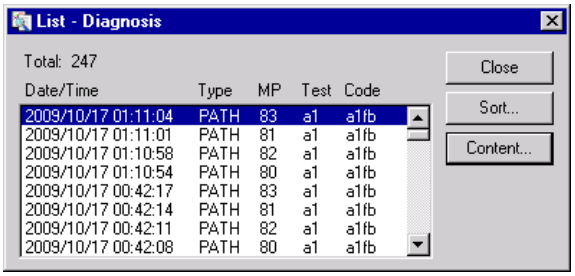
1.

Click the [Diagnosis] button in the “Log” window.
Click the [List...] button.

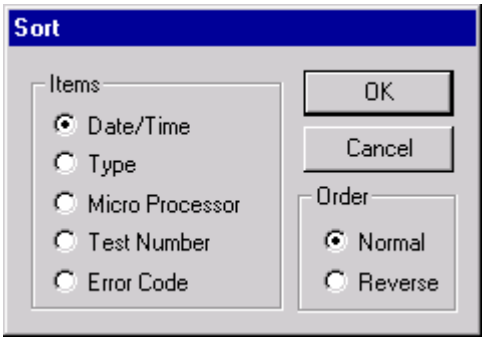


2.

Select the data to be indicated in the “List-Diagnosis” window and click the [Content...] button.



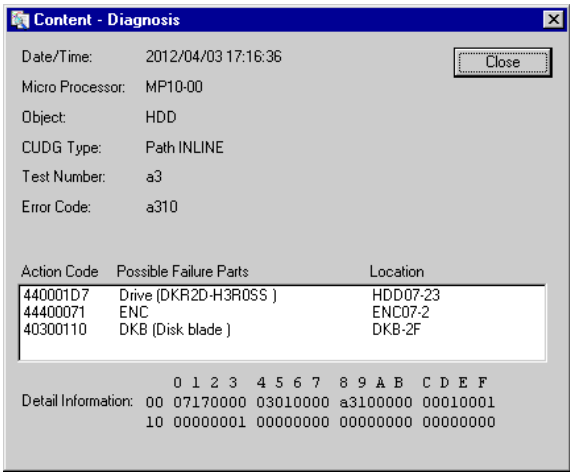
NOTE: To sort and list items, click the [Sort...] button first.
Then select the desired item in the [Items] and [Order] options in the “Sort” window, and click the [OK] button.



Copyright © 2015, 2017, Hitachi, Ltd.

3.

The “Content-Diagnosis” window is displayed.



4.

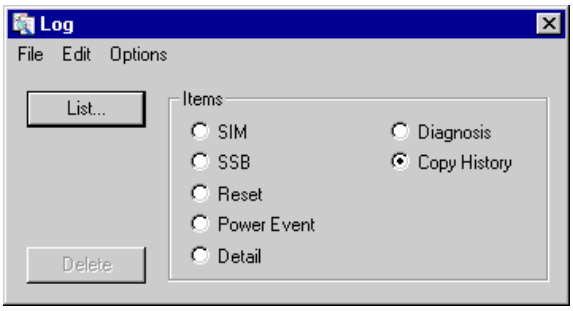
Click the [Close] button in the “Content-Diagnosis” window.
Click the [Close] button in the “List-Diagnosis” window.
Close the “Log” window and close the “Information” window.

Copyright © 2015, 2017, Hitachi, Ltd.

[7] Copy History Log

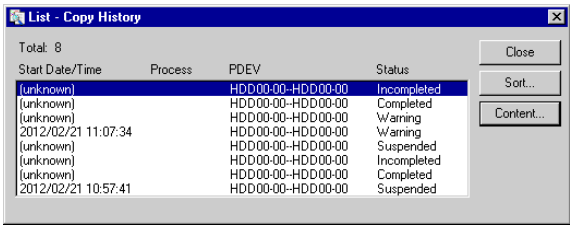
1.

Click the [Copy History] button in the “Log” window.
Click the [List...] button.

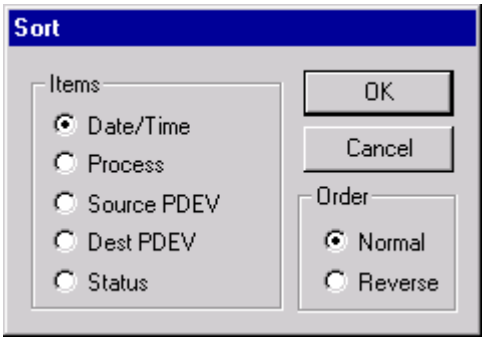


2.

Select the data to be indicated in the “List-Copy History” window and click the [Content...] button.



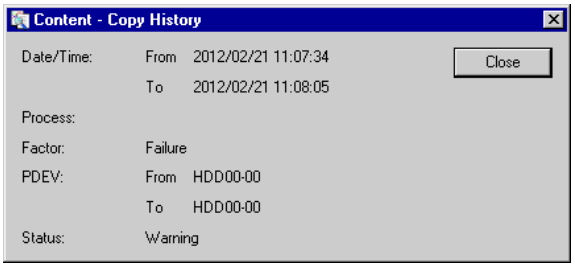
NOTE: To sort and list items, click the [Sort...] button first.
Then select the desired item in the [Items] and [Order] options in the “Sort” window, and click the [OK] button.



Copyright © 2015, 2017, Hitachi, Ltd.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

[8] MP# - Location correspondence table

Location			MP#		
			CBSS/CBSL	CBLM2/CBLM3	CBLH
CL1	MPU-10	MP10-00	0x00	0x00	0x00
		MP10-01	0x01	0x01	0x01
		MP10-02	—	0x02	0x02
		MP10-03	—	0x03	0x03
		MP10-04	—	—	0x04
		MP10-05	—	—	0x05
		MP10-06	—	—	0x06
		MP10-07	—	—	0x07
	MPU-11	MP11-00	0x02	0x04	0x08
		MP11-01	0x03	0x05	0x09
		MP11-02	—	0x06	0x0A
		MP11-03	—	0x07	0x0B
		MP11-04	—	—	0x0C
		MP11-05	—	—	0x0D
		MP11-06	—	—	0x0E
		MP11-07	—	—	0x0F
CL2	MPU-20	MP20-00	0x04	0x08	0x10
		MP20-01	0x05	0x09	0x11
		MP20-02	—	0x0A	0x12
		MP20-03	—	0x0B	0x13
		MP20-04	—	—	0x14
		MP20-05	—	—	0x15
		MP20-06	—	—	0x16
		MP20-07	—	—	0x17
	MPU-21	MP21-00	0x06	0x0C	0x18
		MP21-01	0x07	0x0D	0x19
		MP21-02	—	0x0E	0x1A
		MP21-03	—	0x0F	0x1B
		MP21-00	—	—	0x1C
		MP21-01	—	—	0x1D
		MP21-02	—	—	0x1E
		MP21-03	—	—	0x1F

Copyright © 2015, 2017, Hitachi, Ltd.

[9] Port - Location correspondence table

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-0	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

Copyright © 2015, 2017, Hitachi, Ltd.

5.3.2 Log Delete

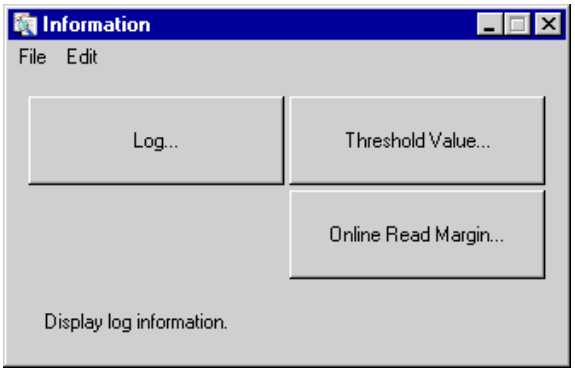
[1] SSB Log
[2] SIM Log
[3] Detail Log
[4] Reset Log
[5] Power Event Log
[6] Diagnosis Log
[7] Copy History Log

1.

Change the mode from [View Mode] to [Modify Mode].
Click the [Information] button in “MPC” window.

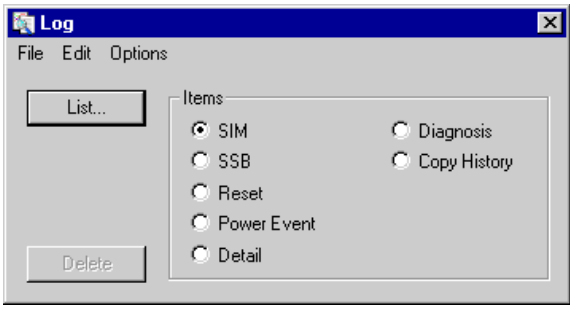
2.

Click the [Log...] button.



3.

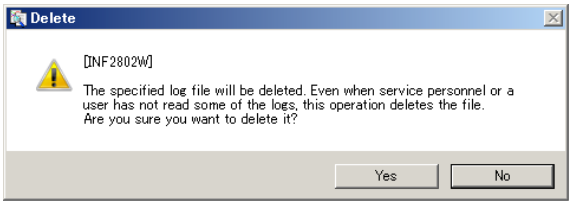
In the “Log” window, select a log to be deleted and click the [Delete] button.
(For example, select [SIM].)



Copyright © 2015, 2017, Hitachi, Ltd.

4.

Click the [Yes] button in the “Delete”[2802] window.



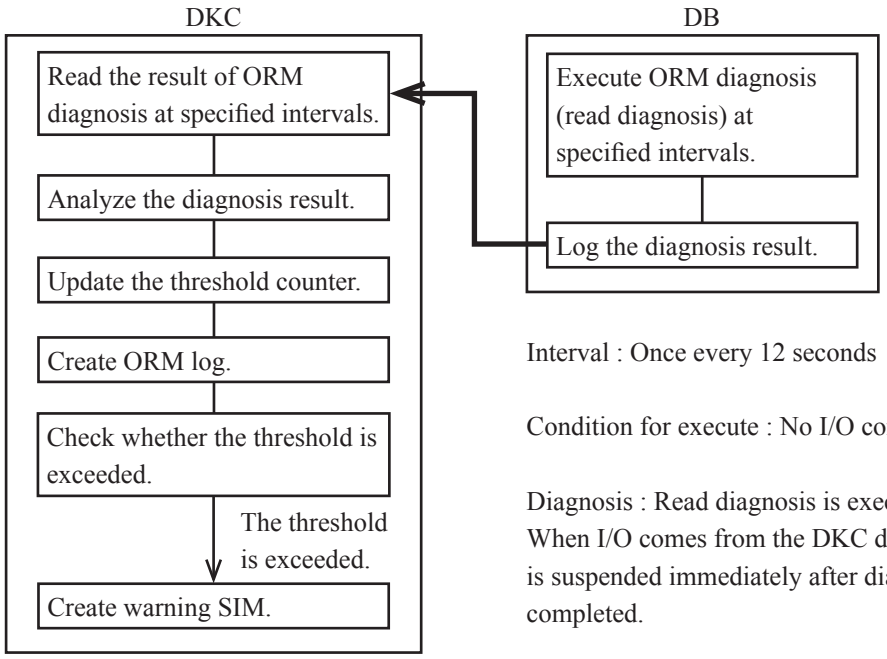
5.

Close the “Log” window and close the “Information” window.
Change the mode from [Modify Mode] to [View Mode].

Copyright © 2015, 2017, Hitachi, Ltd.

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.



Interval : Once every 12 seconds

Condition for execute : No I/O comes from the DKC for 200 ms.

Diagnosis : Read diagnosis is executed for each cylinder.
When I/O comes from the DKC during diagnosis, the read diagnosis is suspended immediately after diagnosis of the current sector is completed.

Copyright © 2015, 2017, Hitachi, Ltd.

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 Unit Error
2	Recovered Read Error		
3	Unrecovered Seek Error	502x (x = 0 ~ f)	Drive Media 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)

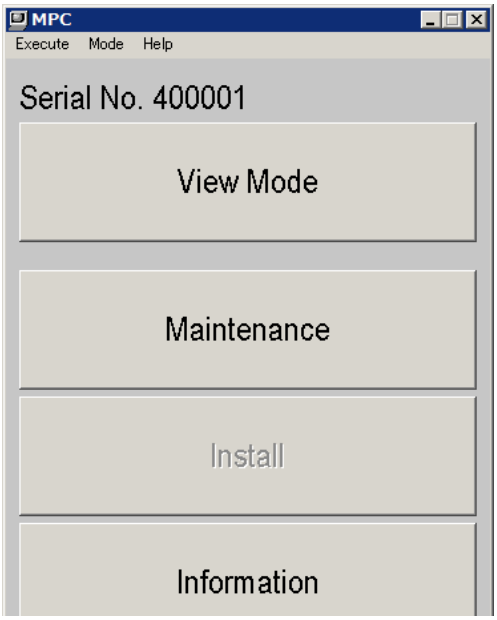
No.	Error Type	Reference Code	Meaning
1	Total Defect Count	501x (x = 0 ~ f)	Drive Unit Error
2	Reboot Error		
3	DMA Error		
4	Memory Error		
5	Uncorrected Error	502x (x = 0 ~ f)	Drive Media Error
6	Used Endurance Indicator	50cx (x = 0 ~ f)	Flash Module Drive End of life
7	Battery Error	501x (x = 0 ~ f)	Drive Unit Error
8	FMD Battery Life Indicator	50dx (x = 0 ~ f)	Flash Module Drive Battery Warning
9	Capacitor Error	501x (x = 0 ~ f)	Drive Unit Error

Copyright © 2015, 2017, Hitachi, Ltd.

[1] Displaying an error count, thresholds, and log ---------- MPC05-420
[2] Resetting an error count ---------- MPC05-470
[3] Displaying thresholds ---------- MPC05-490
[4] Altering a threshold ---------- MPC05-520
[5] Displaying the ORM running status ---------- MPC05-550
[6] Resetting thresholds ---------- MPC05-570
[7] Set of the threshold of all Flash Drive ---------- MPC05-600

Prerequisite Operation

1. Check MPC Mode
   When making the following changes, click [View Mode] in the “MPC” window to change to [Modify Mode].



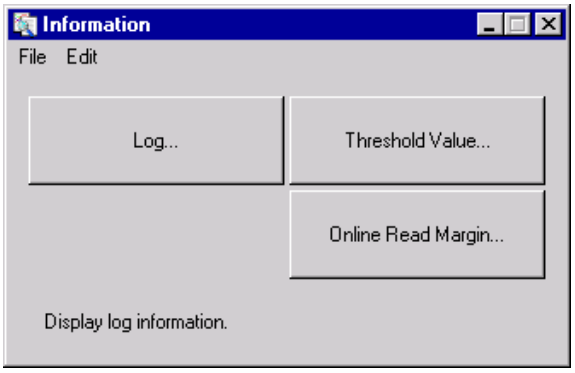
   [2] Resetting an error count
   [4] Altering a threshold
   [6] Resetting thresholds
   [7] Set of the threshold of all Flash Drive
   In the case other than the above, go to Step 2.

2.
   Click the [Information] button in the “MPC” window.

Copyright © 2015, 2017, Hitachi, Ltd.

3.

Click the [Online Read Margin...] button in the “Information” window.

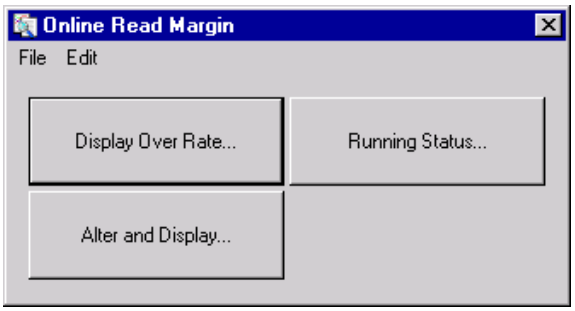


Copyright © 2015, 2017, Hitachi, Ltd.

[1] Displaying an error count, thresholds, and log

1.

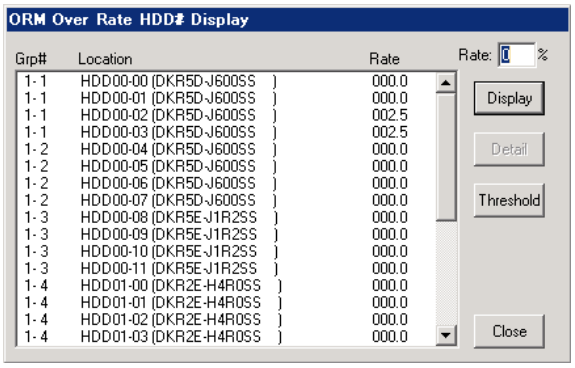
Click the [Display Over Rate...] button in the “Online Read margin” window.



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

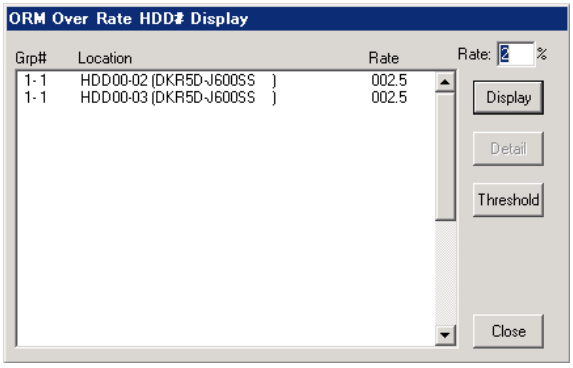
RSRVD : reserved HDD with sparing

* : spare HDD in use.

Copyright © 2015, 2017, Hitachi, Ltd.

3.

When more detailed information is needed for the particular drive, select the HDD from the HDD Location list box.
Click the [Detail] button.

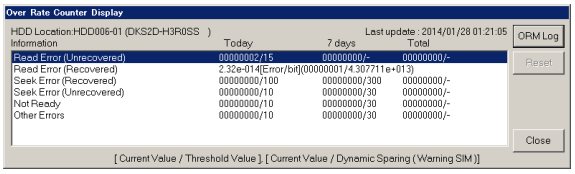


4.

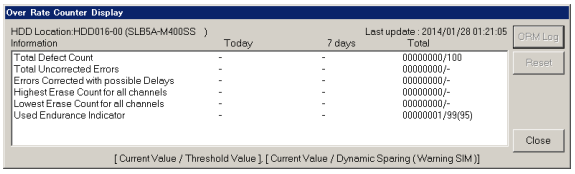
In the “Over Rate Counter Display” window, select the error for which detailed log is to be displayed.
Click the [ORM Log] button.

NOTE: In the case of Flash Drive or Flash Module Drive, you cannot choose the [ORM Log] button.
Click the [Close] button to finish.

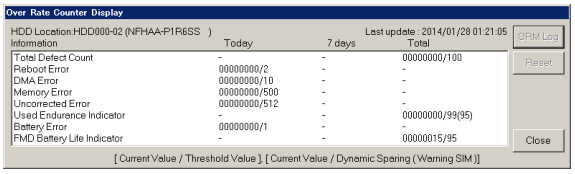
(SAS Drive Selected)



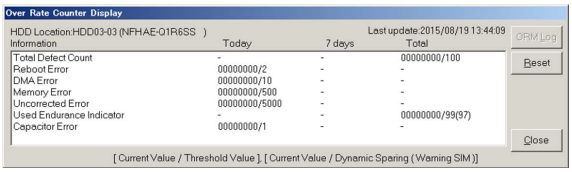
(Flash Drive Selected)



(Flash Module Drive Selected : Drive model NFHxx-Pxxxxx)



(Flash Module Drive Selected : Drive model NFHxx-Qxxxxx)



- 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:

Error rate = Number of error sectors/Number of ORM scan bits

NOTE: Only the result from approximately the latest one volume scan in ORM is used for the calculation.

Copyright © 2015, 2017, Hitachi, Ltd.

• 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)
	Battery Error	Battery Error Count (*2)
	FMD Battery Life Indicator	Warning for lifetime of Flash Module Drive Battery (%) (*2)
	Capacitor Error	Capacitor Error Count (*3)
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)".
*2: When the drive model is NFHxx-Qxxxxx, the battery error count and the lifetime of flash module drive battery are not displayed.
*3: When the drive model is NFHxx-Pxxxxx, the capacitor error count is not displayed.

Because these information is multiplication values since HDD operation time, Maintenance PC display only total indication in case of Flash Drive. Maintenance PC display total indication of "Total Defect Count", "Used Endurance Indicator" and "FMD Battery Life Indicator" and display today indication of the others in case of Flash Module Drive.
The "-" for the Threshold value means no threshold is set.

Copyright © 2015, 2017, Hitachi, Ltd.

5.

The nature of the error selected in Step 4 is displayed.

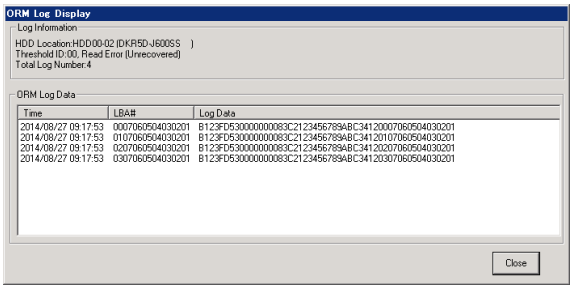


Table 5-10 Descriptions of the ORM Log Data

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.

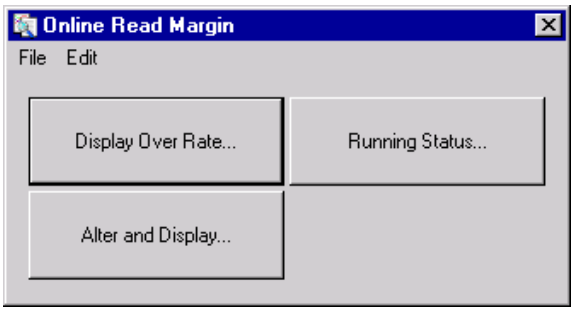
Click the [Close] button in the “ORM Log Display” window.
Click the [Close] button in the “Over Rate Counter Display” window.
Close the “Online Read Margin” window.
Click the [Close] button in the “ORM Over Rate HDD# Display” window.
Close the “Information” window.

Copyright © 2015, 2017, Hitachi, Ltd.

[2] Resetting an error count

1.

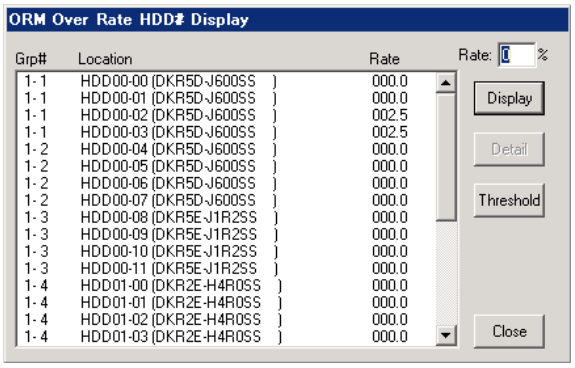
Click the [Display Over Rate...] button in the “Online Read Margin” window.



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

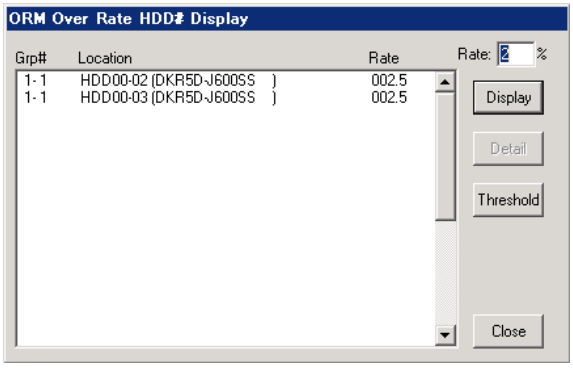
RSRVD : reserved HDD with sparing

* : spare HDD in use.

Copyright © 2015, 2017, Hitachi, Ltd.

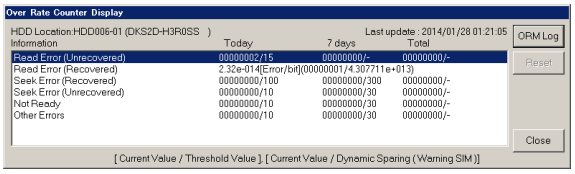
3.

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.

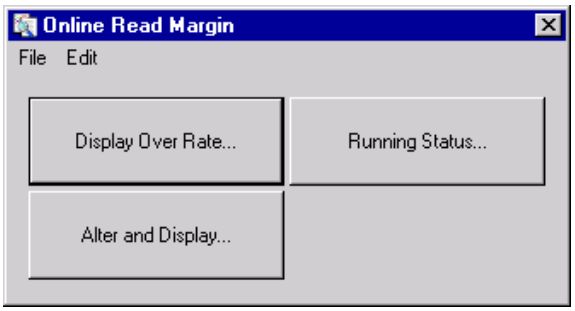
Click the [Close] button in the “Over Rate Counter Display” window.
Click the [Close] button in the “ORM Over Rate HDD# Display” window.
Close the “Online Read Margin” window.
Close the “Information” window.
Change the mode from [Modify Mode] to [View Mode].

Copyright © 2015, 2017, Hitachi, Ltd.

[3] Displaying thresholds

1.

Click the [Alter and Display...] button in the “Online Read Margin” window.



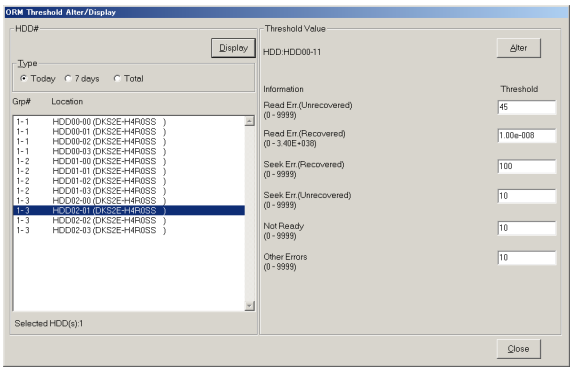
Copyright © 2015, 2017, Hitachi, Ltd.

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.

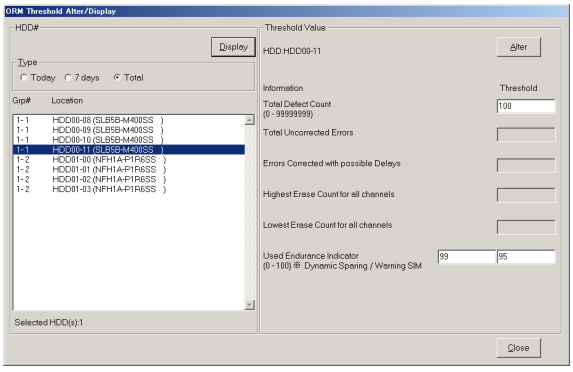
(SAS Drive Selected)



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.

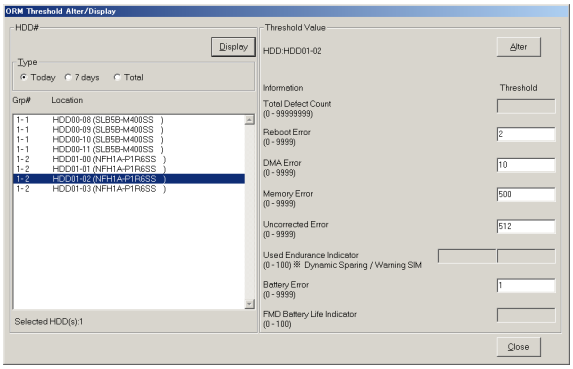
(Flash Drive Selected)



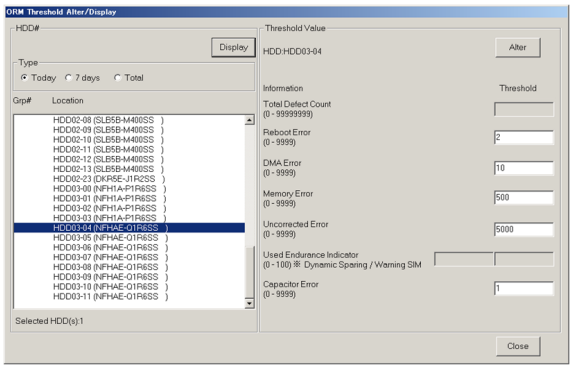
Copyright © 2015, 2017, Hitachi, Ltd.

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”, “Used Endurance Indicator” and “FMD Battery Life Indicator” (When the drive model is NFHxx-Pxxxxx), 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-Pxxxxx)



(Flash Module Drive Selected : Drive model NFHxx-Qxxxxx)



3.

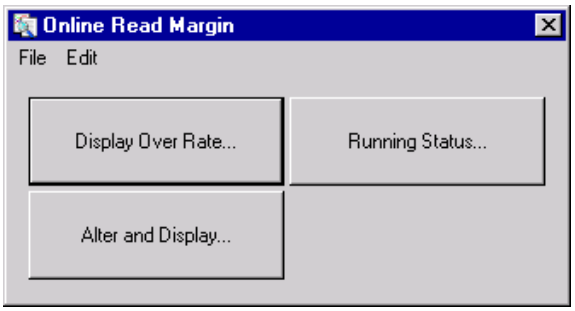
Click the [Close] button in the “ORM Threshold Alter/Display” window.
Close the “Online Read Margin” window.
Close the “Information” window.

Copyright © 2015, 2017, Hitachi, Ltd.

[4] Altering a threshold

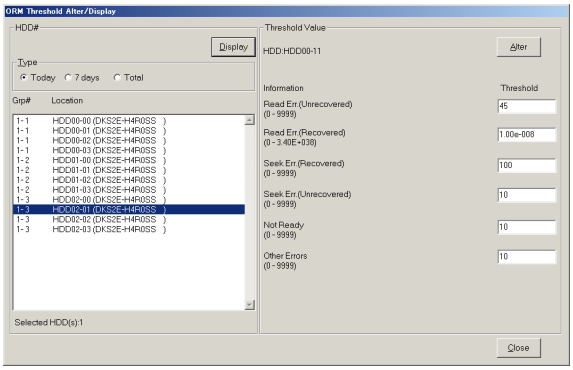
1.

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.

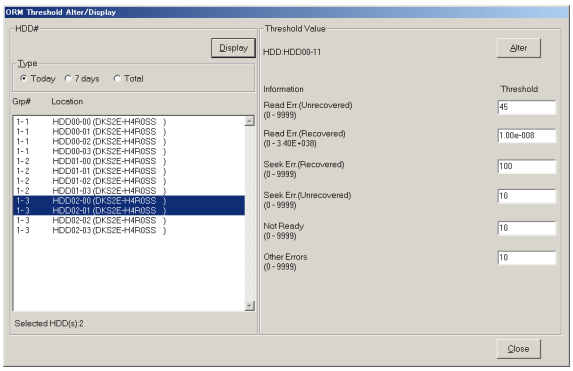
Copyright © 2015, 2017, Hitachi, Ltd.

3.

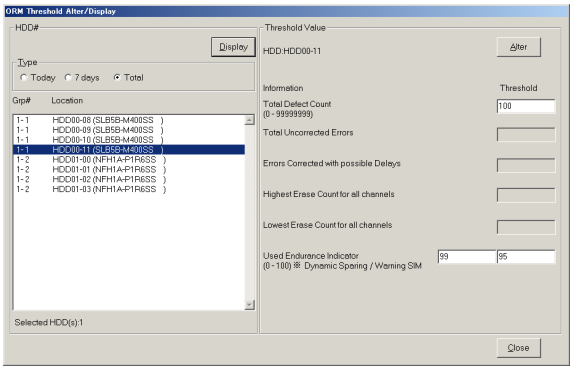
In the “ORM Threshold Alter/Display” window, alter the threshold in the “Threshold” field in the “Threshold Value” list box. Then click the [Alter] button.

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.

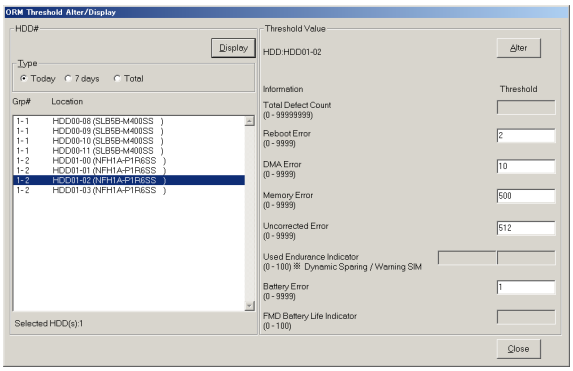
(SAS Drive Selected)



(Flash Drive Selected)

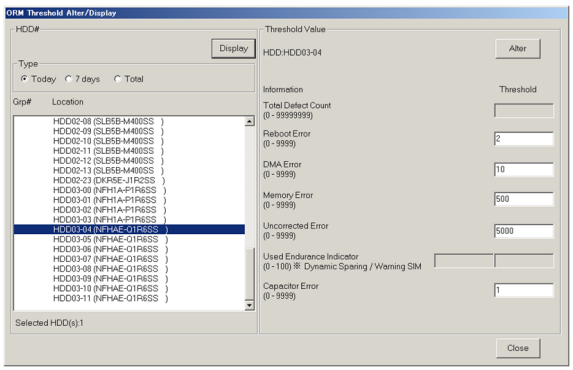


(Flash Module Drive Selected : Drive model NFHxx-Pxxxxx)



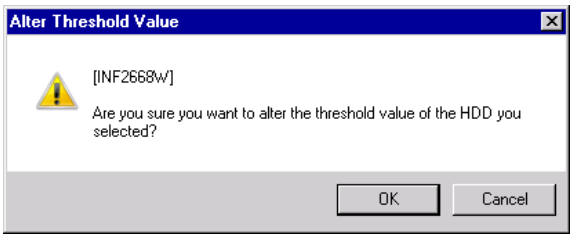
Copyright © 2015, 2017, Hitachi, Ltd.

(Flash Module Drive Selected : Drive model NFHxx-Qxxxxx)



4.

Click the [OK] button in the “Alter Threshold Value” [2668] dialog box.



5.

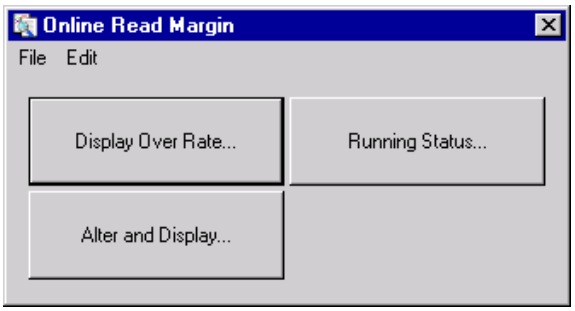
Click the [Close] button in the “ORM Threshold Alter/Display” window.
Close the “Online Read Margin” window.
Close the “Information” window.
Change the mode from [Modify Mode] to [View Mode].

Copyright © 2015, 2017, Hitachi, Ltd.

[5] Displaying the ORM running status

1.

Click the [Running Status...] button.

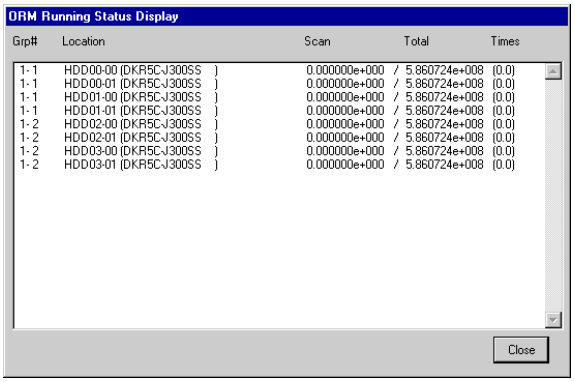


2.

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)

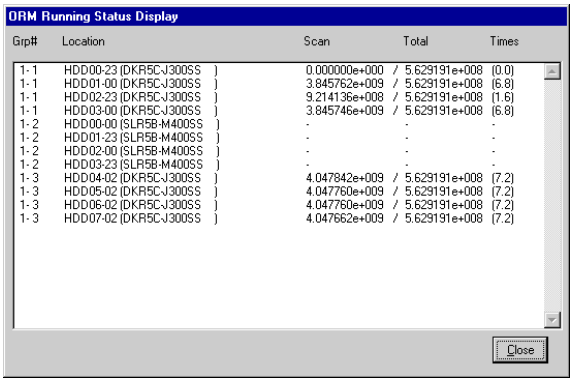


Grp# : the parity group.
SPARE : spare HDD
RSRVD : reserved HDD with sparing
* : spare HDD in use.

Copyright © 2015, 2017, Hitachi, Ltd.

NOTE: When “Flash Drive” or “Flash Module Drive” is displayed, “Scan”, “Total”, “Times” is“-”.

(Flash Drive or Flash Module Drive Selected)



3.

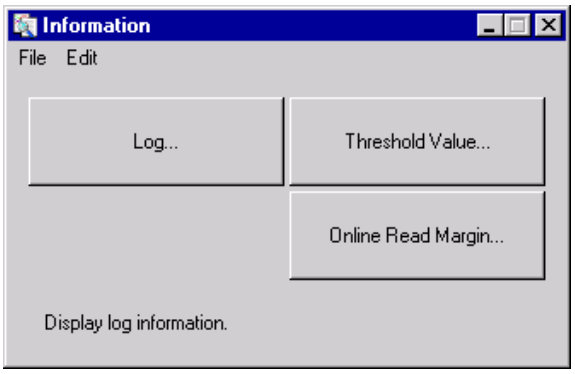
Click the [Close] button in the “ORM Running Status Display” window.
Close the “Online Read Margin” window.
Close the “Information” window.

Copyright © 2015, 2017, Hitachi, Ltd.

[6] Resetting thresholds

1.

Select [File]-[Exit] in the “Information” window.

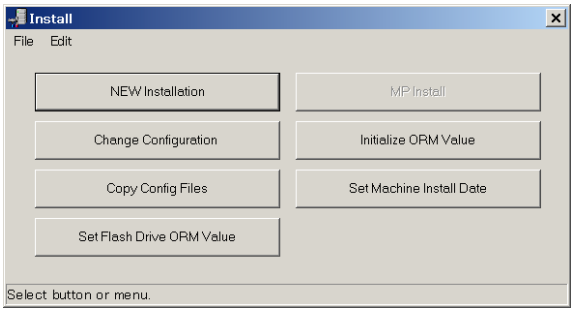


2.

Click the [Install] button in the “MPC” window.

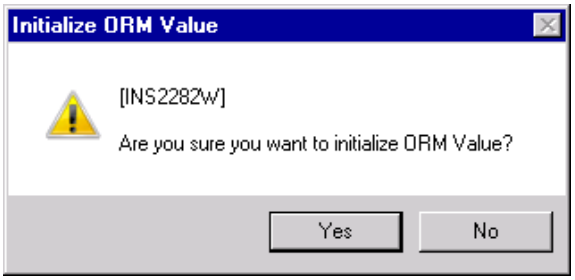
3.

Click the [Initialize ORM Value] button in the “Install” window.



4.

Click the [Yes] button in the “Initialize ORM Value” [2282] dialog box.



Copyright © 2015, 2017, Hitachi, Ltd.

5.

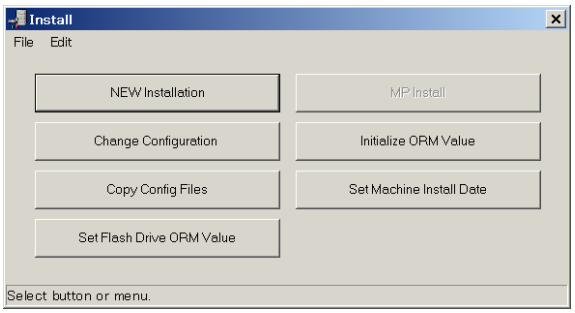
Click the [OK] button in the “Initialize ORM Value” [2281] dialog box.



Copyright © 2015, 2017, Hitachi, Ltd.

6.

After the procedure is completed, return to “Install”.
Select [File]-[Exit].

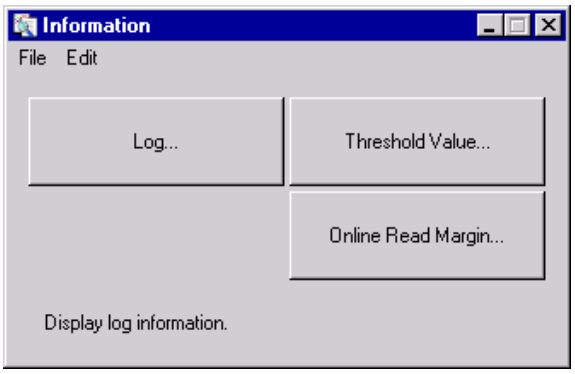


Copyright © 2015, 2017, Hitachi, Ltd.

[7] Set of the threshold of all Flash Drive

1.

Select [File]-[Exit] in the “Information” window.

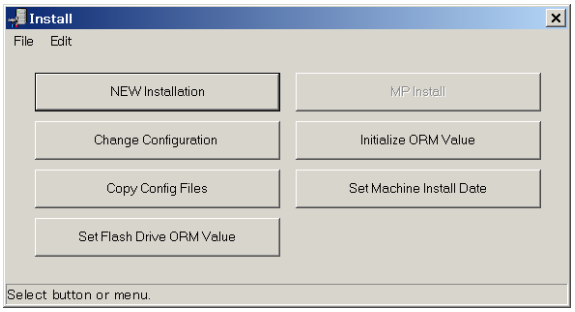


2.

Click the [Install] button in the “MPC” window.

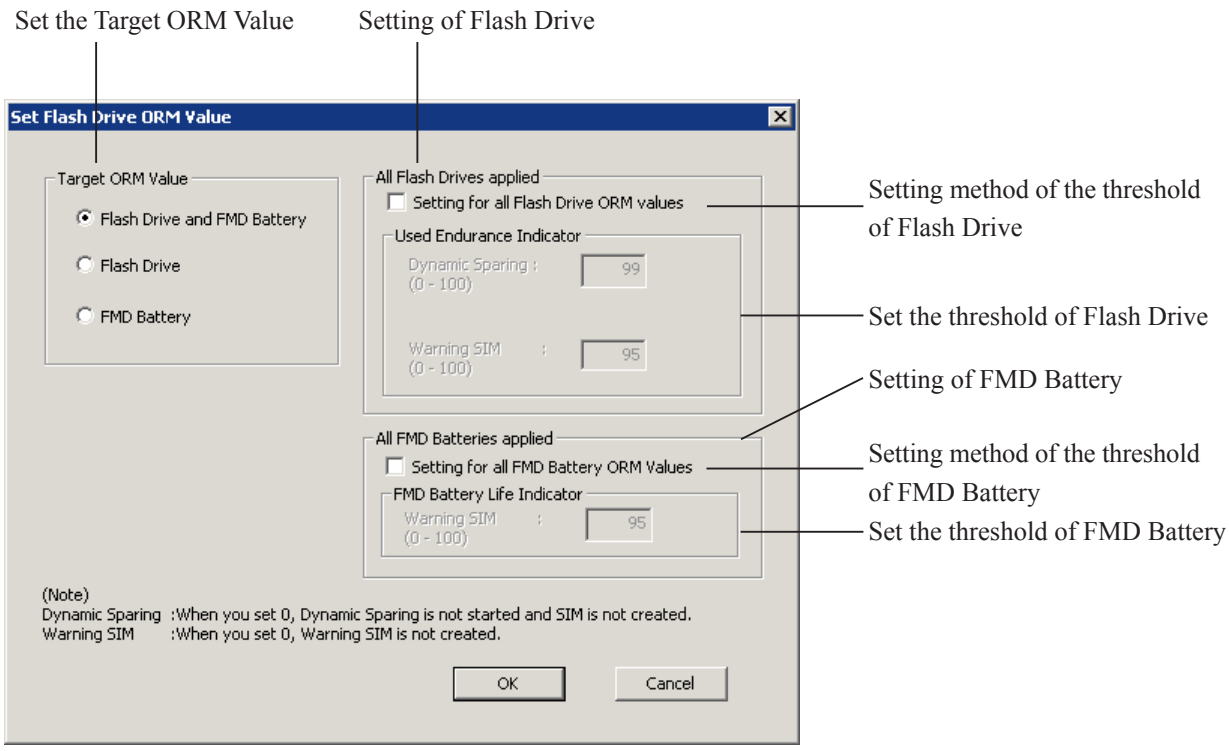
3.

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.



<<Set the Target ORM Value>>

[Target ORM Value]

Flash Drive and FMD Battery	:	This setting changes the threshold of Flash Drive and FMD Battery.
Flash Drive	:	This setting changes the threshold of Flash Drive.
FMD Battery	:	This setting changes the threshold of FMD Battery.

<<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. (MPC05-570)

<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.

<<Setting of FMD Battery>>

[All FMD Batteries applied]

<Setting method of the threshold of FMD Battery>

Setting for all FMD Battery ORM Values

When setting thresholds of Used Endurance Indicator of all mounted FMD Battery collectively, check the checkbox.
When it is checked, the FMD Battery 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 (Warning SIM threshold: 95), do reset operation of the threshold. (MPC05-570)

<Set the threshold of FMD Battery>

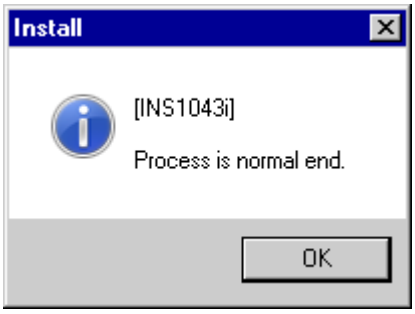
[FMD Battery Life Indicator]

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.

Copyright © 2015, 2017, Hitachi, Ltd.

5.

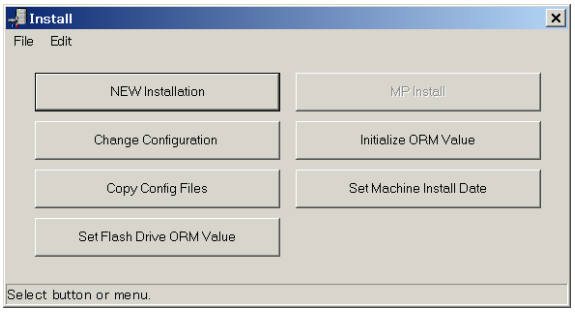
Click the [OK] button in the “[1043] Process is normal end.”.



Copyright © 2015, 2017, Hitachi, Ltd.

6.

After the procedure is completed, return to “Install”. Select [File]-[Exit].

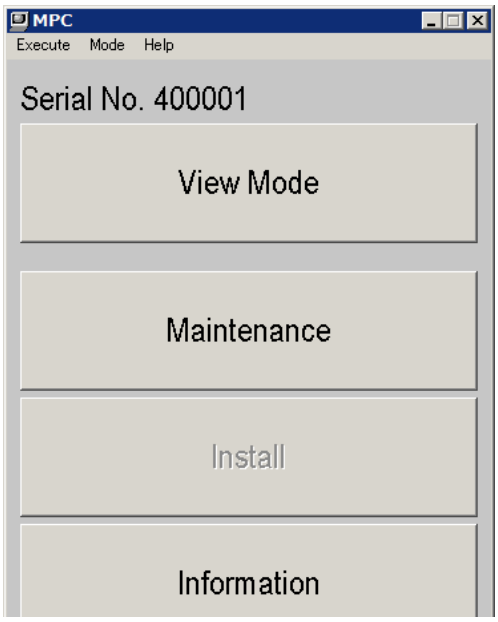


Copyright © 2015, 2017, Hitachi, Ltd.

5.5 Management of Drive Threshold Values

[1] Displaying threshold values ---------- MPC05-660
[2] Altering threshold value ---------- MPC05-680
[3] Displaying an error count ---------- MPC05-700
[4] Resetting an error count ---------- MPC05-710

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).

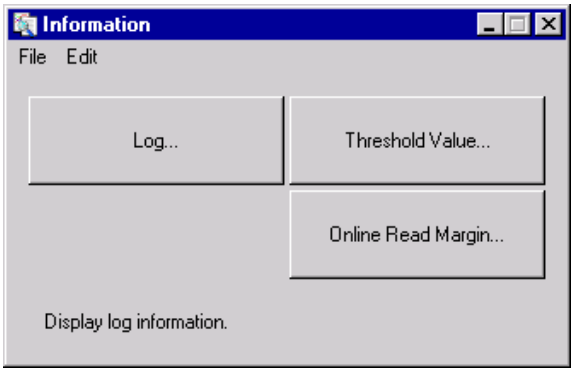
---

   (2)
   Click the [Information] button in the “MPC” window.

Copyright © 2015, 2017, Hitachi, Ltd.

(3)

Click the [Threshold Value...] button in the “Information” window.

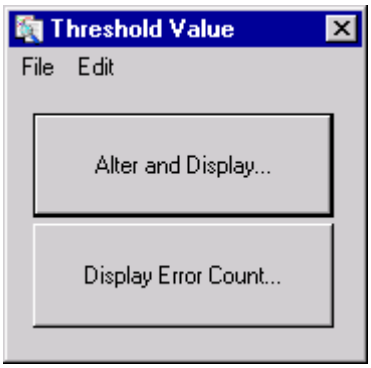


Copyright © 2015, 2017, Hitachi, Ltd.

[1] Displaying threshold values

1.

Click the [Alter and Display...] button in the “Threshold Value” window.

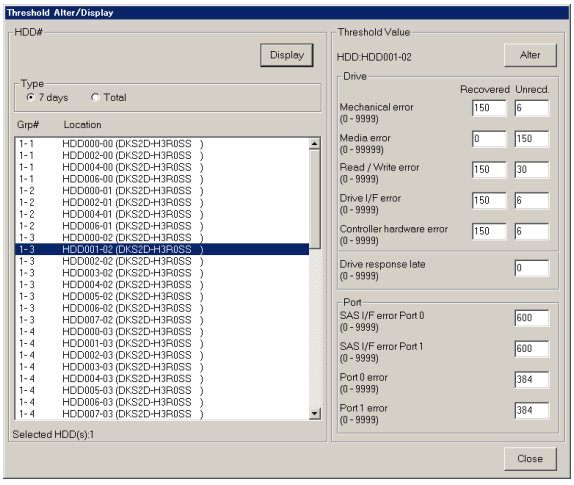


2.

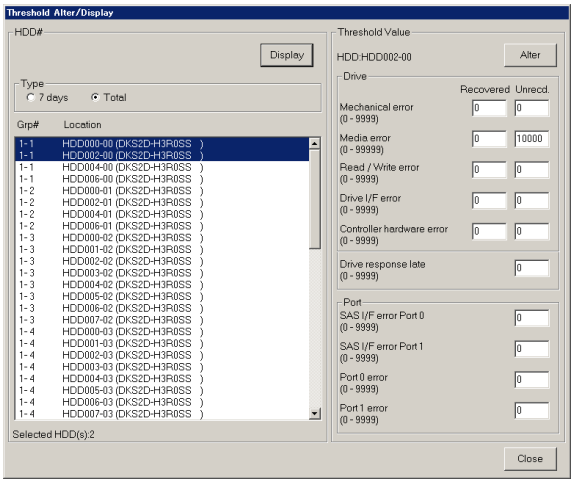
Select an HDD location from the “HDD#” list box in the “Threshold Alter/Display” window and click the [Display] button.
In order to display threshold of another interval, select the interval from the “Type” list box.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

3.

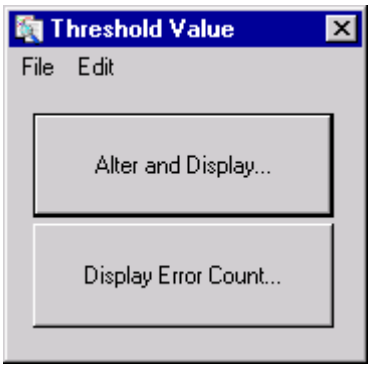
Click the [Close] button in the “Threshold Alter/Display”.
Close the “Threshold Value” window.
Close the “Information” window.

Copyright © 2015, 2017, Hitachi, Ltd.

[2] Altering threshold value

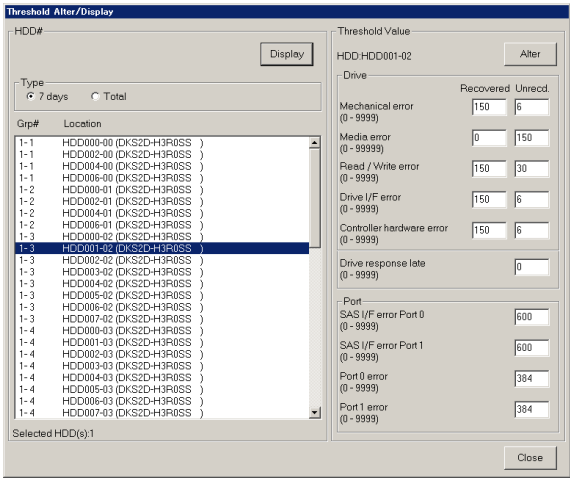
1.

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

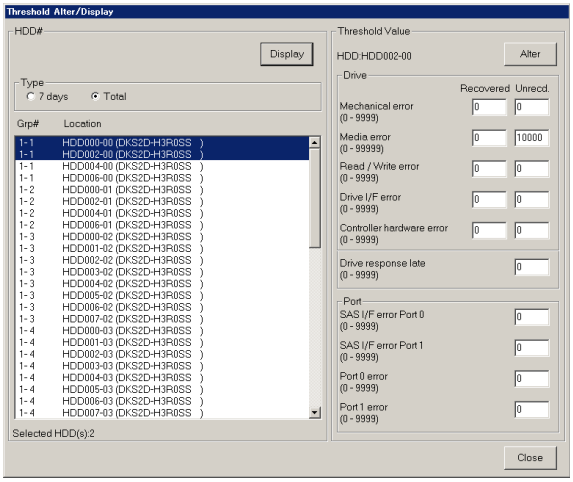
* : spare HDD in use.

Copyright © 2015, 2017, Hitachi, Ltd.

3.

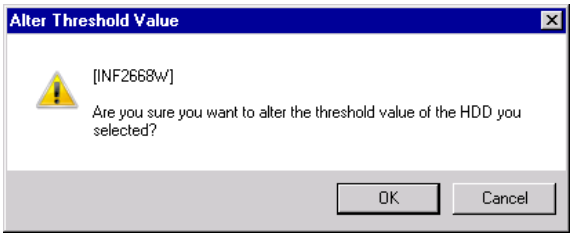
Alter a threshold value in the “Threshold Value” list box in the “Threshold Alter/Display” window.
Then click the [Alter] button.

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.

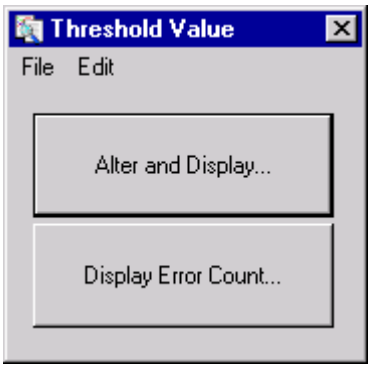
Click the [Close] button in the “Threshold Alter/Display”.
Close the “Threshold Value” window.
Close the “Information” window.

Copyright © 2015, 2017, Hitachi, Ltd.

[3] Displaying an error count

1.

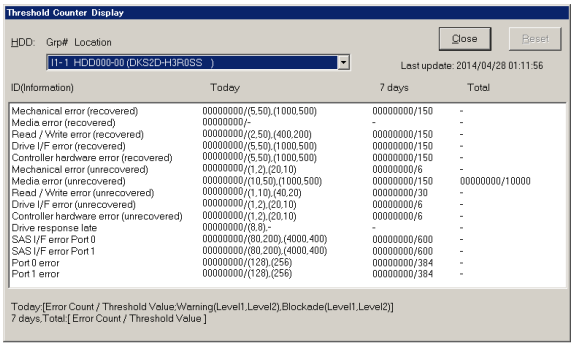
Click the [Display Error Count...] button in the “Threshold Value” Window.



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”.



Grp# : the parity group.
SPARE : spare HDD
RSRVD : reserved HDD with sparing
* : spare HDD in use.

3.

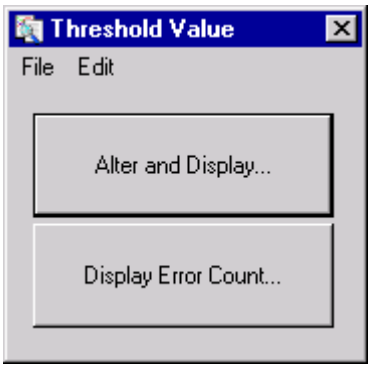
Click the [Close] button in the “Threshold Counter Display”.
Close the “Threshold Value” window.
Close the “Information” window.

Copyright © 2015, 2017, Hitachi, Ltd.

[4] Resetting an error count

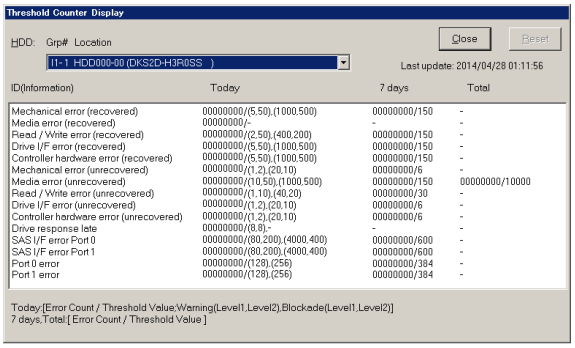
1.

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.



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.



Copyright © 2015, 2017, Hitachi, Ltd.

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.

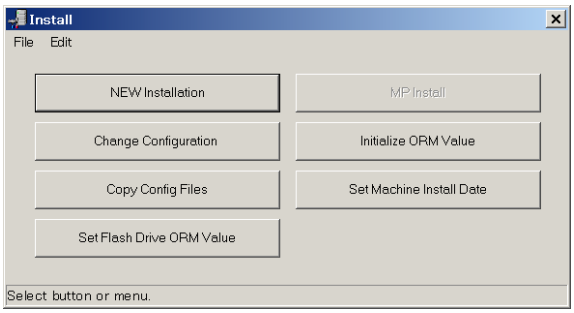
Copyright © 2015, 2017, Hitachi, Ltd.

5.6 Setting Machine Install Data

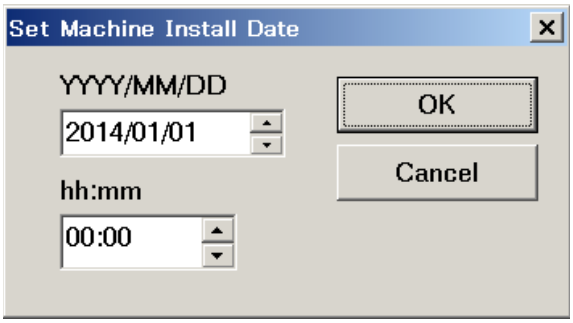
1. Change Mode from [View Mode] to [Modify Mode].

2. Click the [Install] in the [Modify Mode].

3. Click the [Set Machine Install Date] menu in the “Install” window.



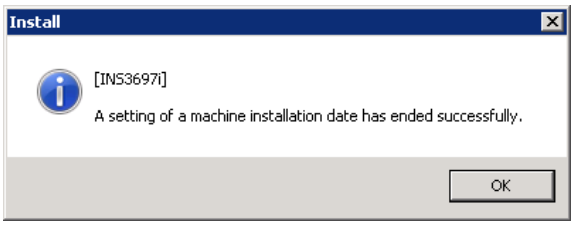
4. Input the Date and Time.
Click the [OK] button.



Copyright © 2015, 2017, Hitachi, Ltd.

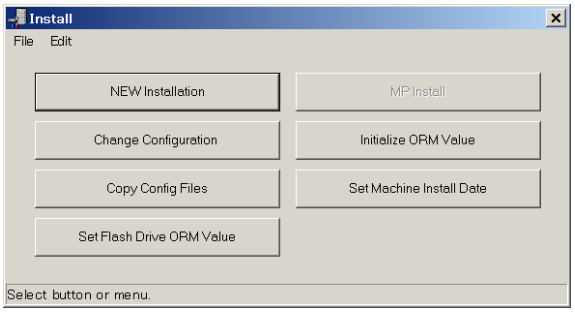
5.

"[3697] A setting of a machine installation data has ended successfully." is displayed.
Click the [OK] button.



6.

Close the "Install" window.



Copyright © 2015, 2017, Hitachi, Ltd.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

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 MPC05-800 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)

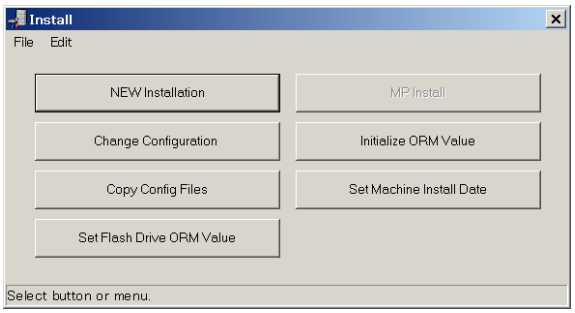
*1: The write through operation:
When a failure occurs in the Controller Board of one of the duplicated systems during a writing of data sent from a host, what is called the write through operation is performed in which completion of a writing is reported to the host after waiting for completion of a 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.

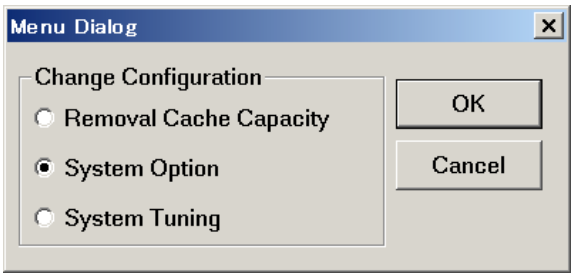
Copyright © 2015, 2017, Hitachi, Ltd.

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.

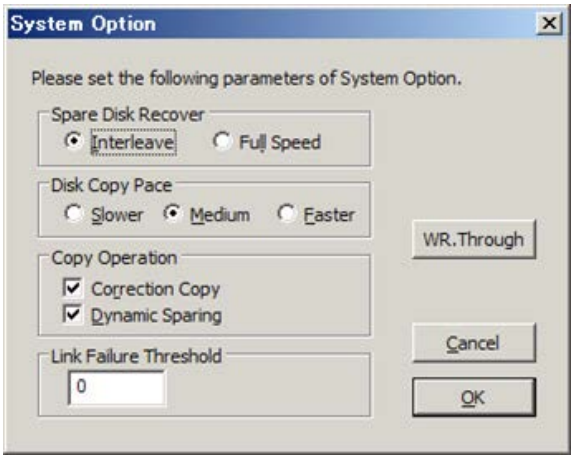


3. <Start System Option window>
   Select the [System Option] in the “Menu Dialog” dialog box and click the [OK] button.



Copyright © 2015, 2017, Hitachi, Ltd.

4. <Definition of System Option>
   Define the system option information in the “System Option” window.

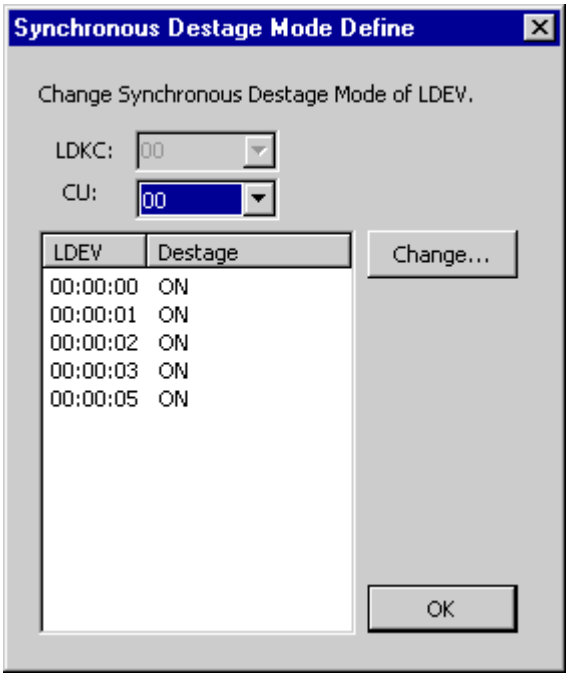


   When [WR.Through] is selected, go to Step 5.

   After all the items are set, click the [OK] button.
   Go to Step 7.

---

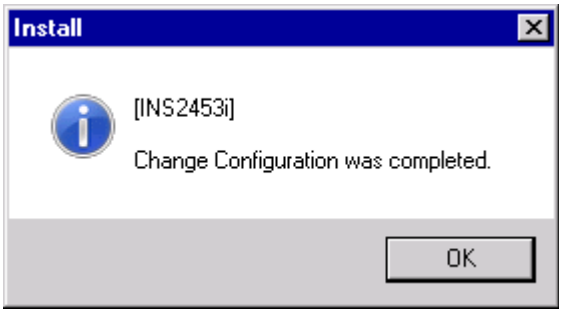
5. <Setting Destage Mode>
   Set the destage mode in the “Synchronous Destage Mode Define” window.
   When [OK] is selected, return to Step 4.
   Select the target LDEV. Click the [Change...] button to switch on/off the destage mode.



Copyright © 2015, 2017, Hitachi, Ltd.

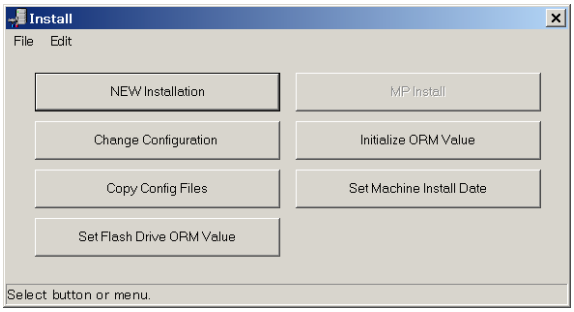
6.

"[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].

Copyright © 2015, 2017, Hitachi, Ltd.

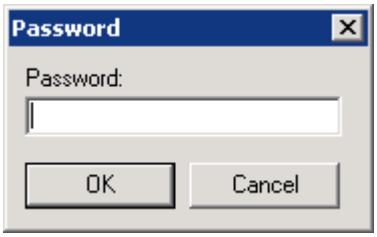
5.8 Setting System Option Mode

1.
Close the all MPC Software menu.

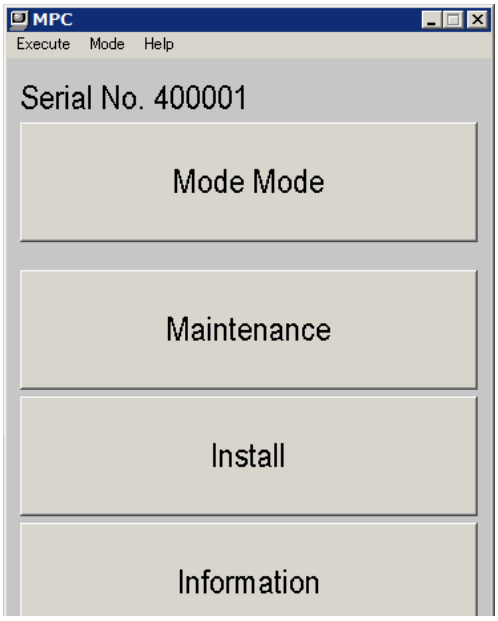
2. <Enter the password>

> **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.)

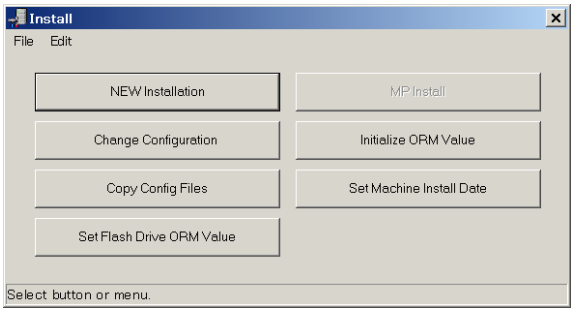


3. <Mode Mode>
[Mode Mode] is displayed.
Click the [Install] button.

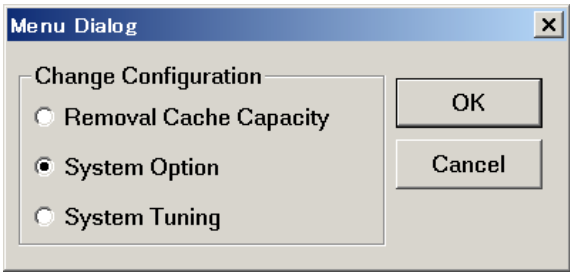


Copyright © 2015, 2017, Hitachi, Ltd.

4. <Install window>
   Click the [Change Configuration] menu in the “Install” window.

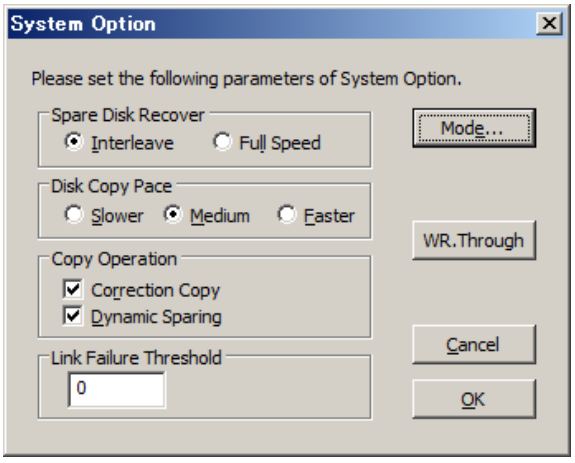


5. <Menu Dialog window>
   Select the [System Option] menu in the “Menu Dialog” window and click the [OK] button.



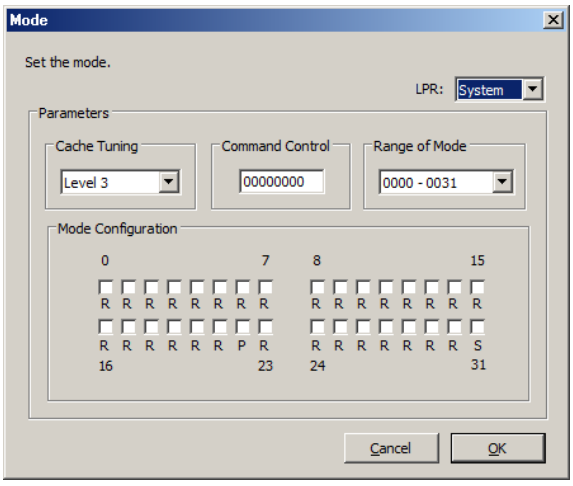
6. <System Option window>
   Click the [Mode...] button in the “System Option”. Go to Step 7.

   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.



Copyright © 2015, 2017, Hitachi, Ltd.

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.

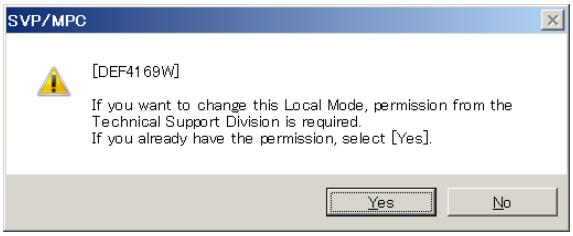
The following is definition of each Mode Class.

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).

Copyright © 2015, 2017, Hitachi, Ltd.

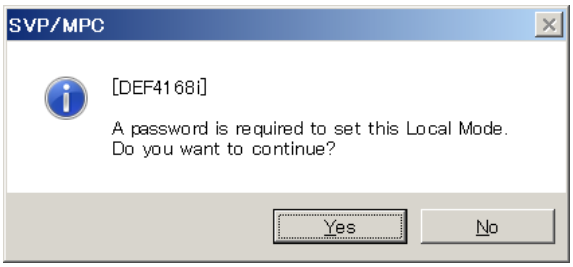
(1)

"[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.



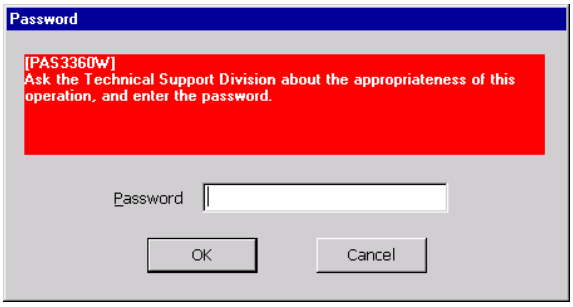
(2)

"[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)

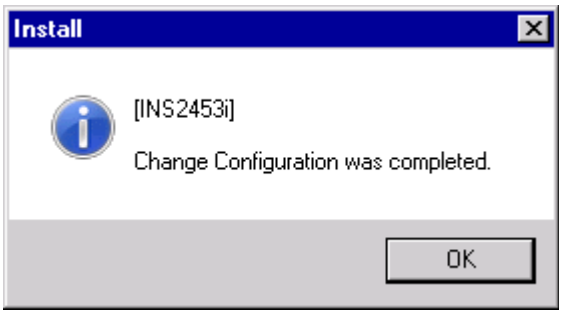
"Password"[3360] window is displayed.
Enter the password and click the [OK] button.
Go back to the Step 7.
Entering the password is required in this operation. Please call Technical Support Division for asking it.



Copyright © 2015, 2017, Hitachi, Ltd.

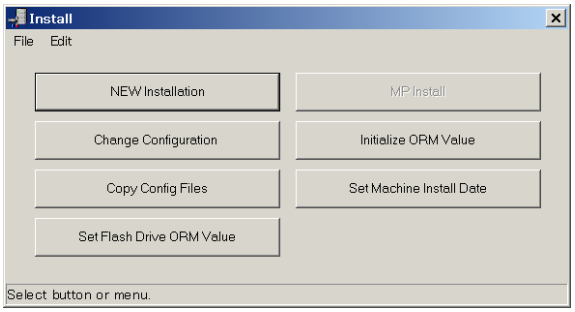
8.

"[2453] Change Configuration was completed." is displayed.
Click the [OK] button.



9.

Return to the "Install" window.

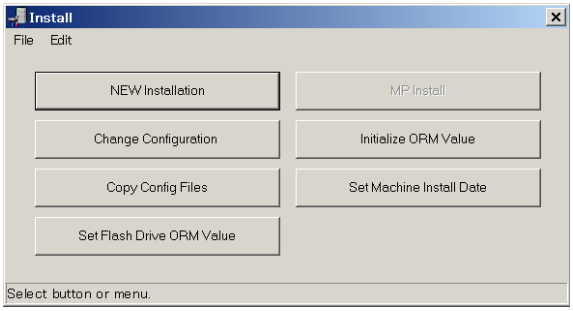


10.

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].

Copyright © 2015, 2017, Hitachi, Ltd.

5.9 System Tuning

NOTICE:	Powering off/on is required owing to the performance of this operation.

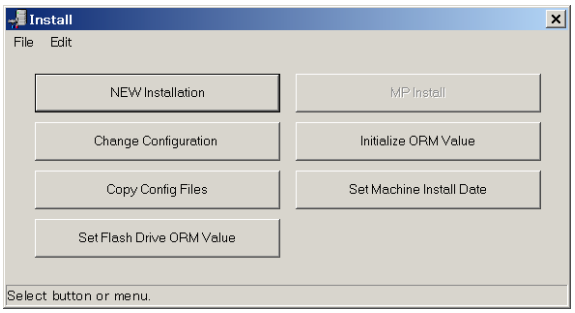
Overview
This function modifies the part of established Storage System configuration data.
The data to be modified is control data closely related to a host device, so the data cannot be modified on-line.
After modification of the data, power DKC off and on.
The data to be modified is listed below.

'DKC Configuration'--------- DKC Serial Number

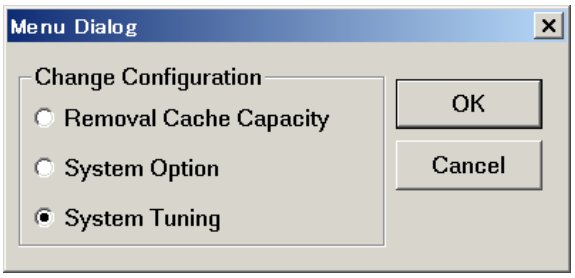
Copyright © 2015, 2017, Hitachi, Ltd.

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.



Copyright © 2015, 2017, Hitachi, Ltd.

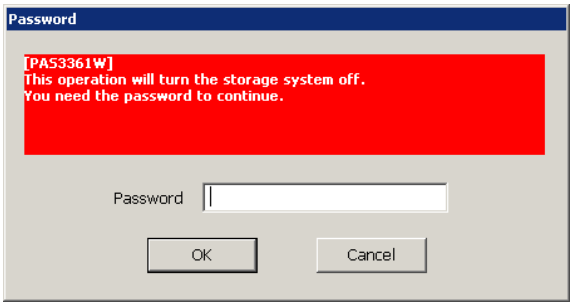
4.

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)

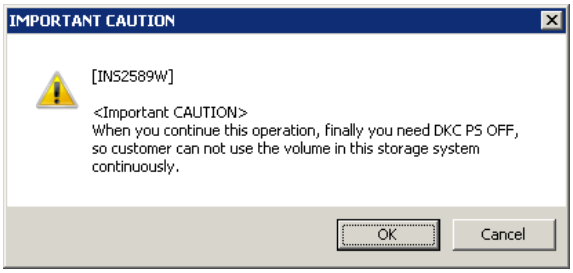
Enter the password and click [OK] in “Password”[3361] window.
Password is needed for this operation.
Please call Technical Support Division to obtain a password and authorization.

If [Cancel] is clicked, return to Step 2.



(2)

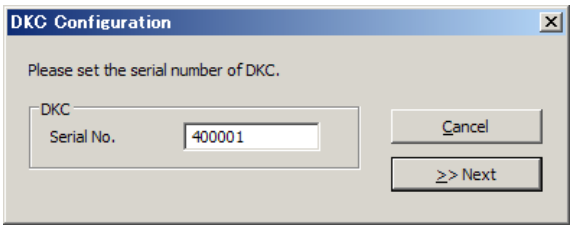
Click [OK] in response to the confirmation message
“[2589] <Important CAUTION> When you continue this operation, finally you need DKC PS OFF, so customer cannot use the volume in this storage system continuously.”.



Copyright © 2015, 2017, Hitachi, Ltd.

5. <DKC Configuration window>
   Define the configuration information following the Storage System configuration worksheet.

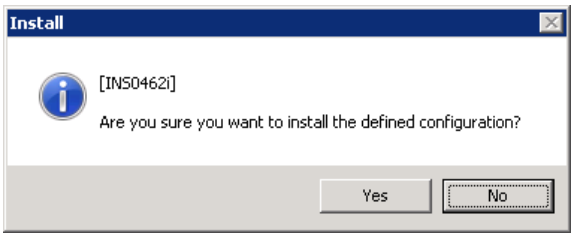
   [>>Next]: Go to Step 6.
   In the case of click [Cancel],
   this operation procedure terminates.



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.

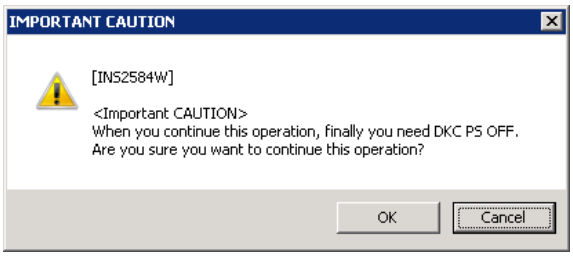
6. <Include configuration information>
   (1)

   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?”.



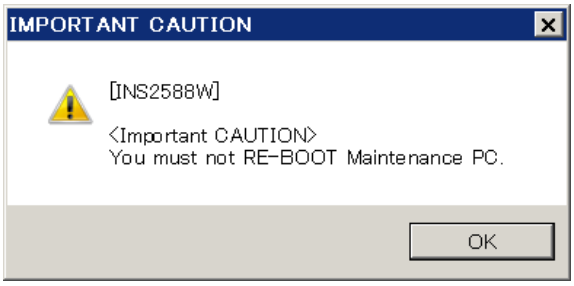
(3)

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.".



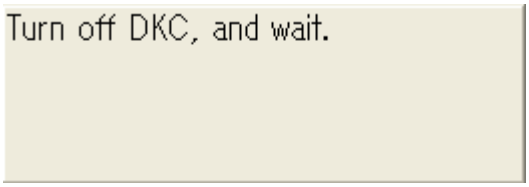
(4)

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.

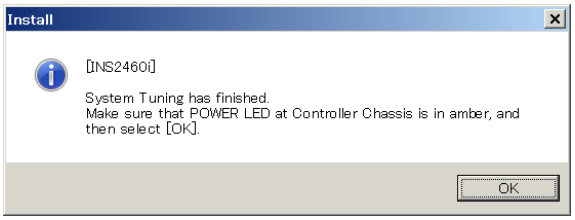


Copyright © 2015, 2017, Hitachi, Ltd.

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.

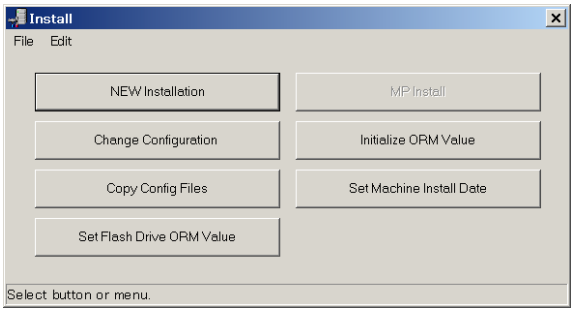


9.

Perform the power-on procedure from the Controller Chassis.

10.

Please click [File]-[Exit] on the Install window.

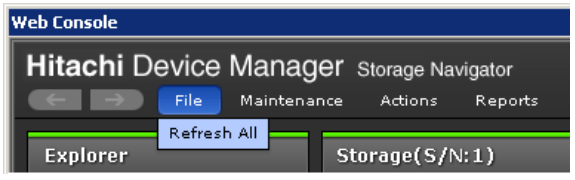


11.

Change the Mode from [Modify Mode] to [View Mode] in the “MPC” window.
Select [Execute]-[Exit].

12.

Please select [File]-[Refresh All] from the menu and update the information in the “Web Console” window.



Copyright © 2015, 2017, Hitachi, Ltd.

5.10 Config Backup

NOTICE:	Use a removable disk or a local disk for the media for backup of this operation.

1.

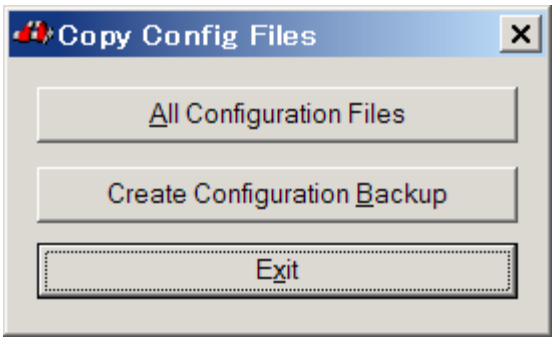
It changes into [Modify Mode] mode in the “MPC” window.

2.

Click [Install] in the “MPC” window and click [Copy Config Files] in the “Install”.

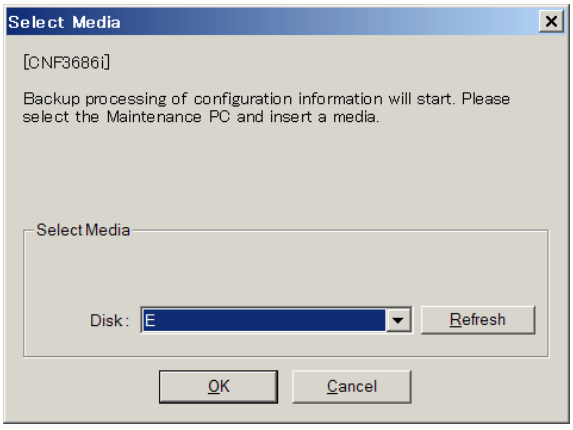
3.

Click [Create Configuration Backup] in the “Copy Config Files”.



4.

“Select Media”[3686] window is displayed.
Insert the Config media for backup into the Maintenance PC.
Click the [Refresh] button and select the drive in which the media was inserted.
Click the [OK] button.

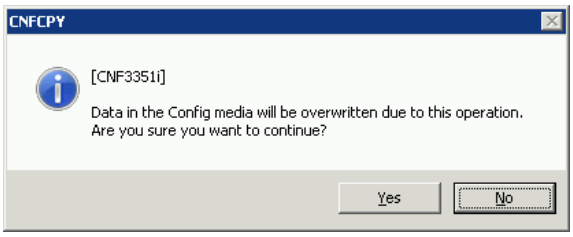


NOTE: If the media was inserted into E drive, the backup configuration information is stored in “E:\DKC200\config\xxxxxx”.
xxxxxx is a serial number.

Copyright © 2015, 2017, Hitachi, Ltd.

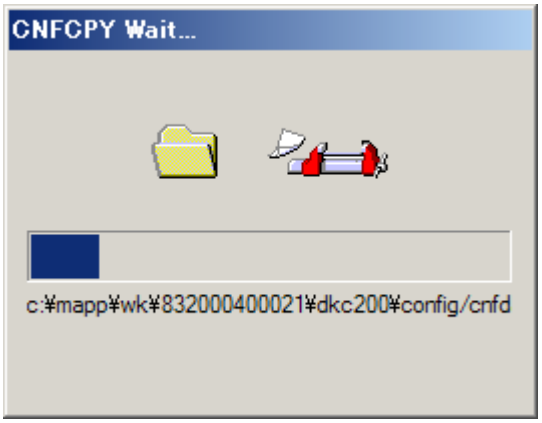
5.

If the configuration information is not saved in the selected media, go to Step 6.
If the configuration information is already saved in the selected media, the information message shown on the “CNFCPY”[3351] window is displayed. When you want to continue the process, click the [Yes] button. When the backup to the Config media is not necessary, click the [No] button and go back to Step 3.



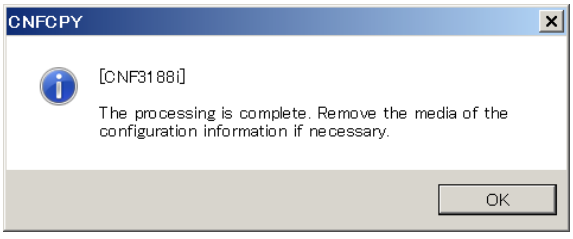
6.

Backup the configuration information to the Config media for backup. While this operation is being done, the “CNFCPY Wait...” window is displayed.



7.

“CNFCPY”[3188] window is displayed.
Remove the configuration information media as needed, and then click the [OK] button.



Copyright © 2015, 2017, Hitachi, Ltd.

8.

Click [Exit] of the “Copy Config Files” to finish this operation.

9.

Close the “Install” window
It changes into [View Mode] in the “MPC” window.

Copyright © 2015, 2017, Hitachi, Ltd.

5.11 Initializing the Configuration Information

NOTICE:	This operation is a special (exceptional) work. Contact the Technical Support Division for validity of the work.

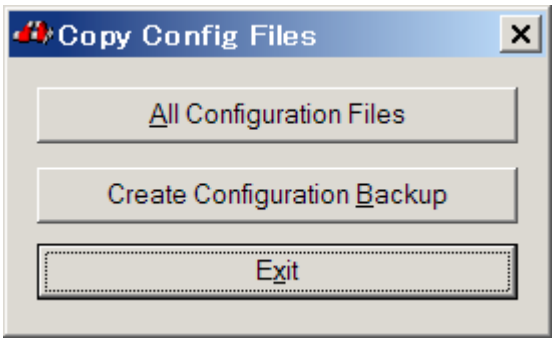
1.

It changes into [Initial Setting] mode on the “MPC” window.
(Press the [Shift] + [Ctrl] + [I] keys, and enter the password and click [OK].)
Click [Install] in the “MPC” window and click [Copy Config Files] in the “Install”.

NOTE: The mode changes to [Initial Setting (Unlocked)] when the Storage System is in CE MODE.

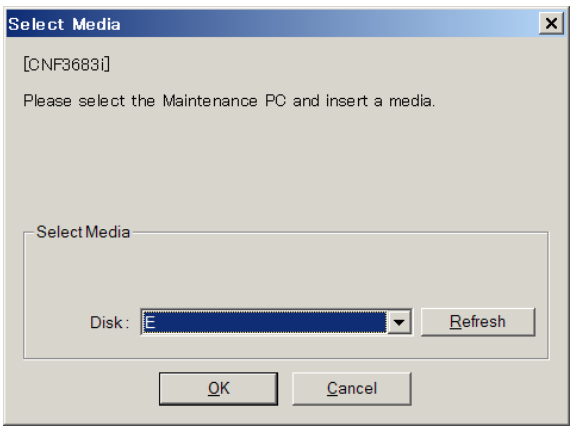
2.

Click the [All Configuration Files] button in the “Copy Config Files”.



3.

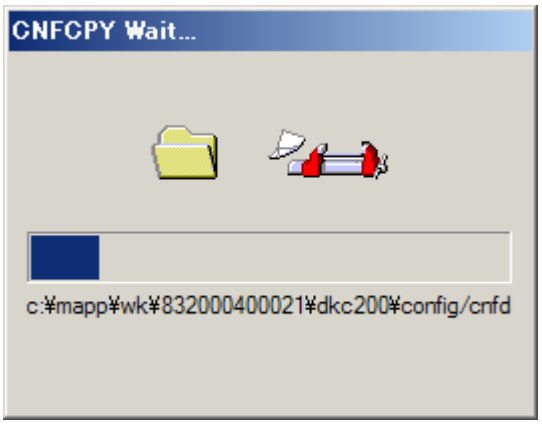
“Select Media”[3683] window is displayed.
Insert the media.
Click the [Refresh] button and select the drive in which the media was inserted.
Click the [OK] button.



Copyright © 2015, 2017, Hitachi, Ltd.

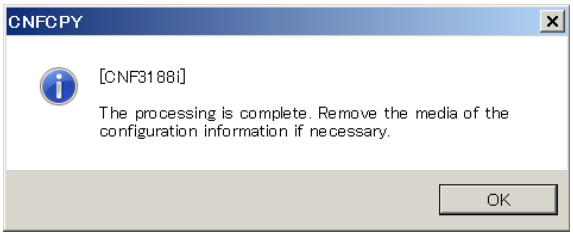
4.

Copy the configuration information from the Config media to the Maintenance PC.
While this operation is being done, the “CNFCPY Wait...” window is displayed.



5.

“CNFCPY”[3188] window is displayed.
Remove the configuration information media as needed, and then click the [OK] button.

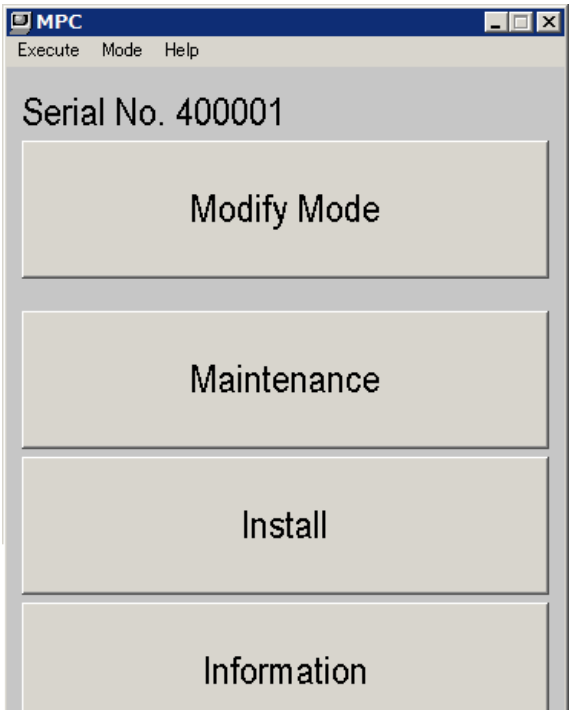


Copyright © 2015, 2017, Hitachi, Ltd.

5.12 Maintenance Screen

5.12.1 Start

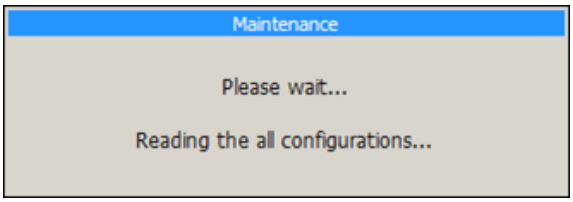
1. <Start>
   Click the [Maintenance] button in the “MPC” window.



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...”



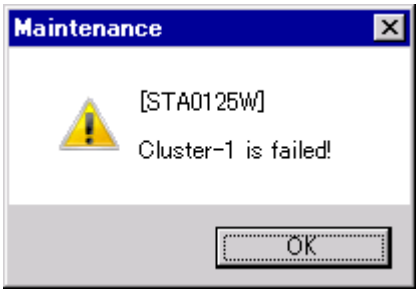
Copyright © 2015, 2017, Hitachi, Ltd.

3. <Start Error>
   When an error occurred while starting the status, the message to indicate the error factor is output.

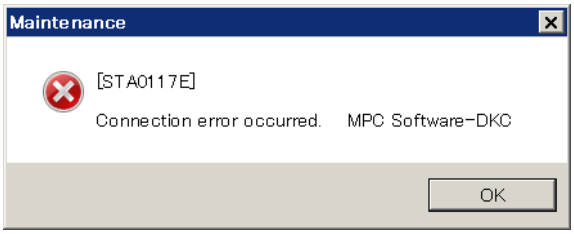
   • Cluster failure
   "[0125/0126] Cluster-n is failed!"
   n: 1 or 2

   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 "11.3.4.2 DKC Information View".)

   Execute the procedure from Step 1 again after checking that the target processing is completed.



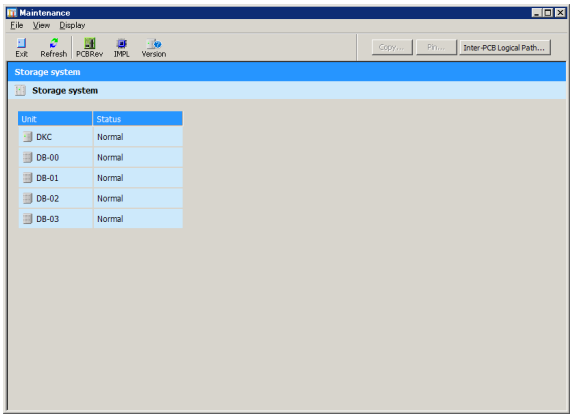
   • Communication failure
   "[0117] Connection error occurred. MPC Software-DKC"
   Refer to TROUBLESHOOTING SECTION "3.10 Recovery Procedure for LAN Error".



Copyright © 2015, 2017, Hitachi, Ltd.

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.)

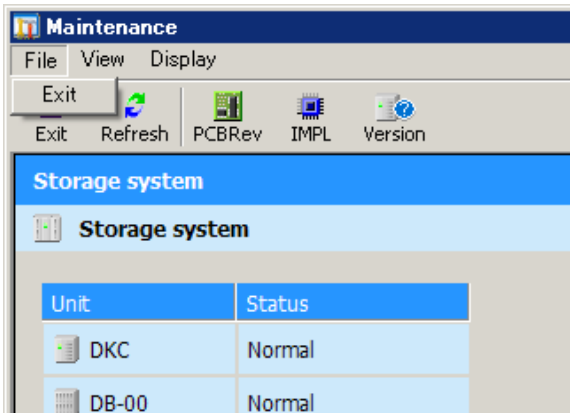
   NOTE: Displayed information is the Storage System information on point that starts the screen.
   To refer to latest information, select the [Refresh] button.
   (Refer to “5.12.3 Update”)



Copyright © 2015, 2017, Hitachi, Ltd.

5.12.2 Terminate

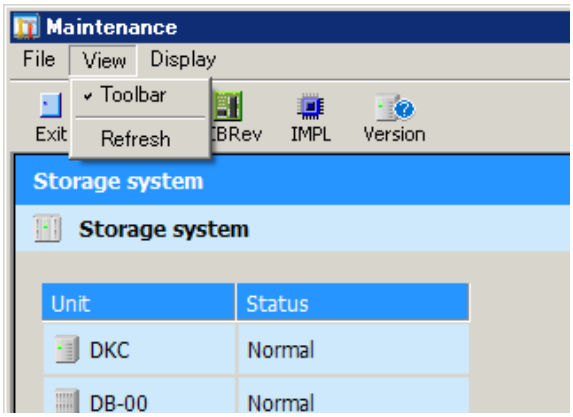
Click [File]-[Exit] on the menu bar in the “Maintenance” window.



Copyright © 2015, 2017, Hitachi, Ltd.

5.12.3 Update

Click [View]-[Refresh] on the menu bar in the “Maintenance” window.



Copyright © 2015, 2017, Hitachi, Ltd.

5.13 Maintenance Procedure

5.13.1 Copy Status View

This window is displayed by selecting [Copy...] on the dialog bar in the main window.

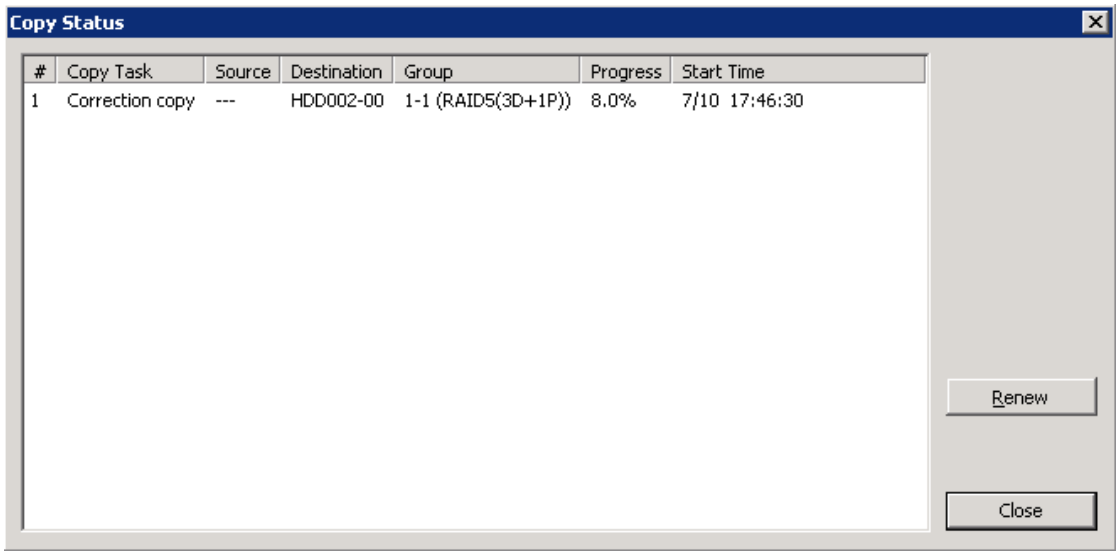


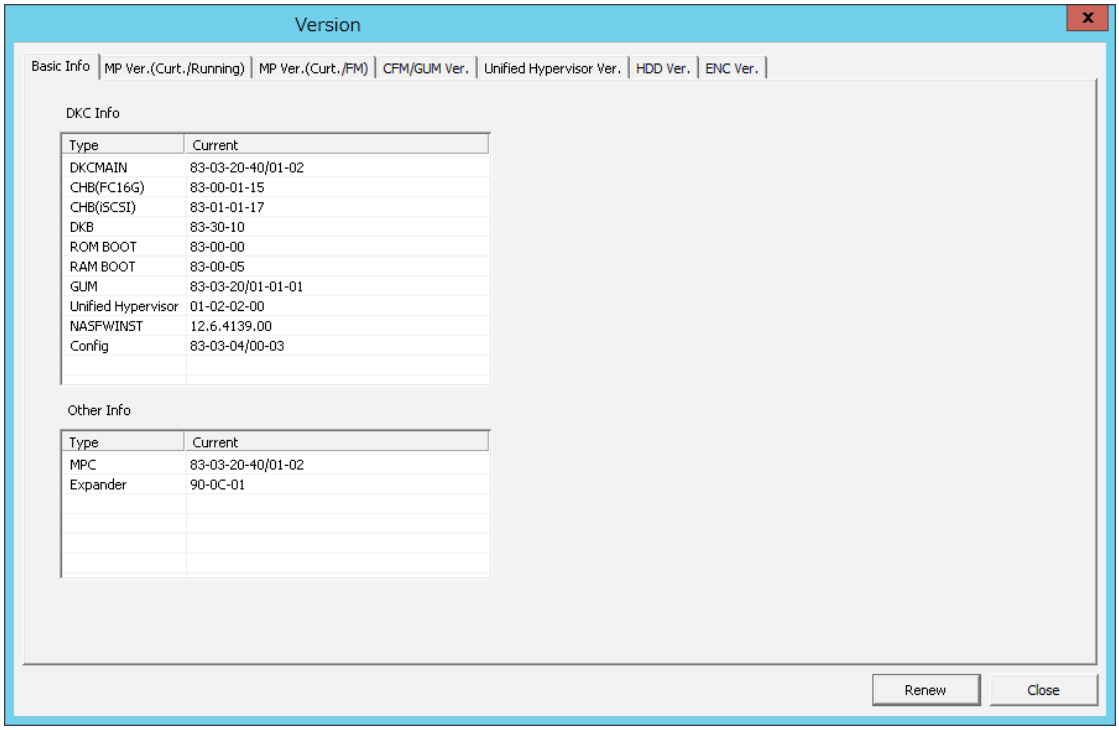
Table 5-12 Copy Status View

Item	Description	
List	Displays the information on the copy operation executing right now.	
	[Copy Task]	Displays the type of the copy operation. "Correction Copy" : Correction copy "*" display: Waiting for the automatic copy back. "Dynamic Sparing" : Dynamic sparing "Copy Back" : Copy back "Drive Copy" : Drive copy
	[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	[Renew]	Updates the information displayed.

5.13.2 Version of Firmware

Click the [Version] button in this order in the “Maintenance” window.
The “Version” window is displayed.

NOTE: When the firmware version is less than 83-03-21-x0/xx, the [Unified Hypervisor] tab is not 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	[Unified Hypervisor]	Displays Unified Hypervisor and NAS firmware versions.
6	[HDD Ver.]	Displays a model and version of each HDD.
7	[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.

Copyright © 2015, 2017, Hitachi, Ltd.

5.13.2.1 Basic Info

The list of Firmware operating on the Storage System and the versions are displayed.

NOTE: When the firmware version is less than 83-03-21-x0/xx, the [Unified Hypervisor] tab is not displayed.

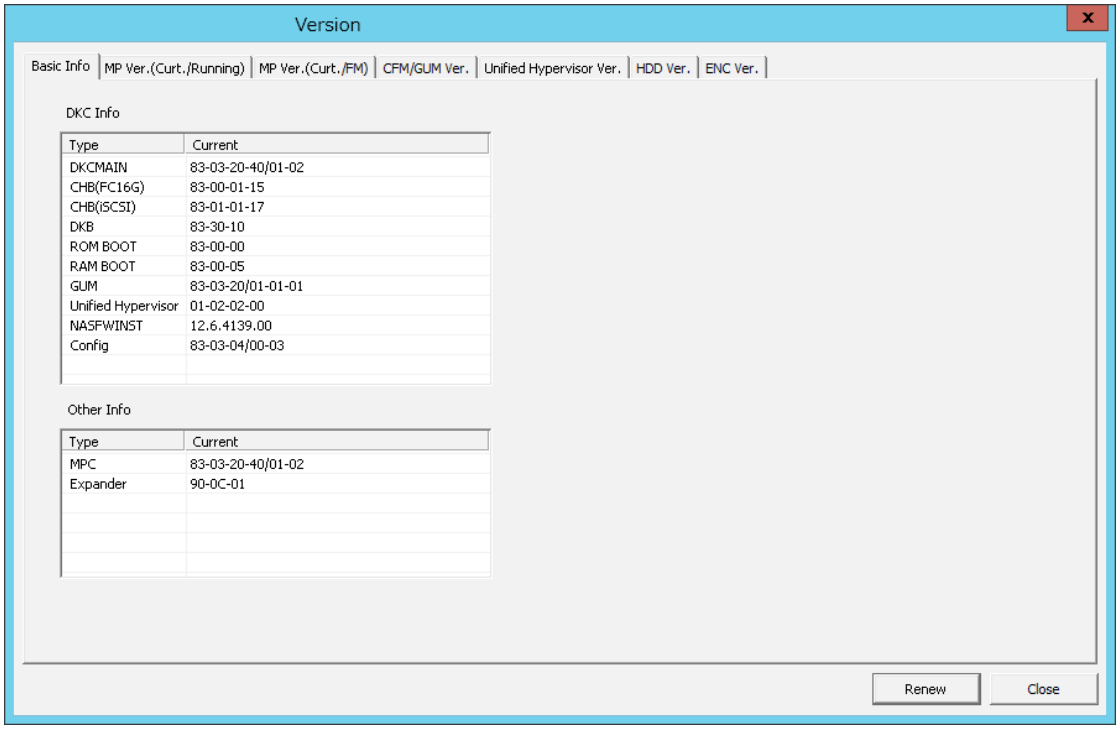


Table 5-13 Displayed information

Item		Description
DKC Info list	Type	Firmware name. <Target> • DKC MAIN • CHB (FC16G) • CHB (FC32G) (*2) • CHB (iSCSI) • DKB • RAM BOOT • ROM BOOT • Unified Hypervisor (*1) • NASFWINST (*1) • GUM • Config
	Current	Main version of the Firmware in use.

*1: When the firmware for NAS is not installed, "-" (Hyphen) is displayed.

*2: When CHB (FC32G) firmware is not installed, "-" (hyphen) is displayed.

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

Item		Description
Other Info list	Type	Firmware name. <Target> MPC Expander
	Current	Main version of the Firmware in use.

Copyright © 2015, 2017, Hitachi, Ltd.

5.13.2.2 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.

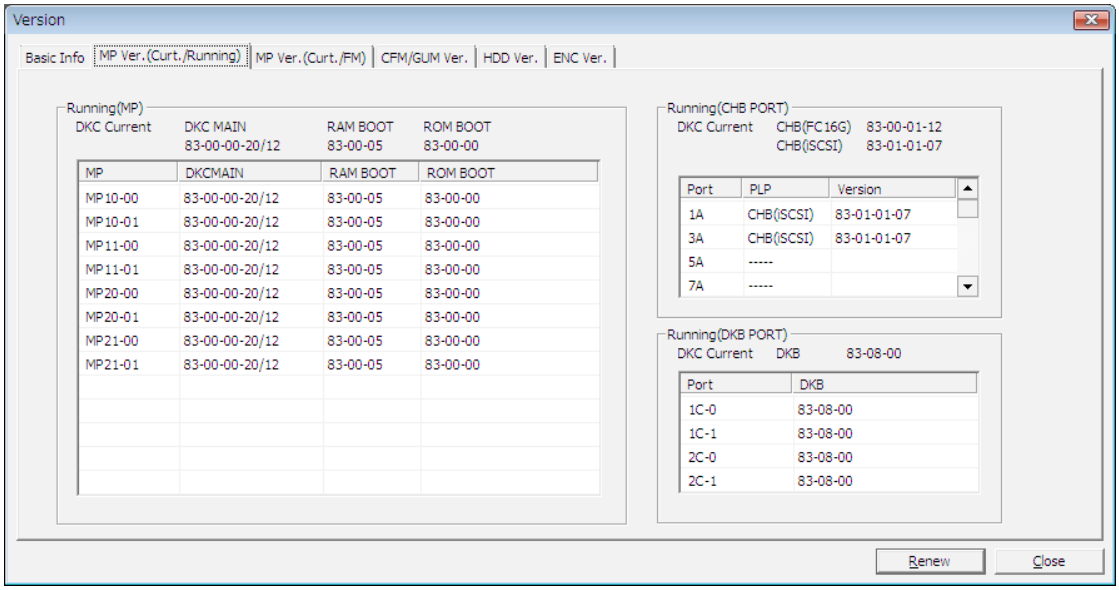


Table 5-14 Displayed information

Item			Description
MP Running area	DKC Current		Displays the version information held by DKC (same as Basic Info tab.) • 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. (*1)
		RAM BOOT	Displays the running RAM BOOT version on MP. (*1)
		ROM BOOT	Displays the running ROM BOOT version on MP. (*1)
		The version highlighted in red/white is unmatched with the DKC Current. The version with "*" at the end is an unmatched item.	

*1: If this is used on NAS, "-" (hyphen) is displayed.

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(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.
		Version	Displays the running Version on Port. 8 G Fibre (CHB (FC8G)) dose not have a firmware, so displayed always "---------".
		The version highlighted in red/white is unmatched with the DKC Current. The version with "*" at the end is an unmatched item.	
DKB Port area	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.	

Copyright © 2015, 2017, Hitachi, Ltd.

5.13.2.3 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".)

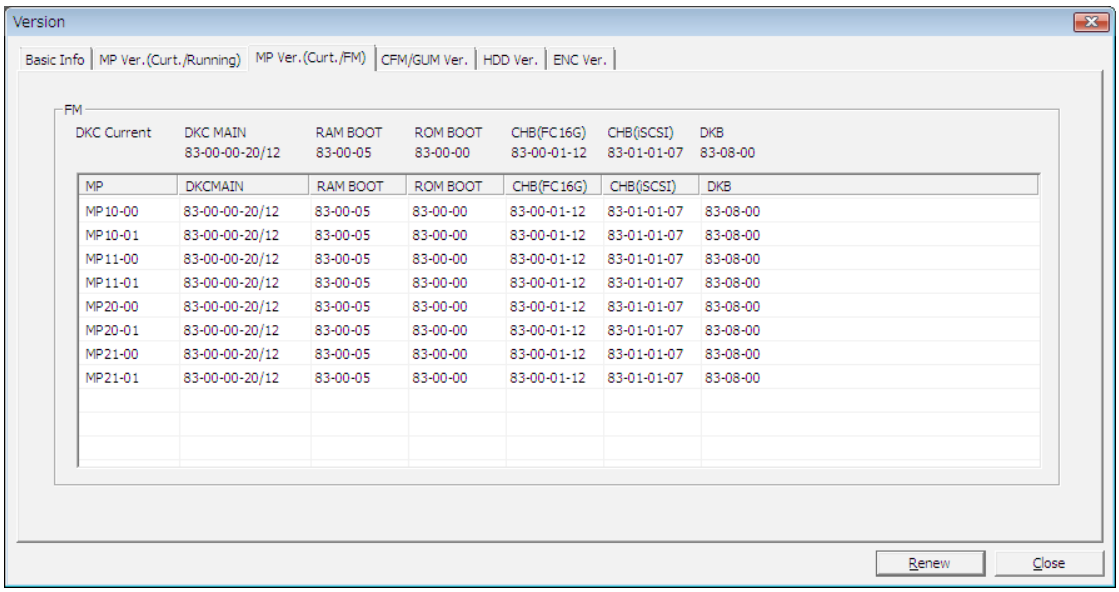


Table 5-15 Displayed information

Item	Description
DKC Current	Displays the version information retained in DKC. The targets are as shown below. (Same as Basic Info tab.) • DKC MAIN • RAM BOOT • ROM BOOT • CHB (FC16G) • CHB (FC32G) • CHB (iSCSI) • DKB

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(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. When CHB (FC32G) firmware is not installed, “-” (hyphen) is displayed.
	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.

Copyright © 2015, 2017, Hitachi, Ltd.

5.13.2.4 CFM/GUM Ver.

The CFM and GUM versions of each CTL are displayed.

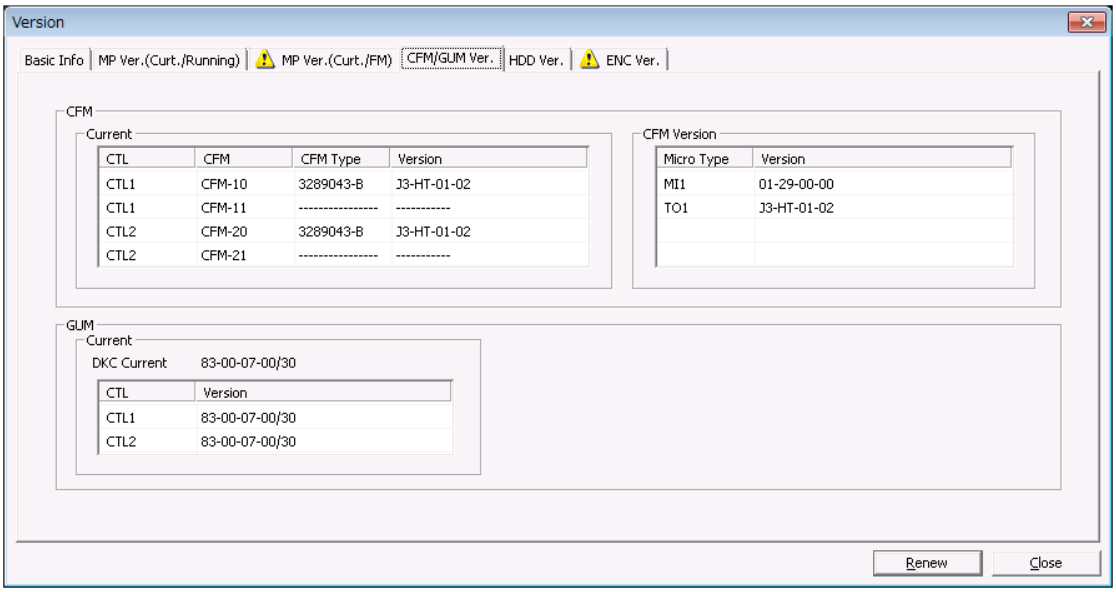


Table 5-16 Displayed information

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.

Copyright © 2015, 2017, Hitachi, Ltd.

5.13.2.5 Unified Hypervisor Ver.

The running versions of Unified Hypervisor, NASFWINST and NASFW are displayed.

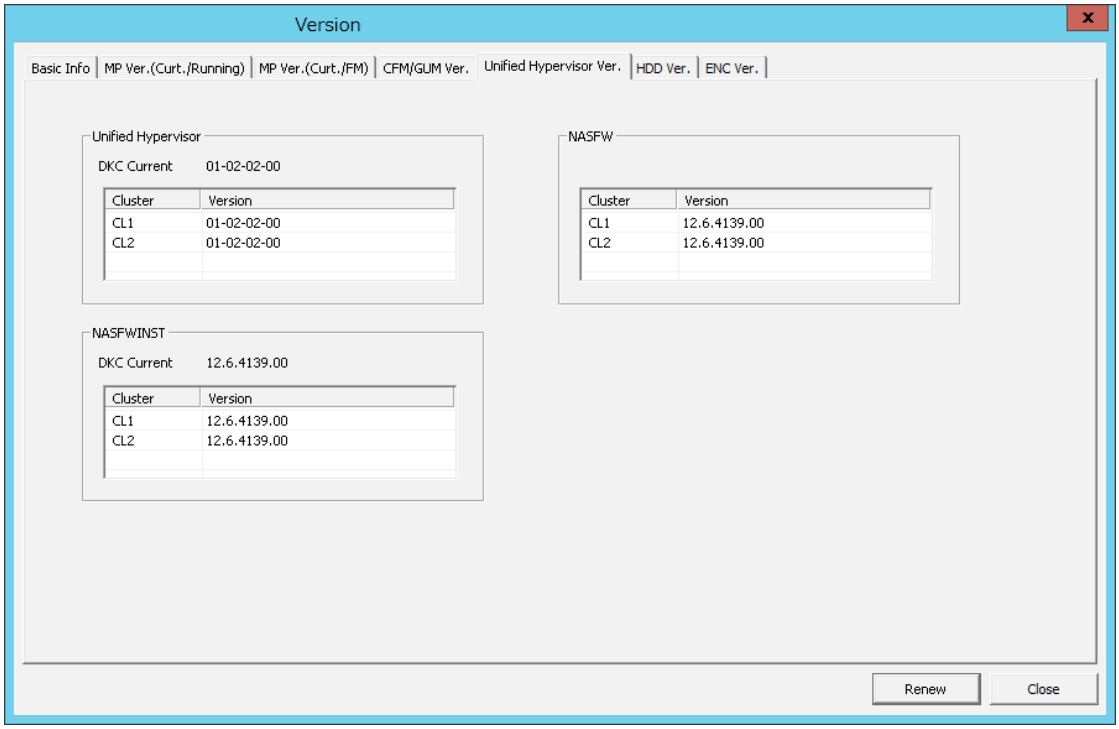


Table 5-17 Displayed information

Item		Description
Unified Hypervisor list	DKC Current	Displays the representative version of Unified Hypervisor.
	Cluster	Displays the Cluster location name.
	Version	Displays the running version. (*1) If the version does not match the DKC current Ver (including acquisition and conversion errors), it is highlighted.
NASFWINST list	DKC Current	Displays the representative version of NASFWINST.
	Cluster	Displays the Cluster location name.
	Version	Displays the running version. (*1) If the version does not match the DKC current Ver (including acquisition and conversion errors), it is highlighted.
NASFW list	Cluster	Displays the Cluster location name.
	Version	Displays the running version. (*1) If the version does not match the CTL1/CTL2 Ver (including acquisition and conversion errors), it is highlighted.

*1: When the firmware for NAS is not installed, “-” (Hyphen) is displayed.

Copyright © 2015, 2017, Hitachi, Ltd.

5.13.2.6 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.

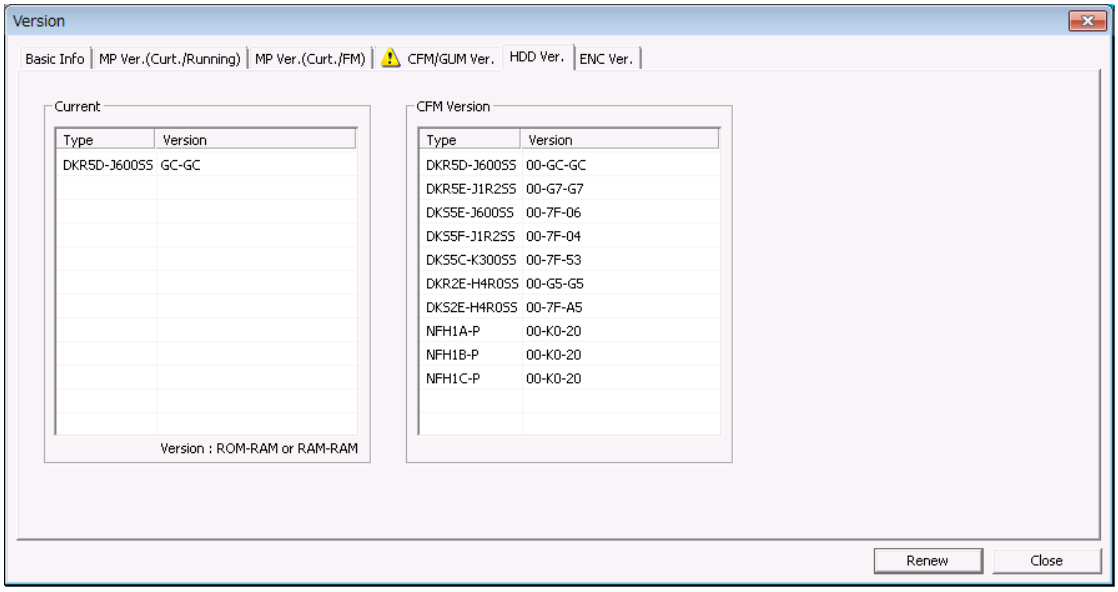


Table 5-18 Displayed information

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.

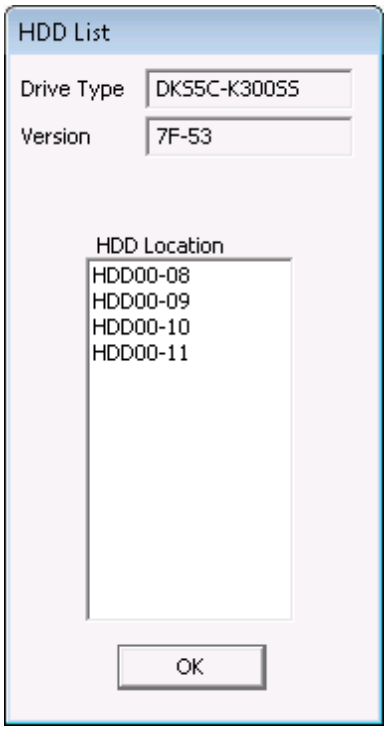


Table 5-19 Displayed information

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.

Copyright © 2015, 2017, Hitachi, Ltd.

5.13.2.7 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.

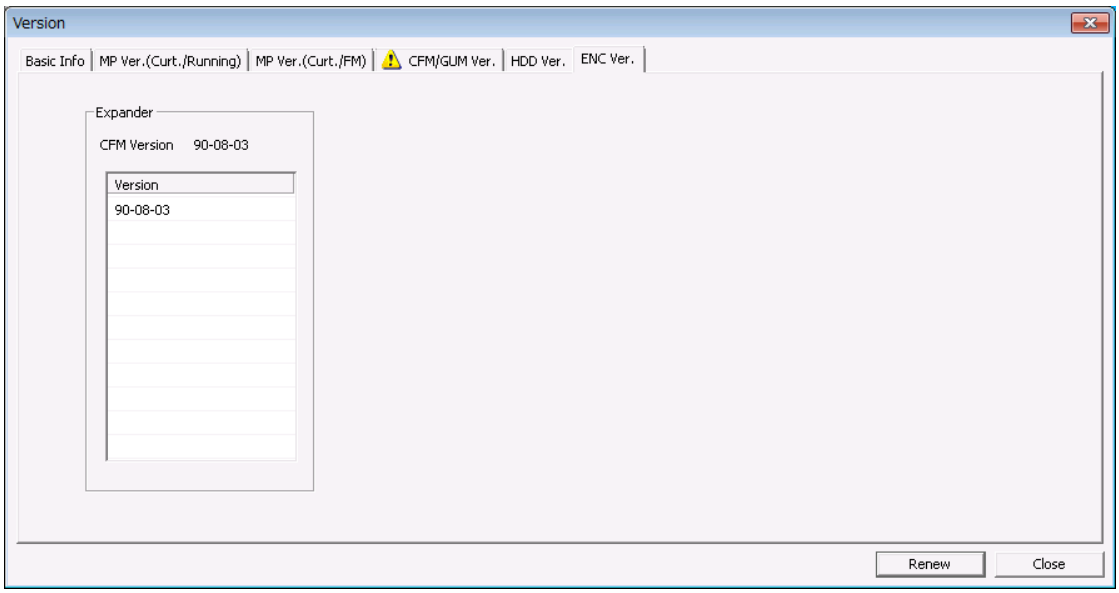


Table 5-20 Displayed information

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 (MPC05-1130) The version highlighted in red/white is unmatched with the CFM Version. The version with "*" at the end is an unmatched item.

Copyright © 2015, 2017, Hitachi, Ltd.

<Display Expander Name>

Double-click a row from the list of [Expander] - [Version].

The “Expander List” window is displayed and the list of the ENCs matched with the information is displayed.

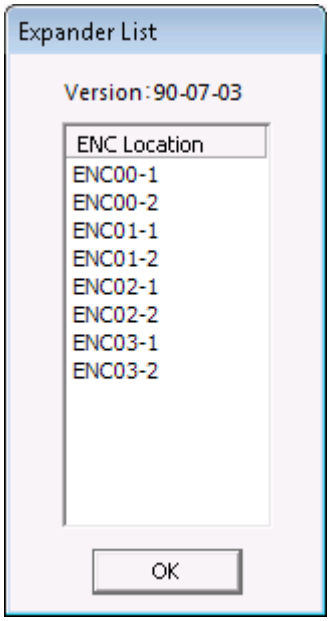


Table 5-21 Displayed information

Item	Description
Version	The selected Expander Firmware version.
ENC Location	A list of ENCs matched with the selected version.

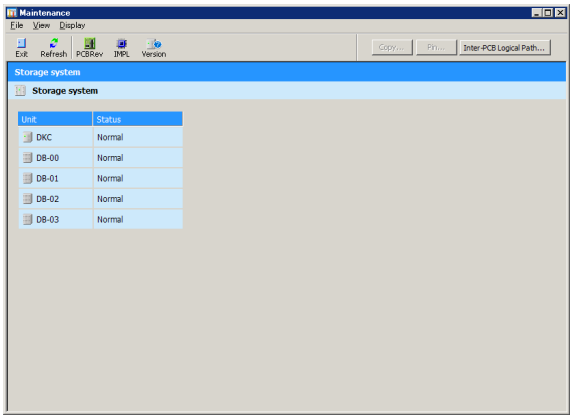
Copyright © 2015, 2017, Hitachi, Ltd.

5.13.3 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.

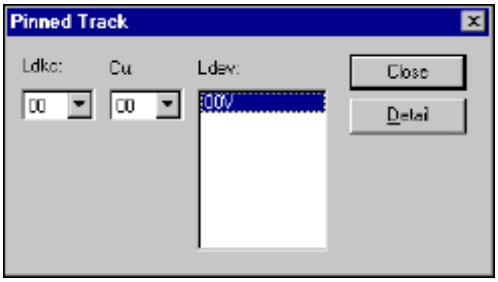


Table 5-22 List of Items

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.

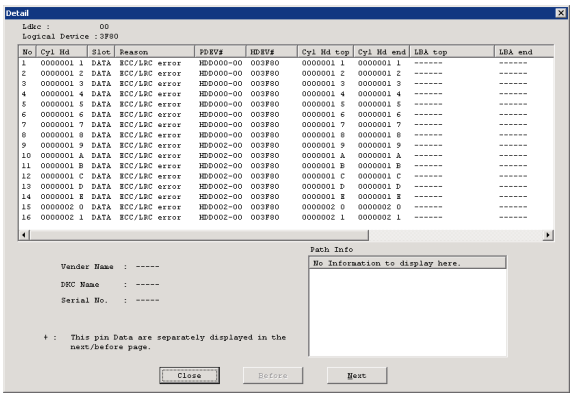


Table 5-23 List of Items

Item	Description
Logical Device	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.
Cyl Hd	Number of an assembly of a cylinder and head in which pinned data exists
Slot	Type of a track on which pinned data exists DATA : Data track PRTY : Parity track
Reason	Cause of pinned data. See the TROUBLESHOOTING SECTION "4.2.1 Pinned Tracks" for the recovery procedure at the following reason. • ECC/LRC error • WRITE error • External VOL Read Error • External VOL Write Error

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from the preceding page)

Item	Description
PDEV#	Number of an HDD of a logical device in which pinned data exists
HDEV#	HDEV number "#": 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.
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)	HDEV number in Dynamic Provisioning "#": 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.
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

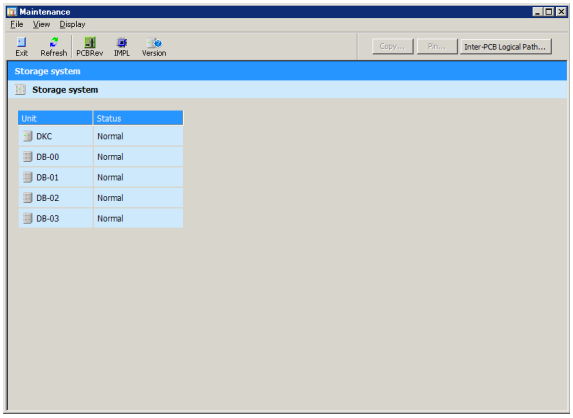
5. Click the [Close] button in the "Detail" window.
   Click the [Close] button in the "Pin Volume" window.
   Close the "Maintenance" window.

Copyright © 2015, 2017, Hitachi, Ltd.

5.13.4 PCB/SFP Revision Display

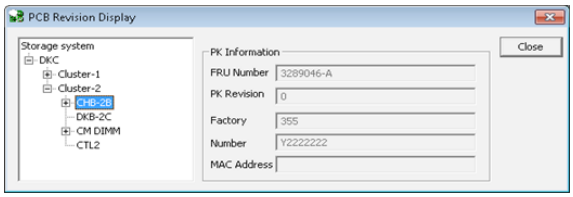
1. Click the [Maintenance] button in the “MPC” window.

2. Click the [PCBRev] button in the “Maintenance” window.



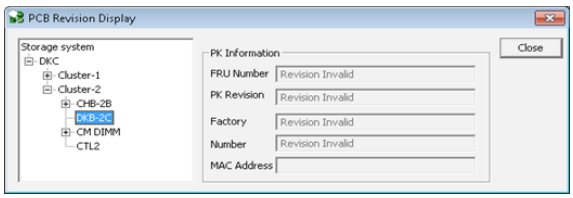
3. “Reading or Writing PCB revision informations...” is displayed.

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.
PORT cannot be selected for the NAS Modules (CHB-xA/xB/xC/xD)

- When selecting a DKB in the CBSS/CBSL, [Revision Invalid] is displayed for all the items.



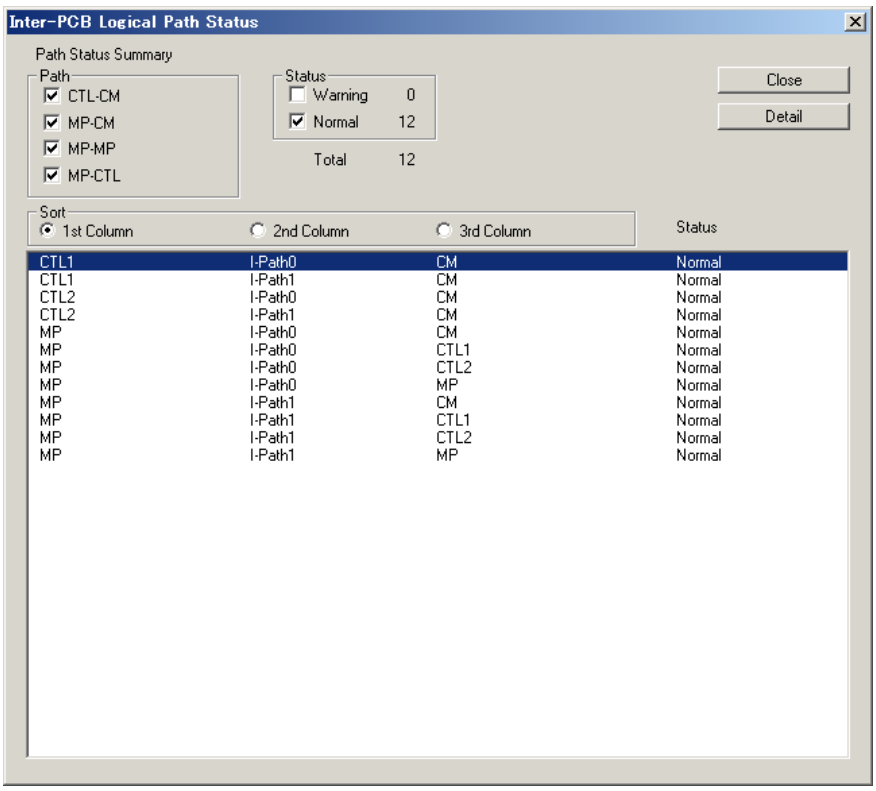
5. Click the [Close] button in the “PCB Revision Display” window.

6. Close the “Maintenance” window.

Copyright © 2015, 2017, Hitachi, Ltd.

5.13.5 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) ----

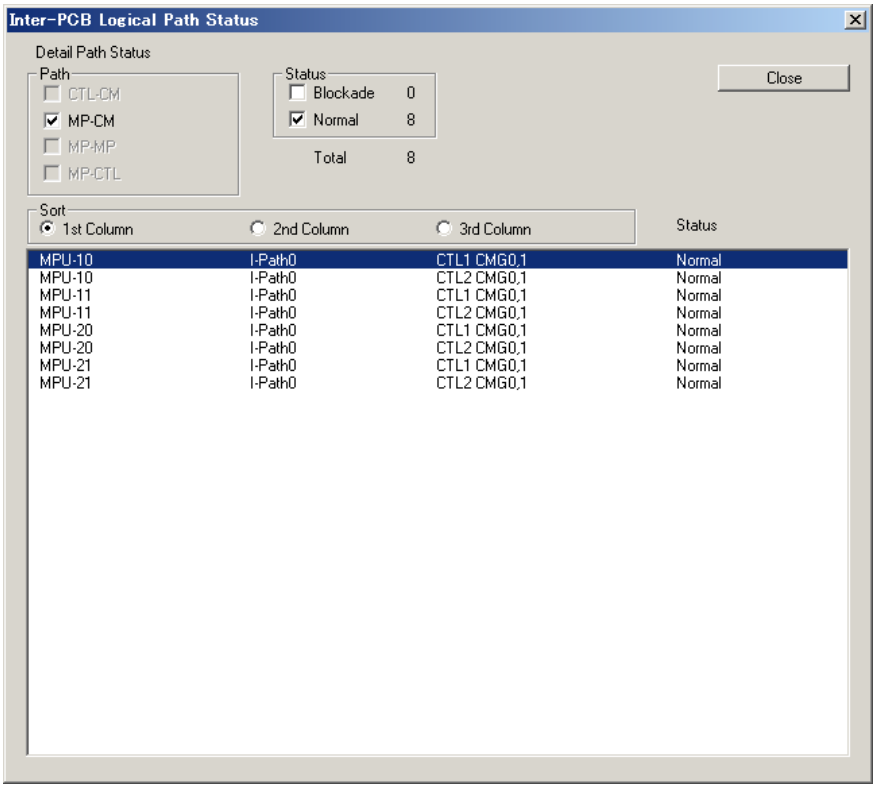
1st Column : Summary path group names are displayed in the row. When this row is selected, the path statuses in the list are sorted using the letter strings in the 1st row as a key word.
2nd Column : CTL location names are displayed in this row. When this row is selected, the path statuses in the list 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.

Copyright © 2015, 2017, Hitachi, Ltd.

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.

Copyright © 2015, 2017, Hitachi, Ltd.

(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.

Copyright © 2015, 2017, Hitachi, Ltd.

5.13.6 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.
> If a failure occurs on the assigned MP, reset Unified Hypervisor. For the reset procedure, see "3.28.2 Resetting Unified Hypervisor".

<Usage Conditions>

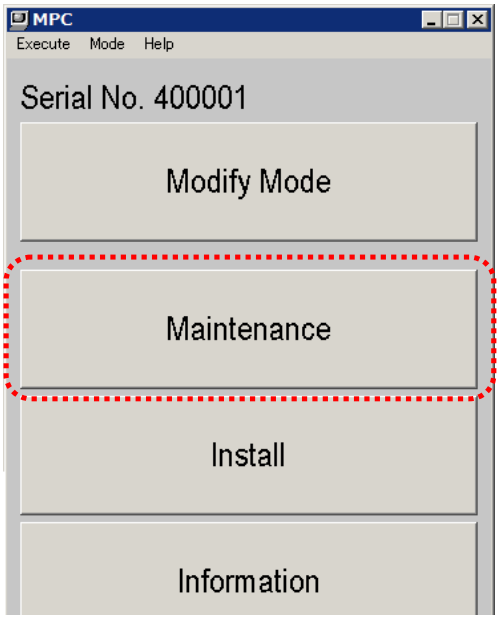
- To recover a MP in which WCHK1 occurred due to a Firmware problem.
  Eg.) Cause of WCHK1 is EC = 1644.
- To recover a MP in which WCHK1 occurred due to an issue outside the DKC (Host/SAN).
  Eg.) Cause of WCHK1 is EC = B405, and it is evident that it is caused by external factor. (Switch etc.)
- Requested 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.

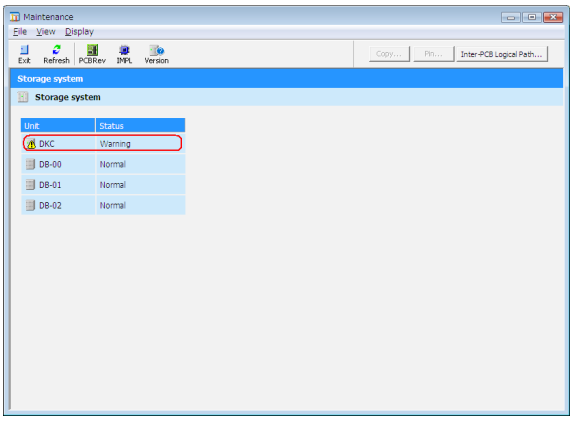
1. <Preparation>
   Close each menu of the starting MPC Software entirely.

2. <Start>
   Change the mode to [Modify Mode].
   Click the [Maintenance] button in the "MPC" window.

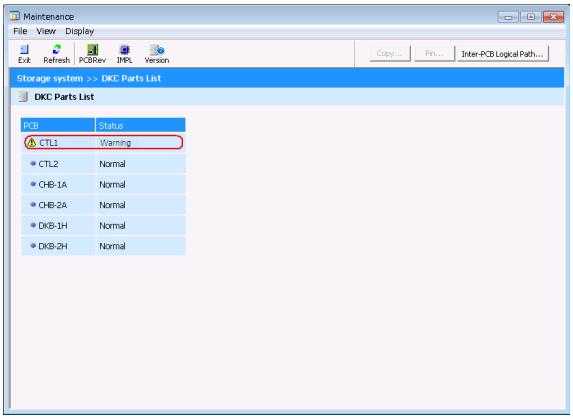


Copyright © 2015, 2017, Hitachi, Ltd.

3. <Display of DKC Information>
   Select the [DKC].

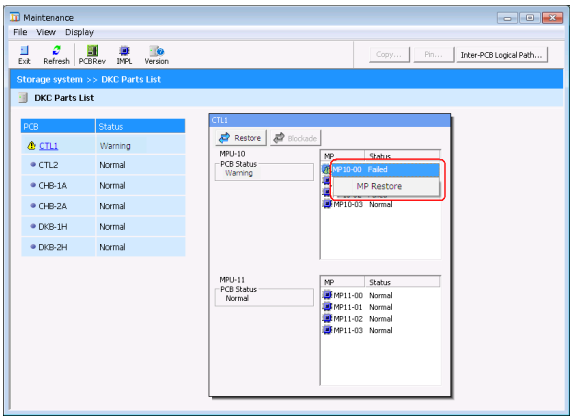


4. <Display of CTL Information>
   Click the [CTLn] button.



5. <Execution>
   Click the right button of the mouse in the status that MP of the maintenance target on the selected.

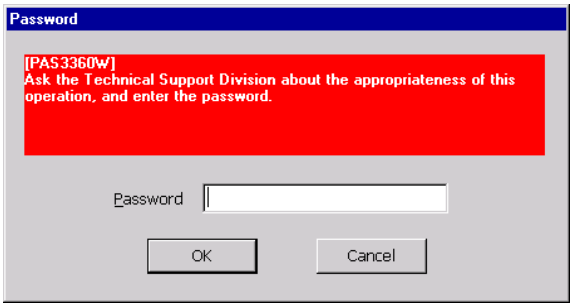
   Click the [MP Restore] button in the displayed popup menu.



6. <Password Input>

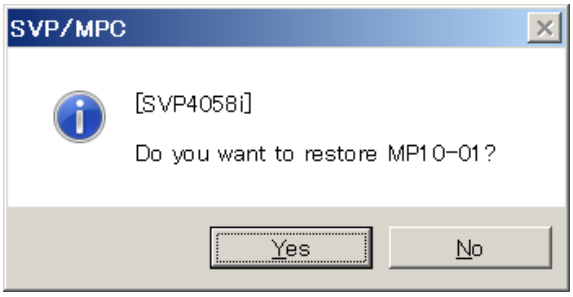
> **CAUTION**
>
> When the blockade of MP attributes to a hardware failure, it is possible that Storage System down or data lost occurs. Ask the technical support division about the appropriateness of the operation, and input the password after getting an approval of executing the operation.

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."



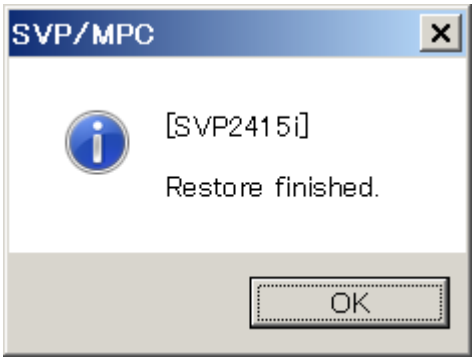
Copyright © 2015, 2017, Hitachi, Ltd.

7. <Execution Check>
   Click the [Yes] button for the following message.
   "[4058] Do you want to restore X?"
   X: Target MP

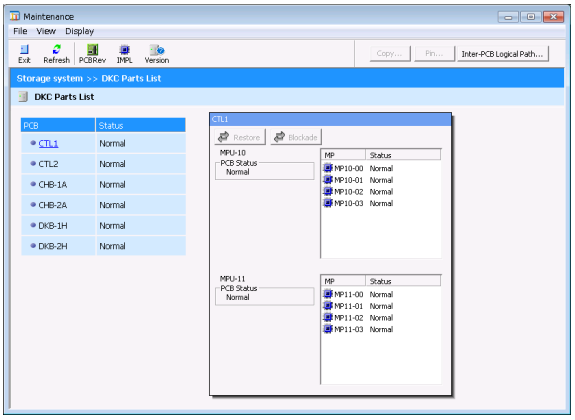


8. <Waiting for the completion of processing>
   The following message is displayed.
   "Please wait... Restoring the MP..."

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.



Copyright © 2015, 2017, Hitachi, Ltd.

11. <Post-processing>
    Close the “Maintenance” window.
    Change the mode to [View Mode].

Copyright © 2015, 2017, Hitachi, Ltd.

5.13.7 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.

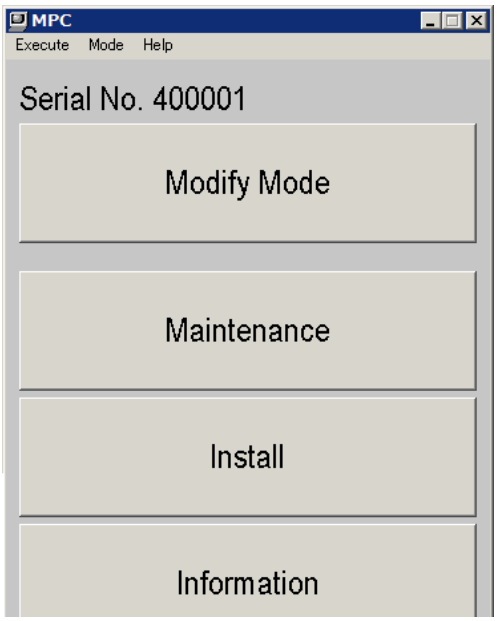
<Usage Conditions>
- Requested as a recovery procedure for an issue notified by an Early Notice/Alert.
- Requested by following the procedure described in Maintenance Manual.

<Usage Restrictions>
- Not to be used to recover hardware failures.

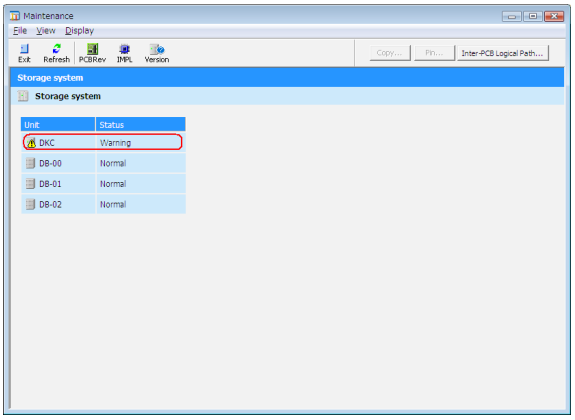
Copyright © 2015, 2017, Hitachi, Ltd.

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.

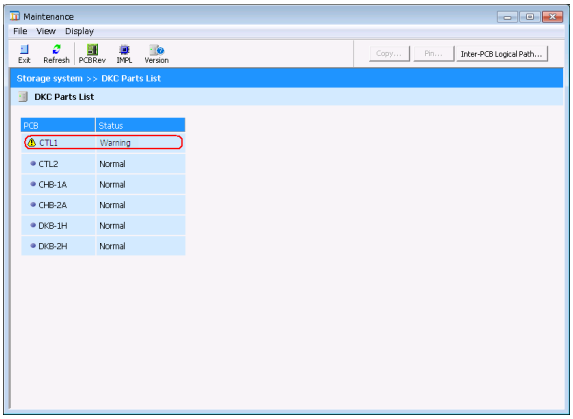


3. <Display of DKC Information>
   Select [DKC].



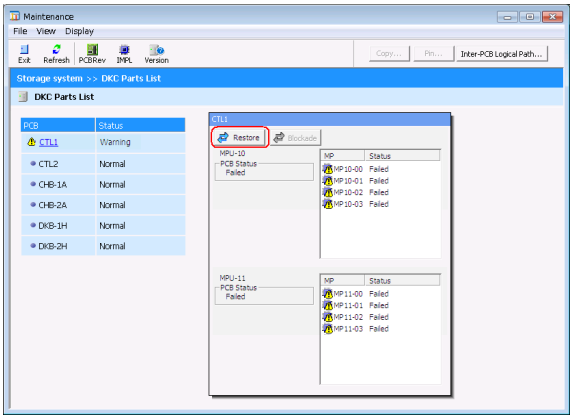
Copyright © 2015, 2017, Hitachi, Ltd.

4. <Display of CTL Information>
   Click the [CTLn] button.



Copyright © 2015, 2017, Hitachi, Ltd.

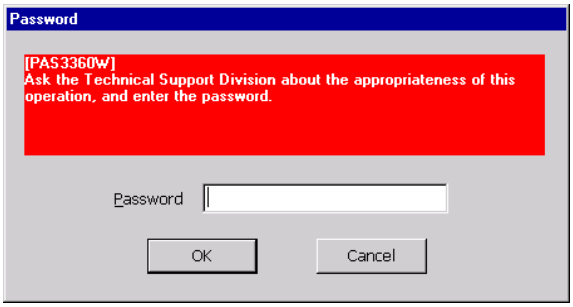
5. <Execution>
   Click the detail view [Restore] button.



6. <Password Input>

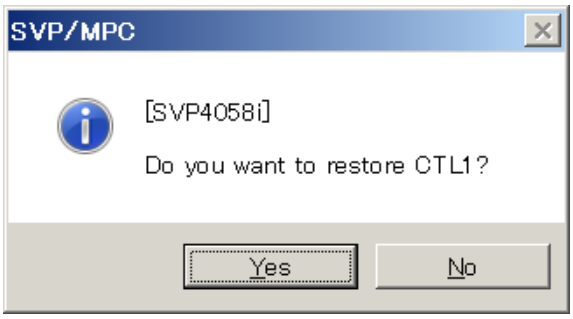
> **⚠ CAUTION**
>
> When the blockade of PCB attributes to a hardware failure, it is possible that Storage System down or data lost occurs. Ask the technical support division about the appropriateness of the operation, and input the password after getting an approval of executing the operation.

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."



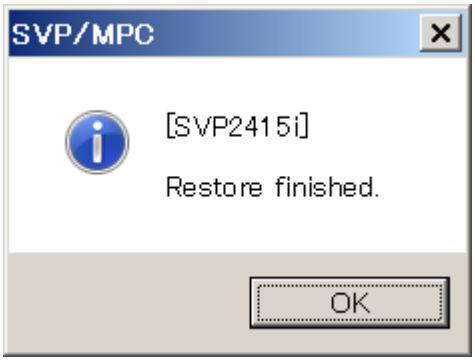
Copyright © 2015, 2017, Hitachi, Ltd.

7. <Execution Check>
   Click the [Yes] button for the following message.
   “[4058] Do you want to restore CTLn?”
   n: Cluster number of target CTL



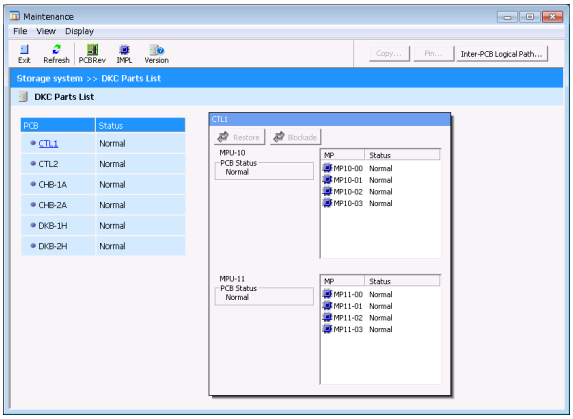
8. <Waiting for the completion of processing>
   The following message is displayed.
   “Please wait... Restoring the CTL1...”
   n: Cluster number of target CTL

9. <Check of the recovery completion>
   Click the [OK] button for the following message.
   “[2415] Restore finished.”



Copyright © 2015, 2017, Hitachi, Ltd.

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].

Copyright © 2015, 2017, Hitachi, Ltd.

5.13.8 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.

Copyright © 2015, 2017, Hitachi, Ltd.

NOTICE: You can operate items other than the those described, but do not operate any items other than the those described unless otherwise instructed.

6. Main Operation Items of NAS Manager

6.1 Logging into/Logging out NAS Manager

6.1.1 Logging into NAS Manager

1. Connect the Maintenance PC to the maintenance port of CTL1.

2. Connect to NAS Manager from the Web browser of the maintenance PC.
   When connecting to Web Manager, enter the following URL.
   http://<IP address of the NAS Platform>

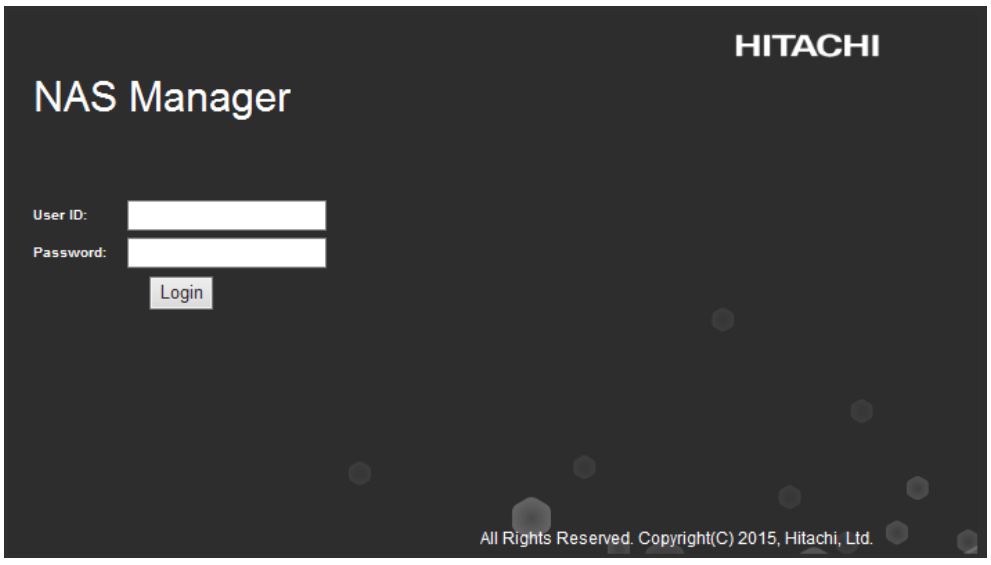
   NOTE : The IP address of the NAS Platform on the CTL1 side is 10.0.0.20 (by default). For the details, see "13.1 IP Addresses of Maintenance Ports and Internal Network".
   If the IP address was changed, contact the system administrator to check the changed IP address.

   If you cannot connect to NAS Manager, exchange the cables of the maintenance ports between CTL1 and CTL2, and then connect to the NAS Manager again.

   NOTE : The IP address of the NAS Platform on the CTL2 side is 10.0.0.21 (by default). For the details, see "13.1 IP Addresses of Maintenance Ports and Internal Network".
   If the IP address was changed, contact the system administrator to check the changed IP address.

3. The Login window is shown below.
   Enter the user name and the password.
   User ID: Enter a user name of the Storage System.
   Password: Enter the password of the Storage System.

   NOTE : If the user name and the password are changed, confirm with the system administrator.



Copyright © 2015, 2017, Hitachi, Ltd.

6.1.2 Logging out from NAS Manager

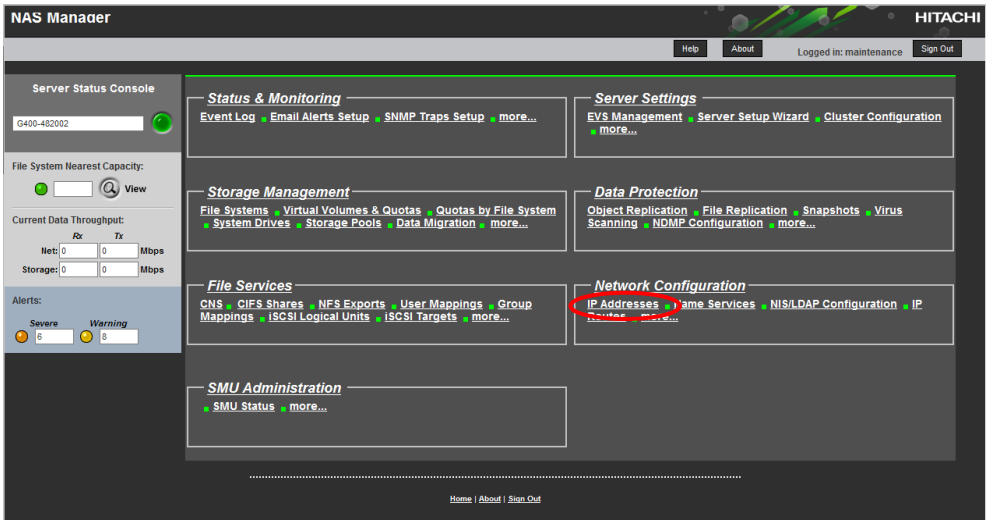
Logging out from NAS Manager is required after completing the maintenance operations.
To log out, press the [Sign Out] button on the right top of the NAS Manager window, and close the Web browser. If the NAS Manager is not terminated, close the Web browser directly.

Copyright © 2015, 2017, Hitachi, Ltd.

6.2 Collecting IP Address Information

1. Connect to NAS Manager from the Web browser of the Maintenance PC.
   For the details, see "6.1 Logging into/Logging out NAS Manager".

2. Click [IP Addresses] in the "Home" window.



3. The “IP Addresses” window is as shown below.

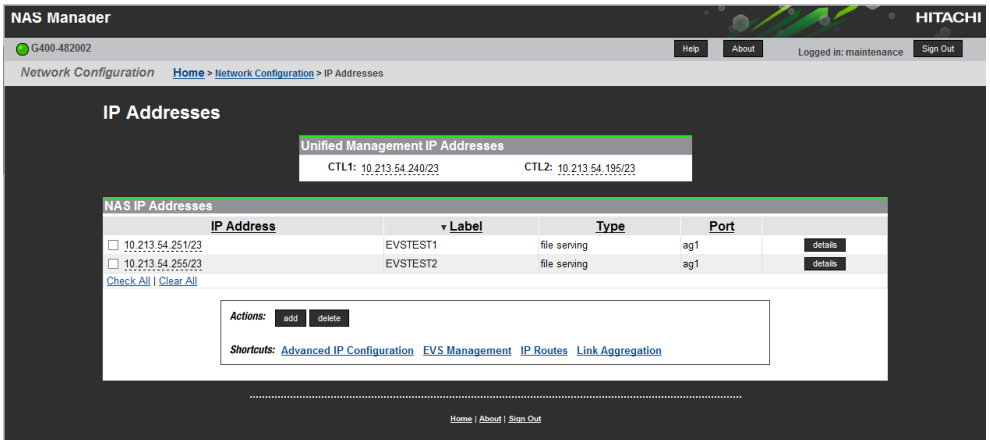


Table 6-1 Items Displayed in the IP Addresses window

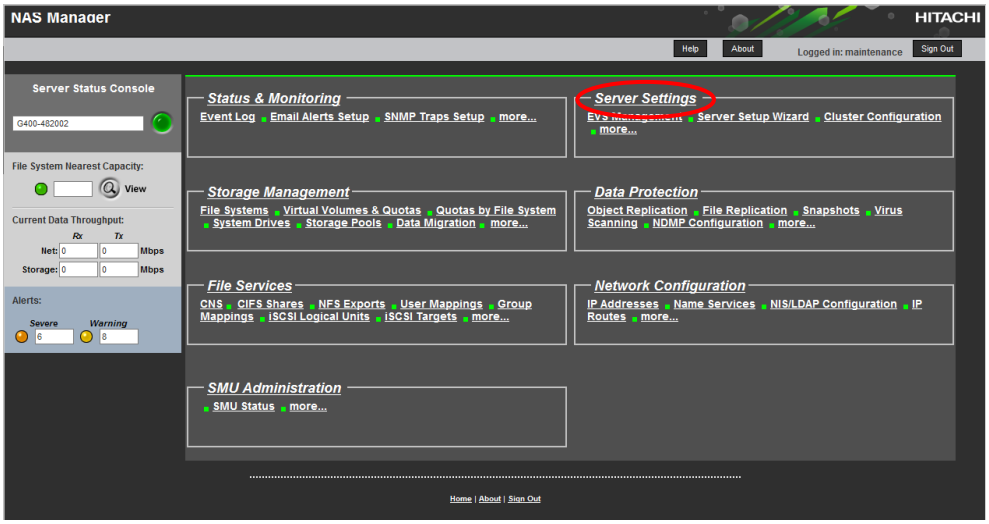
Item		Description
Unified Management IP Addresses		
	CTL1/CTL2	It is the management IP address set on each controller.
NAS IP Addresses		
	IP Address	IP address and the subnet mask used in the management service or the file service.
	Label	If it is used for the file service, it is the EVS name. For other cases, it is the node name in use.
	Type	It is the service type of the node and the settings. File Services: IP address related to the management service of the NAS cluster. The IP address of the management service can exist in the public data network or the private management network. admin services: IP address related to the file service of the NAS cluster. The IP address of the file service needs to be in the public data network.
	Port	It is the following interfaces used by the IP address. • [agX] indicates one of the GbE aggregations.

Copyright © 2015, 2017, Hitachi, Ltd.

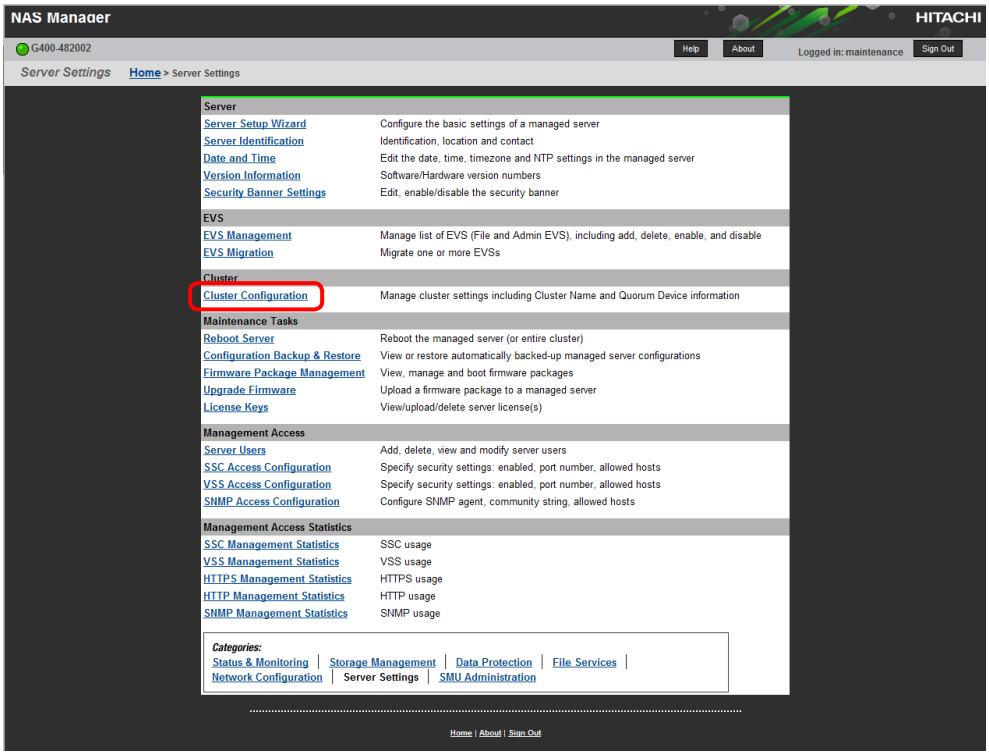
6.3 Confirming the Node Status

1. Connect to NAS Manager from the Web browser of the Maintenance PC.
   For the details, see "6.1 Logging into/Logging out NAS Manager".

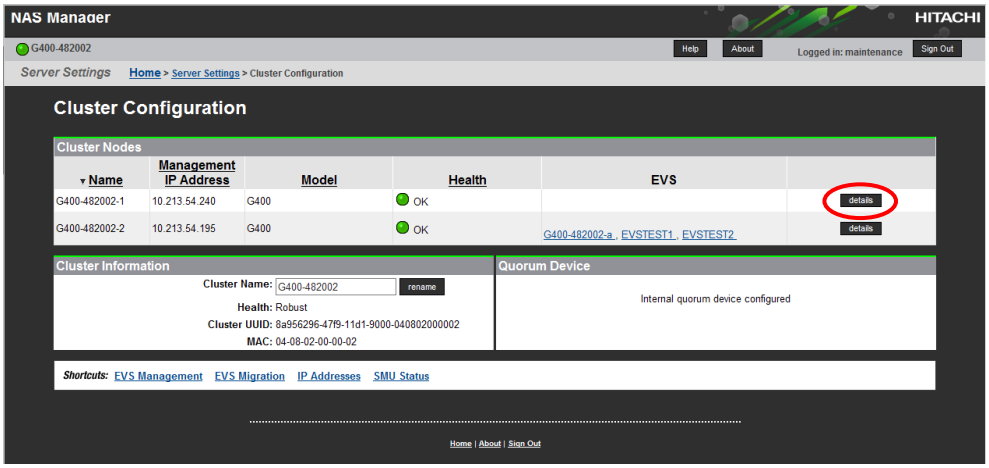
2. Click [Server Settings] in the "Home" window.



3. Click [Cluster Configuration] in the "Server Settings" window.

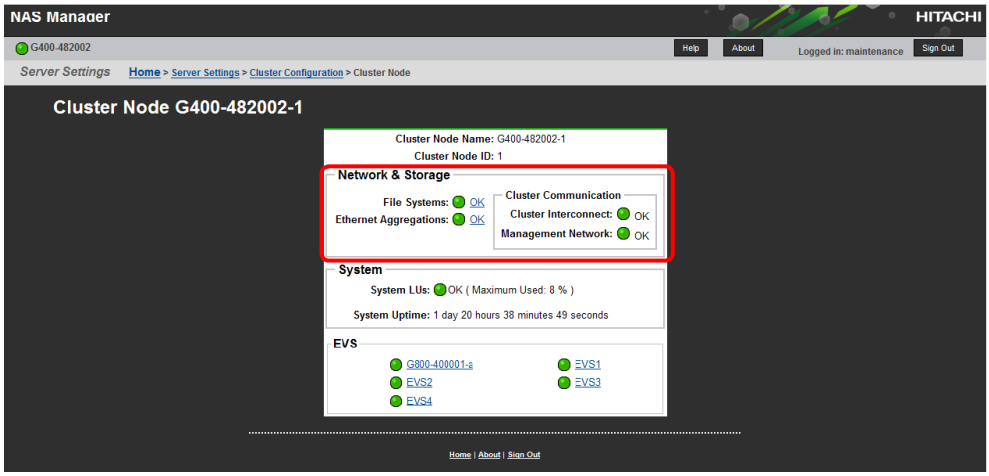


4. Click the [details] button of the node you want to confirm the status with “Cluster Configuration” window, and open the “Cluster Node” window.



Copyright © 2015, 2017, Hitachi, Ltd.

5. The “Cluster Node <Name:>” window is shown below”.



The status displayed in each item is shown below.

Table 6-2 Status of Each Part

Item			Status	Description
Network & Storage				
	File System		OK	All file systems are normal.
			Failed	One or more file systems failed.
	Ethernet Aggregations		OK	All aggregation ports are linked.
			Degraded	One or more ports failed.
			Failed	All ports failed.
	Cluster Communication			
		Cluster Interconnect	OK	Link is operable and heartbeat is received.
			Standby port down	Primary link is operable and heartbeat is received. However, the secondary link is down.
			Link up, no heartbeating	At least one link is operable. However heartbeat is not received.
			Link down	All links are down.
		Management Network	OK	Link is operable and heartbeat is received.
			Link up, no heartbeating	At least one link is operable. However heartbeat is not received.
			Link down	All links are down.

Copyright © 2015, 2017, Hitachi, Ltd.

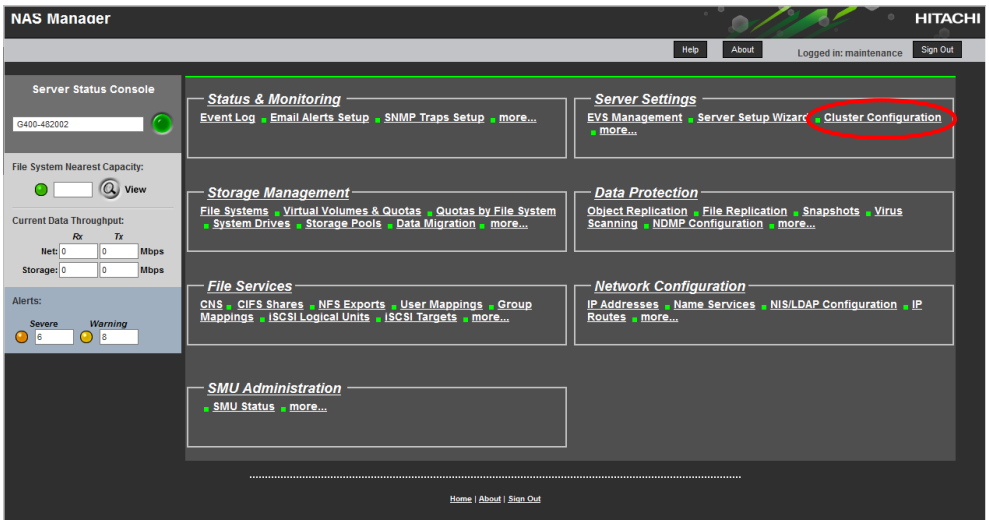
6.4 Migrating EVS

NOTICE:
- When you perform the EVS migration, you cannot access temporarily. Perform the migration after confirming with the system administrator.
- If the migration cannot be performed, contact the Technical Support Devision.

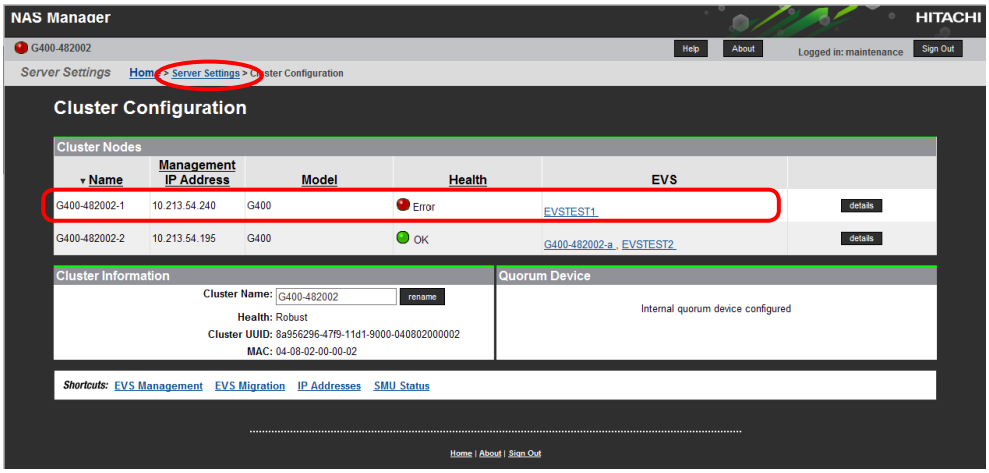
6.4.1 Migration before the Maintenance Operations

1. Connect to NASWeb Manager from the Web browser of the Maintenance PC.
   For the details, see "6.1 Logging into/Logging out NAS Manager".

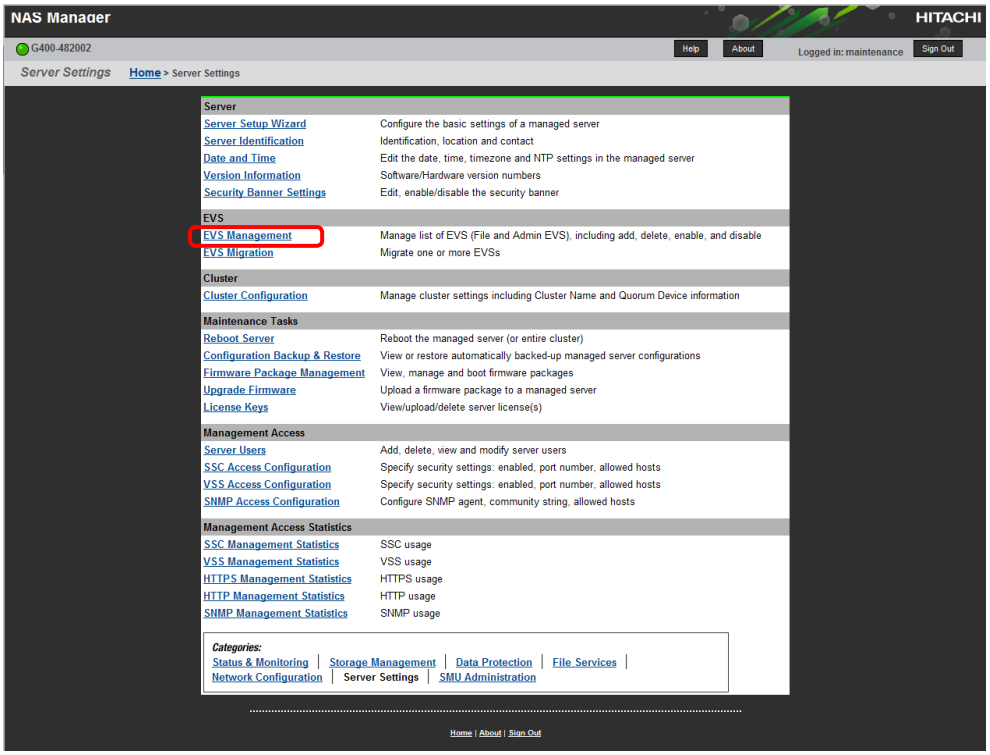
2. Click [Cluster Configuration] in the "Home" window.



3. Confirm the name of the node to be maintained in the "Cluster Configuration" window.
   Confirm the names of the node to be maintained from the [Name] column and record them.
   When the node names are confirmed, click [Server Settings].

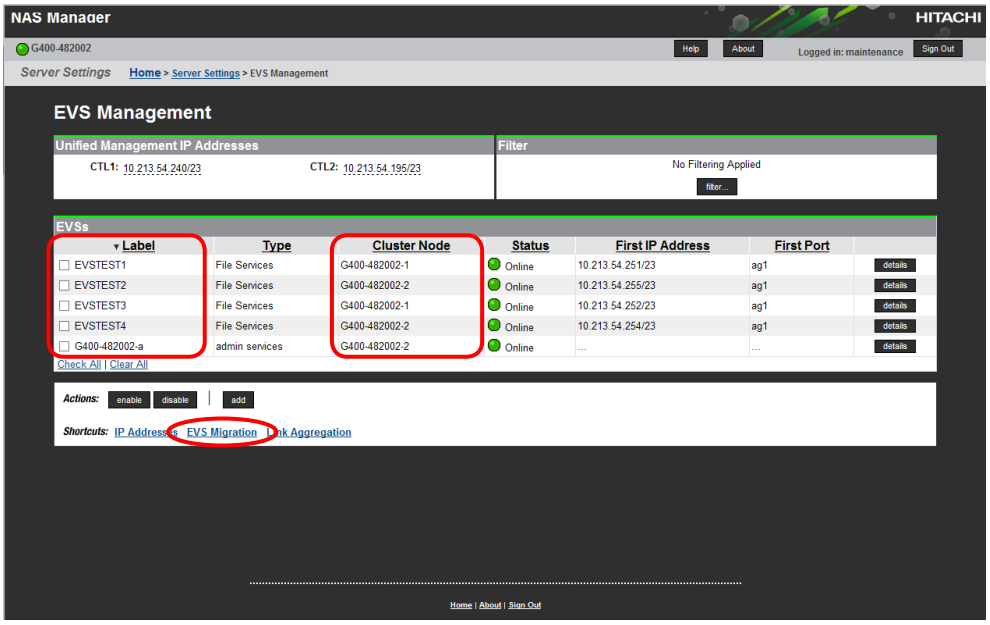


4. Click [EVS Management] in the “Server Settings” window.



5. Record EVS that is operated in the node to be maintained.
   See the “EVS Management” window to find EVS in which the node name that was confirmed in the above Step 3 is displayed in the [Cluster Node] column.
   Record the EVS name that is displayed in the [Label] column.
   If the multiple EVSs that are operated in the node to be maintained are found, record all EVS names.

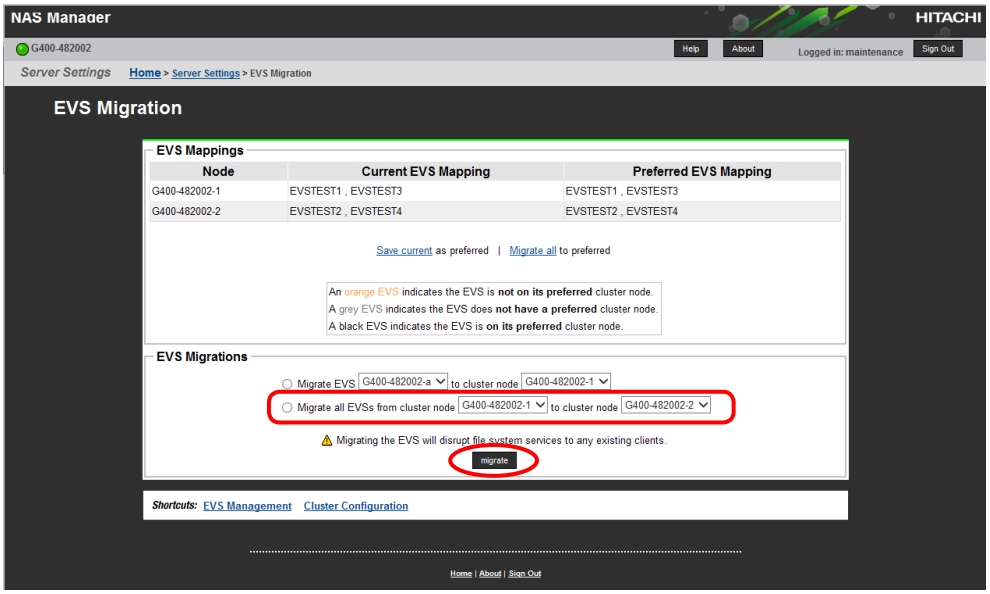
6. Click [EVS Migration] in the “EVS Management” window.



7. Migrate all the EVSs that are operated in the node to be maintained to the normal node.

   NOTE : • A user who is using the NFS client is not influenced while EVS is migrating. However, a user who is using the CIFS client needs to connect again because the file access is terminated temporarily.
   • This procedure is usually performed by the system administrator.
   • Maintenance personnel should ask the system administrator to report to the end-user and perform this procedure.
   • Maintenance personnel should perform this procedure only when asked by the system administrator.

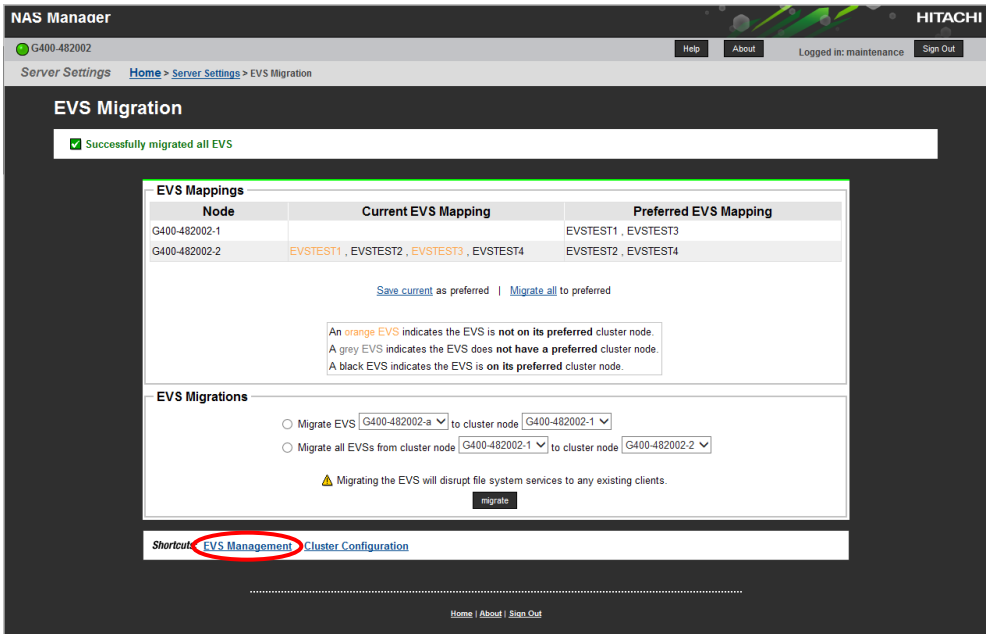
   Perform the followings in the "EVS Migration" window.
   (1) Select the option button [Migrate all EVS from cluster node….].
   (2) Specify the node name in the source directory.
   From the drop-down list [from cluster node], select the node to be maintained (It is the node confirmed in Step 5.).
   (3) Specify the node name in the destination directory.
   From the drop-down list [to cluster node], select any normal node.
   (4) Click the [migrate] button to migrate EVS.



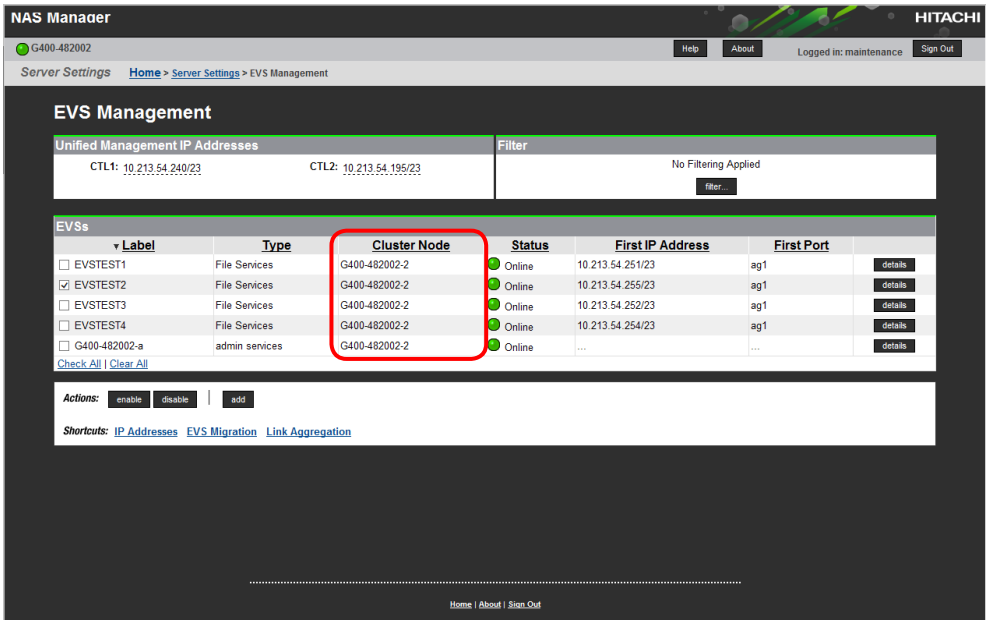
8. The confirmation dialog of Migration is displayed. Check that the operations in the above Step 7 are correct, and then click the [OK] button.
   When the Migration is complete, the message “Successfully migrated all EVS” appears.

   NOTE: When all EVS migrate, Admin EVS also migrates.
   If the message “A suitable IP address could not be found for the running SMU. Direct your browser to the maintenance port for the active SMU.” is displayed, connect to the maintenance port on the other side and start from Step 2 again.

9. Click [EVS Management] in the “EVS Migration” window and return to the “EVS Management” window.



10. Confirm that EVS was migrated from the node to be maintained to the normal node.
    Confirm that the node names in the destination directory for all EVSs recorded in the above Step 5 are displayed in the [Cluster Node] column.

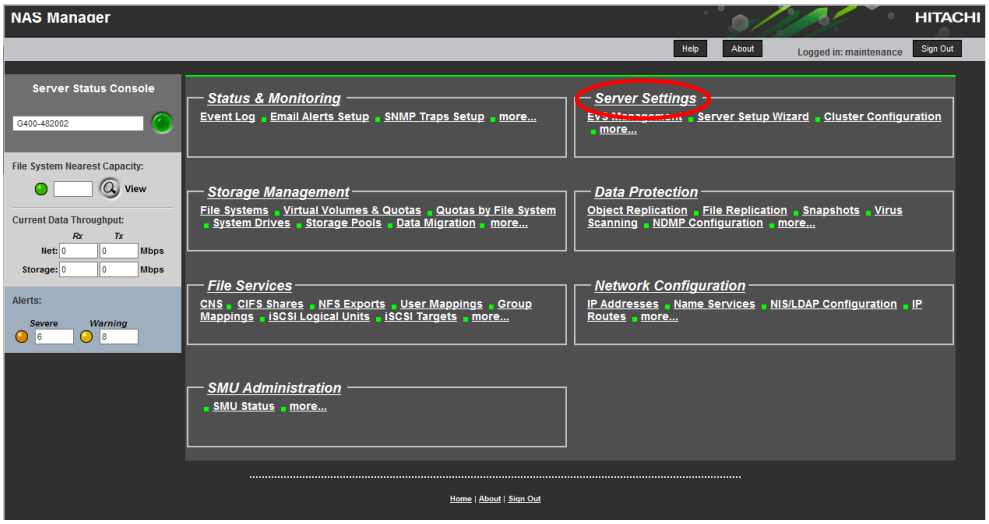


Copyright © 2015, 2017, Hitachi, Ltd.

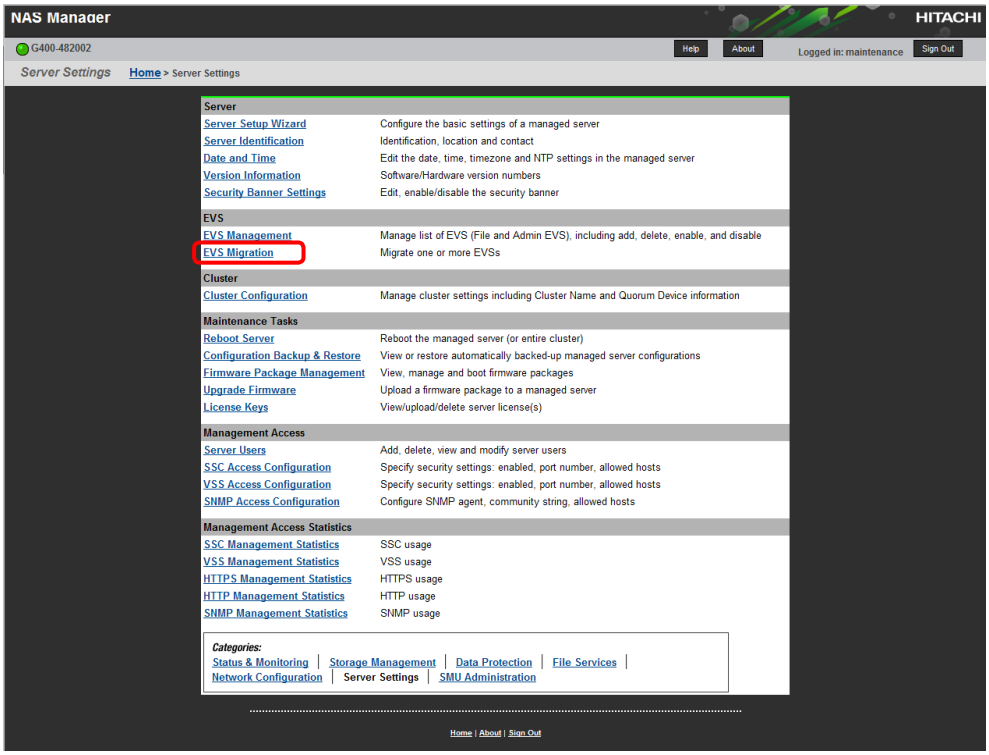
6.4.2 Migration after the Maintenance Operations

1. Connect to NAS Manager from the Web browser of theMaintenance PC.
   For the details, see “6.1 Logging into/Logging out NAS Manager”.

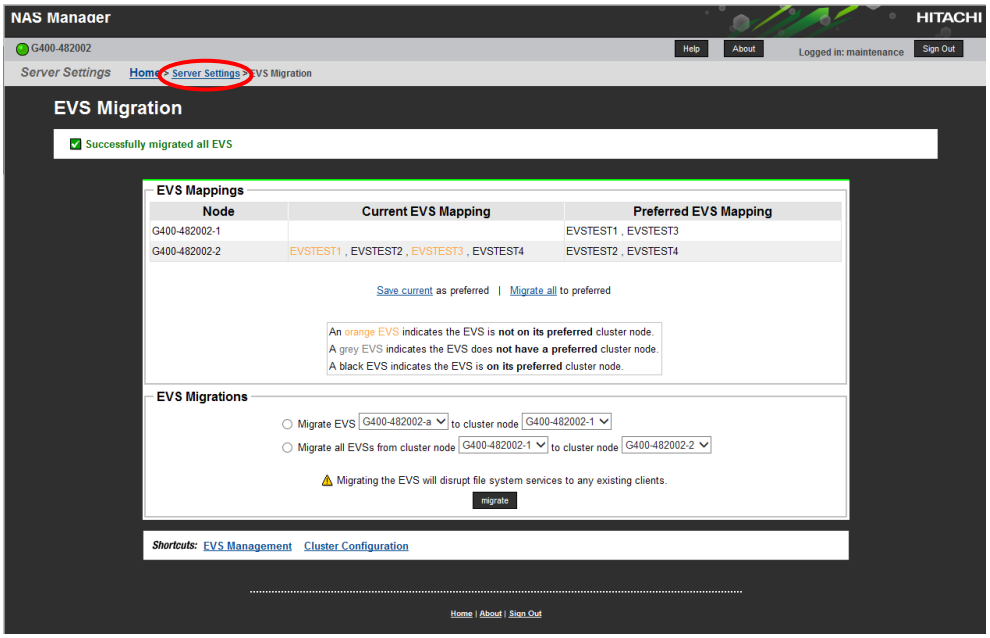
2. Click [Server Settings] in the “Home” window.



3. Click [EVS Migration] in the “Server Settings” window.

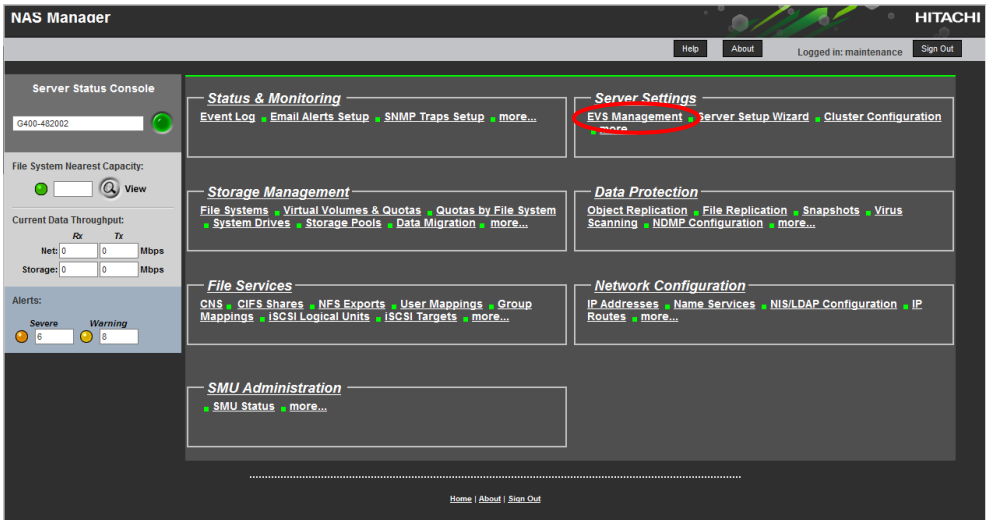


4. The following Migration operations are performed by the system administrator.
   Perform the following operations in the "EVS Migration" window.
   (1) Select the option button [Migrate EVS _ to cluster node _].
   (2) Select EVS to be migrated from the drop-down list [EVS]. This destination node is the recorded node by EVS that was noted by the system administrator in Step 5 of "6.4.1 Migration before the Maintenance Operations".
   (3) From the drop-down list [to cluster node], select the node in which the maintenance operations were performed.
   (4) Click the [migrate] button to migrate EVS.
   Perform the above operations for all EVSs noted by the system administrator in Step 5 of "6.4.1 Migration before the Maintenance Operations".

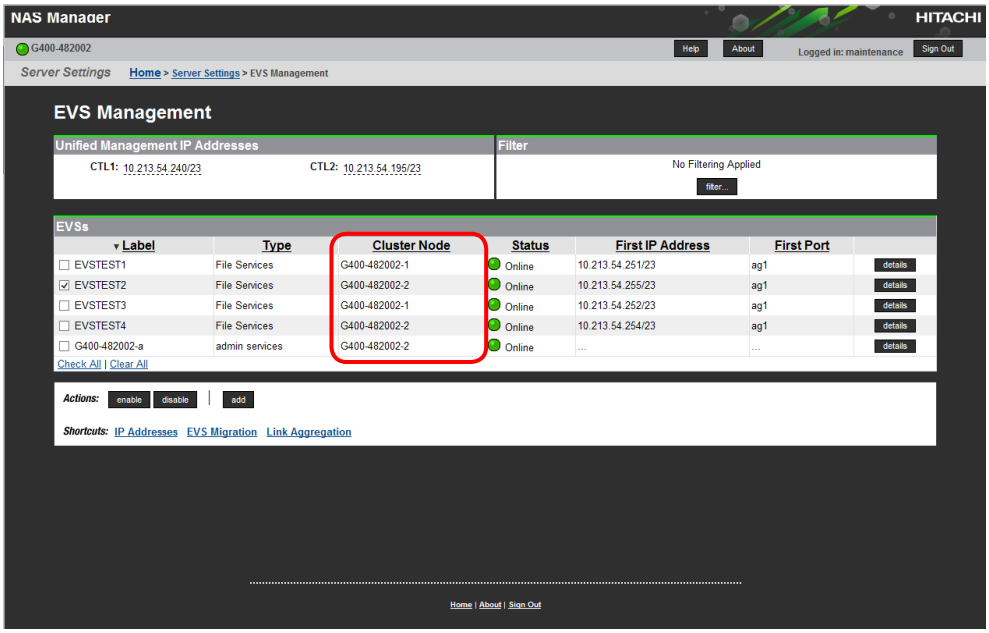


5. The confirmation dialog of Migration is displayed. Check that no mistakes are in the operations of the above Step 4, and then click the [OK] button.
   If the multiple EVSs are found, go back to Step 4 and perform Migration.
   When the migration of all EVSs is completed, click [Home].

6. Click [EVS Management] in the “Home” window.



7. In the “EVS Management” window, confirm that the node names in the destination directory for all EVSs noted by the system administrator in Step 5 of “6.4.1 Migration before the Maintenance Operations” are displayed in the [Cluster Node] column.

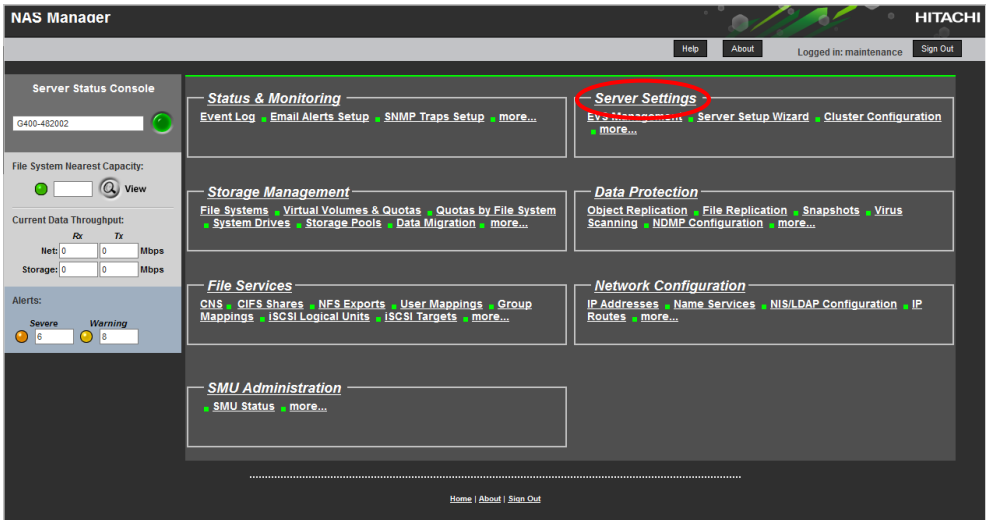


Copyright © 2015, 2017, Hitachi, Ltd.

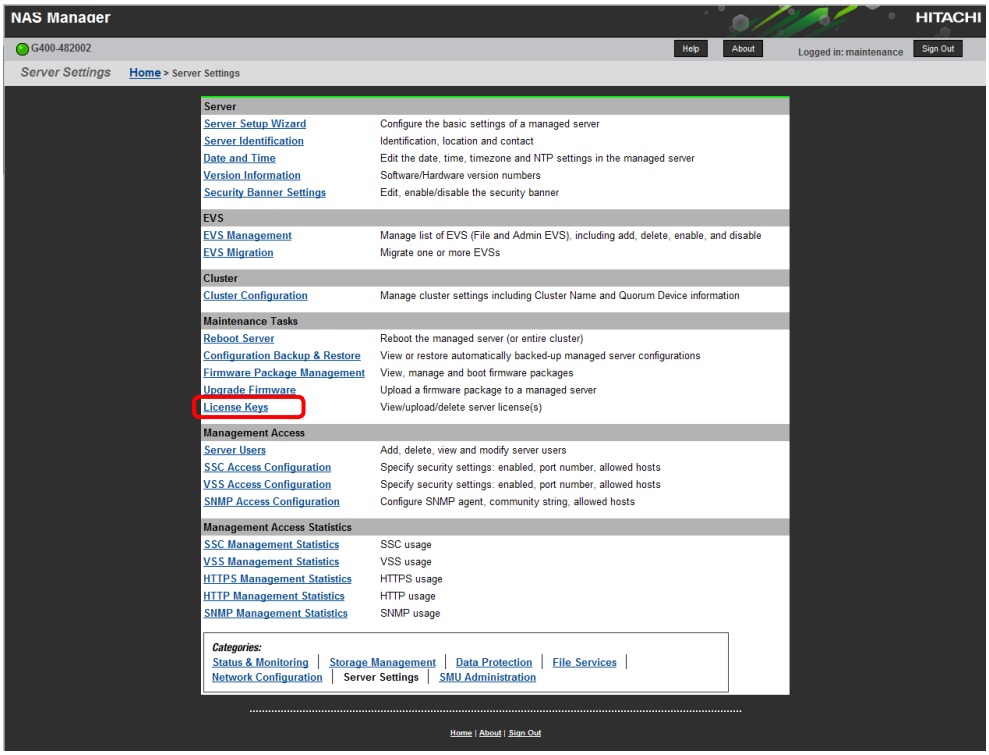
6.5 Adding License Keys

1. Connect to NAS Manager from the Web browser of the Maintenance PC.
   For the details, see "6.1 Logging into/Logging out NAS Manager".

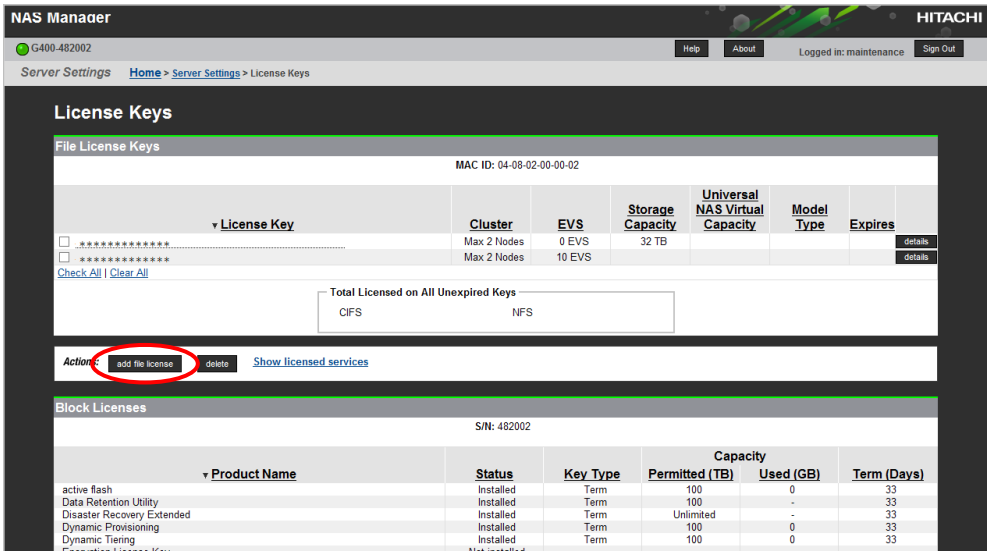
2. Click [Server Settings] in the "Home" window.



3. Click [License Keys] in the "Server Settings" window.



4. Click the [add file license] button in the [File License Keys] column of the “License Keys” window.



5. Add the license key in the “License Key Add” window.
For how to add license keys, see Table 6-3.

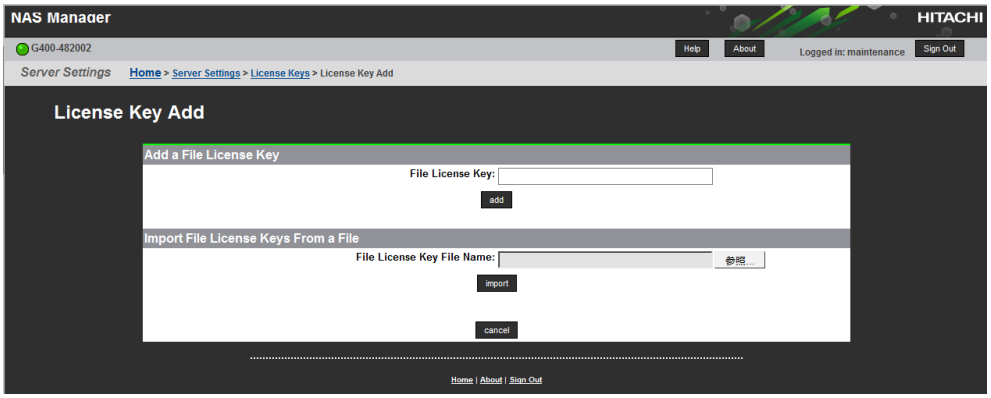


Table 6-3 How to Add License Keys

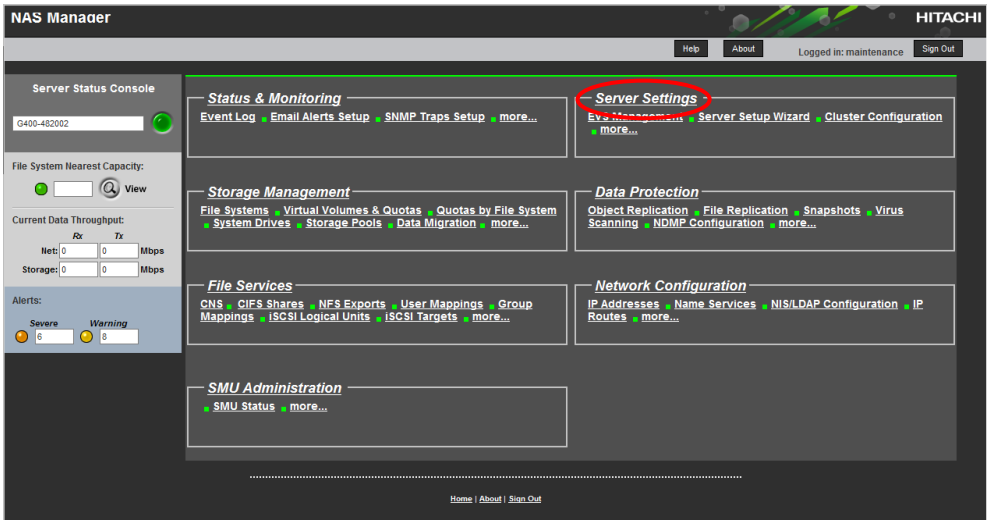
Item	Description
Add a File License Key	Input the issued License Key to add.
Import File License Keys From a File	Click the reference button and select the file stored in the folder to add.

Copyright © 2015, 2017, Hitachi, Ltd.

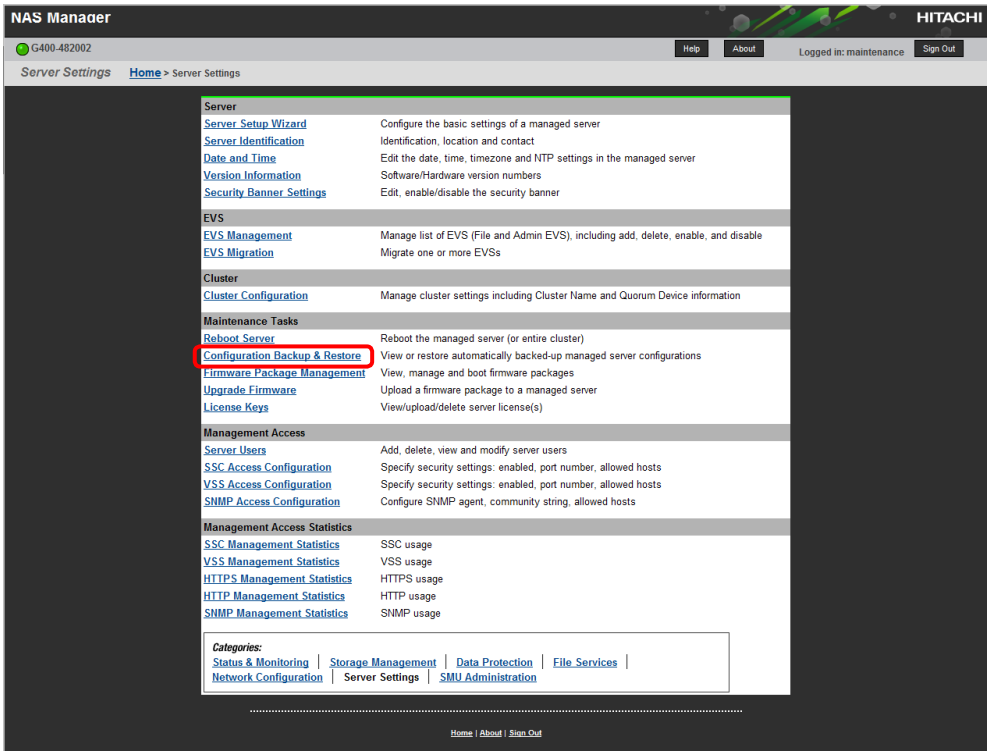
6.6 Backup of Node Registry

1. Connect to NAS Manager from the Web browser of the Maintenance PC.
   For the details, see "6.1 Logging into/Logging out NAS Manager".

2. Click [Server Settings] in the "Home" window.

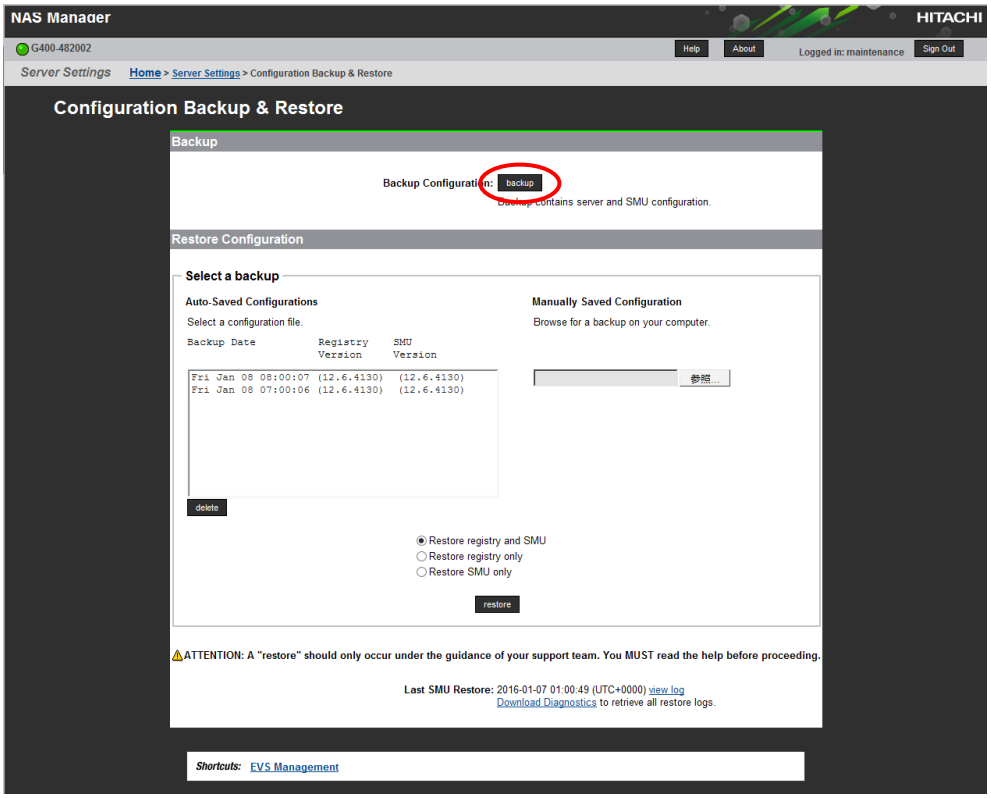


3. Click [Configuration Backup & Restore] in the "Server Settings" window.



Copyright © 2015, 2017, Hitachi, Ltd.

4. Click the [backup] button in the “Configuration Backup & Restore” window.



5. Specify the saving destination of the log.
When the “Download File” dialog box is displayed, click the [Save] button, and specify the saving destination in the Maintenance PC.

NOTE : For the path of the directory in which the backup data is saved, do not include the multibyte characters.

Copyright © 2015, 2017, Hitachi, Ltd.

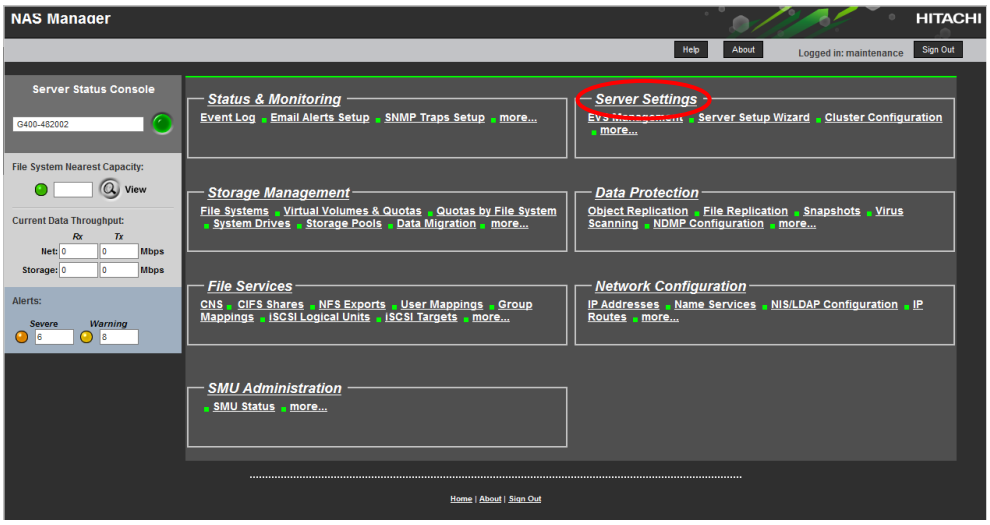
6.7 Restoring the NAS Unified Firmware Configuration Information

NOTICE:	The service personnel perform this procedure only when the backup file is provided and instructed by the system administrator.

1. Connect to NAS Manager from the Web browser on the Maintenance PC.
   For the details, see "6.1 Logging into/Logging out NAS Manager".

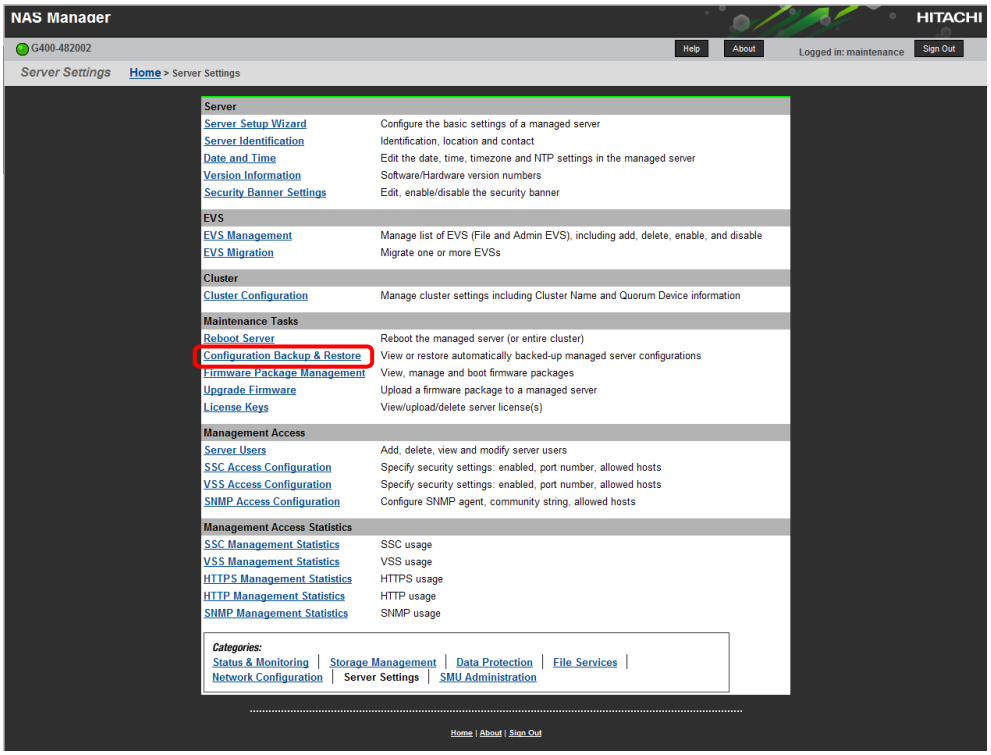
2. Set the license.
   See "6.5 Adding License Keys" and install the license.

3. Restore the NAS Unified Firmware configuration information.
   (1) Click [Server Settings] in the "Home" window.

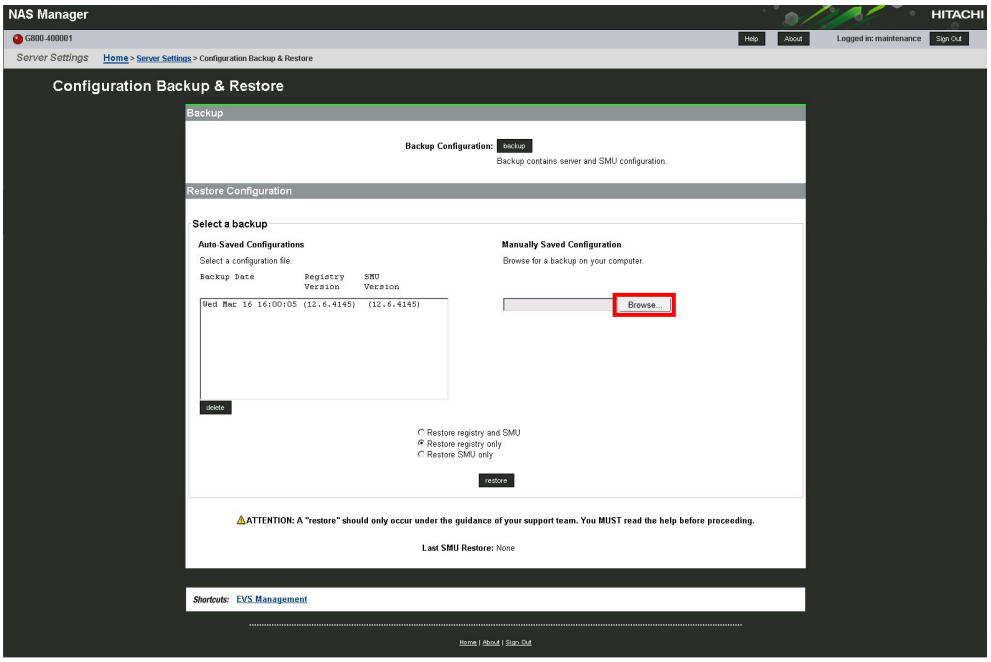


Copyright © 2015, 2017, Hitachi, Ltd.

(2) Click [Configuration Backup & Restore] in the “Server Settings” window.



(3) Select the [Browes] button in the [Manually Saved Configuration] column in the “Configuration Backup & Restore” window.



(4) Select the backup file of the corresponding serial number.
(Default storage destination: C:\Mapp\wk\supervisor\nasbackup\nasbackup\<serial number>\[yyyy][MM][DD][HH][mm][SS].tgz)

(5) Select the [Restore registry only] radio button and click the [restore] button.

Copyright © 2015, 2017, Hitachi, Ltd.

4. Change the Storage Pools setting.
   Use the maintenance command to change the Storage Pool setting.

   (1) Use PuTTY to change the Storage Pool setting.
   For how to connect the maintenance CLI, see "7.2 Logging into Node".

   (2) Run the "span-list" command to check the span list.
   <span-list running example>

```
G800-400001-2:$ span-list
Span instance name     OK?  Free  Cap/GiB  System drives           Con
------------------     ---  ----  -------  -------------           ---
Pool1                  Yes  0%    40       0,1,2,3                 90%
   ** The above span does not belong to this cluster.  Its filesystems cannot
      be mounted, checked or fixed.  Run
      span-list-cluster-uuids Pool1
      and then use 'span-assign-to-cluster', 'span-add-cluster-uuid' or
      'span-deny-access'.

Pool2_tiered           Yes  25%   80       4,5,6,7;8,9,10,11       90%
   ** The above span does not belong to this cluster.  Its filesystems cannot
      be mounted, checked or fixed.  Run
      span-list-cluster-uuids Pool2_tiered
      and then use 'span-assign-to-cluster', 'span-add-cluster-uuid' or
      'span-deny-access'.

G800-400001-2:$
```

   (3) For the span that was checked in Step (2), run the "span-assign-to-cluster" command to enable the access to the Storage System span.

   NOTE: If multiple pools exist in the Span instance name, run the "span-assign-to-cluster" command for all the pools.

   <span-assign-to-cluster Pool1 running example>

```
G800-400001-2:$
G800-400001-2:$ span-assign-to-cluster Pool1   <-------- Pool name of a target is designated.
Assigning the span to this cluster
Success

If any other cluster has loaded this span, it will not see the change you have
just made until you reboot it or, on that remote cluster, unmount any mounted
file systems on the span and run:

sd-rescan-cod Pool1

G800-400001-2:$
```

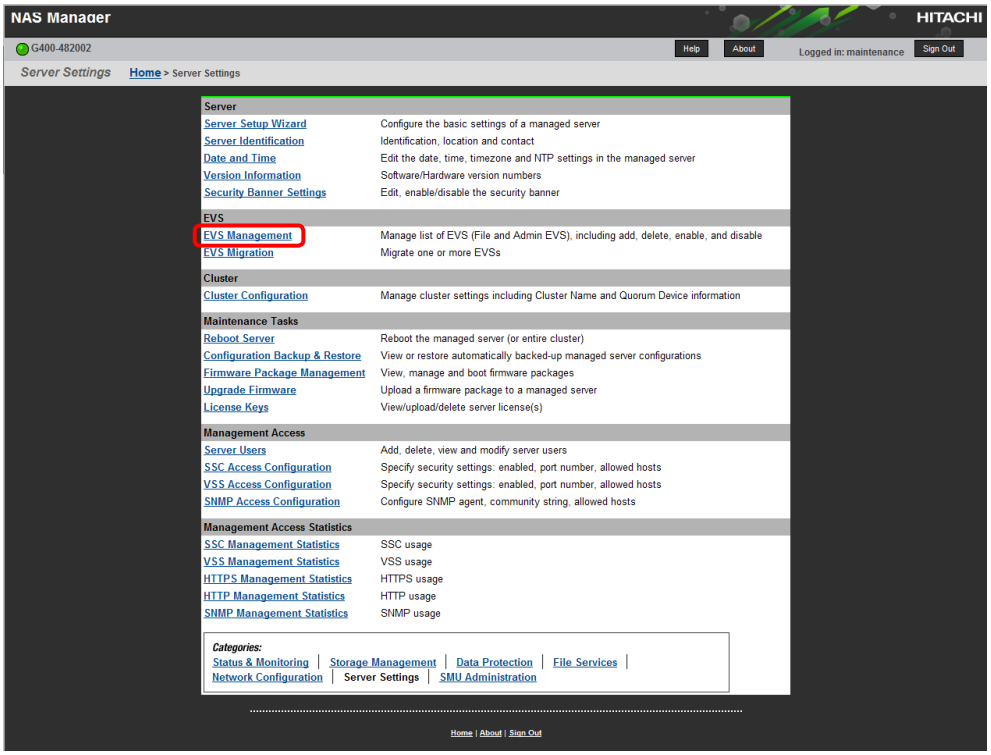
Copyright © 2015, 2017, Hitachi, Ltd.

(4) Run the "span-list" command again and check whether the setting is reflected.
<span-list running example>

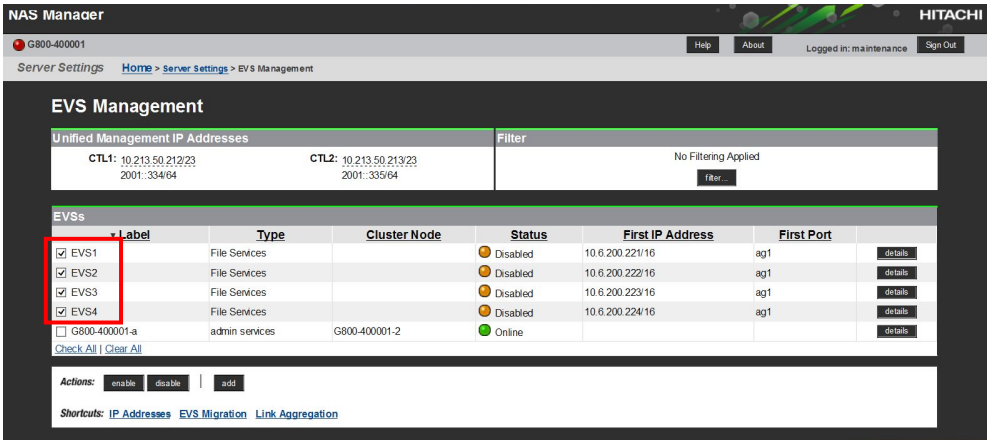
```
G800-400001-2:$ span-list
Span instance name      OK?  Free  Cap/GiB  System drives            Con
------------------      ---  ----  -------  -------------            ---
Pool1                   Yes  0%    40       0,1,2,3                  90%
Pool2_tiered            Yes  25%   80       4,5,6,7;8,9,10,11        90%
G800-400001-2:$
```

5. Start EVS.

(1) Click [EVS Management] in the "Server Settings" window.

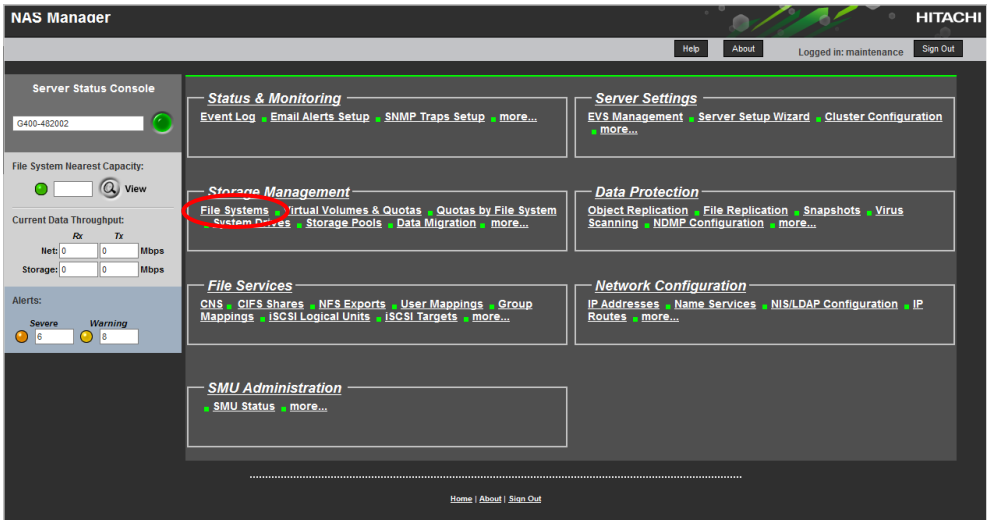


(2) Select "EVS" to be enabled and click the [enable] button.

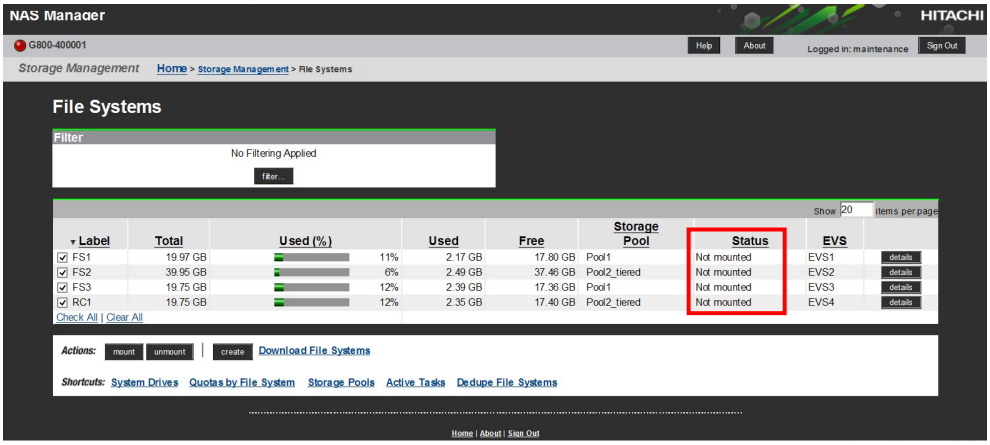


6. Mount File System.

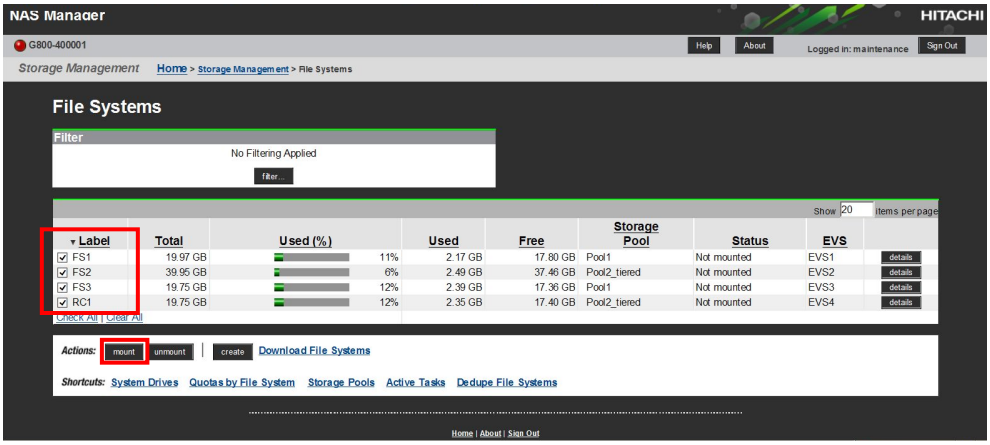
(1) Click [File System] in the [Storage Management] column in the “HOME” window.



(2) Check whether the File System is mounted.

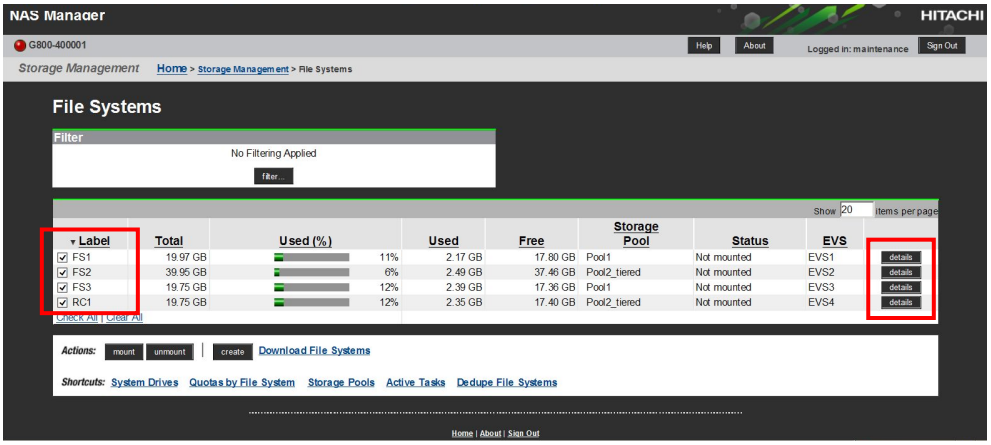


(3) Check the checkbox of File System to be mounted and click the [Mount] button.

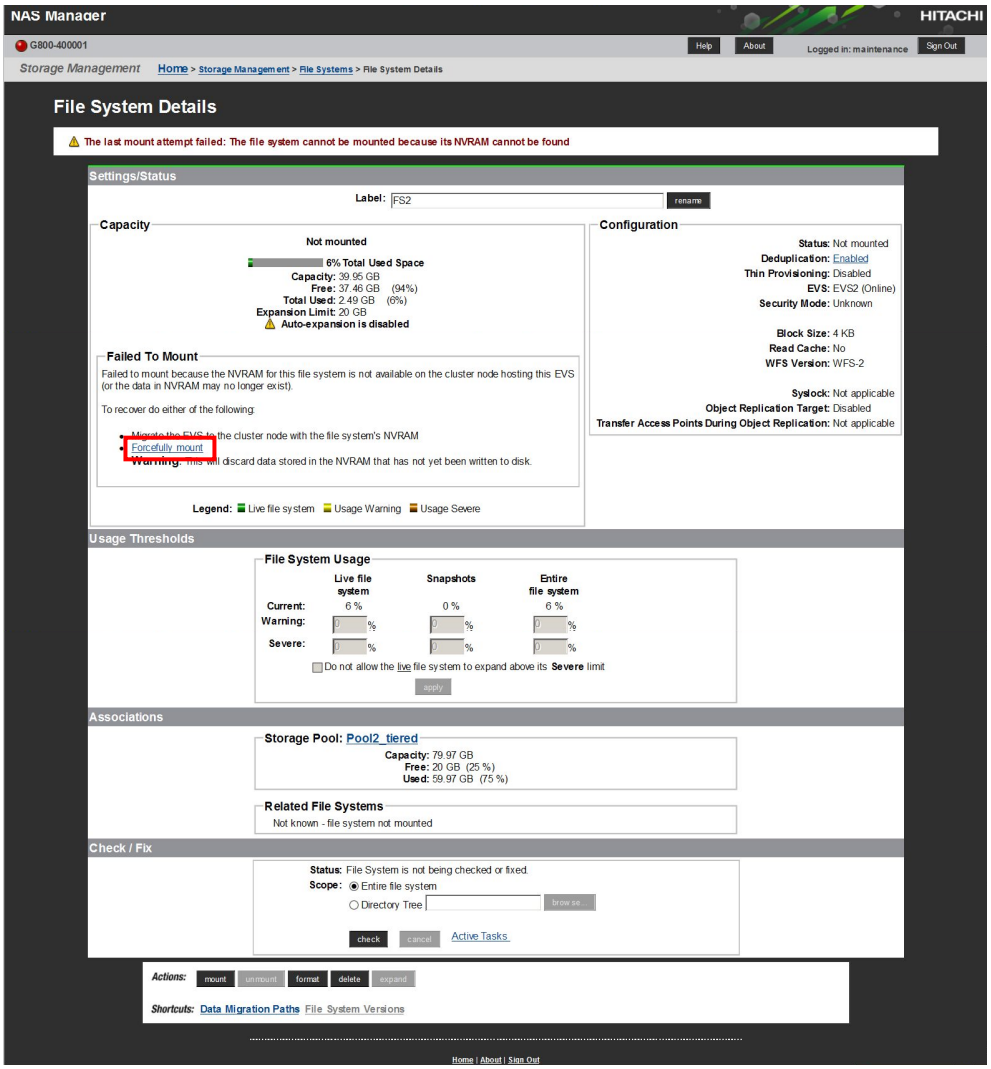


(4) If unmounted File Systems exist, perform the procedure of Step 7.

7. Mount File System forcibly.
   (1) Check the File System to be mounted in the [Label] column and click the [Detail] button.



   (2) Click “Forcefully mount”.
   If multiple File Systems exist, return to Step (1) and perform it for all the File Systems.

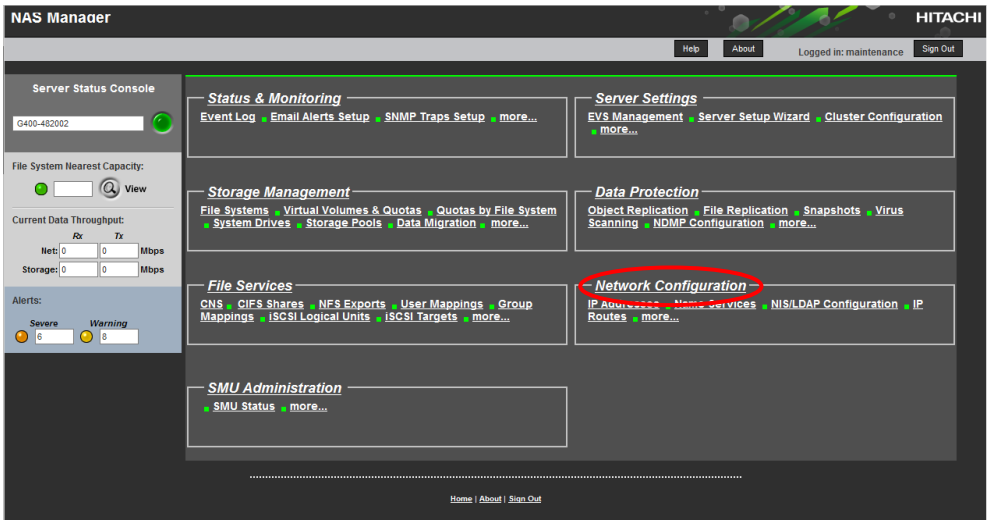


6.8 DNS Settings and Confirmation

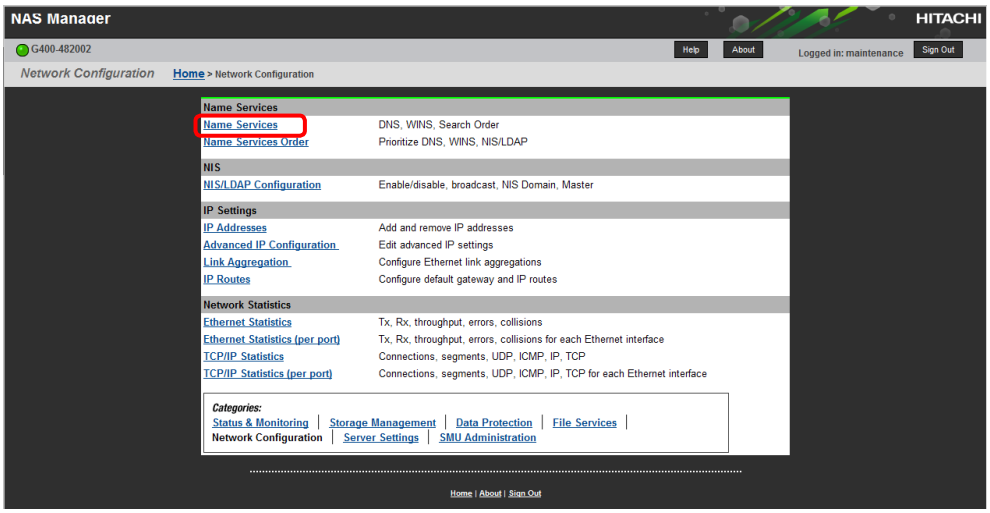
NOTICE: If the DNS Servers, the DNS Domain Name and the Domain Search Order are set by NAS Manager, the set contents are also reflected in the Storage System.

1. Connect to NAS Manager from the Web browser of the Maintenance PC.
   For the details, see "6.1 Logging into/Logging out NAS Manager".

2. Click [Network Configuration] in the "Home" window.

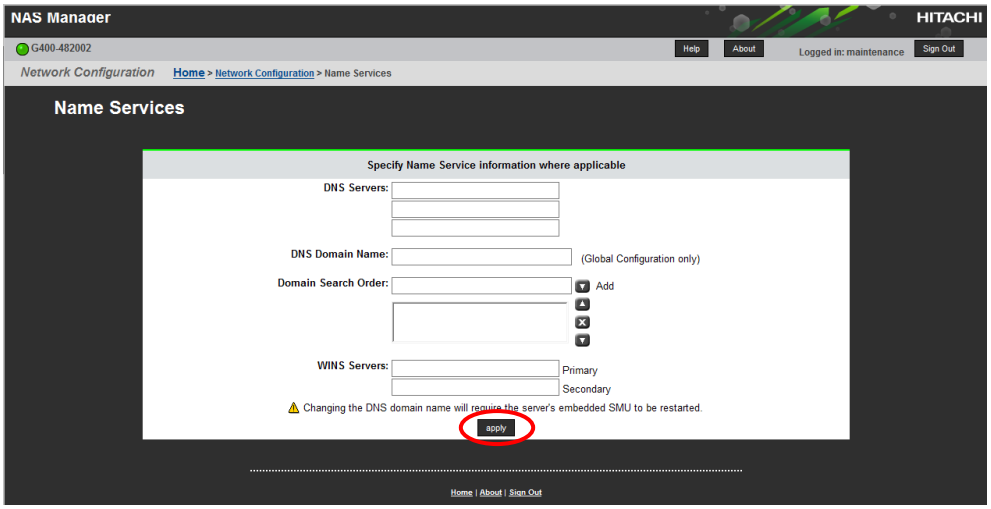


3. Click [Name Services] in the "Network Configuration" window.



Copyright © 2015, 2017, Hitachi, Ltd.

4. Set DNS and if you apply the settings, click the [apply] button.
   - When you still have other tasks or confirmation, click [Home] to move to the “Home” window.
   - If you do not have other tasks, close the browser.



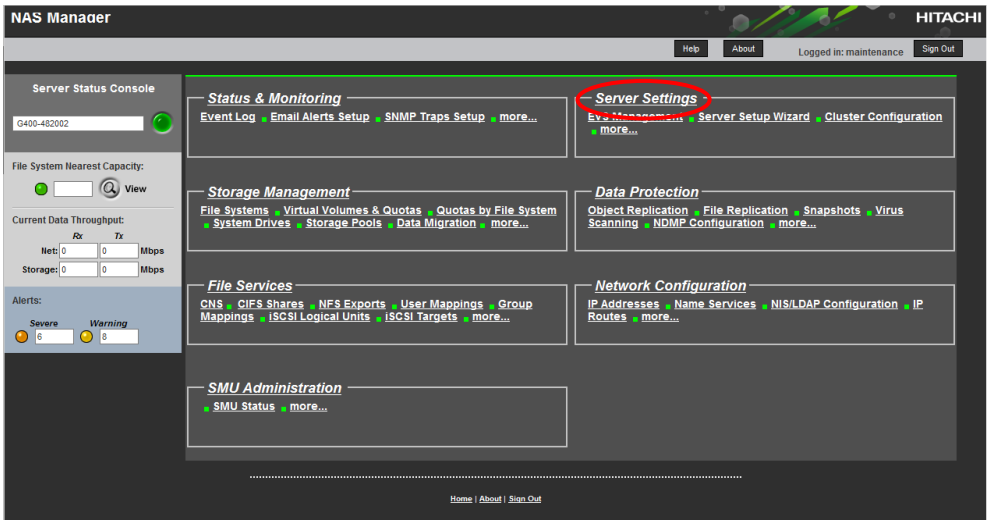
Copyright © 2015, 2017, Hitachi, Ltd.

6.9 Setting the Time and the NTP Server

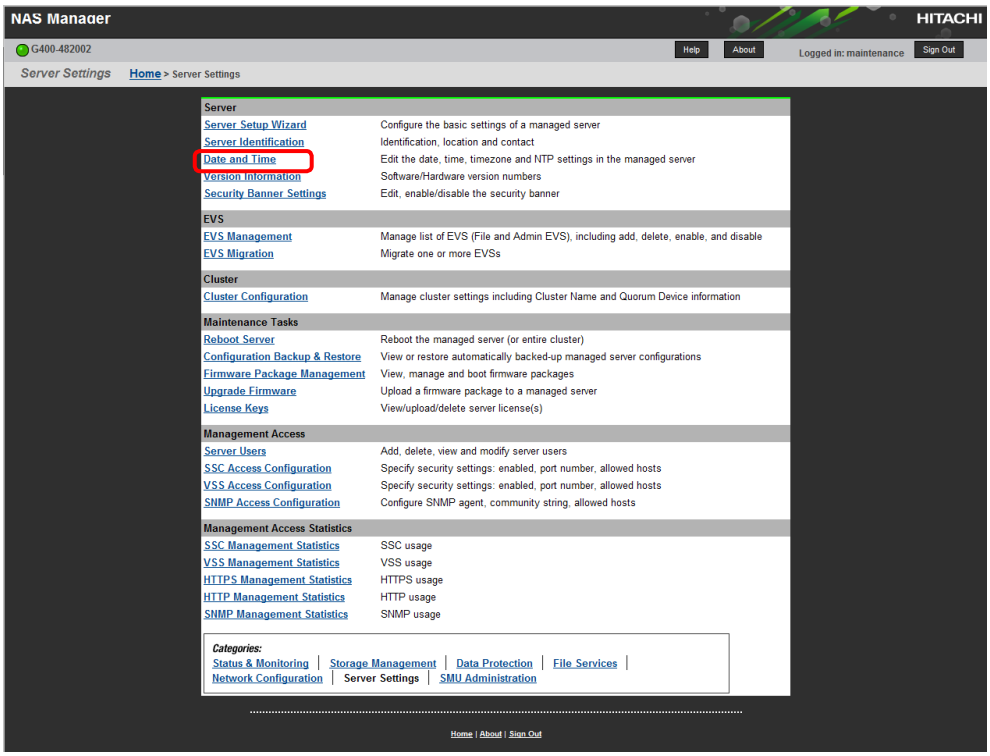
NOTICE:	If the Time, the Date, the Time Zone and the NTP Server are set by NAS Manager, the set contents are also reflected in the Storage System.

1. Connect to NAS Manager from the Web browser of the Maintenance PC.
   For the details, see “6.1 Logging into/Logging out NAS Manager”.

2. Click [Server Settings] in the “Home” window.



3. Click [Date and Time] in the “Server Settings” window.



4. Set the time and the NTP server.
   Set the time according to the Table 6-4 in the “Date and Time” window.

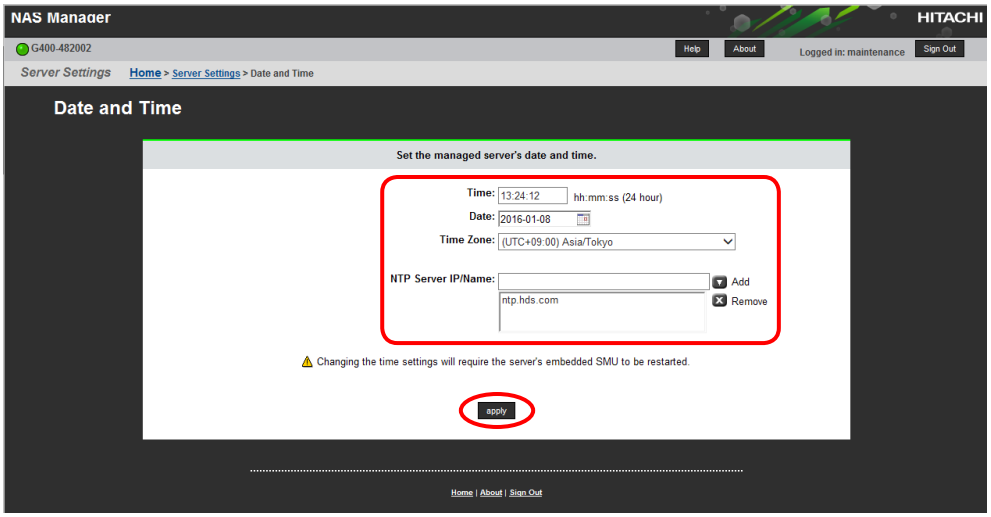
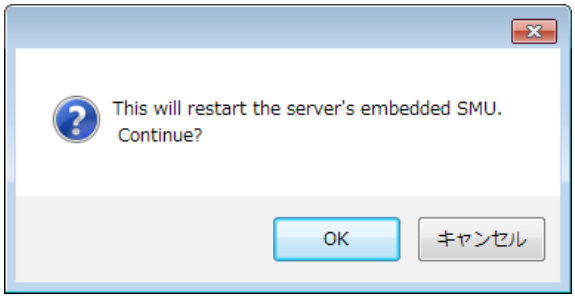


Table 6-4 Time Setting Items

Item Name	Description	Setting Value
Time	Set the time in 24 hours format. (HH:MM:SS)	Set the time to match the time of the NTP server.
Date	Set the date.	When clicking the entry column, a calendar is displayed. Then, click the date you want to enter.
Time Zone	Set the time zone.	In the case of Japan, set [Asia/Tokyo] (Click Asia/Tokyo from the drop-down list).
NTP Server IP/Name	Specify the IP address or host name of the NTP server.	Specify the IP address or the host name of the NTP server.

5. Set the time and when applying the settings, click the [apply] button.

6. When the confirmation dialog appeared, click the [OK] button.



- When you still have other tasks or confirmation, click [Home] to move to the “Home” window.
- If you do not have other tasks, close the browser.

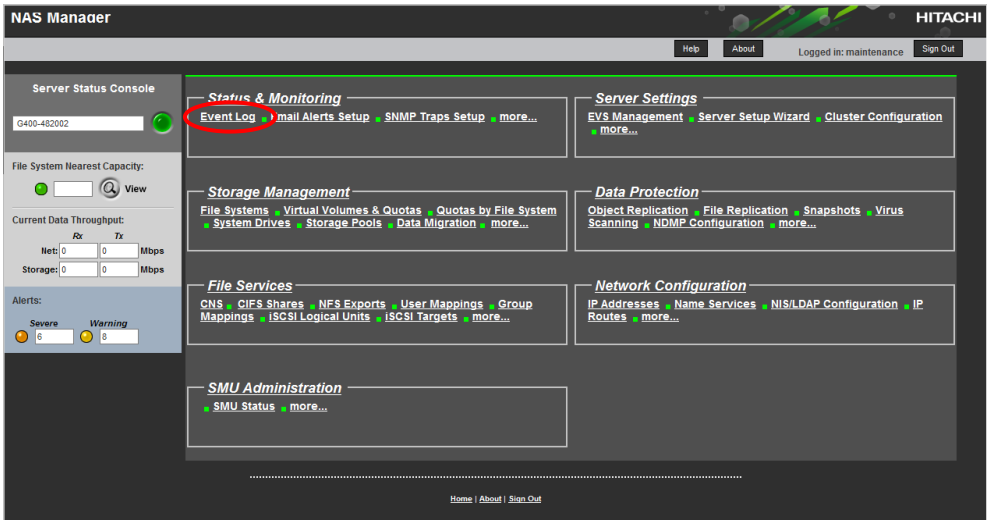
NOTE : If the time or the settings of the NTP server changed, SMU is restarted.

Copyright © 2015, 2017, Hitachi, Ltd.

6.10 Confirming the Event Log

1. Connect to NAS Manager from the Web browser of the Maintenance PC.
   For the details, see “6.1 Logging into/Logging out NAS Manager”.

2. Click [Event Log] in the “Home” window.



3. The “Event Log” window is displayed.

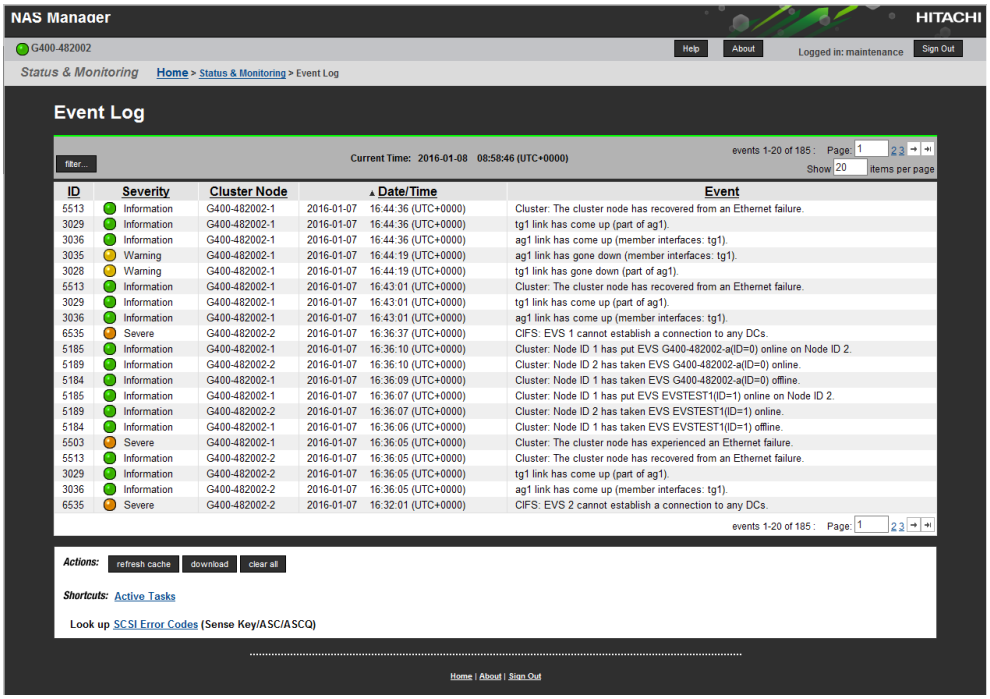


Table 6-5 describes the items of each column in the “Event Log” window.

Table 6-5 Each Item of Event Log window

Item Name	Description
ID	It indicates the ID of the occurred event.
Severity	It indicates the severity of the occurred event. Information: Recovery notification of the occurred problem. Warning: Problem at warning level occurs. Severe: Serious problem occurs. Critical: Critical problem occurs.
Cluster Node	It indicates the node name in which the problem occurred.
Date/Time	It indicates the date and time when the problem occurred.
Event	It describes the contents of the occurred problem.

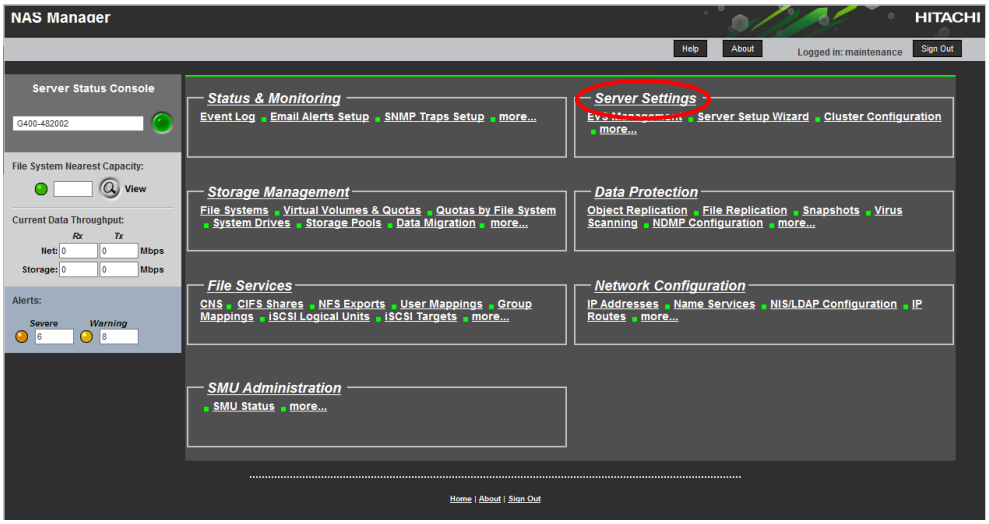
For the details of the event log ID, see MESSAGE SECTION “4. NAS Manager Event Log ID”.

Copyright © 2015, 2017, Hitachi, Ltd.

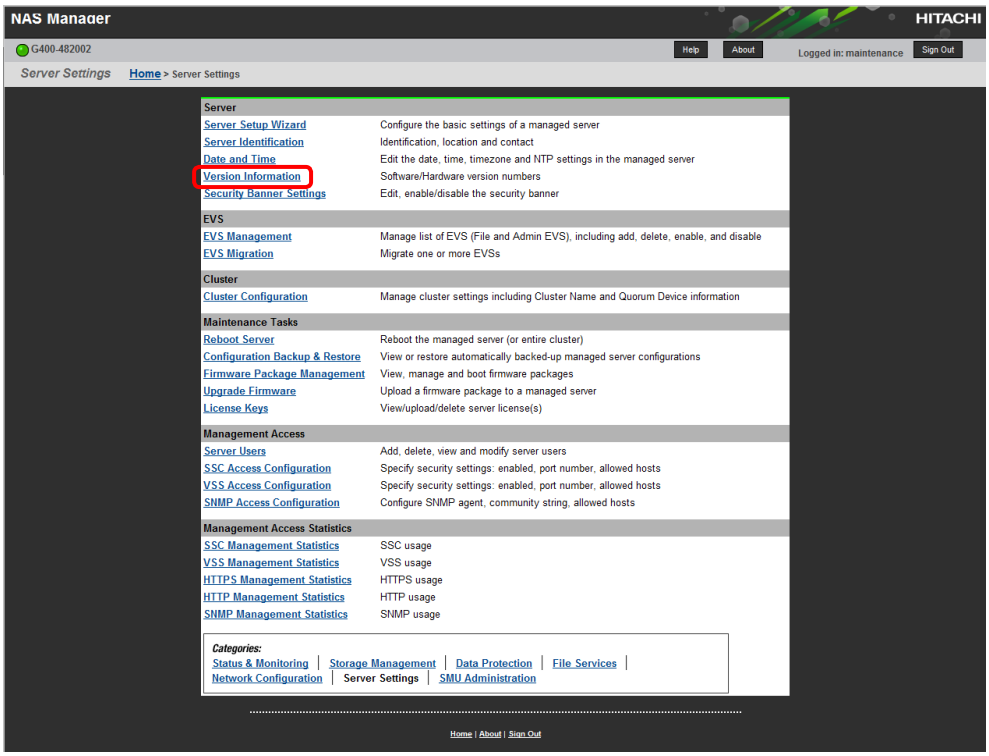
6.11 Confirming the Firmware Version of the Node

1. Connect to NAS Manager from the Web browser of the Maintenance PC.
   For the details, see “6.1 Logging into/Logging out NAS Manager”.

2. Click [Server Settings] in the “Home” window.

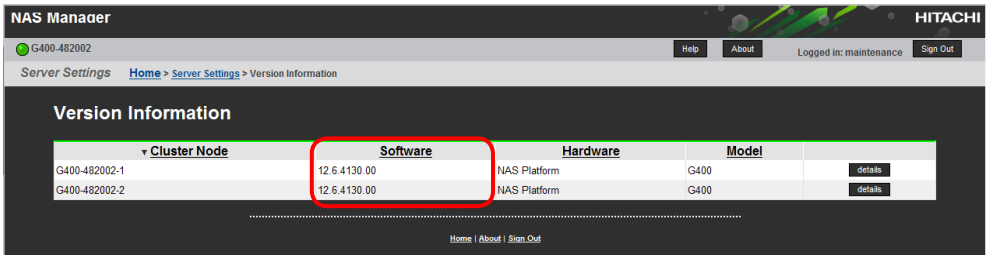


3. Click [Version Information] in the “Server Settings” window.



Copyright © 2015, 2017, Hitachi, Ltd.

4. The currently installed firmware version is displayed in the [Software] column of the “Version Information” window.
   Check that the firmware version displayed in the [Software] column is correct.

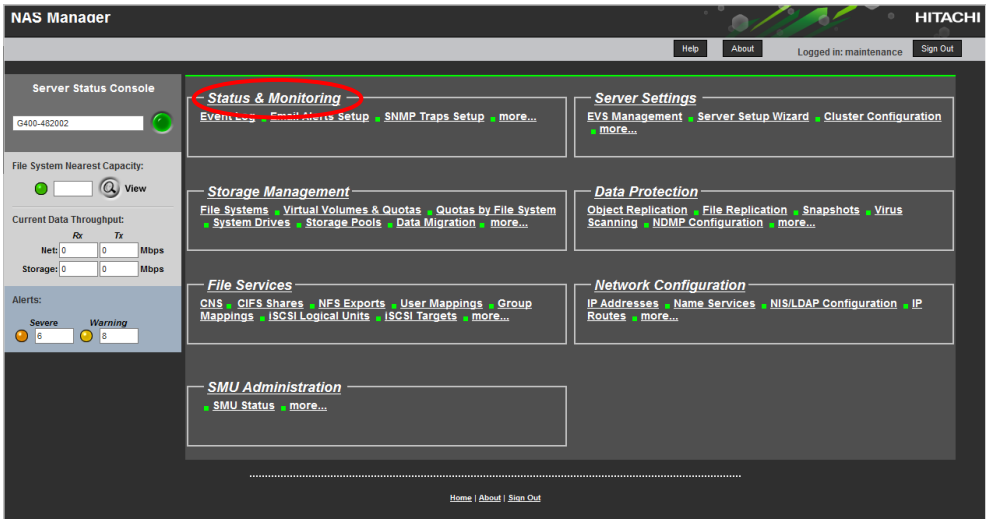


Copyright © 2015, 2017, Hitachi, Ltd.

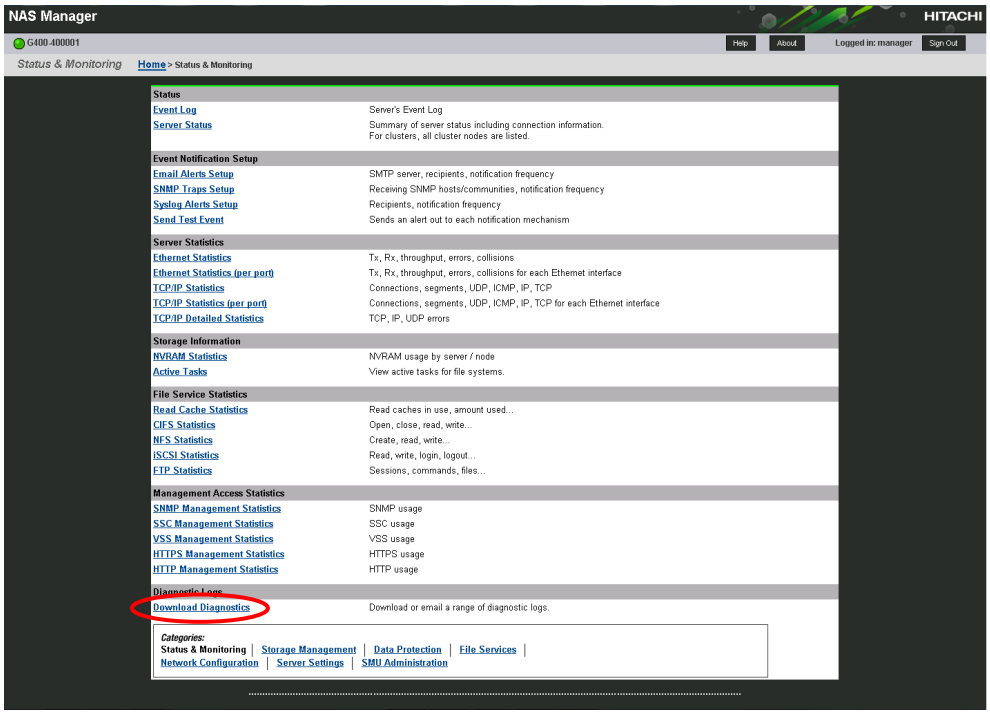
6.12 Collecting Logs of Node and SMU

1. Connect to NAS Manager from the Web browser of the Maintenance PC.
   For the details, see "6.1 Logging into/Logging out NAS Manager".

2. Click [Status & Monitoring] in the "Home" window.



3. Click [Download Diagnostics] in the "Status & Monitoring" window.



Copyright © 2015, 2017, Hitachi, Ltd.

4. Select the log to be collected.
   In the “Download Diagnostics” window, select items as shown below.

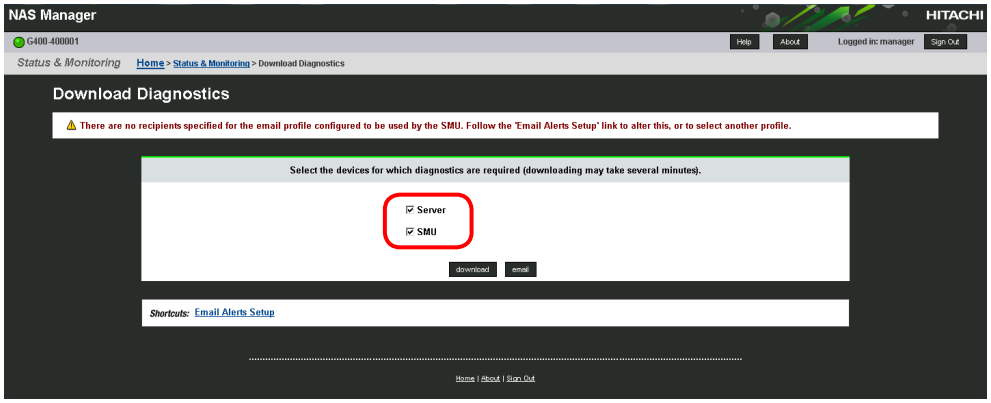
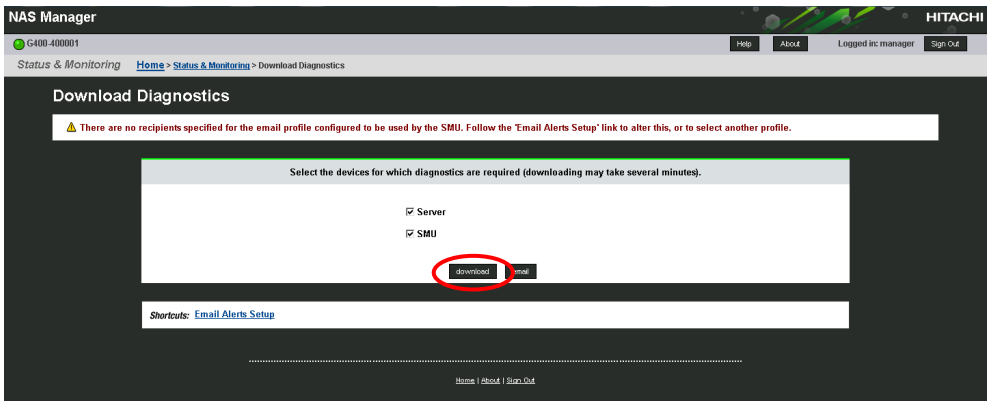


Table 6-6 Selection Items when Collecting Log

Item	Settings
Server	Select (ON) the check box.
SMU	Select (ON) the check box.

5. Start to collect the log.
   Click the [download] button in the “Download Diagnostics” window. Then, the processing to collect the selected log begins. This processing takes about one minute.



NOTE : When the character strings “FILES_MISSING” are included in the file name of the collected diagnostic information, a collection of the partial diagnostic information failed.
In this case, collect the diagnostic information again after waiting for about 10 minutes. If the collection fails again, contact the Technical Support Division.

6. Specify the saving destination of the log.
   When the Download File dialog is displayed, click the [Save] button, and specify the file destination to be saved in the Maintenance PC.

Copyright © 2015, 2017, Hitachi, Ltd.

7. Maintenance CLI

Perform the maintenance operation using the command on the Maintenance PC that can communicate with a node.
The procedures of performing each maintenance function such as each setting and collection of information are shown below.

7.1 Operation Procedure of the Command

Preparations to operate the command and how to run the command are described below.

7.1.1 Before Using the Command

Use the maintenance CLI command to perform the maintenance operation.
To use the command, you need to log into the node by ssh. Therefore, install the communication software (PuTTY or so on) corresponding to ssh in the Maintenance PC in advance.
Be sure to use ssh2 for the ssh protocol version. Also, set the Maintenance PC to be able to use scp to perform the file transfer.

7.1.2 Logging into the Node

To run the maintenance CLI command, you need to connect the Maintenance PC.
Connect the cable to the maintenance port on the Controller Board that runs the command.
Maintenance personnel logs into the node through ssh by using the communication software (PuTTY) corresponding to ssh2 that is prepared on the Maintenance PC. The ssh key is not required because it is connected by the password authentication. For the input information to login by ssh, see Table 7-1.

Table 7-1 Input Information for Login

No.	Item	Description
1	Address	Specify the IP address of the maintenance port.
2	Account	Enter a user name of the Storage System.
3	Password	Enter a Password of the Storage System.

NOTE: Information in Table 7-1 is not used by other than maintenance personnel. Maintenance personnel must be careful of managing the information to prevent leaking of the information.

For the detailed procedure of the maintenance CLI, see "7.2 Logging into Node".
Also for the commands that can be used, see "7.4 List of Commands to be Used".

Copyright © 2015, 2017, Hitachi, Ltd.

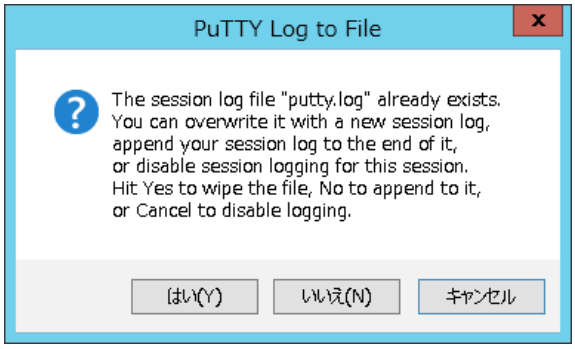
7.1.3 How to Run the Command

The procedure until before running the command is described below.

1. Start the communication software (PuTTY) corresponding to ssh2 and connect to the target node. To use PuTTY, double-click “PUTTY.EXE” and start it.

2. Enter the account name and the password to login.
   For the account name and the password, see No.2 and No.3 in Table 7-1.

   NOTE: • If you cannot login, review the setting information, cable and connection status.
   • After clicking [Open] button, the following warning might be displayed.
   In that case, click [Yes] button.



3. Run the command using the command.
   The running example of the command in case of using the status command is as shown below.

```
G400-482002-1:$ status
Cluster Communication:
Cluster Interconnect:      OK
Management Network: OK
Quorum Device:      OK

Board temperature:
HFB Inlet sensor:   OK (36 C)
HFB WFS FPGA sensor:       OK (45 C)
HFB DI FPGA sensor: OK (48 C)
HFB TAN FPGA sensor:       OK (52 C)

Chassis disk status:
/    :   OK    8% full.
/opt:   OK    3% full.
/var:   OK    2% full.

Ethernet Aggregations:
ag1:   Up

Server uptime:      8 days, 12 hours, 15 minutes, 36 seconds
Server date/time:   2016-01-14 09:07:45+00:00
```

Also, for the detailed procedure of the command to be used for the maintenance, see the running procedure of each command.

Copyright © 2015, 2017, Hitachi, Ltd.

7.1.4 Logging out of the Node

You need to log out after the completion of the maintenance operation.
Run the “exit” command twice in the communication software window to exit the command.
f you cannot run the command, close the window directly.

Copyright © 2015, 2017, Hitachi, Ltd.

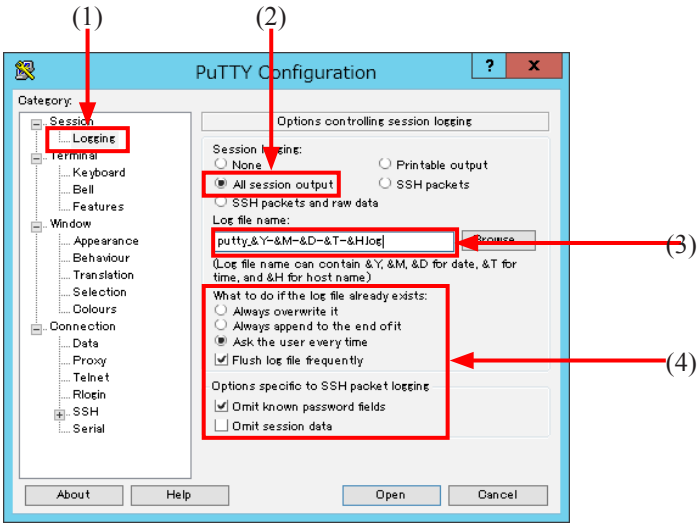
7.2 Logging into Node

The procedure for logging into the node is shown below.

1. Run Putty.exe that is installed in the following folder.
   C:\Mapp\OSS\Putty

   NOTE: C:\Mapp is the directory in which the software for the Maintenance PC is installed. If a directory other than C:\Mapp is specified for the installation directory, replace C:\Mapp to the specified installation directory.

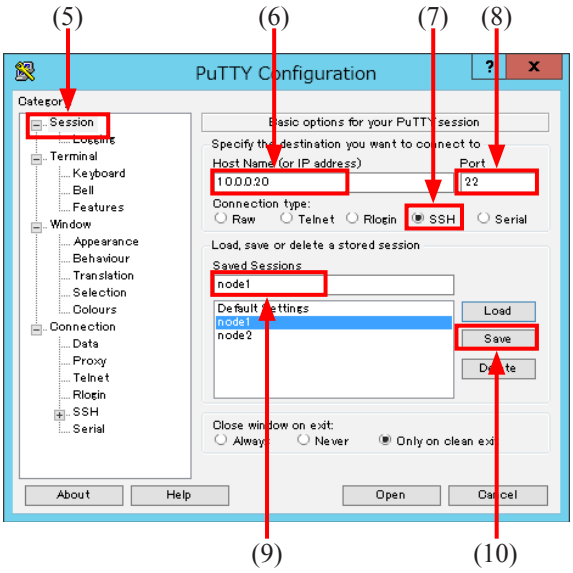
2. Set the PuTTY in accordance with the following procedure.
   (1) Select “Logging” from the “Category” column on the left side of “Putty Configuration”.



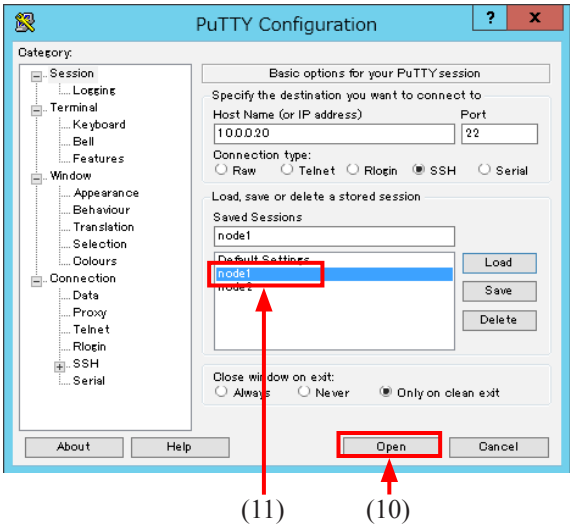
   (2) Select “All session output” in the “Session logging” column.
   (3) Enter the log file name in “Log file name”. For the log file name, the format that the file creation time is included in the file name automatically is recommended.
   Log file name “putty_&Y-&M-&D-&T-&H.log”.
   For the log output destination, enter “C:\Mapp\OSS\Putty” (or arbitrary).
   (4) Check the following checkboxes.
   - For the item “What to do if the log file already exists:”, check the “Ask the user every time” box.
   - Check the “Flush log file frequency” box.
   - For the “Options specific to SSH packet logging” item, check the “Omit known password fields” box.

Copyright © 2015, 2017, Hitachi, Ltd.

(5) Select “Session” from the “Category” column.
(6) Entert the IP address “10.0.0.20 (default)” of the maintenance port on the node 1.
If the IP address changed, ask the system administrator for the IP address after the change.
(7) For the “Connection type”, check the “SSH” box.
(8) For “Port”, enter 22.
(9) Enter “node1”.
(10) Click “Save”.



(11) Select “node 1” and click.
(12) Click “Open”.



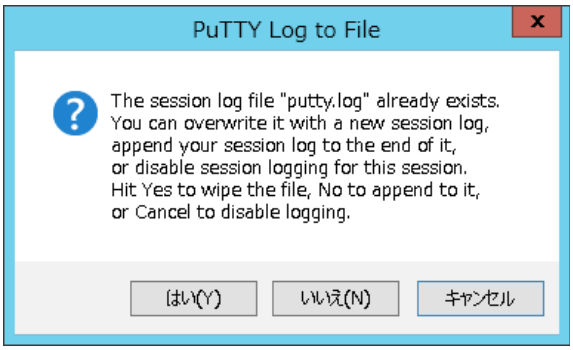
Copyright © 2015, 2017, Hitachi, Ltd.

3. The login window is displayed.
   Perform the settings in accordance with the following procedure.
   (1) Enter the user name of the Storage System in “login as:”.
   (2) Enter the password of the storage system in “Password:”.

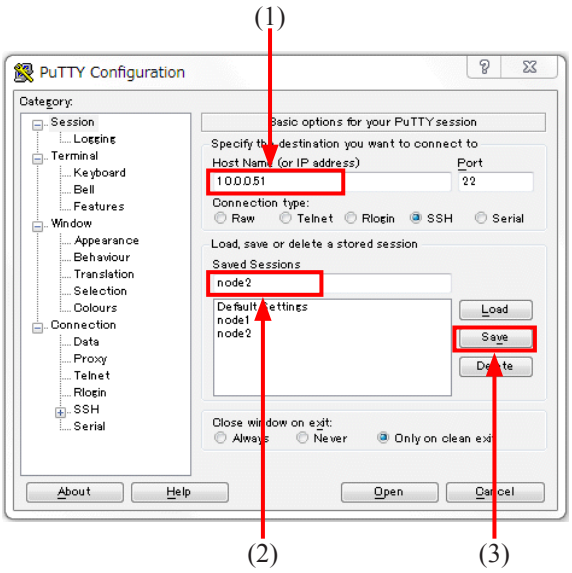
NOTE: If the user name and the password are changed, confirm with the system administrator.



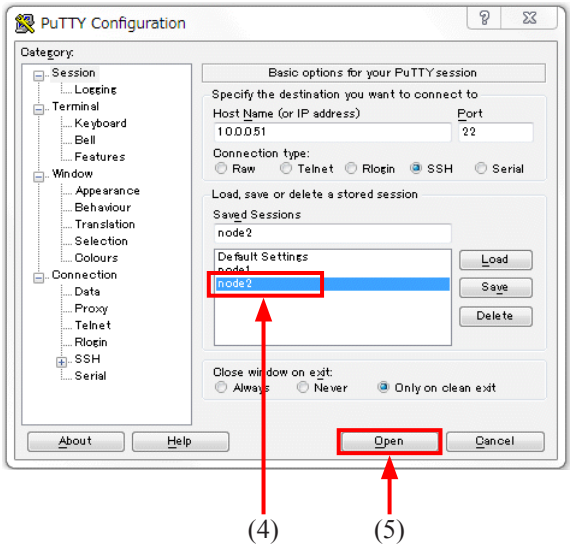
NOTE: After clicking [Open] button, the following warning might be displayed.
In that case, click [Yes] button.



4. To log into node2, repeat the procedure from Step 1 to Step 3. Also, when repeating Step 2, replace with the following.
   (1) Entert the IP address “10.0.0.21 (default)” of the maintenance port on the node 2.
   If the IP address changed, ask the system administrator for the IP address after the change.
   (2) Enter “node2”.
   (3) Click “Save”.



   (4) Select “node2” and click.
   (5) Click “Open”.



Copyright © 2015, 2017, Hitachi, Ltd.

7.3 Dumps for NAS

NOTICE: Collect NAS dumps and NAS-OS dumps when instructed to do so.

7.3.1 Collecting NAS Dumps Manually

This function is supported in the firmware version 83-03-21-x0/xx or later.
NAS Dump collects dumps using the dump collection command, and then download them on the maintenance PC using the file transfer command. The following shows the procedure.

1. Connect the Maintenance PC to the CTL to collect NAS Dump.

2. Select the command prompt from the [Start] menu of the Maintenance PC.

3. Run “cd c:\Mapp\OSS\putty” in the “Command Prompt” window.

4. Run PLINK to collect NAS Dump. The following shows the format of PLINK.

   PLINK.EXE △ -ssh △ -l △ maintenance △ xxxx △ getdiagnostic △ -f △ /var/tmp/diagnostic/yyyy.zip

   △ : One-byte space
   xxxx : Set the NAS platform address of the target CTL.
   The NAS platform address (default value) of CTL1 is 10.0.0.20 and that of CTL2 is 10.0.0.21.
   If the IP address changed, ask the system administrator of the changed IP address.
   yyyy : Set the NAS Dump file name. Set “nasdump1” for the NAS Dump collection of CTL1 and “nasdump2” for that of CTL2.

   The following shows an example when transferring to the PLINK run folder. Enter the password of the Storage System when required.

```
C:\Mapp\OSS\putty>PLINK.EXE -ssh -l maintenance 10.0.0.20 getdiagnostic -f /var/tmp/
diagnostic/nasdump1.zip
maintenance@10.0.0.20's password:
Stored diagnostics bundle to /var/tmp/diagnostic/nasdump1.zip
```

Copyright © 2015, 2017, Hitachi, Ltd.

5. Transfer the collected NAS Dump to the Maintenance PC.
   Run PSCP and download the file on the Maintenance PC. The following shows the PSCP format.

Download destination of file	PSCP format
When transferring to PSCP run folder	PSCP.EXE △ maintenance@xxxx:yyyy △ .
When transferring to arbitrary folder	PSCP.EXE △ maintenance@xxxx:yyyy △ zzzz

△ : One-byte space
xxxx : Set the NAS platform address of the target CTL.
The NAS platform address (default value) of CTL1 is 10.0.0.20 and that of CTL2 is 10.0.0.21.
If the IP address changed, ask the system administrator of the changed IP address.
yyyy : Set the file name of the transfer source.
zzzz : Set the folder name of the transfer destination and the file name. Set an arbitrary path when transferring the file to an arbitrary folder. Set an arbitrary file name when renaming the file. Set “.” (period) when transferring the file with the name unchanged to the PSCP running folder.

The following shows an example when transferring to the PSCP run folder. Enter the password of the Storage System when required.

```
C:\Mapp\OSS\putty>PSCP.EXE maintenance@10.0.0.20:/var/tmp/diagnostic/nasdump1.zip .
maintenance@10.0.0.20's password:
nasdump1.zip              | 101803 kB | 3284.0 kB/s | ETA: 00:00:00 | 100%

C:\Mapp\OSS\putty>
```

Copyright © 2015, 2017, Hitachi, Ltd.

If the following message is output, enter “y”, and then press “Enter”.

```
The server's host key is not cached in the registry.
Youhave no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 ff:ae:e6:16:72:89:16:fb:f8:4a:fc:9f:04:26:7d:fa
If you trust this host, enter "y" to add the key to PuTTY's cache and carry on
connecting.
If you want to carry on connecting just once, without adding the key to the cache,
enter "n".
If you do not trust this host, press Return to abandon the connection.
Store key in cache? (y/n) y
```

```
WARNING - POTENTIAL SECURITY BREACH!
The server's host key does not match the one PuTTY has cached in the registry.
This means that either the server administrator has changed the host key, or you have
actually connected to another computer pretending to be the server.
The new rsa2 key fingerprint is:
ssh-rsa 2048 a7:c7:ec:d0:d9:e0:3d:98:02:43:fd:f6:1a:9e:af:3f
If you were expecting this change and trust the new key, enter "y" to update PuTTY's
cache and continue connecting.
If you want to carry on connecting but without updating the cache, enter "n".
If you want to abandon the connection completely, press Return to cancel. Pressing
Return is the ONLY guaranteed safe choice.
Update cached key? (y/n, Return cancels connection) y
```

6. If the download fails, the failure factors are displayed in the window. Therefore, remove the factors, and then perform the procedure from Step 5 again.

7. If NAS Dump of the other CTL is required, repeat the procedure from Step 1.

Copyright © 2015, 2017, Hitachi, Ltd.

7.3.2 Collecting NAS-OS Dump

This function is supported in the firmware version 83-03-21-x0/xx or later.
The NAS-OS dump file is downloaded to the Maintenance PC using the file transfer command. The following shows the procedure for collecting dump files.

1. Log into the running node by ssh on the Maintenance PC.
   See "7.2 Logging into Node" for how to login.

2. Run "exit" in the "Command Prompt" window "7.2 Logging into Node", and move to NAS-OS.

3. Run "ls -lL /dump" and check that the [dumpfile_YYYYMMDDhhmmss.tar.xz] file exists.
   If multiple [dumpfile_YYYYMMDDhhmmss.tar.xz] files exist under [/dump], all dump files are to be collected. The following shows an example.

```
maintenance@G400-442004-1(bash):~$ ls -lL /dump
total 124140
-rw-r—-r-- 1 root root 53129484 Mar 1 15:52 dumpfile_20160301155028.tar.xz
-rw-r—-r-- 1 root root 73984140 Mar 1 20:59 dumpfile_20160301205758.tar.xz
manager@G400-442004-1(bash):~$
```

4. Use the file transfer command and download all dump files to the Maintenance PC.

   (1) Select a command prompt from the [Start] menu on the Maintenance PC.

   (2) Run "cd c:\Mapp\OSS\putty" in the Command Prompt window.

   (3) Run PSCP and download the file on the Maintenance PC.
   The following shows the PSCP format.

Download destination of file	PSCP format
When transferring to PSCP run folder	PSCP.EXE △ maintenance@xxxx:yyyy △ .
When transferring to arbitrary folder	PSCP.EXE △ maintenance@xxxx:yyyy △ zzzz

xxxx : Set the NAS platform (host address) of the target CTL.
The NAS platform (host address) default value of CTL1 is 10.0.020.
That of CTL2 is 10.0.0.21.
See "13.1.1 Maintenance Port Addresses" for the host address.
yyyy : Set the file name (dumpfile_YYYYMMDDhhmmss.tar.xz) of the transfer source.
△ : One-byte space
zzzz : Set the folder name of the transfer destination and the file name.
Set an arbitrary path when transferring the file to an arbitrary folder.
Set an arbitrary file name when renaming the file.
Set "." (period) when transferring the file with the name unchanged to the PSCP running folder.

Copyright © 2015, 2017, Hitachi, Ltd.

The following shows an example when transferring to the PSCP run folder.
Enter the password of the Storage System when required.

```
c:\Mapp\OSS\putty>PSCP.EXE maintenance@10.0.0.20:/dump/dumpfile_20160303015345.
tar.xz .
maintenance@10.0.0.20's password:
dumpfile_20160303015345.t | 69784 kB | 17446.2 kB/s | ETA: 00:00:00 | 100%

c:\Mapp\OSS\putty>
```

If the following message is output, enter “y”, and then press “Enter”.

```
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 ff:ae:e6:16:72:89:16:fb:f8:4a:fc:9f:04:26:7d:fa
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n) y
```

```
WARNING - POTENTIAL SECURITY BREACH!
The server's host key does not match the one PuTTY has
cached in the registry. This means that either the
server administrator has changed the host key, or you
have actually connected to another computer pretending
to be the server.
The new rsa2 key fingerprint is:
ssh-rsa 2048 a7:c7:ec:d0:d9:e0:3d:98:02:43:fd:f6:1a:9e:af:3f
If you were expecting this change and trust the new key,
enter "y" to update PuTTY's cache and continue connecting.
If you want to carry on connecting but without updating
the cache, enter "n".
If you want to abandon the connection completely, press
Return to cancel. Pressing Return is the ONLY guaranteed
safe choice.
Update cached key? (y/n, Return cancels connection) y
```

(4) If the download fails, the failure factors are displayed in the window. Therefore, remove the factors, and then perform the procedure from Step (2) again.

5. After completing the file download, check that all dump files were downloaded to the Maintenance PC. Check that the file names and the sizes are identical for how to check the downloaded files.

   Run “ls -lL/dump” for the files under [/dump] and check that the file names and the sizes are identical.

Copyright © 2015, 2017, Hitachi, Ltd.

7.4 List of Commands to be Used

Perform the each maintenance operation by using the commands listed in Table 7-2.
Table 7-2 shows the list of the commands to be used.

Table 7-2 List of the Commands to be Used

No.	Command	Overview	Reference Page	Responsible Person	Running System
1	ifconfig	Network status is displayed	"7.5 Displaying the Network Status (ifconfig)"	Maintenance personnel	BALI
2	shutdown	Shutting down of NAS Modules"	"7.6 Shutting down NAS Modules"	Maintenance personnel	BALI
3	status	Displaying of Hardware Status	"7.7 Displaying Hardware Status (status)"	Maintenance personnel	BALI
4	setdate	Setting Date and Confirmation	"7.8 Setting Date and Confirmation (setdate)"	Maintenance personnel	BALI
5	settime	Setting Time and Confirmation	"7.9 Setting Time and Confirmation (settime)"	Maintenance personnel	BALI
6	ver	Confirming the Version of NAS Modules	"7.10 Confirming the Version of NAS Modules (ver)"	Maintenance personnel	BALI
7	ipaddr	Managing of IP Addresses	"7.11 Managing IP Addresses (ipaddr)"	Maintenance personnel	BALI
8	cluster-show	Displaying the NAS Module Status	"7.12 Displaying the NAS Module Status (cluster-show)"	Maintenance personnel	BALI
9	evs migrate	EVS Migration	"7.13 EVS Migration (evs migrate)"	Maintenance personnel	BALI
10	evs list	Displaying the EVS list	"7.14 EVS Information (evs list)"	Maintenance personnel	BALI
11	evs disable	Disable the EVS	"7.15 Stopping EVS (evs disable)"	Maintenance personnel	BALI
12	evs enable	Enable the EVS	"7.16 Booting EVS (evs enable)"	Maintenance personnel	BALI
13	evsipaddr	Setting the IP Address	"7.17 Setting IP Address (evsipaddr)"	Maintenance personnel	BALI
14	smu-version	Confirming of SUM Version	"7.18 Confirming SUM Version (smu-version)"	Maintenance personnel	BALI
15	smu-service-status	Confirming of SMU Running Status	"7.19 Confirming SMU Running Status (smu-service-status)"	Maintenance personnel	BALI
16	reboot	Rebooting NAS Module	"7.20 Rebooting NAS Module (reboot)"	Maintenance personnel	BALI
17	help	Displaying the help of the command.	"7.21 Confirming Command Contents (help)"	Maintenance personnel	BALI

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from preceding page)

No.	Command	Overview	Reference Page	Responsible Person	Running System
18	ls	Displaying the directories list	“7.22 Displaying List of Directories (ls)”	Maintenance personnel	BALI
19	ping	Transmit the packet and request the response	“7.23 Confirming Network Communication (ping)”	Maintenance personnel	BALI
20	span-list	Displaying the span list	“7.24 Displaying List of Spans (span-list)”	Maintenance personnel	BALI
21	span-assign-to-cluster	Enables the access to spans	“7.25 Enabling Access to Spans (span-assign-to-cluster)”	Maintenance personnel	BALI
22	sd-list	Displaying the system drives list	“7.26 Displaying List of System Drives (sd-list)”	Maintenance personnel	BALI
23	df	Display the disk utilization ratio	“7.27 Displaying Disk Utilization Ratio (df)”	Maintenance personnel	BALI
24	cluster-node-delete	Deleting clusters	“7.28 Deleting Clusters (cluster-node-delete)”	Maintenance personnel	BALI
25	mount	Mounting File System	“7.29 Mounting File System (mount)”	Maintenance personnel	BALI
26	post-status	Power On Self Test (POST) Result	“7.30 Power On Self Test (POST) Result (post-status)”	Maintenance personnel	BALI
27	expandfs	Expanding Specific File System	“7.31 Expanding Specific File System (expandfs)”	Maintenance personnel	BALI
28	nvpages	Displaying NVRAM utilization ratio	“7.32 Displaying NVRAM utilization ratio (nvpages)”	Maintenance personnel	BALI

Copyright © 2015, 2017, Hitachi, Ltd.

7.5 Displaying the Network Status (ifconfig)

Displaying the Network Status (ifconfig)

7.5.1 Command Line

The format of the ifconfig command is as follows.

ifconfig [-v] [interface]

Table 7-3 describes the options.

Table 7-3 Descriptions of Options

No.	Option	Description	Remarks
1	-v	Displays the all interfaces including unused interfaces.	
2	Interface	Displays the specified network interface information.	

7.5.2 ifconfig Output Format

Running example of the ifconfig command is as shown below.

```
G400-482002-1:$ ifconfig
ag1       Link encap:1          HWaddr 00-1f-67-ef-20-a6
          inet addr:10.213.54.251  Bcast:10.213.55.255  mask:255.255.254.0
          inet addr:10.213.54.252  Bcast:10.213.55.255  mask:255.255.254.0
          inet6 addr: fe80::21f:67ff:feef:20a6/64 Scope:Link
          Link:UP   Admin:UP   MTU:1500  Metric:1  txqueuelen:64
   ①                                  - omission -
eth1      Link encap:1          HWaddr 00-00-87-33-b4-d5                    ②
          inet addr:10.1.48.1  Bcast:10.1.255.255  mask:255.255.0.0
          inet6 addr: fe80::200:87ff:fe33:b4d5/64 Scope:Link
          Link:UP   Admin:UP   MTU:1500  Metric:4  txqueuelen:64
             ③         ④
lo        Link encap:1
          inet addr:127.0.0.1  Bcast:127.255.255.255  mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Global
          inet6 addr: fe80::200:ff:fe00:0/64 Scope:Link
          Link:UP   Admin:UP   MTU:1500  Metric:4  txqueuelen:64
```

For the details of the output format, see “Table 7-4 Descriptions of the Output Format”.

Copyright © 2015, 2017, Hitachi, Ltd.

Table 7-4 Descriptions of the Output Format

No.	Description	Remarks
①	Displays the network interface name.	
②	Displays the network interface information.	Link encap: Connection method (1 indicates Ethernet) Hwaddr: MAC address inet addr: IP address inet6 addr: IPv6 address Bcast: Broadcast address mask: Netmask MTU: MTU value Metric: Metric tequeuelen: Size of the transmitting queue
③	Indicates the connection status of the network interface.	Link: UP Linking up Link: DOWN Linking down
④	Indicates the IP address assignment of the network interface.	Admin: UP Address is assigned Admin: DOWN Address is not assigned

Copyright © 2015, 2017, Hitachi, Ltd.

7.5.3 ifconfig -v Output Format

Running example of the ifconfig -v command is as shown below.
It is used to confirm the 10GbE LAN status.
The descriptions of the output format are the same as those of the ifconfig command.

```
G400-482002-1:$ ifconfig -v
ag1       Link encap:1          HWaddr 00-1f-67-ef-20-a6
          inet addr:10.213.54.251  Bcast:10.213.55.255  mask:255.255.254.0
          inet addr:10.213.54.252  Bcast:10.213.55.255  mask:255.255.254.0
          inet6 addr: fe80::21f:67ff:feef:20a6/64 Scope:Link
          Link:UP   Admin:UP   MTU:1500  Metric:1  txqueuelen:64

c0        Link encap:1          HWaddr 00-1f-67-ef-20-ac
          inet addr:240.0.0.2  Bcast:240.255.255.255  mask:255.0.0.0
          inet6 addr: fe80::21f:67ff:feef:20ac/64 Scope:Link
          Link:UP   Admin:UP   MTU:1488  Metric:2  txqueuelen:64

eth0      Link encap:1          HWaddr 00-00-87-33-b4-d4
          inet addr:10.0.0.20  Bcast:10.0.0.255  mask:255.255.255.0
          inet6 addr: fe80::200:87ff:fe33:b4d4/64 Scope:Link
          Link:UP   Admin:UP   MTU:1500  Metric:4  txqueuelen:64

eth1      Link encap:1          HWaddr 00-00-87-33-b4-d5
          inet addr:10.1.48.1  Bcast:10.1.255.255  mask:255.255.0.0
          inet6 addr: fe80::200:87ff:fe33:b4d5/64 Scope:Link
          Link:UP   Admin:UP   MTU:1500  Metric:4  txqueuelen:64

fsmc0     Link encap:1          HWaddr 00-30-17-ff-ff-01
          inet addr:243.0.1.1  Bcast:243.0.1.255  mask:255.255.255.0
          inet6 addr: fe80::230:17ff:feff:ff01/64 Scope:Link
          Link:UP   Admin:DOWN MTU:1500  Metric:1  txqueuelen:64

lo        Link encap:1
          inet addr:127.0.0.1  Bcast:127.255.255.255  mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Global
          inet6 addr: fe80::200:ff:fe00:0/64 Scope:Link
          Link:UP   Admin:UP   MTU:1500  Metric:4  txqueuelen:64

tg1       Link encap:1          HWaddr 00-1f-67-ef-20-a6                    ①
          Link:UP   Admin:DOWN MTU:1500  Metric:1  txqueuelen:64

tg2       Link encap:1          HWaddr 00-1f-67-ef-20-a1
          Link:DOWN Admin:DOWN MTU:1500  Metric:1  txqueuelen:64

tg3       Link encap:1          HWaddr 00-1f-67-ef-20-a2
          Link:DOWN Admin:DOWN MTU:1500  Metric:1  txqueuelen:64

tg4       Link encap:1          HWaddr 00-1f-67-ef-20-a3
          Link:DOWN Admin:DOWN MTU:1500  Metric:1  txqueuelen:64

tg5       Link encap:1          HWaddr 00-1f-67-ef-20-a4
          Link:DOWN Admin:DOWN MTU:1500  Metric:1  txqueuelen:64

tg6       Link encap:1          HWaddr 00-1f-67-ef-20-a5
          Link:DOWN Admin:DOWN MTU:1500  Metric:1  txqueuelen:64
```

Copyright © 2015, 2017, Hitachi, Ltd.

Port locations and the descriptions of the output format are as shown below.

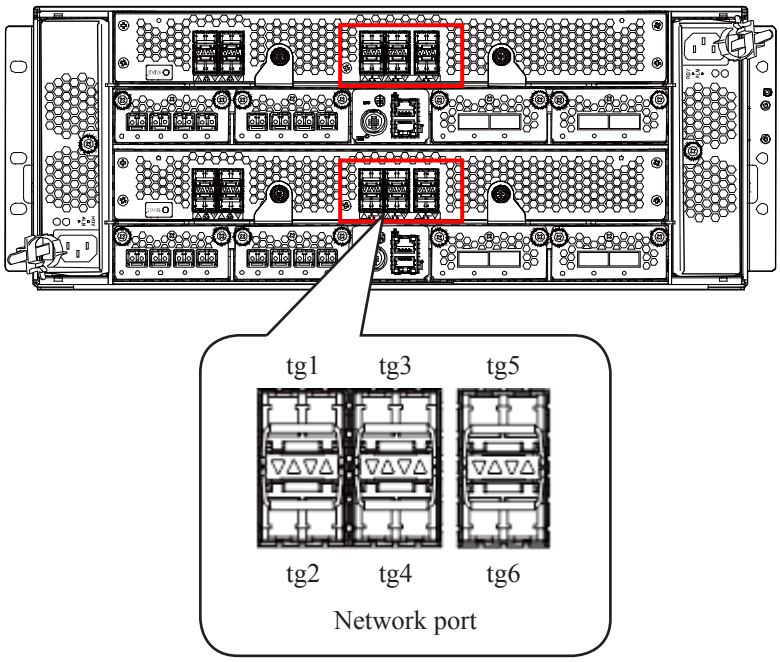


Table 7-5 Descriptions of the Output Format

No.	Description	Remarks
①	It is the network port. It supports from tg1 to tg6.	On the completion of the maintenance operation, confirm that the ports to be operated are linking up.

Copyright © 2015, 2017, Hitachi, Ltd.

7.5.4 Procedure for Isolating Failure Causes

This section describes how to identify the LAN failure from the command running result.

1. Focus on the part of “inet addr” of ② in the ifconfig command output format. If “inet addr” does not exist, IP address is not set. Set the IP address as necessary.

2. If “inet addr” of ② exists and the status of ③ is “Link:DOWN”, isolate it as having a failure.
   If “inet addr” of ② exists and the status of ③ is “Link:DOWN”, it is the no failure status.
   If “inet addr” of ② does not exist, it is the no failure status even if the status of ③ is “Link:DOWN”.

3. Specify the failed network interface and take notes.

4. Confirm that the failed network interface connection settings have no problem.

5. If no problem with the settings, return to the caller.

Copyright © 2015, 2017, Hitachi, Ltd.

7.6 Shutting down NAS Modules

The shutdown command suspends NAS Modules.

NOTE: Run this command only when a special instruction is given.

7.6.1 Command Line

The format of the shutdown command is as follows.

shutdown [-s|--seconds <seconds>] [-f|--force] [-a|--all] [-n|--ship] [-c|--cluster] [-p|--powerdown]

Table 7-6 describes the options.

Table 7-6 Descriptions of Options

No.	Option	Description	Remarks
1	-s	The NAS Module is shut down after the specified seconds.	
2	-f	The NAS Module in the connection destination is shut down by force.	To shut down the both NAS Modules, change the connection of the maintenance port, and then perform it again.
3	-a	Shuts down all NAS Modules at once.	
4	-n	Disables the failover to the battery for shipping.	
5	-c	Shuts down all NAS Modules one by one.	
6	-p	Turns off the power supply at the end of the shutdown sequence.	

7.6.2 shutdown Output Format

Running example of the shutdown command is as shown below.

```
G400-482002-1:$ shutdown -f
G400-482002-1:$ Connection closed by foreign host.
manager@G400-482002-1(bash):~$
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.7 Displaying Hardware Status (status)

The status command displays the hardware status.

7.7.1 Command Line

The format of the status command is as follows.

status [-h | [-s] [-a]]

Table 7-7 describes the options.

Table 7-7 Descriptions of Options

No.	Option	Description	Remarks
1	-h	Displays the voltage/temperature of the NAS Module.	
2	-s	Displays the status of the NAS Module.	
3	-a	Displays the status of all NAS Modules.	
4	-s -a	Displays the status overview of all NAS Modules.	

7.7.2 status Output Format

Running example of the status command is as shown below.

```
G400-482002-1:$ status
Cluster Communication:
Cluster Interconnect:      OK
Management Network: OK
Quorum Device:      OK

Board temperature:
HFB Inlet sensor:   OK (36 C)
HFB WFS FPGA sensor:       OK (45 C)
HFB DI FPGA sensor: OK (49 C)
HFB TAN FPGA sensor:       OK (53 C)

Chassis disk status:
/    : OK              8% full.
/opt: OK               3% full.
/var: OK               2% full.

Ethernet Aggregations:
ag1: Up

Server uptime:    2 days, 16 hours, 38 minutes, 21 seconds
Server date/time: 2016-01-18 09:02:12+00:00
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.7.3 status -h Option Output Format

Running example and the output format of the status -h command are as shown below.

```
G400-482002-1:$ status -h

ADC data from HFB - Lattice ispPAC-POWR1220AT8 ADC (TAN)                    ①
VV0090PTAN_CORE          0.91V
VV0105PTAN_VCCT          1.03V
VV0105PTAN_VCCR          1.04V
VV0150PTAN               1.49V
VV0150PTAN_IO            1.50V
VV0250PMAIN              2.48V
VV0330PMAIN              3.26V
VV0300PTAN               2.98V
VV1200PHFB_HS            12.14V
VV1200PPL_HS             12.46V

ADC data from HFB - Lattice ispPAC-POWR1220AT8 ADC (DI)
VV0090PDI_CORE           0.91V
VV0105PDI_VCCT           1.03V
VV0105PDI_VCCR           1.05V
VV0150PDI                1.50V
VV0150PDI_IO             1.50V
VV0330PSTBY              3.34V
VV0330PSTBY_TAN_LATTICE  3.34V
VV0330PSTBY_WFS_LATTICE  3.34V
VV0300PDI                3.00V
VV0250PDIWFS             2.47V
VV0330PDIWFS             3.23V

ADC data from HFB - Lattice ispPAC-POWR1220AT8 ADC (WFS)
VV0090PWFS_CORE          0.90V
VV0105PWFS_VCCT          1.05V
VV0105PWFS_VCCR          1.04V
VV0150PWFS               1.49V
VV0150PWFS_IO            1.50V
VV0330PSTBY_DI_LATTICE   3.35V
VV0300PWFS               3.00V

Service time (h): 298

Temp sensor                          Board inlet                WFS FPGA      ②
Status                                   Temp OK                 Temp OK
Temperature                                  36C                     45C

Temp sensor                              DI FPGA                TAN FPGA
Status                                   Temp OK                 Temp OK
Temperature                                  49C                     53C
```

Table 7-8 Descriptions of the Output Format

No.	Item	Description	Remarks
①	ADC data from HFB - Lattice ispPAC-POWR1220AT8 ADC	Displays the voltage on MFB.	
②	Temp sensor	Displays the location of the temperature sensor.	
	Status	Displays the temperature status.	
	Temperature	Displays the current temperature.	

Copyright © 2015, 2017, Hitachi, Ltd.

7.7.4 status -s Option Output Format

Running example and the output format of the status -s command is as shown below.

```
G400-482002-1:$ status -s

       Cluster:      OK                                                    ①
       Temperature:  OK
Ethernet Aggregations:            OK
```

Table 7-9 Descriptions of Output Format

No.	Item	Description	Remarks
①	Cluster	Displays the status of the NAS Module.	
	Temperature	Displays the temperature status (current temperature).	
	Ethernet Aggregations	Displays the status of Ethernet.	

Copyright © 2015, 2017, Hitachi, Ltd.

7.7.5 status -a Option Output Format

Running example and the output format of the status -a command are as shown below.

```
G400-482002-1:$ status -a

G400-482002-1
-------------
Cluster Communication:
Cluster Interconnect: OK
Management Network:   OK
Quorum Device:        OK

Board temperature:
HFB Inlet sensor:   OK (36 C)
HFB WFS FPGA sensor:   OK (46 C)
HFB DI FPGA sensor:   OK (49 C)
HFB TAN FPGA sensor:   OK (53 C)

Chassis disk status:
/    : OK              8% full.
/opt: OK               3% full.
/var: OK               2% full.

Ethernet Aggregations:
ag1: Up

Server uptime:    2 days, 18 hours, 13 minutes, 16 seconds
Server date/time: 2016-01-18 10:37:05+00:00

G400-482002-2
-------------
Cluster Communication:
Cluster Interconnect: OK
Management Network:   OK
Quorum Device:        OK

:(Same contents as shown above are displayed)
```

①
②
③
④
⑤

Copyright © 2015, 2017, Hitachi, Ltd.

Table 7-10 Descriptions of Output Format

No.	Item	Description	Remarks
①	Cluster Communication		
	Cluster Interconnect	Displays the connection status.	
	Management Network	Displays the management LAN status.	
	Quorum Device	Displays the SMU status.	
②	Board temperature		
	HFB Inlet sensor	Displays the status of the inlet temperature sensor. (Temperature display)	
	HFB WFS FPGA sensor	Displays the status of the WFS FPGA temperature sensor. (Temperature display)	
	HFB DI FPGA sensor	Displays the status of the DI FPGA temperature sensor. (Temperature display)	
	HFB TAN FPGA sensor	Displays the status of the TAN FPGA temperature sensor. (Temperature display)	
③	Chassis disk status	Displays the disk status.	
④	Ethernet Aggregations		
	ag1	Displays the status of ag1.	
⑤	Server uptime	Displays the continuous operating time.	
	Server date/time	Displays the current date and time.	

Copyright © 2015, 2017, Hitachi, Ltd.

7.8 Setting Date and Confirmation (setdate)

The setdate command displays/sets the date of NAS Modules.

7.8.1 Command Line

The format of the setdate command is as follows.

setdate [date]

Table 7-11 describes the options.

Table 7-11 Descriptions of Options

No.	Option	Description	Remarks
1	date	When setting the date, specify in the following formats. • [dd mm yyyy] • dd: Date to be set • mm: Month to be set • yyyy: Year to be set (Dominical year)	

7.8.2 setdate Output Format

Running example of the setdate command is as shown below.

- Displays the current date.

```
G400-482002-1:$ setdate
2016-01-18 11:07:23+00:00       Daylight saving time is not in effect
G400-482002-1:$
```

- Sets the date.

```
G400-482002-1:$ setdate 20 01 2016
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.9 Setting Time and Confirmation (settime)

The settime command displays/sets the time of NAS Modules.

7.9.1 Command Line

The format of the settime command is as follows.

settime [settime]

Table 7-12 describes the options.

Table 7-12 Descriptions of Options

No.	Option	Description	Remarks
1	settime	When setting the time, specify in the following formats. • [hh mm ss] • hh: Time to be set • mm: Minutes to be set • ss: Seconds to be set	

7.9.2 settime Output Format

Running example of the settime command is as shown below.

- Displays the current time.

```
G400-482002-1:$ setdate
2016-01-18 11:07:23+00:00       Daylight saving time is not in effect
G400-482002-1:$
```

- Sets the time.

```
G400-482002-1:$ setdate 13 45 30
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.10 Confirming the Version of NAS Modules (ver)

The ver command displays the hardware/software version of NAS Modules.

7.10.1 Command Line

The format of the ver command is as follows.

ver [-h|-s|-v|-t]

Table 7-13 describes the options.

Table 7-13 Descriptions of Options

No.	Option	Description	Remarks
1	-h	Displays the detailed version of the hardware.	
2	-s	Displays the detailed version of the software.	
3	-v	Displays the detailed version of VLSI.	
4	-t	Displays the overviews of the board type.	

7.10.2 ver Output Format

Running example of the ver command is as shown below.

```
G400-482002-1:$ ver

Model: G400   ①

Software: 12.6.4130.00 (built 2015-12-10 03:32:33+00:00)   ②

Hardware: NAS Platform (482002)

board  LPAR-Type1
mmb    12.6.4130.00 release (2015-12-10 03:32:33+00:00)

board  HFB1
hfb1hw MB v0AC6 WL v0AC6 TD v0AC6 FD v0AC6 TC v0AC6 RY v0AC6 TY v0AC6 WF v
   046A FS v046A OS v046A WD v046A IC v08AD DI v08AD
Serial no    3553289079-H00000026 (Tue Sep  1 11:15:53 2015)
```

Table 7-14 Descriptions of Output Format

No.	Item	Description	Remarks
①	Model	Displays the model name.	
②	Software	Displays the firmware version.	

Copyright © 2015, 2017, Hitachi, Ltd.

7.10.3 ver -h Option Output Format

Running example of the ver -h command is as shown below.

```
G400-482002-1:$ ver -h

Product serial no: 482002

HFB1

Serial number:       3553289079-H00000026 (Tue Sep  1 11:15:53 2015)
Package revision:    A/D1.D
Marketing name:      HFB1000
MAC base:            00 1F 67 EF 20 A0
First date:          2015-09-01 11:15:53+00:00
MTDS test count:     3
MTDS pass status:    Pass
ESS pass status:     Not run / unknown
Card ID:             0xA0
Card Revision:       0x04
Glue Revision:       0x1C
DI_CACHE_MEM:        16384 MB
DI_CTRL0_MEM:        8192 MB
DI_CTRL1_MEM:        8192 MB
TAN_BUFF_MEM:        16384 MB
TAN_CTRL0_MEM:       8192 MB
TAN_CTRL1_MEM:       8192 MB
WFS_WFILE_MEM:       8192 MB
WFS_WDIR_MEM:        8192 MB
WFS_POBJ_MEM:        8192 MB
WFS_SOBJ_MEM:        8192 MB

Processor:           Xeon; Type 0, Family 6, Model 62, Stepping 4; Cores 4

TAN Chip version:0xac6 repo:0x1004
TAN Flash def version:0x74 repo:0xfa0
TAN Flash app version:0xac6 repo:0x1004

DI Chip version:0x8ad repo:0x1004
DI Flash def version:0x31 repo:0xfa0
DI Flash app version:0x8ad repo:0x1004

Lattice TAN chip version:       01.01.01.01
Lattice DI chip version:        01.02.01.01
Lattice WFS chip version:       01.03.01.01
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.11 Managing IP Addresses (ipaddr)

The ipaddr command lists and displays the IP addresses of NAS Modules.

7.11.1 Command Line

The format of the ipaddr command is as follows.

ipaddr [-i <addr> -m <mask>] [-r] [-c]

Table 7-15 describes the options.

Table 7-15 Descriptions of Options

No.	Option	Description	Remarks
1	-i	Sets and changes the specified IP address.	
2	-m	Sets and changes the specified net mask.	
3	-r	Deletes the IP address settings.	
4	-c	Confirms the update or deletion of the IP address.	

7.11.2 ipaddr Output Format

Running example of the ipaddr command is as shown below.

```
G400-482002-1:$ ipaddr
Cluster node ID = 1
##      IP Address     Mask / Prefix Length   Port
--    -------------    -------------------   -----
 1    10.213.54.240      255.255.254.0       CTL1

Cluster node ID = 2
##      IP Address     Mask / Prefix Length   Port
--    -------------    -------------------   -----
 1    10.213.54.195      255.255.254.0       CTL2
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.12 Displaying the NAS Module Status (cluster-show)

The cluster-show command displays the parameter and the status of NAS Modules.

7.12.1 Command Line

The format of the cluster-show command is as follows.

cluster-show [-a | --all] [-c | --admin] [-l | --local] [-y | --node] [-q | --quorum] [-v | --EVS]

Table 7-16 describes the options.

Table 7-16 Descriptions of Options

No.	Option	Description	Remarks
1	-a	Displays the all cluster information.	
2	-c	Displays the cluster Admin Service information.	
3	-l	Displays the EVS information in local.	
4	-y	Displays the cluster node information.	
5	-q	Displays the quorum device information.	
6	-v	Displays the EVS information.	

Copyright © 2015, 2017, Hitachi, Ltd.

7.12.2 cluster-show -a Option Output Format

Running example and the output format of the cluster-show-a command are as shown below.

```
G400-482002-1:$ cluster-show -a
Overall Status = Online
Cluster Health = Robust                                                    ①
Cluster Mode = Clustered
Cluster Name = G400-482002
Cluster UUID = 8a956296-47f9-11d1-9000-040802000002
Cluster Size = 2
   Node Name = G400-482002-1
     Node ID = 1
Cluster GenId = 3
Cluster Master = No

Server Quorum Version: 15                                                  ②
QD IP Address     Status   Quorum Device(QD) Name  Versions
-------------  ---------- ----------------------  -----------
127.0.0.1      Configured  I       nternalQD       15, 14

                                Ethernet   Mgmnt                           ③
ID     Node Name    Status   FS Access  Aggs  Netwrk  FC   EVS IDs
--   -------------  -------  ---------  -----  ------  ---  -------
1    G400-482002-1  ONLINE      OK       OK      OK    NA   []
2    G400-482002-2  ONLINE      OK       OK      OK    NA   [0,1,2,3,4]

Cluster Communications Status:

Cluster Interconnect                                                       ④
From  To=> Node 1  Node 2
Node 1       --      OK
Node 2       OK      --

Management Network
From  To=> Node 1  Node 2
Node 1       --      OK
Node 2       OK      --

Node  EVS ID   Type       Label       Enabled  Status     IP Address     Port
------  ----------   -------------  --------  ------     ----------     ------
   1         Cluster  G400-482002-1    Yes    Online     10.0.0.20      eth0
                                                          10.1.48.1      eth1
   2         Cluster  G400-482002-2    Yes    Online     10.0.0.21      eth0
                                                          10.1.52.1      eth1
   2    0    Admin    G400-482002-a    Yes    Online     10.1.48.2      eth1
                                                        2002::a01:3002   eth1
   2    1    Service      EVSTEST1     Yes    Online     10.213.54.251  ag1
   2    2    Service      EVSTEST2     Yes    Online     10.213.54.255  ag1
   2    3    Service      EVSTEST3     Yes    Online     10.213.54.252  ag1
   2    4    Service      EVSTEST4     Yes    Online     10.213.54.254  ag1
```

Copyright © 2015, 2017, Hitachi, Ltd.

Table 7-17 Descriptions of Output Format

No.	Item	Description	Remarks
①	Displays the cluster basic information.		
	Cluster Health	Displays the cluster status.	Robust: Communicating in all clusters. Degraded: The heartbeat communication is not performed in one or more nodes. Critical: Only minimum requirements are fulfilled as a cluster.
	Cluster Mode	Displays the cluster mode.	
	Cluster Name	Displays the cluster name.	
	Cluster UUID	Displays the UUID of the cluster.	
	Cluster Size	Displays the cluster size.	Displays how many nodes exist in a cluster.
	Node Name	Displays the own node name.	
	Node ID	Displays the own node ID.	
②	Displays the status of Quorum Device		
	QD IP Address	Displays the IP address of Quorum Device.	
	Status	Displays the Quorum Device status.	Owned: Owing Quorum Device by the own node.
	Quorum Device (QD) Name	Displays the name of Quorum Device.	
	Versions	Displays the version of Quorum Device.	
③	Displays the cluster node status		
	ID	Displays the node ID.	
	Node Name	Displays the node name.	
	Status	Displays the node status.	
	FS Access	Displays the access availability to the file system.	
	Ethernet Aggs	Displays the availability of the data LAN.	
	Mgmnt Netwrk	Displays the availability of the management LAN.	
	FC	Displays the availability of the FC channel.	
	EVS IDs	Displays the EVS ID existing on the node.	

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from the preceding page)

No.	Item	Description	Remarks
④	Displays the cluster communication status		
	Cluster Interconnect	Displays the cluster communication status.	
	Management Network	Displays the management LAN communication status.	
	Node	Displays the node ID.	
	EVS ID	Displays the EVS ID.	
	Type	Displays the type.	Cluster Admin Service by type.
	Label	Displays the label.	CLUSTER NODE EVS by label type.
	Enabled	Displays the availability of the communication.	
	Status	Displays the communication status.	
	IP Address	Displays the IP address.	
	Port	Displays the using port.	

Copyright © 2015, 2017, Hitachi, Ltd.

7.13 EVS Migration (evs migrate)

NOTE: When performing the EVS migration, you cannot access to NAS Module temporarily. Confirm with the system administrator before performing the EVS migration.

The evs migrate command is used for the EVS migration.

7.13.1 Command Line

The format of the evs migrate command is as follows.

evs migrate (-e <evs-specifier> | --all <src-nodeid>) -n <dst-nodeid> [-c | --confirm]

Table 7-18 describes the options.

Table 7-18 Descriptions of Options

No.	Option	Description	Remarks
1	-e <EVS ID>	Specifies the EVS ID number to be operated.	
2	--all <target node ID>	Changes all EVS to the target EVS to be oeparted.	
3	-n <migration destination node ID>	Specifies the node ID number in the migration destination.	
4	-c-|-confirm	It does not output the running confirmation message of the operation.	

7.13.2 evs migrate Output Format

Running example of the evs migrate command is as shown below.

- When migrating by specifying EVS

```
G400-482002-1:$ evs migrate -e TESTEVS1 -n 2
Warning: Migrating the EVS will disrupt File System services to any existing
clients.
Do you want to continue?(Y/N)[N]:
```

- When migrating all EVS

```
G400-482002-1:$ evs migrate --all 1 -n 2
Warning: Migrating the EVS will disrupt File System services to any existing
clients.
Do you want to continue?(Y/N)[N]:
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.14 EVS Information (evs list)

The evs list command is used to indicate the EVS information.

7.14.1 Command Line

The format of the evs list command is as follows.

list [-t <admin | serv> | -e <evs-id>]

Table 7-19 describes the options.

Table 7-19 Descriptions of Options

No.	Option	Description	Remarks
1	-t <admin | serv>	Specifies the EVS Type to be operated.	
2	-e <EVS ID>	Specifies the EVS ID number to be operated.	

7.14.2 evs list Output Format

Running example of the evs list command is as shown below.

```
400-482002-1:$ evs list

Node      EVS ID    Type            Label Enabled Status          IP Address Port
----      ------    ------------    ------------- -------         ----------------
   1        Cluster G400-482002-1     Yes Online   10.213.54.240      CTL1
                                                       10.0.0.20      eth0
                                                       10.1.48.1      eth1
   1      0   Admin G400-482002-a     Yes Online       10.1.48.2      eth1
                                                   2002::a01:3002     eth1
   1      1 Service  EVSforFileIO     Yes Online 128.128.200.101       ag1
   1      2 Service     EVSTEST01     Yes Online  128.128.200.11       ag1
   1      3 Service     EVSTEST02     Yes Online  128.128.200.12       ag1
   2        Cluster G400-482002-2     Yes Online   10.213.54.195      CTL2
                                                       10.0.0.21      eth0
                                                       10.1.52.1      eth1
   2      4 Service     EVSTEST03     Yes Online  128.128.200.13       ag1
   2      5 Service     EVSTEST04     Yes Online  128.128.200.14      ag1
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.15 Stopping EVS (evs disable)

NOTE: When performing the EVS migration, you cannot access to NAS Module at all.

The evs disable command is used to stop EVS.

7.15.1 Command Line

The format of the evs disable command is as follows.

disable -e <evs-specifier> [-c | --confirm]

Table 7-20 describes the options.

Table 7-20 Descriptions of Options

No.	Option	Description	Remarks
1	-e <EVS ID>	Specifies the EVS ID number to be operated.	
2	-c-|-confirm	It does not output the running confirmation message of the operation.	

7.15.2 evs disable Output Format

Running example of the evs disable command is as shown below.

- Stop EVS

```
G400-482002-1:$ evs disable -e 5
Do you want to proceed?(Y/N)[N]:
```

- Check that EVS stops

```
G400-482002-1:$ evsipaddr -l

EVS Type   Label           IP Address          Mask             Port
--------   -------------   ----------------    --------------   -----
 admin     G400-482002-a   10.1.48.2           255.255.0.0       eth1
 admin     G400-482002-a   2002::a01:3002              /64       eth1
 evs 1     EVSforFileIO    128.128.200.101     255.255.255.0      ag1
 evs 2     EVSTEST01       128.128.200.11      255.255.255.0      ag1
 evs 3     EVSTEST02       128.128.200.12      255.255.255.0      ag1
 evs 4     EVSTEST03       128.128.200.13      255.255.255.0      ag1
 evs 5     EVSTEST04       128.128.200.14 (I)  255.255.255.128    ag1
```

: An IP address with (I) is in the Inactive status.

Copyright © 2015, 2017, Hitachi, Ltd.

7.16 Booting EVS (evs enable)

The evs enable command is used to boot EVS.

7.16.1 Command Line

The format of the evs enable command is as follows.

enable -e <evs-specifier>

Table 7-21 describes the options.

Table 7-21 Descriptions of Options

No.	Option	Description	Remarks
1	-e <EVS ID>	Specifies the EVS ID number to be operated.	

7.16.2 evs enable Output Format

Running example of the evs enable command is as shown below.

- Boot EVS

```
G400-482002-1:$ evs enable -e 5
```

- Confirm that EVS booted

```
G400-482002-1:$ evsipaddr -l

EVS Type   Label            IP Address          Mask              Port
--------   ------------     ---------------     --------------    -----
 admin     G400-482002-a    10.1.48.2           255.255.0.0        eth1
 admin     G400-482002-a    2002::a01:3002            /64          eth1
 evs 1     EVSforFileIO     128.128.200.101     255.255.255.0       ag1
 evs 2     EVSTEST01        128.128.200.11      255.255.255.0       ag1
 evs 3     EVSTEST02        128.128.200.12      255.255.255.0       ag1
 evs 4     EVSTEST03        128.128.200.13      255.255.255.0       ag1
 evs 5     EVSTEST04        128.128.200.14      255.255.255.128     ag1
```

: When NAS Module starts, (I) becomes hidden and the status is Active.

Copyright © 2015, 2017, Hitachi, Ltd.

7.17 Setting IP Address (evsipaddr)

The evsipaddr command sets the IP address of EVS.

7.17.1 Command Line

The format of the evsipaddr command is as follows.

evsipaddr [-e <evs-id>|-l] [-a|-r|-u] [-i <addr>|<addr/prefix-length>] [-m <mask>] [-p <port>] [-c | --confirm]

- When displaying the IP address given to all EVS.
  evsipaddr –l

- When giving the IP address to EVS
  evsipaddr -e <EVS ID> -a -i <IP address> -m <net mask> -p <interface name>

- When deleting the IP address given to EVS
  evsipaddr -e <EVS ID> -r -i <IP address>

Table 7-22 describes the options.

Table 7-22 Descriptions of Options

No.	Option	Description	Remarks
1	-e <EVS ID>|-l	Options to be specified are as follows. -e <EVS ID>: Specified EVS ID -l: All EVS	
2	-a|-r|-u	Options to be specified are as follows. -a: Sets the IP address to EVS -r: Deletes the IP address from EVS -u: Changes the set IP address	
3	-i <IP address>	Specifies the value of the IP address.	
4	-m <net mask>	Specifies the net mask.	
5	-p <interface name>	Specifies the interface name.	
6	-c | --confirm	It does not output the running confirmation message of the operation.	

Copyright © 2015, 2017, Hitachi, Ltd.

7.17.2 evsipaddr Output Format

Running example of the evsipaddr command is as shown below.

1. Refer the IP address set for EVS.

```
G400-482002-1:$ evsipaddr -l

EVS Type            Label          IP Address              Mask      Port
--------     -------------     --------------     -------------     ----
   admin     G400-482002-a          10.1.48.2       255.255.0.0     eth1
   admin     G400-482002-a      2002::a01:3002              /64     eth1
   evs 1          EVSTEST1       10.213.54.251     255.255.254.0      ag1
   evs 2          EVSTEST2       10.213.54.255     255.255.254.0      ag1
   evs 3          EVSTEST3       10.213.54.252     255.255.254.0      ag1
   evs 4          EVSTEST4       10.213.54.254     255.255.254.0      ag1
```

2. Set the IP address.

```
G400-482002-1:$ evsipaddr -e 1 -a -i 10.213.54.3 -m 255.255.255.0 -p ag1
```

3. Confirm that the setting is for the set IP address.

```
G400-482002-1:$ evsipaddr -l

EVS Type            Label          IP Address              Mask      Port
--------     -------------     --------------     -------------     ----
   admin     G400-482002-a          10.1.48.2       255.255.0.0     eth1
   admin     G400-482002-a      2002::a01:3002              /64     eth1
   evs 1          EVSTEST1       10.213.54.251     255.255.254.0      ag1
   evs 1          EVSTEST1        10.213.54.3      255.255.255.0      ag1
   evs 2          EVSTEST2       10.213.54.255     255.255.254.0      ag1
   evs 3          EVSTEST3       10.213.54.252     255.255.254.0      ag1
   evs 4          EVSTEST4       10.213.54.254     255.255.254.0      ag1
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.18 Confirming SUM Version (smu-version)

The smu-version command displays the SUM version.

7.18.1 Command Line

The format of the smu-version command is as follows.

smu-version

7.18.2 smu-version Output Format

Running example of the smu-version command is as shown below.

```
G400-482002-1:$ smu-version

Cluster Node                                                          SMU Version
-----------  ------------------------------------------------------------------------
  1          System Management Unit (SMU) Version: 12.6.4130.00 Thu Dec 10, 2015
05:35:37 PST

  2          System Management Unit (SMU) Version: 12.6.4130.00 Thu Dec 10, 2015
05:35:37 PST
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.19 Confirming SMU Running Status (smu-service-status)

The smu-service-status command confirms in which side the command is running.

7.19.1 Command Line

The format of the smu-service-status command is as follows.

smu-service-status

7.19.2 smu-service-status Output Format

Running example of the smu-service-status command is as shown below.

```
G400-482002-1:$ smu-service-status

Cluster Node     SMU Status
---------------     --------------
          1          standby
          2           active
```

: Active displaying side is running.

Copyright © 2015, 2017, Hitachi, Ltd.

7.20 Rebooting NAS Module (reboot)

The reboot command is used to reboot NAS Module.

7.20.1 Command Line

The format of the reboot command is as follows.

reboot [-s|--seconds <seconds>] [-n|--now] [-f|--force] [-a|--all] [-c|--cluster] [--app]

Table 7-23 describes the options.

Table 7-23 Descriptions of Options

No.	Option	Description	Remarks
1	-s	Reboot after <seconds> seconds.	
2	-n	The corresponding NAS Module reboots immediately.	
3	-f	Reboot forcibly.	
4	-a	The both sides reboot at the same time.	
5	-c	Reboots one side at a time.	
6	--app	Perform the file serving again.	

7.20.2 reboot Output Format

Running example of the reboot command is as shown below.

```
G400-482002-1:$ smu-service-status
Are you sure you want to reboot all cluster nodes? (Y/N)[N]:
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.21 Confirming Command Contents (help)

The help command displays the help of the command.

7.21.1 Command Line

The format of the help command is as follows.

help [-k] all|<command>

Table 7-24 describes the options.

Table 7-24 Descriptions of Options

No.	Option	Description	Remarks
1	-k <command>	Chain to apropos if no exact match	
2	all	Show brief description of all commands	

7.21.2 help Output Format

Running example of the help command is as shown below.

```
G400-482002-1:$ help -k all
  adjoinedfs-create This command has been deprecated.
  adjoinedfs-expand This command has been deprecated.
  adjoinedfs-status While adjoined file systems are deprecated, the command displays the
state of a given one.
  adjoinedfs-unlink Unlinks adjoined file system leaving it as an ordinary file system.
  adjoinedfs-update-status While adjoined filesystems are deprecated, the command
updates the status of a given one.
  agg              Configure/Display aggregation interfaces
  agg-upgrade      Upgrade aggregation configuration
  aggedit          Configure an aggregation interface
  aggregate-linux-interface-create Create an eth-ag interface
  aggregate-linux-interface-delete Delete an eth-ag interface
  aggregate-linux-interface-show Display eth-ag interfaces
  alert-mail       Report/configure alerts by email
  alert-send-test  Immediately send an alert to all configured recipients
  alert-snmp       Report/configure alerts by SNMP
  alert-summary    Send alert summary now
  alert-syslog     Report/configure alerts by syslog
  apppro-stats     Display AppPro statistics
  apropos          Search command names and descriptions and man pages
  arp              ARP table manipulation
  async-lock-perf  Display asynchronous file region lock statistics
  at               Manipulate at job table
  audit-log-clear  Clear (empty) the current audit log for a file system
  audit-log-consolidated-cache Control or display the Audit log consolidated cache file
and its options
  audit-log-consolidated-cache-clear Clear (empty) the audit log consolidated cache file
  audit-log-consolidated-cache-reset Reset the audit log consolidated cache file
  audit-log-consolidated-cache-save Save a copy of the audit log consolidated cache file
  audit-log-consolidated-cache-show Display the audit log consolidated cache file
  audit-log-perf   Display filesystem audit log performance statistics
  audit-log-save   Save a copy of the current audit log for a file system
  audit-log-show   Display the audit log for a file system
  audit-log-stats  Display basic file system audit log statistics
  audit-syslog     Report/configure audit events by syslog
  autodoc          Auto document commands
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.22 Displaying List of Directories (ls)

The Is command is used to display the list of directories.

7.22.1 Command Line

The format of the ls command is as follows.

ls [-a] [-d] [-h] [-l] [-r] [-i] [-s <sort option>] [-C <resume cookie>] [<path>]

Table 7-25 describes the options.

Table 7-25 Descriptions of Options

No.	Option	Description	Remarks
1	-a	Do not hide entries starting with the '.' character	
2	-C	Resume on the entry with the specified cookie	
3	-d	Show the directory itself, instead of its contents	
4	-h	Show human-readable file lengths	
5	-i	Sort names case insensitively	
6	-l	Use a long listing format. The second column in the listing represents file type. Supported file types are C=file-clone, X=CVL/XVL, I=ingested and -=regular/others.	
7	-r	Reverse the sort direction	
8	-s	Sort the list. Options are none, name, time, atime and size.	The default is to sort by name.
9	-v	Verbose listing format	

7.22.2 ls Output Format

Running example of the ls -lL command is as shown below.

```
maintenance@G400-442004-1(bash):~$ ls -lL /dump
total 124140
-rw-rr-- 1 root root 53129484 Mar 1 15:52 dumpfile_20160301155028.tar.xz
-rw-rr-- 1 root root 73984140 Mar 1 20:59 dumpfile_20160301205758.tar.xz
manager@G400-442004-1(bash):~$
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.23 Confirming Network Communication (ping)

The ping command is used to transmit the packet and request the response.

7.23.1 Command Line

The format of the ping command is as follows.

ping [-c <count>][-I source-IP-address[%interface]][-s <packetsize>] <IP-address or hostname> [%interface]

Table 7-26 describes the options.

Table 7-26 Descriptions of Options

No.	Option	Description	Remarks
1	-c	The number of ECHO_REQUESTS to send. The default is 4; the minimum is 1.	
2	-I	Set the source IP address of the request to the supplied IP address.	
3	-s	Set the number of data bytes to be sent. The default is 56 which mean that 64 bytes of IPv4 data is sent over the wire.	

7.23.2 ping Output Format

Running example of the ping command is as shown below.

```
G400-482002-1:$ ping -c 5 128.128.200.101
128.128.200.101...
--
5 packets transmitted, 0 packets received, 100% packet loss
G400-482002-1:$ ping -c 5 128.128.200.10
128.128.200.10...
64 bytes from 128.128.200.10: icmp_seq=0 time=1 ms
64 bytes from 128.128.200.10: icmp_seq=1 time <1 ms
64 bytes from 128.128.200.10: icmp_seq=2 time <1 ms
64 bytes from 128.128.200.10: icmp_seq=3 time <1 ms
64 bytes from 128.128.200.10: icmp_seq=4 time <1 ms
--
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0/0/1 ms
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.24 Displaying List of Spans (span-list)

The span-list command is used to display the list of one or all spans.

7.24.1 Command Line

The format of the span-list command is as follows.

span-list [--sds] [--filesystems] [--verbose] [<span-instance-name>]

7.24.2 span-list Output Format

Running example of the span-list command is as shown below.

```
G400-482002-1:$ span-list
Span instance name    OK?   Free   Cap/GiB   System drives           Con
------------------    ---   ----   -------   ---------------------   ---
Span1                 Yes    50%        80   0,1,2,3,4,5,6,7          90%
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.25 Enabling Access to Spans (span-assign-to-cluster)

The span-assign-to-cluster command enables the access to spans.

7.25.1 Command Line

The format of the span-assign-to-cluster command is as follows.

span-assign-to-cluster [--danger-ignore-sd-sites] [--danger-ignore-stale-cod] <span-base-or-instance-name> [<cluster-uuid> <cluster-name>]

7.25.2 span-assign-to-cluster Output Format

Running example of the span-assign-to-cluster command is as shown below.

```
G800-400001-2:$ span-assign-to-cluster Pool1
Assigning the span to this cluster
Success

If any other cluster has loaded this span, it will not see the change you have
just made until you reboot it or, on that remote cluster, unmount any mounted
file systems on the span and run:

sd-rescan-cod Pool1

G800-400001-2:$
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.26 Displaying List of System Drives (sd-list)

The sd-list command is used to display the list of system drives.

7.26.1 Command Line

The format of the sd-list command is as follows.

sd-list [<formatting-options>] [<other-options>] [<selection-criteria>] [<system-drives>]

7.26.2 sd-list Output Format

Running example of the sd-list command is as shown below.

```
G400-482002-1:$ sd-list
Device   Status    Alw  GiByte  Mirror   In span                  Span Cap
------   ------    ---  ------  ------   -------------------      --------
   0      OK       Yes      10   Pri      Span1                         80
   1      OK       Yes      10   Pri      Span1                         80
   2      OK       Yes      10   Pri      Span1                         80
   3      OK       Yes      10   Pri      Span1                         80
   4      OK       Yes      10   Pri      Span1                         80
   5      OK       Yes      10   Pri      Span1                         80
   6      OK       Yes      10   Pri      Span1                         80
   7      OK       Yes      10   Pri      Span1                         80
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.27 Displaying Disk Utilization Ratio (df)

The df command is used to display the disk utilization ratio by file systems.

7.27.1 Command Line

The format of the df command is as follows.

df [-f <file-system> | -a] [-k] [-h] [-A] [-s] [-i]

Table 7-27 describes the options.

Table 7-27 Descriptions of Options

No.	Option	Description	Remarks
1	-f	Displays disk utilization for the named file system only.	
2	-a	Displays disk utilization for all file systems on all EVSs.	
3	-i	Displays the volume number of the file system in addition to its volume ID.	
4	-k	By default all capacities are displayed in reasonable units for the quantities involved. Use this option to force all capacities to be displayed in kilobytes.	
5	-h	Add HTML formatting. Internally used by the server.	
6	-A	By default file systems are displayed individually.	
7	-s	Display committed disk space utilization.	

7.27.2 df Output Format

Running example of the df command is as shown below.

```
G400-482002-1:$ df

ID   Label   Size    Used          Snapshots  Deduped  Avail        Thin  FS Type
---  ------- ----    ----------    ---------  -------  -----------  ----  -----
1024 Span1FS 39.75GB 28.84GB (73%) 0 B (0%)     NA     10.91GB (27%)  No    32 KB,WFS-2,128 DSBs
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.28 Deleting Clusters (cluster-node-delete)

The cluster-node-delete command is used to delete nodes.

7.28.1 Command Line

The format of the cluster-node-delete command is as follows.

cluster-node-delete <node name> <node id>

Table 7-28 describes the options.

Table 7-28 Descriptions of Options

No.	Option	Description	Remarks
1	<node name>	The name of the node to be removed	
2	<node id>	The cluster node id of the node to be removed	

7.28.2 cluster-node-delete Output Format

Running example of the cluster-node-delete command is as shown below.

```
G400-482002-1:$ cluster-node-delete G400-482002-2 2

This command will remove the configuration of (and reboot) node NODE-2
Do you want to continue?(Y/N)[N]:
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.29 Mounting File System (mount)

The mount command is used to mount one or multiple file systems.

7.29.1 Command Line

The format of the mount command is as follows.

mount [--async] [-rfpd] [-a | <file-system>...]

Table 7-29 describes the options.

Table 7-29 Descriptions of Options

No.	Option	Description	Remarks
1	-a	Mount all the unmounted file systems currently visible to the "df" command.	
2	--async	Mount the file system in the background.	
3	-r	Mount the file system read-only.	
4	-f	Mount will normally fail if an NVRAM record cannot be found for the file system. This option allows the mount to continue if the NVRAM record can not be found.	
5	-p	Performs the pre-mount processing but does not proceed to mount the file system.	
6	-d	This option specifically tells the mount command to not enable snapshot deletion support for the specified file system.	

7.29.2 mount Output Format

Running example of the mount command is as shown below.

```
G400-400001-1:$ mount --async
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.30 Power On Self Test (POST) Result (post-status)

The post-status command displays whether Power On Self Test of the hardware fails at the time of start-up. If POST fails, the complete output is displayed.

7.30.1 Command Line

The format of the post-status command is as follows.

post-status

7.30.2 post-status Output Format

Running example of the post-status command is as shown below.

```
G400-400001-1:$ post-status
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.31 Expanding Specific File System (expandfs)

The expandfs command expands the file system that failed before again. This command is used only when it is shown as necessary at the event of the event log.

7.31.1 Command Line

The format of the expandfs command is as follows.

expandfs <file-system>

7.31.2 expandfs Output Format

Running example of the expandfs command is as shown below.

```
G400-400001-1:$ expandfs <file-system>
```

Copyright © 2015, 2017, Hitachi, Ltd.

7.32 Displaying NVRAM utilization ratio (nvpages)

Using the nvpages command can display the NVRAM utilization ratio in the cluster.

7.32.1 Command Line

The format of the nvpages command is as follows.

nvpages list

7.32.2 nvpages Output Format

Running example of the nvpages command is as shown below.

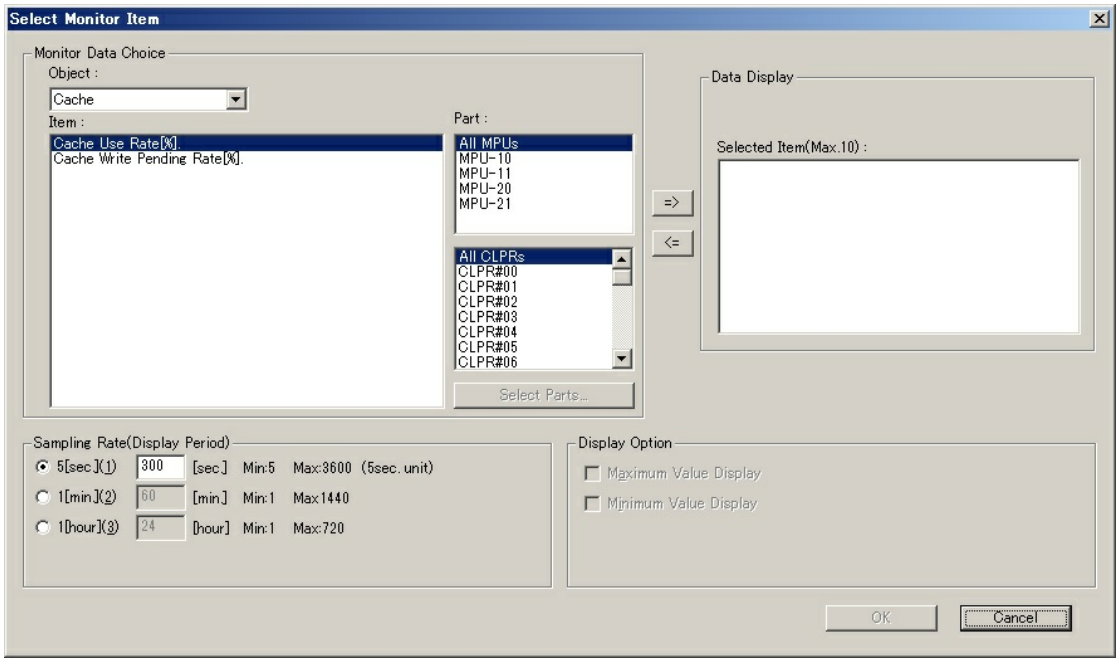
```
G400-400001-1:$ nvpages list
```

Copyright © 2015, 2017, Hitachi, Ltd.

8. Monitoring

When monitoring, perform it by reference to “5. The configuration when monitoring” of “1.2.1 Attachment Procedure of Maintenance PC”.

<Description of the Select Monitor Item dialog>



■ Monitor Data Choice

Object ..... Select the desirable object. You can select “Cache”, “Processor”, “Port”, or “Ldev” (Logical Device).

Item..... Items corresponding to the selected object are displayed. You can select multiple items.

Part..... Parts corresponding to the selected object are displayed.

■ Data Display

Selected Item ..... The selected items are displayed. You can select up to 10 items in one panel.

[=>] button..... This button adds the displayed items. The selected data is added as data that is already selected as the displayed data.

[<=] button..... The selected items are removed from the list of displayed data.

Copyright © 2015, 2017, Hitachi, Ltd.

■ Sampling Rate(Display Period)

Specify the time interval of updating data and the period that data is displayed.
You can specify the display period depending on the selected time interval.

	Display period
5[sec.]	5 seconds to 3,600 seconds (1 hour) (units of 5 seconds)
1[min.]	1 minute to 1,440 minutes (24 hours)
1[hour]	1 hour to 720 hours (30 days)

*1: If you specify 1,440 minutes, the data may not be displayed depending on the window size.

■ Display Option

You can select either to display or not to display the maximum/minimum values when you specify 1[min.] or 1[hour] in the “Sampling Rate(Display Period)”. When you select this option, the maximum/minimum values are indicated by the dotted lines in the graph.
If you place a check mark in “Maximum Value Display”, the maximum value will be displayed. If you place a check mark in “Minimum Value Display”, the minimum value will be displayed.

Copyright © 2015, 2017, Hitachi, Ltd.

■ Display data item list

#	Part	Item	Description	Remarks
1	Cache	Cache Use Rate	Cache Use Rate	
2		Cache Write Pending Rate	Cache Write Pending Rate	
3	MP	MP processing Rate	MP processing Rate	
4		MP Processing Rate Open-Target	MP Processing Rate Open-Target	
5		MP Processing Rate Open-Initiator	MP Processing Rate Open-Initiator	
6		MP Processing Rate Open-External	MP Processing Rate Open-External	
7		MP Processing Rate BackEnd	MP Processing Rate BackEnd	
8		MP Processing Rate Others	MP Processing Rate Others	
9	Port (Fibre)	Loss of Signal Count (Fibre)	Loss of Signal Count	Displaying only with Fibre PCB.
10		Bad Received Character Count (Fibre)	Bad Received Character Count	
11		Loss of Synchronization Count (Fibre)	Loss of Synchronization Count	
12		Link Failure Count (Fibre)	Link Failure Count	
13		Received EOFa Count (Fibre)	Received EOFa Count	
14		Discarded Frame Count (Fibre)	Discarded Frame Count	
15		Bad CRC Count (Fibre)	Bad CRC Count	
16		Protocol Error Count (Fibre)	Protocol Error Count	
17		Expired Frame Count (Fibre)	Expired Frame Count	
18		Forward Error Correction (Fibre)	Forward Error Correction	
19	Port (iSCSI)	MAC CRC Error Count (iSCSI)	MAC CRC Error Count	Displaying only with iSCSI PCB.
20		IP Error Packet Count (iSCSI)	IPv4 Error Packet Count	
21		IPv6 Error Packet Count (iSCSI)	IPv6 Error Packet Count	
22		TCP Retransmit Timer Expired Count (iSCSI)	TCP Retransmit Timer Expired Count	
23		iSCSI Header Digest Error Count (iSCSI)	iSCSI Header Digest Error Count	
24		iSCSI Data Digest Error Count (iSCSI)	iSCSI Data Digest Error Count	
25	Port	Target Port Total IOPS	Target IOPS (Read/Write Command Transfer)	
26		Target Port Total Transfer Rate	Target Transfer Rate (Read/Write Command Transfer)	
27		Target Port Total Response Time	Target Response Time (Read/Write Command Transfer)	
28		Target Port Input IOPS	Target IOPS (Write Command Transfer)	
29		Target Port Input Transfer Rate	Target Transfer Rate (Write Command Transfer)	
30		Target Port Input Response Time	Target Response Time (Write Command Transfer)	
31		Target Port Output IOPS	Target IOPS (Read Command Transfer)	
32		Target Port Output Transfer Rate	Target Transfer Rate (Read Command Transfer)	

(To be continued)

Copyright © 2015, 2017, Hitachi, Ltd.

(Continued from the preceding page)

#	Part	Item	Description	Remarks
33	Port	Target Port Output Response Time	Target Response Time (Read Command Transfer)	
34		Initiator Port Total IOPS	Initiator IOPS (Read/Write Command Transfer)	
35		Initiator Port Total Transfer Rate	Initiator Transfer Rate (Read/Write Command Transfer)	
36		Initiator Port Total Response Time	Initiator Response Time (Read/Write Command Transfer)	
37		Initiator Port Input IOPS	Initiator IOPS (Read Command Transfer)	
38		Initiator Port Input Transfer Rate	Initiator Transfer Rate (Read Command Transfer)	
39		Initiator Port Input Response Time	Initiator Response Time (Read Command Transfer)	
40		Initiator Port Output IOPS	Initiator IOPS (Write Command Transfer)	
41		Initiator Port Output Transfer Rate	Initiator Transfer Rate (Write Command Transfer)	
42		Initiator Port Output Response Time	Initiator Response Time (Write Command Transfer)	
43	LDEV	IOPS	IOPS	
44		Transfer Rate	Transfer Rate	
45		Read Hit Rate	Read Hit Rate (A hit rate only for random read.)	

Copyright © 2015, 2017, Hitachi, Ltd.

1. Display the Monitor panel
   Press the “Monitor” button in the “MPC” window to start the monitoring feature.

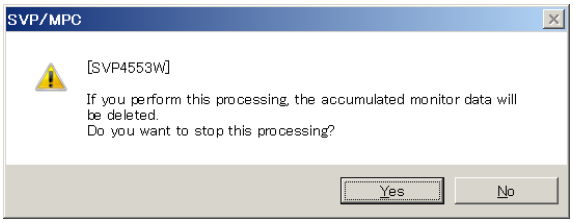
2. Start the Change Monitoring Status window
   Select [Edit]-[Monitoring Switch] from the menu in the Monitor panel.



3. Change the monitoring status
   (1) Start the monitoring
   Select [Enable] in the “Monitoring Switch” window and click the [OK] button.



The confirmation message [4553] to start the monitoring is displayed. To continue the processing, click the [No] button.



NOTE: This operation deletes the accumulated monitor data.
To store the accumulated monitor data, acquire the dump type “Monitor” from AutoDump first.

Copyright © 2015, 2017, Hitachi, Ltd.

(2) Stop the monitoring
Select [Disable] in the “Monitoring Switch” window and click the [OK] button.



4. Display the Select Monitor Item panel
Select [Monitor]-[Open...] from the menu in the Monitor panel.



Copyright © 2015, 2017, Hitachi, Ltd.

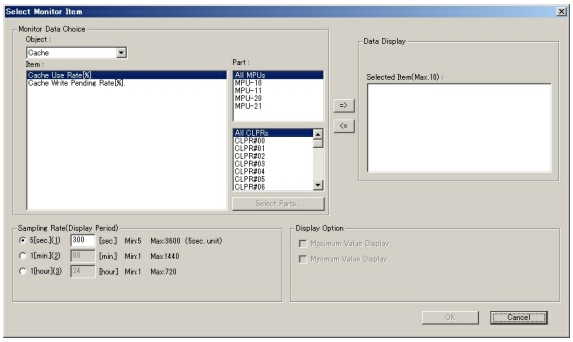
5. Select data to be displayed

(1) Select the data you want to display

Select the category whose data you want to display in [Object] in “Monitor Data Choice”. Available data will appear in [Item]. Select the data you want to display (You can select multiple items). The parts relevant to the selected item will be displayed in [Part]. Choose the desirable part. After selecting [Object], [Item], and [Part], select [=>] button to add the selected items to [Selected Item].

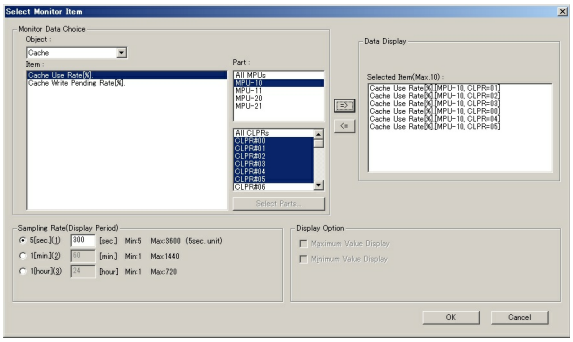
You can display data on up to 10 items. If there is no data in [Selected Item], the [OK] button will not be activated.

If the same item is multiply displayed in the list box of the “Select Monitor Item” dialog, open the dialog again and operate while the items are correctly displayed.



(2) Select the display interval and period

In “Sampling Rate(Display Period)”, specify the time interval of updating data and the period that data is displayed. Select 5[sec.], 1[min.], or 1[hour] for the time interval of updating data. The interval depends on the data you have selected. You can change the period that the data is displayed.



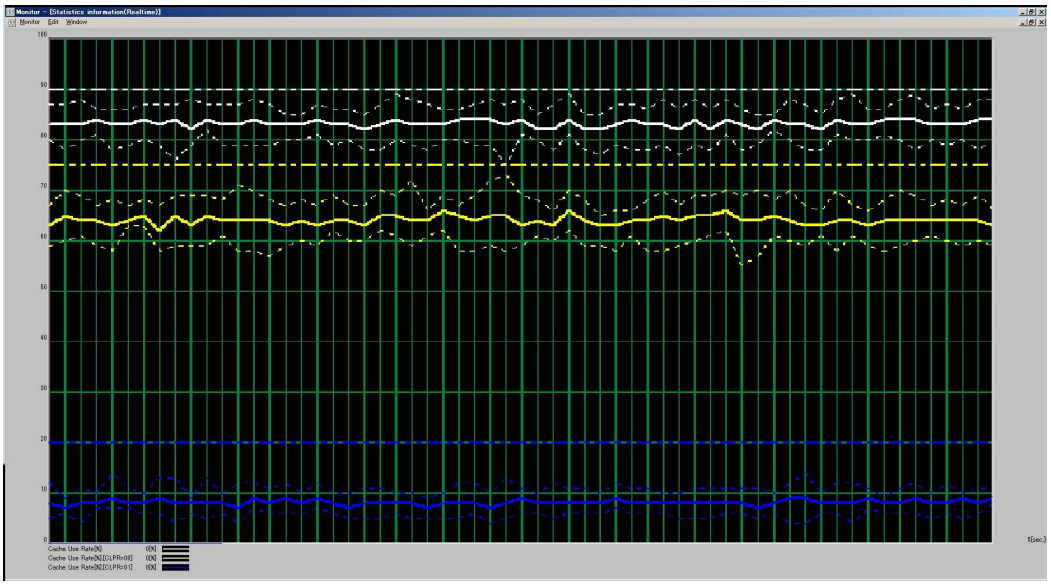
(3) Specify the display option

When you select 1[min.] or 1[hour] in “Display Period”, you can choose either to display or not to display the maximum/minimum value within the time interval.

After selecting all the necessary items, click the [OK] button to display the Statistics information panel.

Copyright © 2015, 2017, Hitachi, Ltd.

6. Description of “Statistics information” panel
   The specified data obtained during the specified display period is displayed in the panel, and it is updated in the specified time interval. The data on the left is older data, and that on the right is newer data.
   The legends are displayed under the graph (Selected data and colors of lines in the graph). The solid lines indicate the data. The thin dotted lines of the same color as the solid lines indicate the maximum/ minimum values of the data.

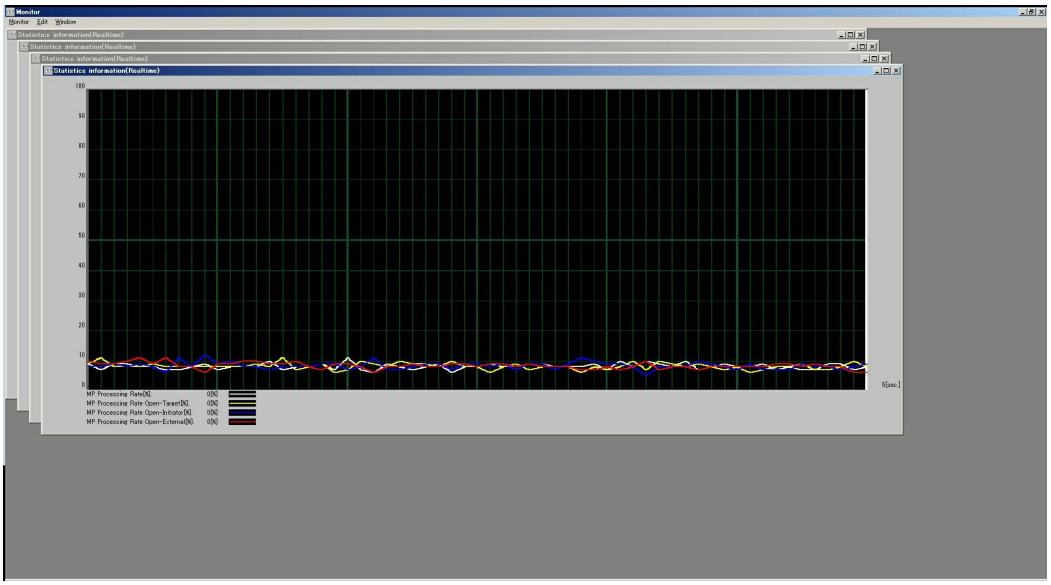


NOTE: If the Storage System is undergoing the following maintenance operations or CHK1A, CHK1B and CHK3 occurs, the monitoring data might contain extremely large values.

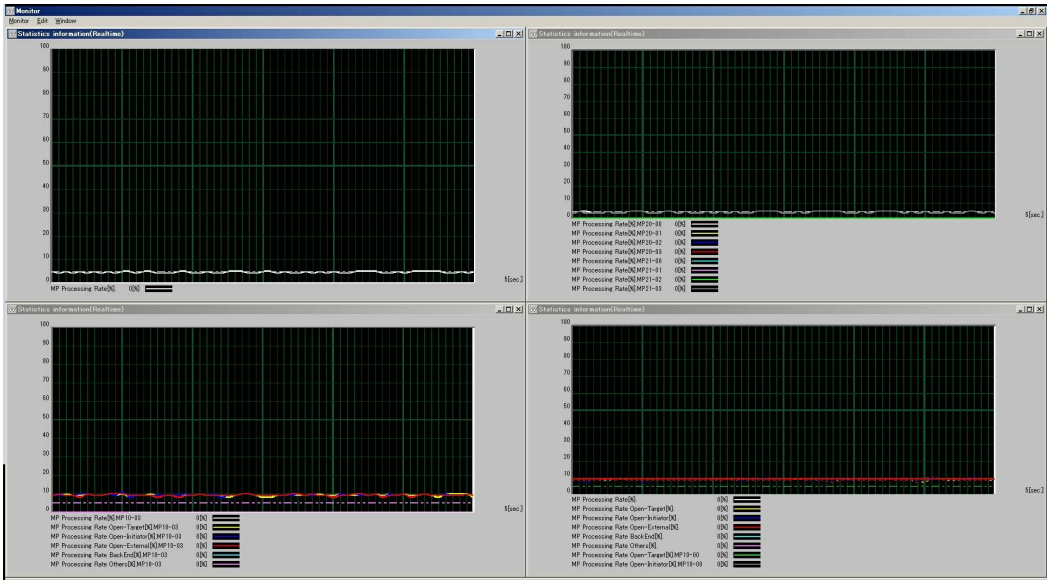
- Adding on, replacing, or removing cache memories.
- Adding on, replacing, or removing disk drives.
- Replacing the CTL
- Changing the system configuration.
- Update Firmware.
- Formatting LDEVs (including Quick Format).
- PS OFF/ON

Copyright © 2015, 2017, Hitachi, Ltd.

7. Align the displayed windows
   You can align the windows from the [Window] menu.
   To cascade the windows, select [Window]-[Cascade].
   To tile them, select [Window]-[Tile].
   To arrange the minimized windows, select [Window]-[Icon].
   To close all windows, select [Window]-[All Close].



   A list of available windows is displayed under the menu. You can select one window to display it in the foreground.



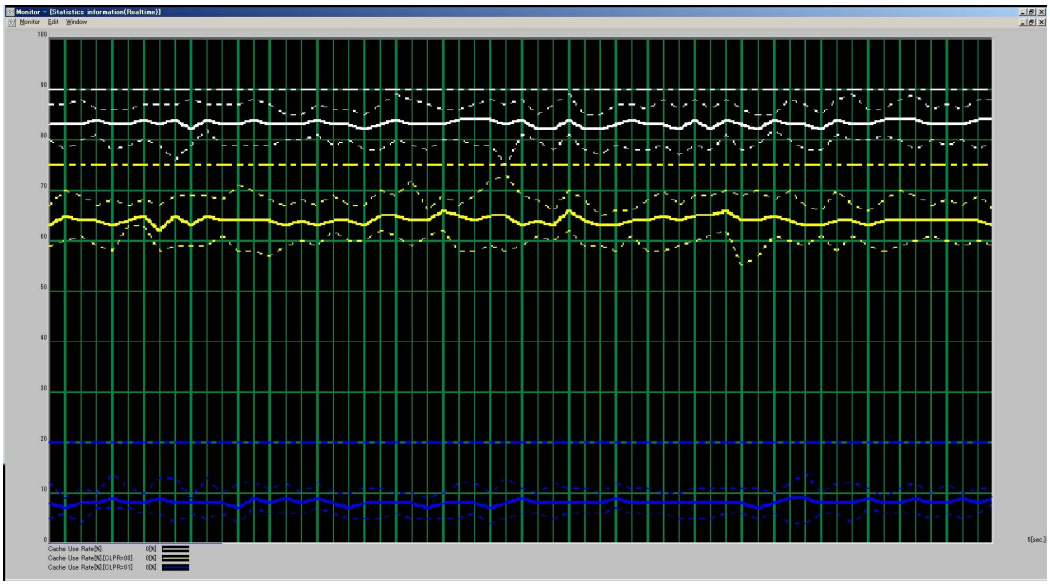
8. Exit the Monitor window
   Select [Monitor]-[Exit] from the menu.

Copyright © 2015, 2017, Hitachi, Ltd.

9. Change the contents displayed in the Statistics information window

(1) Display the “Select Monitor Item” panel

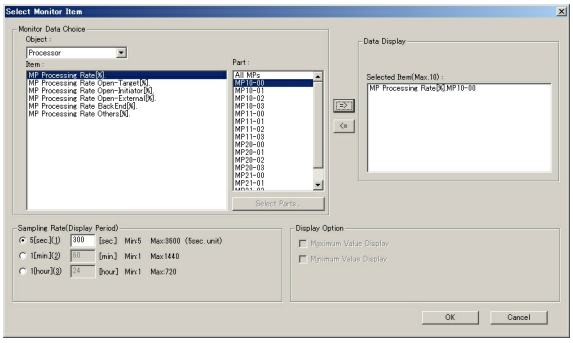
From the menu in the “Monitor” window, select [Edit]-[Item Add/Delete...].



(2) Change display items

To add display items, select the category of data you want to display in [Object] in “Monitor Data Choice”. Available data will appear in [Item]. Select the data you want to display. The parts relevant to the selected items will be displayed in [Part]. Choose the desirable part. After selecting [Object], [Item], and [Part], select [=>] button to add the selected items to [Selected Item].

To delete display items, select the items you want to delete from [Selected Item]. After selecting the items you want to delete, click the [<=] button to delete the selected items from [Selected Item].



NOTE: You can select up to ten types of data to be displayed.

Copyright © 2015, 2017, Hitachi, Ltd.

(3) Change the display interval and period
In “Sampling Rate(Display Period)”, specify the time interval of updating data and the period that data is displayed.

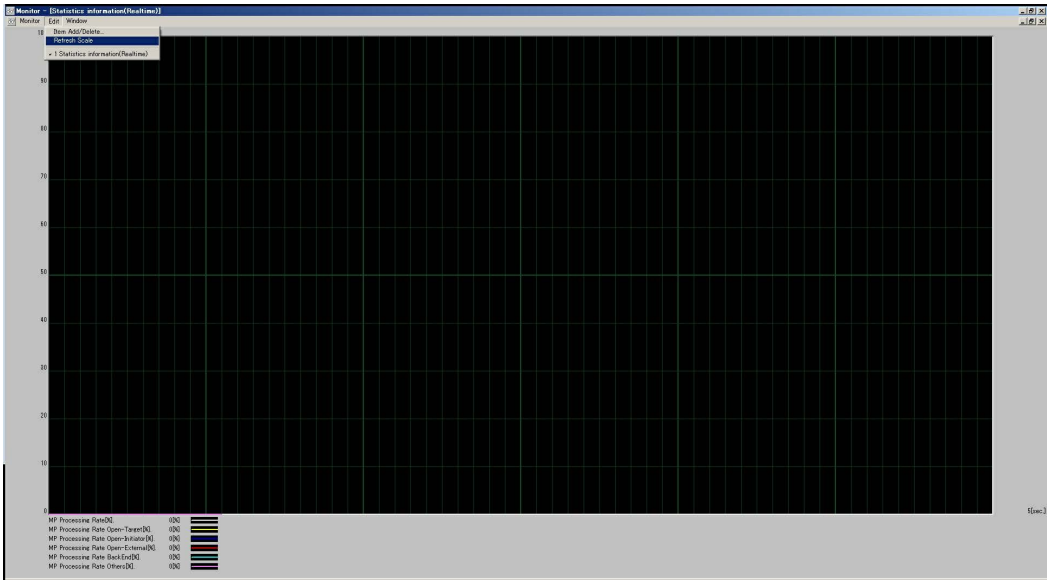
(4) Change the display option
When you select “1[min.]” or “1[hour]” in “Display Period”, you can choose either to display or not to display the maximum/minimum value within the time interval.

After selecting all the necessary items, click the [Close] button to close the “Select Monitor Item” panel.

---

10. Scale refresh method of the data display screen

(1) Scale refresh
Select the [Monitor]-[Edit]-[Refresh Scale] from the menu.



NOTE: You cannot appoint the scale size. It is changed to the most suitable scale by performing scale refresh.

Copyright © 2015, 2017, Hitachi, Ltd.

9. 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	Operation Procedure
Dump file name Conversion Tool OnlineDumpTool	Operate it in accordance with "9.2.3 Operating procedure of Dump file name Conversion Tool".

9.1 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.

9.1.1 Installation

[1] Pre-check

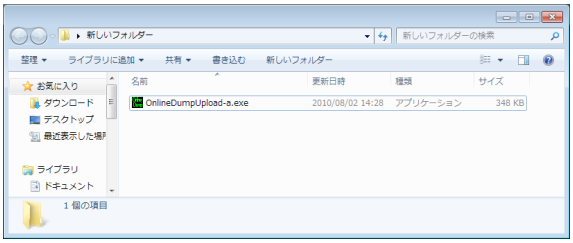
Please check if a PC to be installed can access to Internet using a browser, Internet Explorer®.

[2] Installation of tool

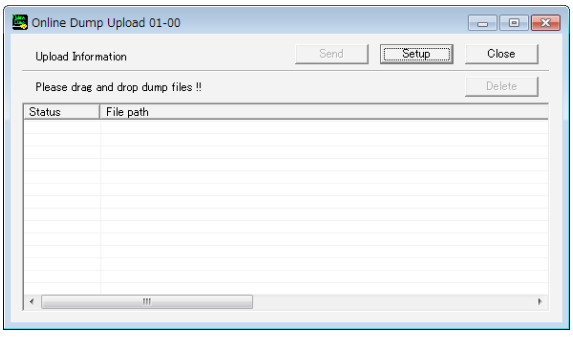
Please create a folder where you wish in your PC to be installed, and copy the following file:
OnlineDumpUpload-a.exe
"-a" stands for a version of the tool (a to z)

[3] Settings

1. Double-click "OnlineDumpUpload-a.exe".



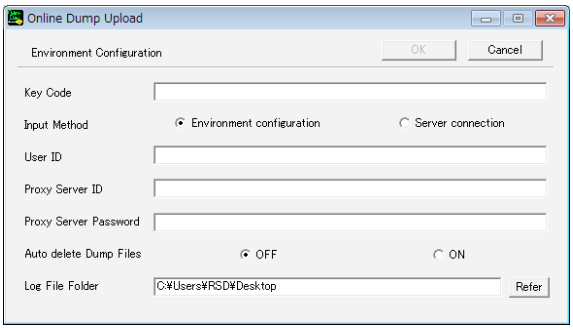
2. The "Upload Information" window is displayed, and then click the [Setup] button.



Copyright © 2015, 2017, Hitachi, Ltd.

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).

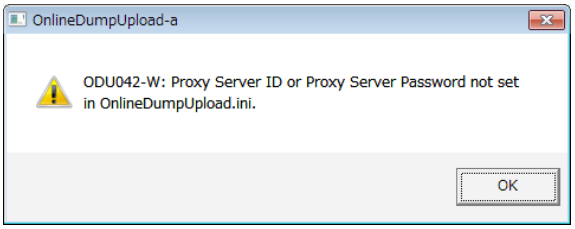
Copyright © 2015, 2017, Hitachi, Ltd.

(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			
				Input Method setting			
				Environment configuration		Server connection	
	Proxy Server Exist/ None Exist	Proxy Server password Exist/ None Exist	How to check	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: - your network environment is not Case 1; and - window [a] is displayed, when setting Proxy Server ID & Password as blank and selecting [OK] in the Step (4).	No setting necessary	No setting necessary		
Case 3	None Exist	None Exist	If: - your network environment is not Case 1; and - window “a” is not displayed, when setting Proxy Server ID & Password as blank and selecting [OK] in the Step (4).	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

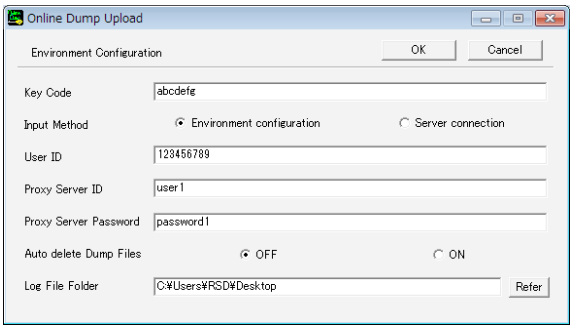
A location of a folder in which history files are stored is specified here.

Copyright © 2015, 2017, Hitachi, Ltd.

The default value is the same folder as the tool is stored.
A folder can be selected by selecting [Refer].

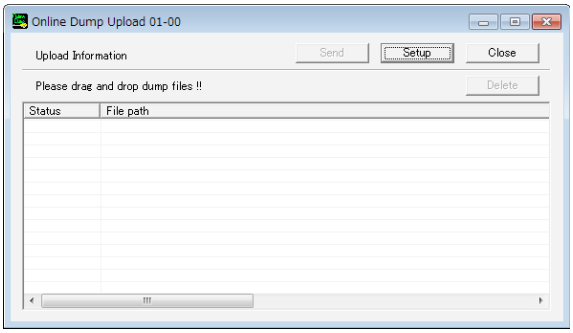
4.

Click the [OK] button in the “Environment Configuration” window.



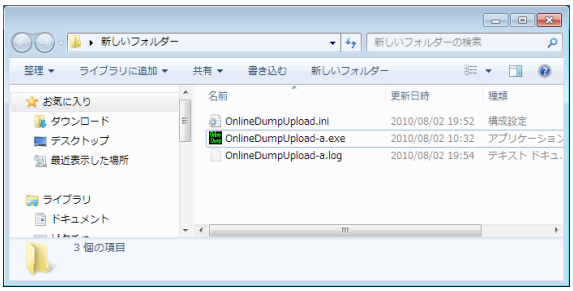
5.

Click the [Close] button in the “Upload Information” window.



6.

The following files are created in the same folder as OnlineDumpUpload-a.exe is stored:
OnlineDumpUpload.ini
OnlineDumpUpload-a.log (property: hidden file)



Copyright © 2015, 2017, Hitachi, Ltd.

9.1.2 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)

Copyright © 2015, 2017, Hitachi, Ltd.

9.1.3 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).

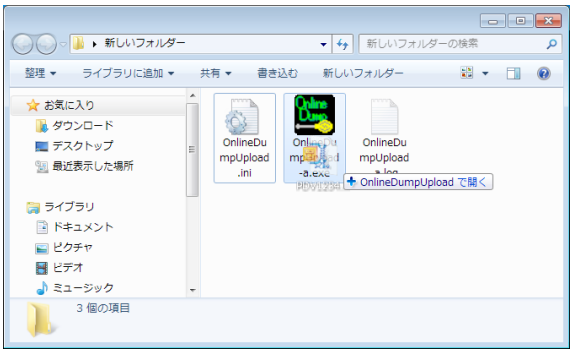
Execute uploading by running OnlineDumpTool.	
Feature	Uploading all dump files at once after confirming the file names.
Procedure	From 2-(1) to 2-(6).

1. The procedure for uploading dump files onto the OnlineDumpTool by dragging and dropping.

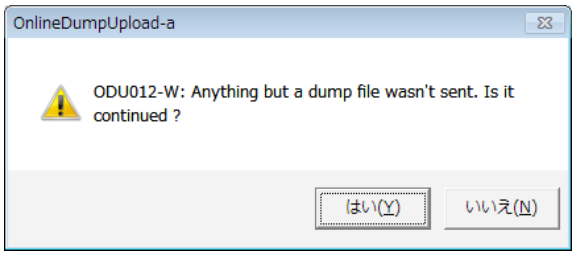
---

(1)

Drag and drop a dump file you wish to upload onto the OnlineDumpUpload-a.exe icon.



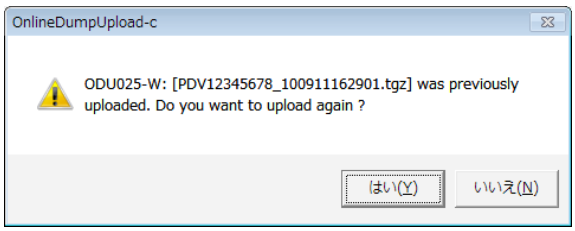
NOTE:
- Multiple files can be uploaded at a time.
- Any files except for a dump file cannot be uploaded.
  If you select other files, the following window is displayed.



[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.

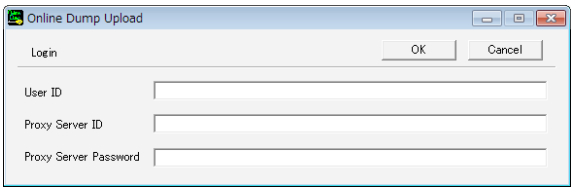


[Yes]: Uploading is executed.

[No]: Uploading is canceled.

(2)

When selecting the “Server connection” in the field of “Input Method” in the setting of MPC09-20 Step (2), the following “Login” window is displayed.
(The window is not displayed when the “Environment configuration” is selected. Go to Step (3).)

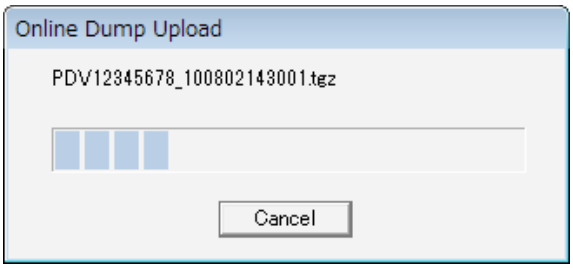


Input “User ID”, “Proxy Server ID”, “Proxy Server Password”, and click the [OK] button.
Refer to MPC09-30 Step (4) for the input value of “Proxy Server ID” and “Proxy Server Password”.

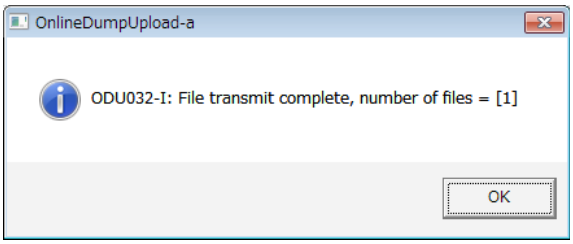
Copyright © 2015, 2017, Hitachi, Ltd.

(3)

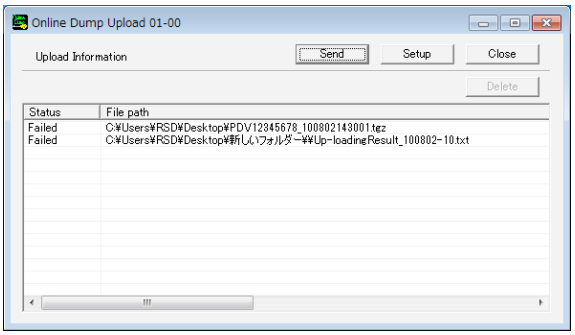
Start uploading
During uploading, the following window is displayed.



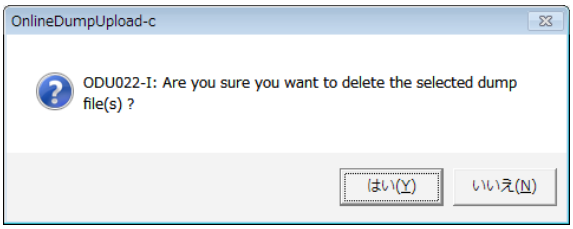
When all selected files are uploaded, the following window is displayed.
Click the [OK] button.



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 MPC09-30 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.

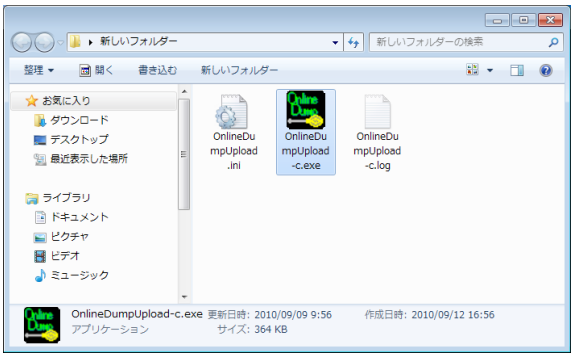


*1: The deleted file is sent to the recycle bin.

2. The procedure for uploading dump files by running the OnlineDumpTool.

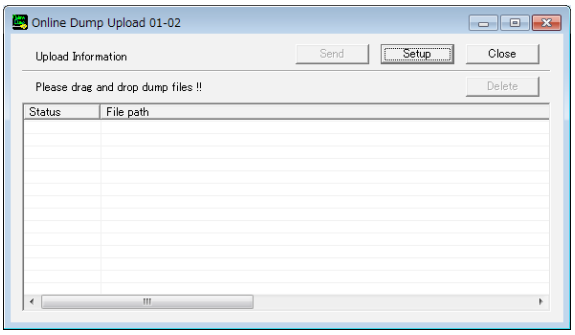
(1)

Double-click the OnlinedumpUpload-a.exe icon.



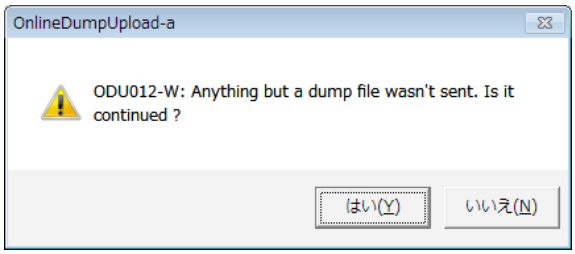
(2)

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.

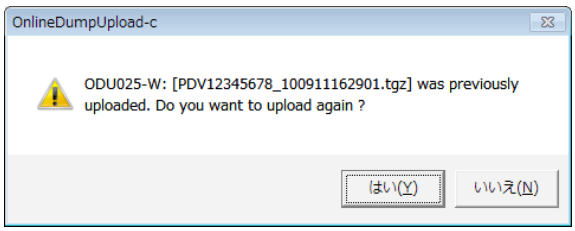


[Yes]: Execute uploading except for the file which was not sent, if multiple files are selected.

[No]: Stop uploading.

Copyright © 2015, 2017, Hitachi, Ltd.

- When the uploading has completed, the reconfirmation message is displayed.



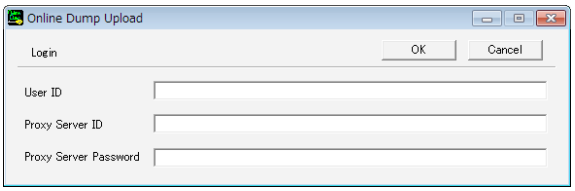
[Yes]: Uploading is executed.

[No]: Uploading is canceled.

---

(3)

When selecting the “Server connection” in the field of “Input Method” in the setting of MPC09-20 Step (2), the following “Login” window is displayed.
(The window is not displayed when the “Environment configuration” is selected. Go to Step (4).)

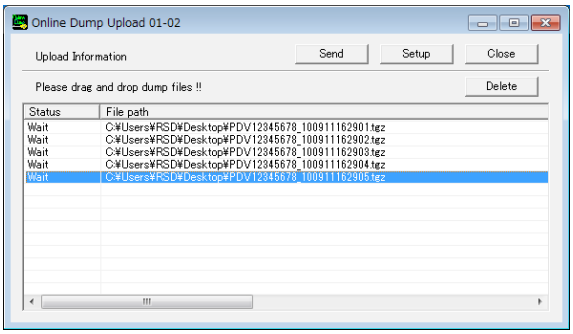


Input “User ID”, “Proxy Server ID”, “Proxy Server Password”, and click the [OK] button.
Refer to MPC09-30 Step (4) for the input value of “Proxy Server ID” and “Proxy Server Password”.

---

(4)

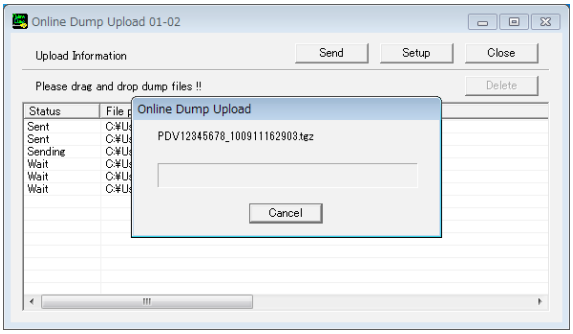
Click the [Send] button to start uploading.



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)

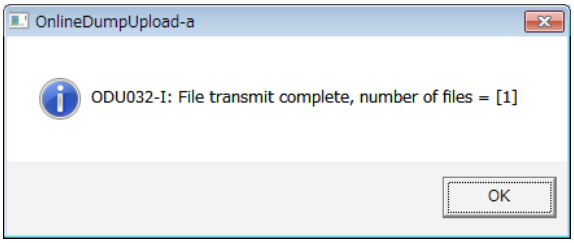
The uploading window is displayed.
The uploading status is displayed in the Status field during uploading.



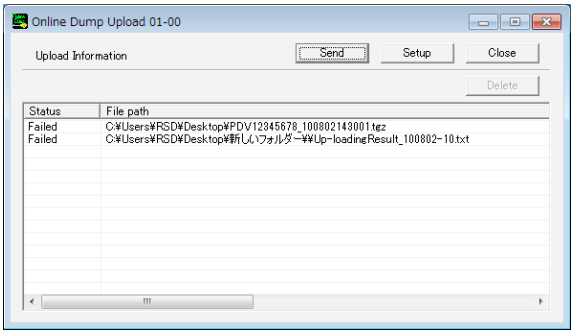
Connecting: In the connecting process to the server.
Sending: Uploading.
Sent: Uploaded. (completed)
Wait: Waiting to start uploading.
Failed: The uploading has failed.
Cancel: The uploading has canceled.

(6)

When all selected files are uploaded, the following window is displayed.
Click the [OK] button.

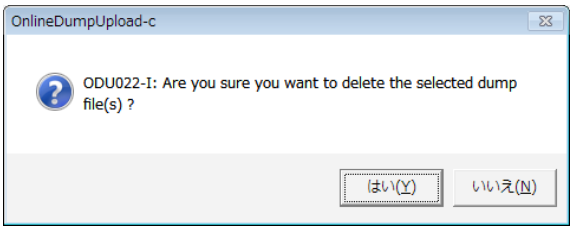


If there is/are file(s) failed to upload in selected files, the following window is displayed.
If you wish to retry uploading, click the [Send] button.
If you wish to exit without retry, click the [Close] button.



Copyright © 2015, 2017, Hitachi, Ltd.

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.

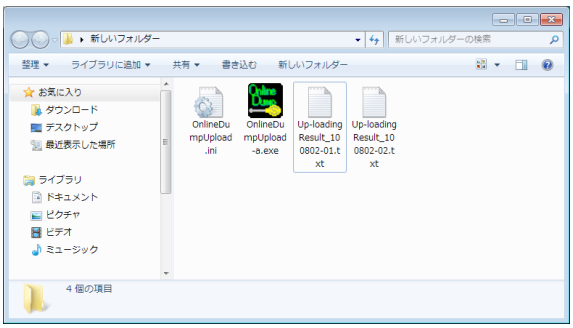


*1: The deleted file is sent to the recycle bin.

Copyright © 2015, 2017, Hitachi, Ltd.

9.1.4 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 MPC09-10 [3] Settings.
A history file is created every transmission.



Copyright © 2015, 2017, Hitachi, Ltd.

9.1.5 Message Table

The messages that are displayed on OnlineDumpTool are described below Table 9-1.

Table 9-1 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" massage 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)

Copyright © 2015, 2017, Hitachi, Ltd.

(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”; • 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 then 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)

Copyright © 2015, 2017, Hitachi, Ltd.

(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.

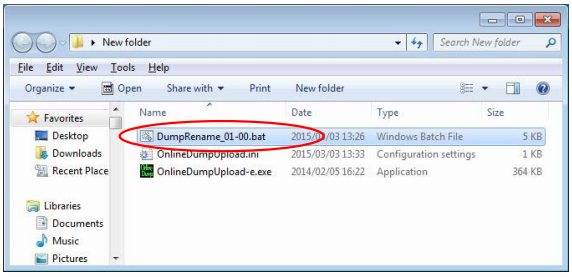
Copyright © 2015, 2017, Hitachi, Ltd.

9.2 Dump file name Conversion Tool

9.2.1 Installation of Dump file name Conversion Tool

Dump file name Conversion Tool is installed in a service PC.
Install Online Dump Tool in the service PC in advance.

1. Open the Windows explorer of the service PC and copy Dump file name Conversion Tool (DumpRename_xx-xx.bat) to the same folder as Online Dump Tool. (Refer to “9.1.1 Installation”)
(“xx-xx” stands for a revision of the tool (any value))



2. If you have changed dump storage folder of maintenance PC from default value (C:\Mapp), change the settings of DumpRename_xx-xx.bat file in the procedures of (1) to (5).

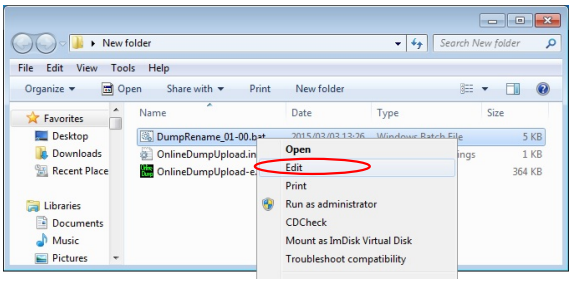
   The collected dump files are stored in the following folder of maintenance PC.
   C:\Mapp\wk\83xxxxyyyyyy\dkc200\tmp\

   C:\Mapp : This is the installation folder of maintenance PC program.
   If you have changed the settings at the time of maintenance PC program installation, please change them in this procedure.

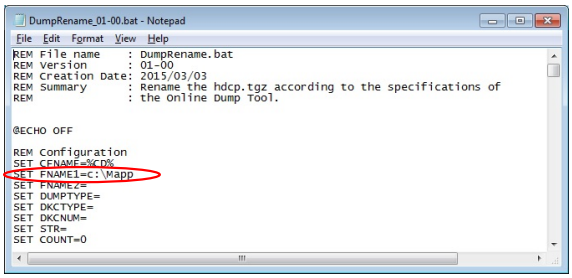
   wk\83xxxxyyyyyy\dkc200\tmp : This value is fixed at each DKC.
   (xxxxyyyyyy : Model name of DKC and serial number)

   In case of the default value (C:\Mapp), the installation is completed by storing the DumpRename_xx-xx.bat file.

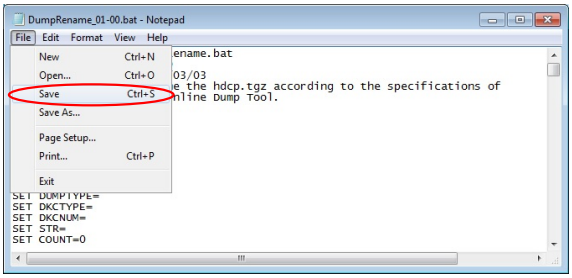
(1) Right-click on the DumpRename_xx-xx.bat file, and crick [Edit] in the pull down menu.



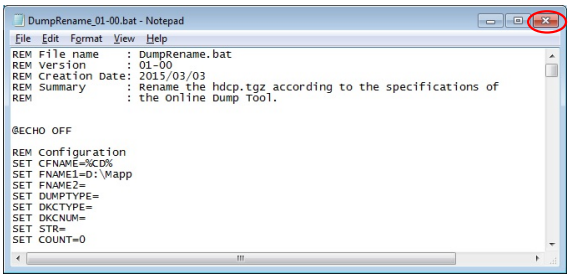
(2) Rename the value of SET FNAME1= in the DumpRename_xx-xx.bat file from the default value to the change destination folder.



(3) Crick the [File]-[Save] on the menu bar.



(4) Close the window.



(5) Close the Windows Explorer.

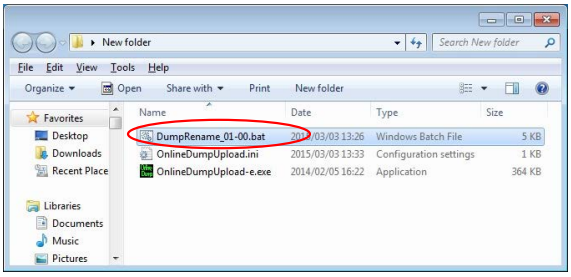
Copyright © 2015, 2017, Hitachi, Ltd.

9.2.2 Uninstallation of Dump file name Conversion Tool

1. Open Windows Explorer, and delete DumpRename_xx-xx.bat file.
   ("xx-xx" stands for a revision of the tool (any value)) (Refer to "9.2.1 Installation of Dump file name Conversion Tool" for the storage place)

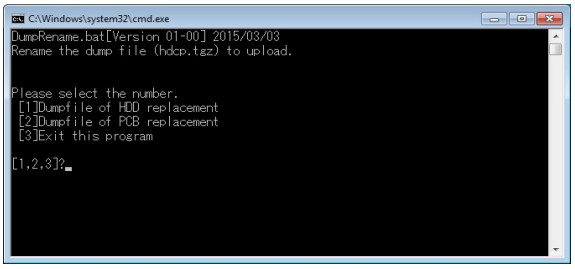
9.2.3 Operating procedure of Dump file name Conversion Tool

1. Open Windows explorer, and double crick DumpRename_xx-xx.bat.
   ("xx-xx" stands for a revision of the tool (any value))

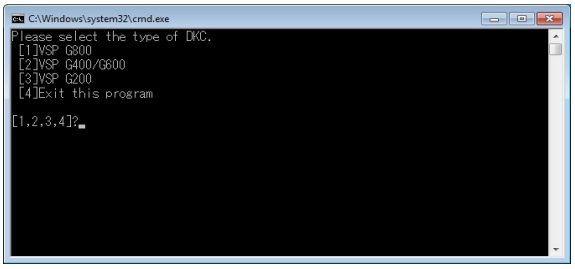


2. Select the type of dump that you have collected.
   - In the case of dump that was collected at the time of HDD of maintenance parts replacement: Press the [1] key
   - In the case of dump that was collected at the time of PCB of maintenance parts replacement: Press the [2] key

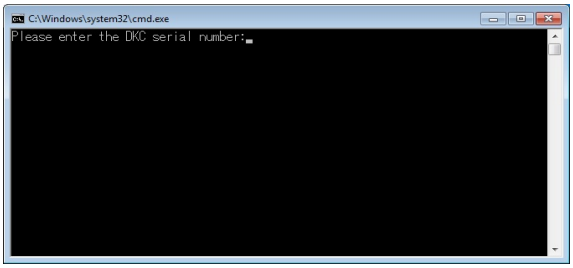
   Pressing the [Enter] key after select dump type.



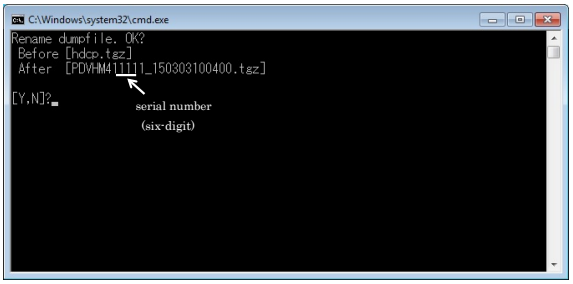
3. Select a controller (DKC) of model collected a dump, and press the [Enter] key.
   Correspondence of the Model and the Model name, please see to the OPTION & FIRMWARE VERSION SECTION "1. Relationship between Option and Firmware Version".



4. Enter the serial number (6-digit fixation) of controller (DKC) on which a dump was collected, and press the [Enter] key.



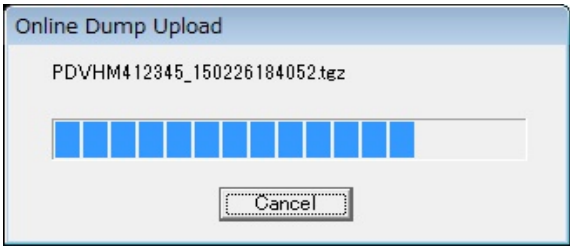
5. File name after conversion is displayed. If serial number is correct, pressing the [Y] key.
   - In the case of dump that was collected at the time of HDD of maintenance parts replacement (If pressing [1] key at Step 2.)



   - In the case of dump that was collected at the HDD of maintenance parts replacement (If pressing [2] key at Step 2.)

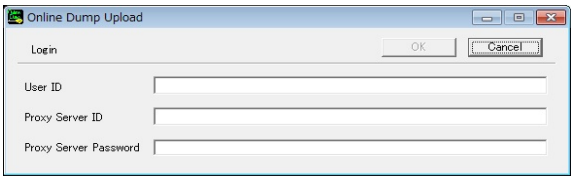


6. OnlineDumpTool is automatically started.
   (1) If you have selected “Environment configuration” in “Input Method” (MPC09-20 Step (2)) settings of OnlineDumpTool:
   Start upload.



Copyright © 2015, 2017, Hitachi, Ltd.

(2) If you have selected “Server connection” in ”Input Method” (MPC09-20 Step (2)) settings of OnlineDumpTool:
“Login” window is displayed.
Enter “User ID”, ”Proxy Server ID”, ”Proxy Server Password”, and click the [OK] button, and then start upload.
Refer to the paragraph MPC09-30 Step (4) for the input value of “Proxy Server ID”, ”Proxy Server Password”



(3) When the file name of the dump file to be uploaded is the same as the name of the dump file uploaded before, the reconfirmation message is displayed.
Select the [Yes] button, and then start upload.

---

7. “9.1.3 Upload Procedure” Step (3) (MPC09-80).

NOTE: When Online Dump Tool is not installed in the same folder as Dump file name Conversion Tool, the dump file name is only replaced but the dump file is not uploaded.

Copyright © 2015, 2017, Hitachi, Ltd.

10. 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 TROUBLESHOOTING SECTION "3.29.2 About Other MPC Troubles" for recovery when you have deleted a folder (and a file) of the software of the Storage System by mistake.

NOTICE:	Before uninstalling software from the Maintenance PC, close the Event Viewer of Windows.

10.1 OSS Uninstallation

Table 10-1 OSS Uninstallation

Item	Uninstallation work
JRE	Uninstall the software. Follow the procedure of "10.2 Maintenance PC Software Uninstallation". Individual uninstallation is not required.
Perl	
Apache	
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.)

Copyright © 2015, 2017, Hitachi, Ltd.

10.2 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.

⚠ CAUTION

When the firmware in which you installed for the first time is less than 83-01-25-x0/xx, or 83-02-01-x0/xx or later and less than 83-02-03-x0/xx, other Hitachi software might not operate normally if the storage management software is removed. In this case, update the storage management software to 83-03-21-x0/xx or later, and then remove the storage management software.

NOTICE: Gather Dumps of the system information before uninstallation.
Before removal, perform "12.4 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 the MPC Software that has been installed with the MPC Software version less than 83-04-00-xx/00 is deleted, the folder for Command Control Interface (CCI) contained in the drive with the same drive letter as assigned to the drive for the MPC Software is removed.
  If a file such as a user script exists in the folder for CCI (HORC folder), move the file into a different folder before deleting the MPC Software.
  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.

When the firmware version is less than 83-01-21-x0/xx, perform the procedure from Step 1.
Start from Step 3 when the Firmware version is 83-01-21-x0/xx or more.

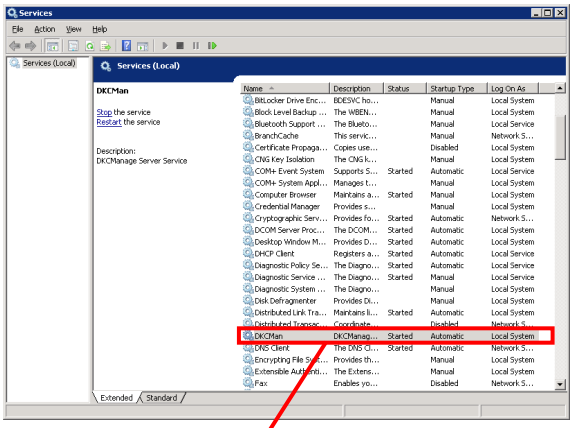
1. Stop the Storage system
   Stop the Storage System by the device list, and then update the Maintenance PC. Refer to "1.6.4 Stopping/Starting the Service of Storage System" for detail.

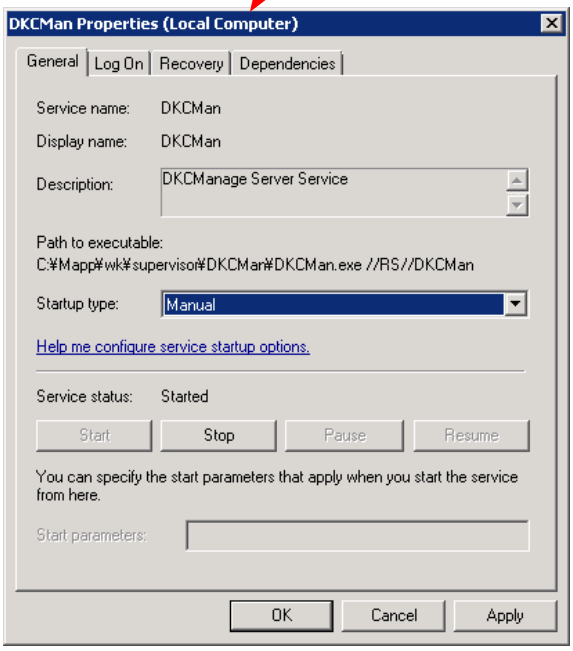
Copyright © 2015, 2017, Hitachi, Ltd.

2. Stop service processes of Storage Navigator
   Stop service processes of Storage Navigator, and then update the Maintenance PC.

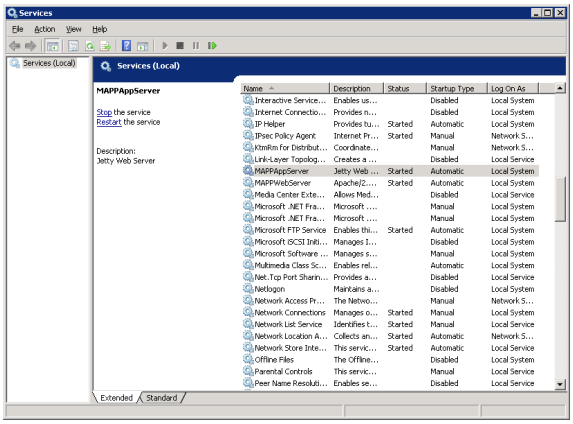
   (1) Select [control panel]-[Administrative Tools]-[services] from Windows start menue.

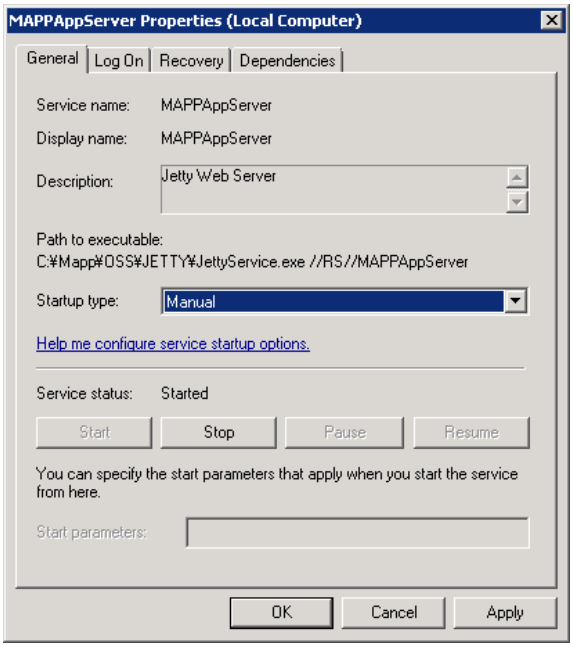
   (2) Display the property of DKCMan service, and then make the Startup type manual.

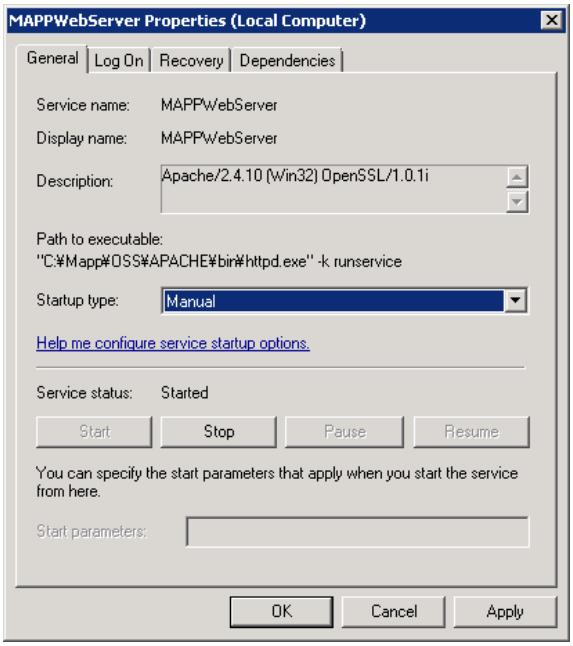




(3) Set it about the MAPPAppServer and MAPPWebServer equally.



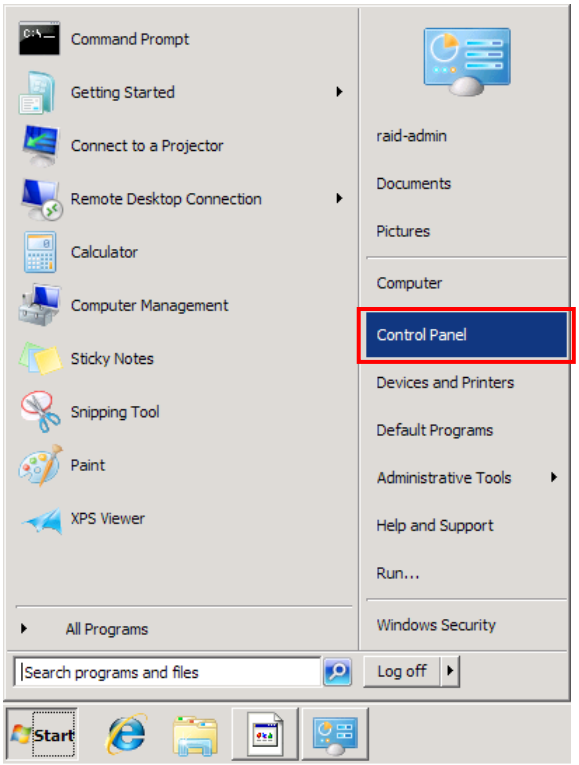




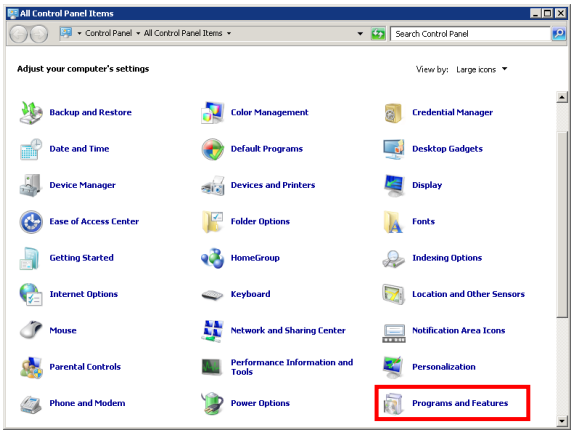
(4) Reboot the maintenance PC, you complete to change the setting of the service.

Copyright © 2015, 2017, Hitachi, Ltd.

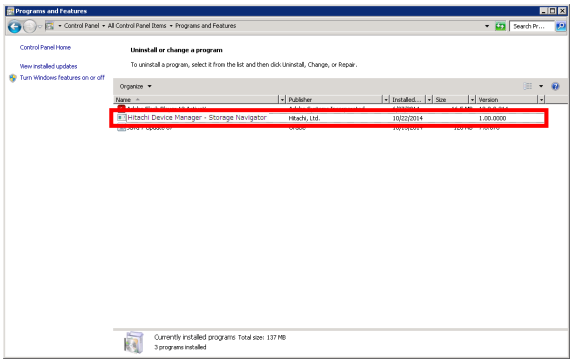
3. Select [Start] - [Control Panel].



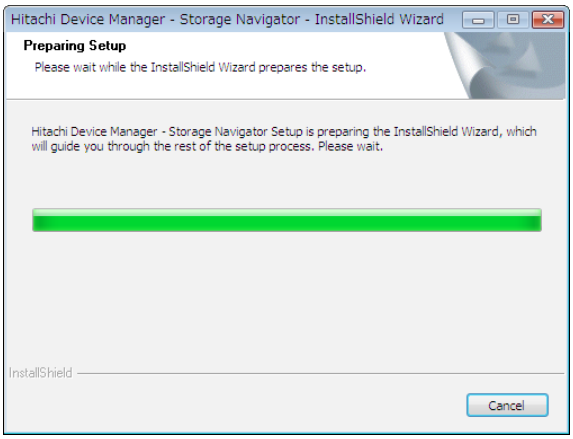
4. Click [Programs and Features].



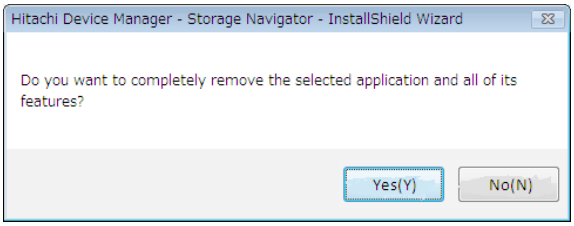
5. Select [Hitachi Device Manager - Storage Navigator] and click [Uninstall].
   If the UAC control window of Windows is displayed when executing the uninstallation, click the [Continue] button.
   When [Hitachi Device Manager - Storage Navigator] is not on the list, go to Step 10.



6. 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.



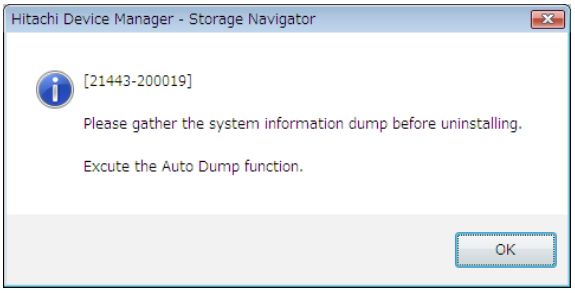
7. Checking the deletion
   The window for checking whether to delete the MPC Software completely is displayed.
   Click the [Yes] button.



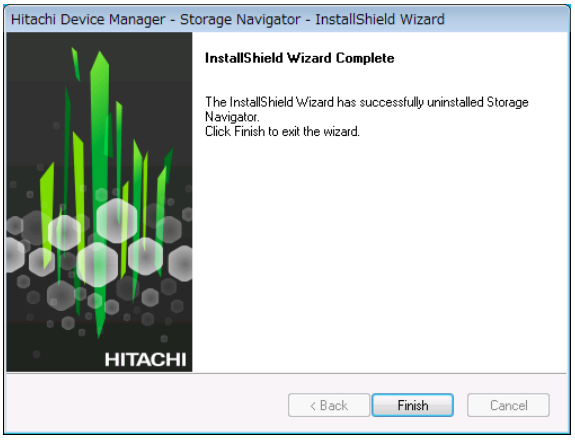
Copyright © 2015, 2017, Hitachi, Ltd.

8. 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.



9. Completion message
   The uninstallation completion message is displayed.
   Click the [Finish] button to close the window.



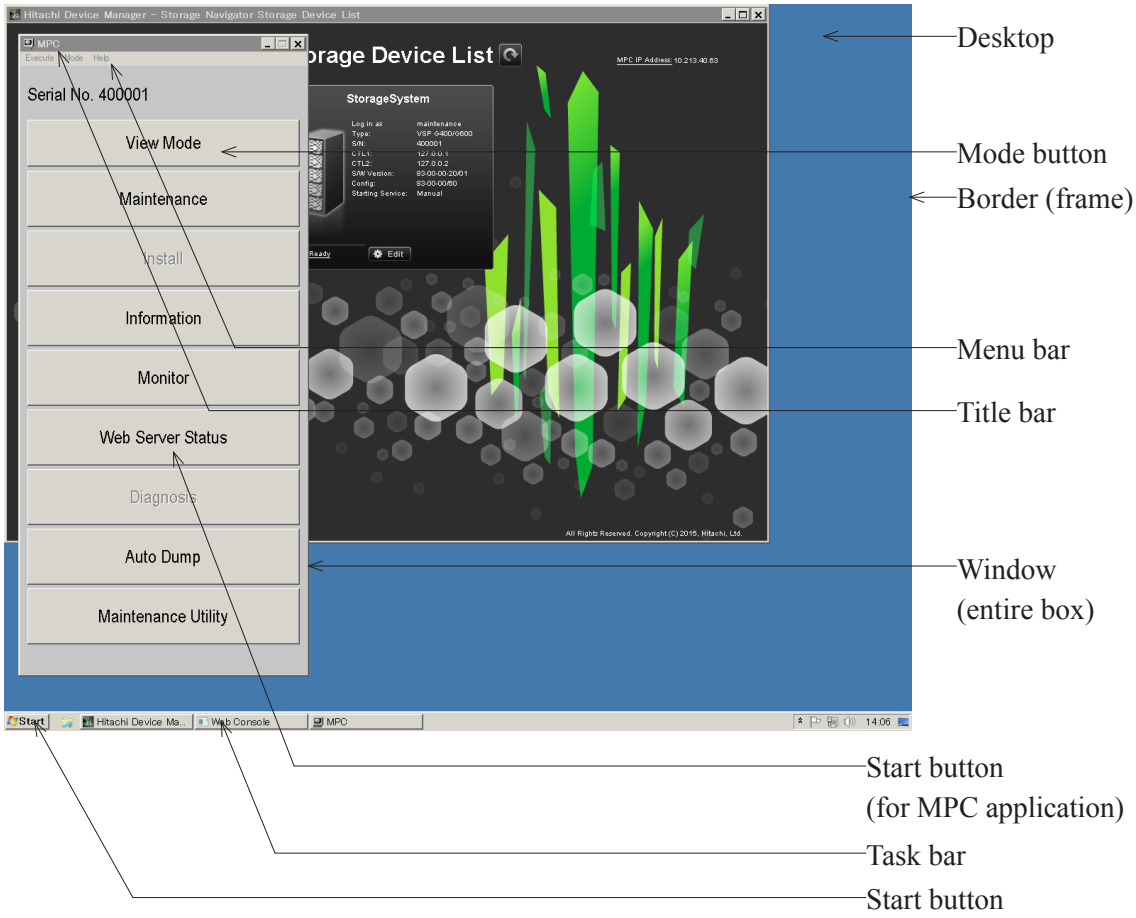
10. Checking the uninstallation result
    Check that [Hitachi Device Manager - Storage Navigator] is deleted from [Programs and Functions].
    Click the [X] button to close this window.

Copyright © 2015, 2017, Hitachi, Ltd.

11. Description of Windows

11.1 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.

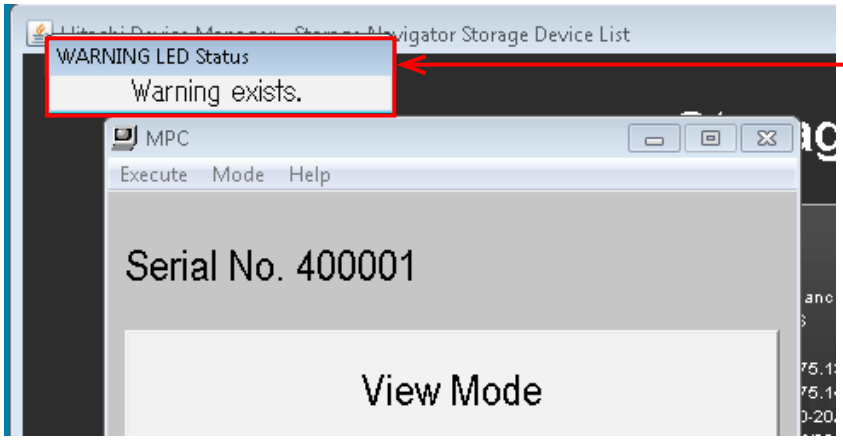
“WARNING LED Status”

Copyright © 2015, 2017, Hitachi, Ltd.

11.2 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 11-1 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



“WARNING LED Status” Window

Table 11-1 WARNING LED state and display message

WARNING LED	Display message
Lighting	Warning exists.
Blinking	Unconfirmed SIM exists.

Copyright © 2015, 2017, Hitachi, Ltd.

11.3 Maintenance Window

11.3.1 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.

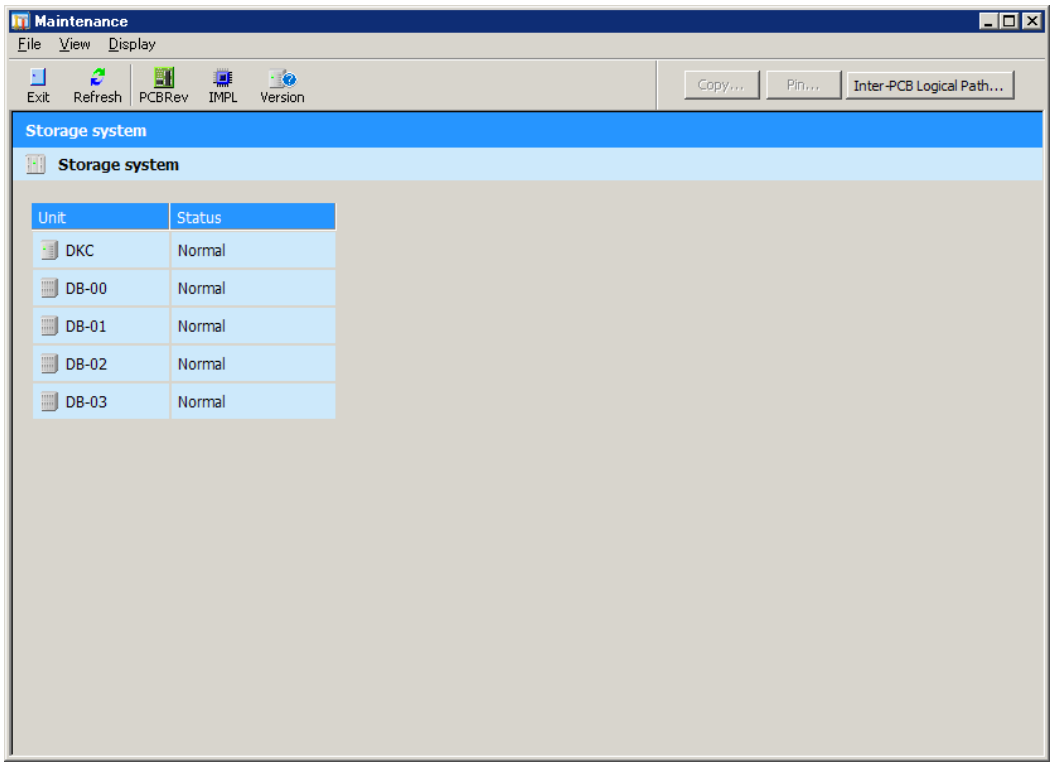


Table 11-2 Overview of Each Part in the Main Window

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.

Copyright © 2015, 2017, Hitachi, Ltd.

11.3.2 Operation Menu

This menu displays the operation in the “Maintenance” window. Menu items are also placed in the tool bar.

Table 11-3 Menu/Tool Bar

Menu	Sub Menu	Description	Tool bar
File	Exit	The Maintenance window is finished.	
View	Toolbar	Displays/does not display the tool bar.	—
	Refresh	Updates information being displayed.	
Display	PCB Revision...	Displays the “PCB Revision Display”.	
	IMPL Status...	Displays the “IMPL Status”.	
	Version...	Displays the “Version”.	

Copyright © 2015, 2017, Hitachi, Ltd.

11.3.3 Dialog Bar

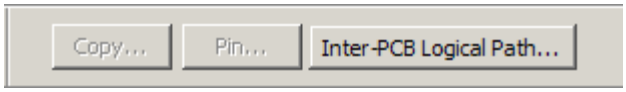


Table 11-4 Dialog Bar

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"(MPC05-1010).
Pin...	Pin information Blinking of the button : Pin information is present. Extinction of the button : No Pin information is present.	Displays "Pinned Track"(MPC05-1140).
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"(MPC05-1180).

Copyright © 2015, 2017, Hitachi, Ltd.

11.3.4 Information Display View

Display whether parts are installed/uninstalled, normal/abnormal and select/execute a maintenance target.

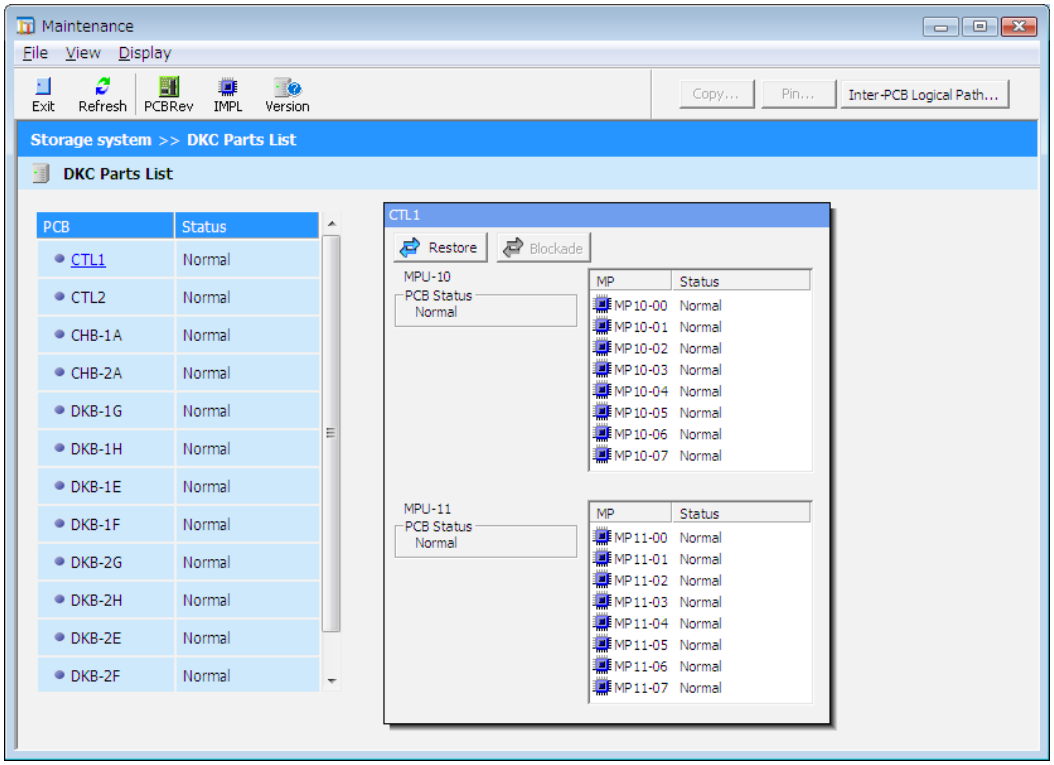


Table 11-5 Information Display View

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.

11.3.4.1 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.

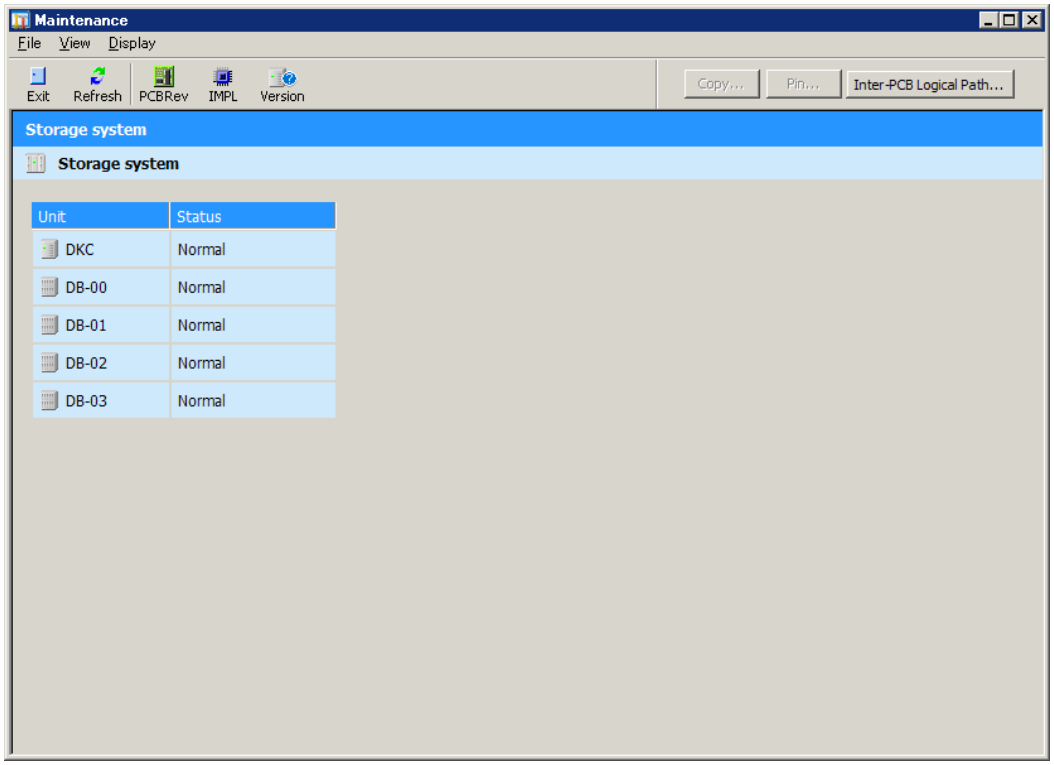


Table 11-6 Storage System Information View

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)

Copyright © 2015, 2017, Hitachi, Ltd.

11.3.4.2 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.

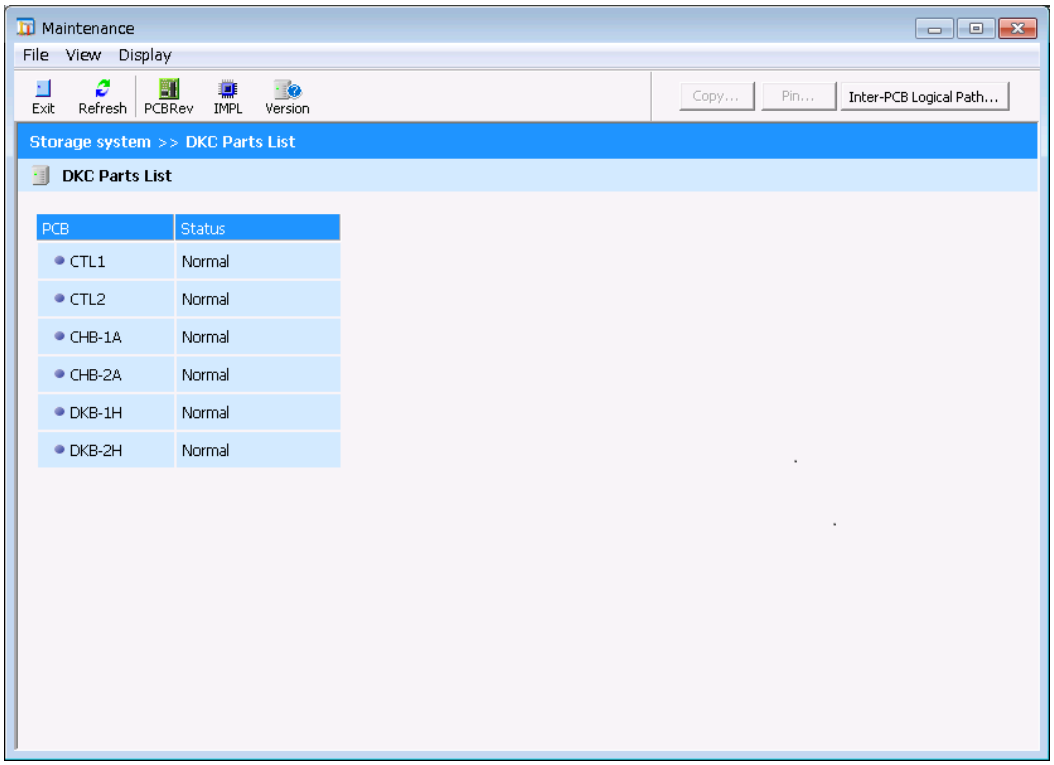


Table 11-7 DKC Information View

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.

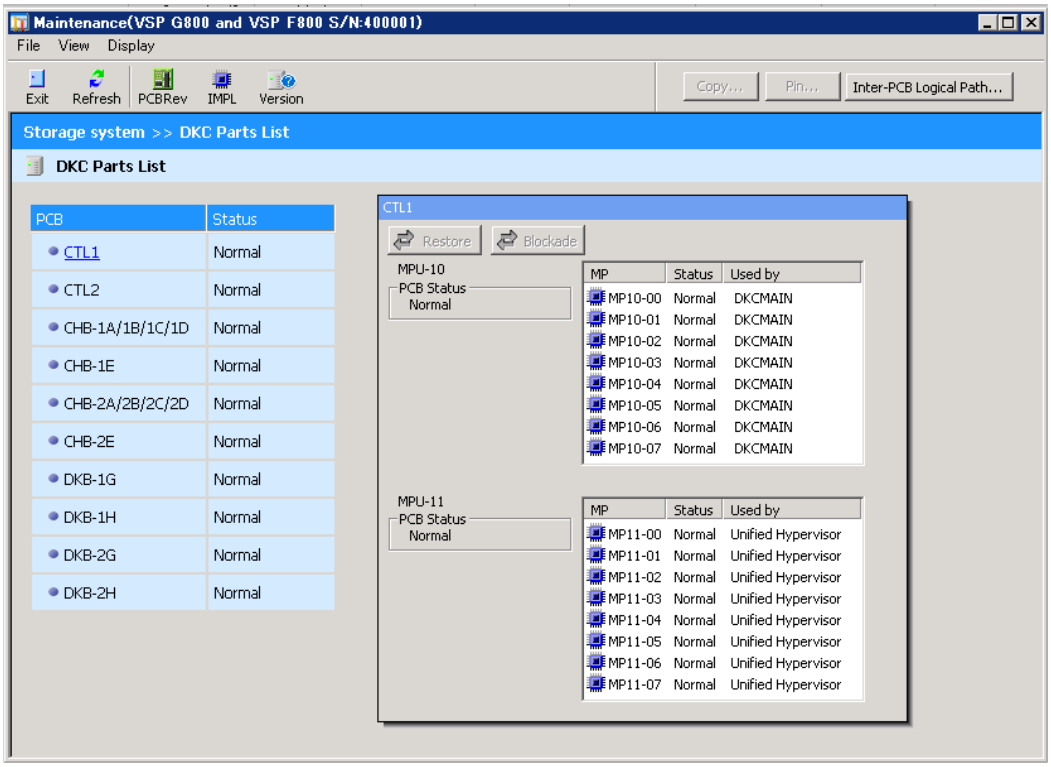
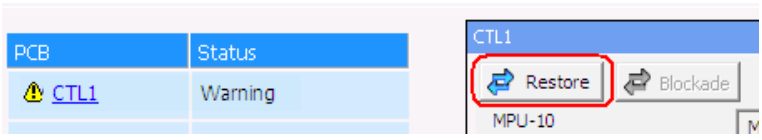


Table 11-8 CTL View

Item	Description
Title	Display a CTL location.
Maintenance button	Execute maintenance processing. [Restore] : Execute a parts restore. (See "5.13.7 Failed CTL Recovery".) Enable to operate when a CTL failure occurs. 
PCB status	Display a PCB status. Normal : Normal Failed : Abnormal Blocked : Maintenance is blocked/to be blocked Warning : Mixed status
MPU location name	Display an MP location.
MP list	Display an MP status. Normal : Normal Failed : Abnormal Blocked : Maintenance is blocked/to be blocked

(2) CHB/DKB view

Display a CHB/DKB status and execute the maintenance operation.

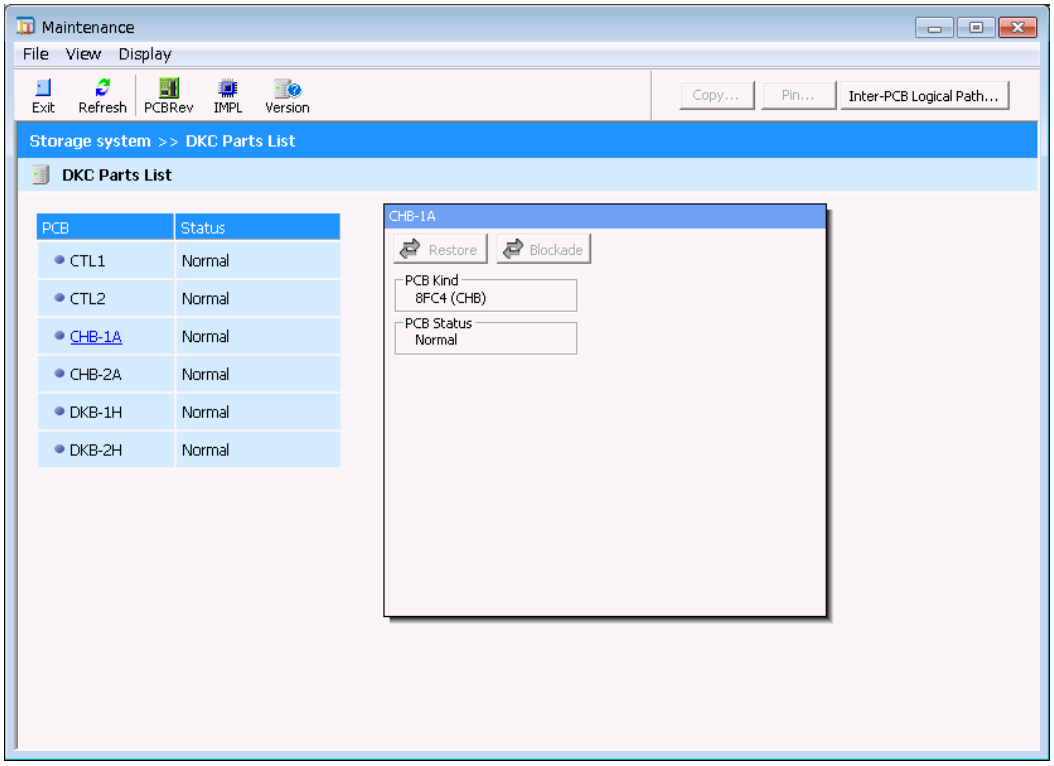


Table 11-9 CHB/DKB View

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

Copyright © 2015, 2017, Hitachi, Ltd.

11.3.4.3 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.

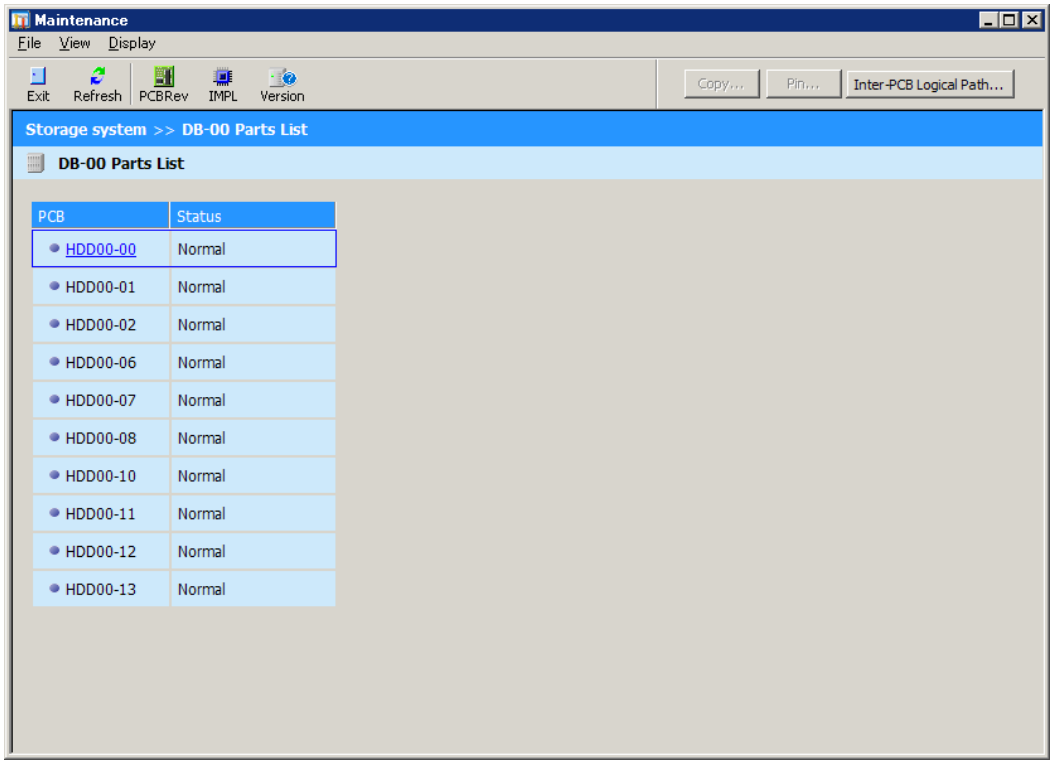


Table 11-10 HDD Information View

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.

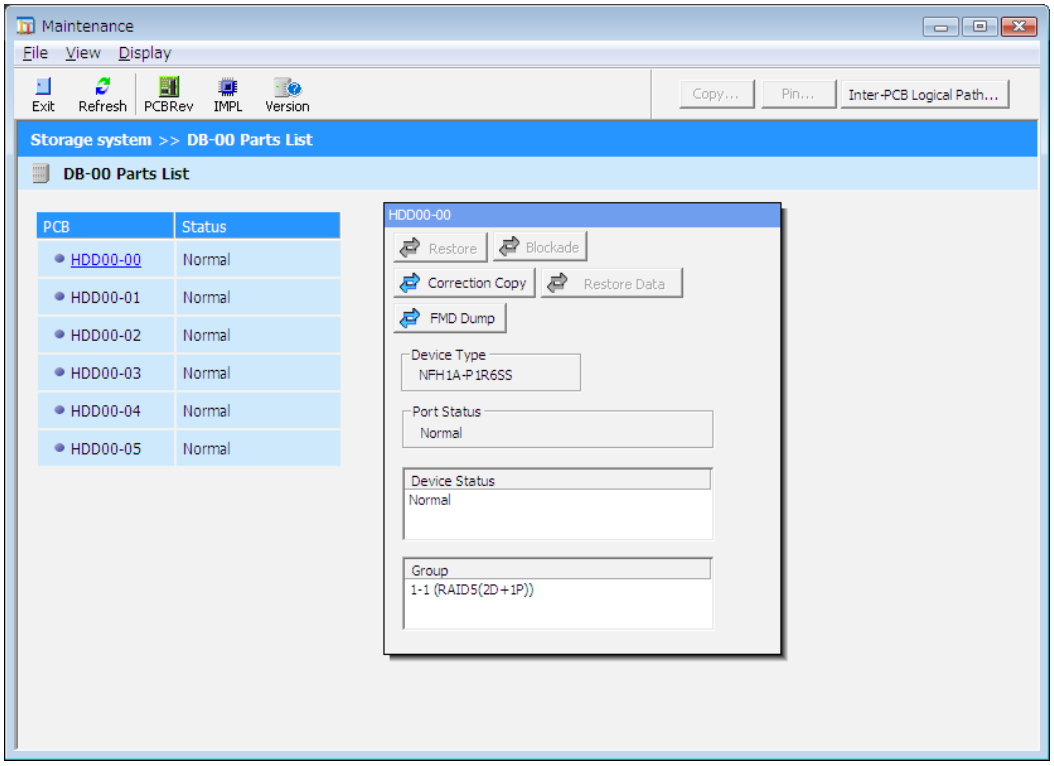


Table 11-11 HDD Information View

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 Drvie” ③ In case of Free Drives “Free Drive”

Copyright © 2015, 2017, Hitachi, Ltd.

*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”

Copyright © 2015, 2017, Hitachi, Ltd.

11.3.4.4 Dialog

A dialog displayed by the maintenance operation is configured as shown below.

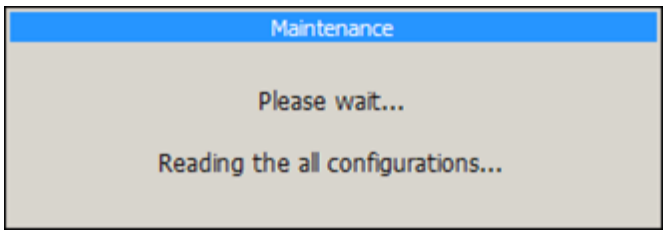


Table 11-12 List of Dialogs

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

Copyright © 2015, 2017, Hitachi, Ltd.

12. Changing/Initializing Port Numbers Used by the SVP

You can change the port numbers used by the SVP to arbitrary port numbers.
Furthermore, you can reset the port numbers to the initial setting status by initializing them.

To confirm the port numbers allocated to each storage system, “See the port numbers to be used in the SVP”
Unused port numbers are automatically allocated for some port numbers of the SVP software with the version 83-03-01-xx/00 or later. (Automatic allocation)
To change the automatic allocation setting, perform the following according to the purposes.

- To change the automatically allocated port numbers, “12.3 Reallocating Automatically Allocated Port Numbers”
- To initialize the automatically allocated port numbers, “12.4 Initializing Automatically Allocated Port Numbers”
- To change the range of the port numbers to be allocated automatically, “12.5 Changing Range of Port Numbers to be Allocated Automatically”
- To initialize the range of the automatically allocated port numbers, “12.6 Initializing Range of Port Numbers to be Allocated Automatically”
- To confirm the port numbers allocated to each storage system, “12.7 See the Port Number to be Used in the SVP”

When the version is less than 83-03-01-xx/00, perform this work only if the port numbers used by other applications and the SVP are duplicated.

Copyright © 2015, 2017, Hitachi, Ltd.

12.1 Changing Port Numbers Used by the SVP

Change the port numbers used by the SVP to arbitrary port numbers. The services used by the SVP restart according to the change.

1. Terminate all Storage Navigators connected to the SVP.
2. Start the Windows command prompt by the SVP with the administrator authority.
3. Move the current directory to the directory in which the tool (MappSetPortEdit.bat) exists and execute the next command.
   C:\Mapp\wk\Supervisor\MappIniSet>MappSetPortEdit.bat △ [Service Port Number Key Name] △ [Port Number]
   A " △ " mark indicates a space.
   The values in [ ] indicates a parameter.

NOTE: The following shows changeable "Port Number Key Name" and "Initial Value of Port Number". In the Storage System with the SVP software version 83-03-01-xx/00 or later, the server program automatically allocates the port numbers of the following port number keys to each registered Storage System.

- PreRMIServer
- SMIS_CIMOM
- DeviceJettyStart
- DeviceJettyStop

Port Number Key	Protocol	Initial Value of Port Number	Applicable SVP software version
MAPPWebServer	HTTP	80	83-01-20-xx/00 or later
MAPPWebServerHttps	HTTPS	443	83-01-20-xx/00 or later
RMIClassLoader	RMI	51099	83-01-20-xx/00 or later
RMIClassLoaderHttps	RMI(SSL)	5443	83-01-20-xx/00 or later
RMIIFRegist	RMI	1099	83-01-20-xx/00 or later
PreRMIServer	RMI	51100	83-01-20-xx/00 or later
		Automatic allocation	83-03-01-xx/00 or later
DKCManPrivate	RMI	11099	83-01-24-xx/00 or later
SLP	SLP	427	83-01-24-xx/00 or later
SMIS_CIMOM	SMI-S	5989	83-01-20-xx/00 or later
		Automatic allocation	83-03-01-xx/00 or later
CommonJettyStart	HTTP	8080	83-01-24-xx/00 or later
CommonJettyStop	HTTP	8210	83-01-24-xx/00 or later
RestAPIServerStart	HTTP	9080	83-04-01-xx/00 or later
RestAPIServerStop	HTTP	9210	83-01-24-xx/00 or later
RestAPIClientStart (*1)	UDP	36000	83-04-01-xx/00 or later
RestAPIClientEnd (*1)	UDP	37000	83-04-01-xx/00 or later
DeviceJettyStart	HTTP	8081	83-01-24-xx/00 or later
		Automatic allocation	83-03-01-xx/00 or later
DeviceJettyStop	HTTP	8211	83-01-24-xx/00 or later
		Automatic allocation	83-03-01-xx/00 or later

*1: For RestAPIClientStart and RestAPIClientEnd, only port numbers required for a processing are assigned and used as needed from the specified range, 36000 to 37000.

Copyright © 2015, 2017, Hitachi, Ltd.

- 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 two or more command input parameters “[Service Port Number Key Name] △ [Port Number]”. △ : One-byte space
  (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 SVP by the procedure described in “12.7 See the Port Number to be Used in the SVP”.

4. The completion message is displayed following the service restart message.
5. The message “Press any key to continue...” is displayed. Enter an arbitrary key.
6. Close the command prompt.

Copyright © 2015, 2017, Hitachi, Ltd.

12.2 Initializing Port Numbers Used by the SVP

Reset the port numbers used by the SVP to the initial setting status. The services used by the SVP restart according to the initialization.
To initialize the automatically allocated port numbers, see “12.4 Initializing Automatically Allocated Port Numbers”.

1. Terminate all Storage Navigators connected to the SVP.
2. Start the Windows command prompt by the SVP with the administrator authority.
3. Move the current directory to the directory in which the tool exists and execute the next command.
   C:\Mapp\wk\Supervisor\MappIniSet>MappSetPortInit.bat
4. 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].
5. A completion message is displayed following a service restart message.
6. The message “Press any key to continue …” is displayed. Enter an arbitrary key.
7. Close the command prompt.

Copyright © 2015, 2017, Hitachi, Ltd.

12.3 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. Log out of Storage Navigator in the Storage System to be reallocated.
2. Stop the service of the Storage System to be reallocated.
3. Start the Windows command prompt by the SVP with the administrator authority.
4. Move the current directory to the directory in which the tool exists and execute the next command.
   C:\Mapp\wk\Supervisor\MappIniSet>MappPortManageRenum.bat △ [Serial numbers] (arbitrary)
   When the serial numbers are omitted, the command is performed for the Storage System with the version 83-03-01-xx/00 or later.
5. 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.
6. The completion message is displayed.
7. The message “Press any key to continue …” is displayed. Enter an arbitrary key.
8. Close the command prompt.
9. Start the services of the reallocated Storage System.

Copyright © 2015, 2017, Hitachi, Ltd.

12.4 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 "12.3 Reallocating Automatically Allocated Port Numbers" for the storage system.

1. Log out the Storage Navigator.
2. Stop the services of all the Storage Systems whose status of Storage Device List is Ready.
3. Start the Windows command prompt by the SVP with the administrator authority.
4. Move the current directory to the directory in which the tool exists and execute the next command.
   C:\Mapp\wk\Supervisor\MappIniSet>MappPortManageInit.bat
5. 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.
6. The completion message is displayed.
7. The message "Press any key to continue …" is displayed. Enter an arbitrary key.
8. Perform reallocation.
   C:\Mapp\wk\Supervisor\MappIniSet>MappPortManageRenum.bat △ [Serial numbers] (arbitrary)
   When the serial numbers are omitted, the command is performed for the Storage System with the version 83-03-01-xx/00 or later.
9. 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.
10. The completion message is displayed.
11. The message "Press any key to continue …" is displayed. Enter an arbitrary key.
12. Perform Step 8. to Step 11. to reallocate the port numbers for all the registered storage systems.
13. Close the command prompt.
14. Start the service of the storage system to be operated.

Copyright © 2015, 2017, Hitachi, Ltd.

12.5 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 Windows command prompt by the SVP with the administrator authority.
2. Move the current directory to the directory in which the tool exists and execute the next command.
   C:\Mapp\wk\Supervisor\MappIniSet>MappPortRangeSet.bat △ [Service port number key name] △ [Port number range]
   A " △ " mark indicates a space.
   The values in [ ] indicates a parameter.

   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	
SMIS_CIMOM	5989 to 6244	
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 available character strings in the effective range are as follows.
     Character strings: "Number" "," "-" "rm"
     When "rm" is specified, delete the setting of the specified port number key.
   - You can specify more than one command input parameter "[Service port number key name] △ [Port number range] △ : one-byte space
     Example: MappPortRangeSet.bat PreRMIServer 51200-55000 SMIS_CIMOM 5989-6244,8000
   - 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.

3. The completion message is displayed.
4. The message "Press any key to continue …" is displayed. Enter an arbitrary key.
5. Close the command prompt.

Copyright © 2015, 2017, Hitachi, Ltd.

12.6 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 Windows command prompt by the SVP with the administrator authority.
2. Move the current directory to the directory in which the tool exists and execute the next command.
   C:\Mapp\wk\Supervisor\MappIniSet>MappPortRangeInit.bat
3. 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.
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.

Copyright © 2015, 2017, Hitachi, Ltd.

12.7 See the Port Number to be Used in the SVP

You can see the port numbers to be used in the SVP.

1. Start the Windows command prompt by the SVP with the administrator authority.
2. Move the current directory to the directory in which the tool exists and execute the next command.
   C:\Mapp\wk\Supervisor\MappIniSet>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.
3. The information of the port numbers to be used in the SVP is displayed.
   For the ports whose numbers are not allocated, “Not Defined” is displayed.
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.

Copyright © 2015, 2017, Hitachi, Ltd.

12.8 Checking the Application Using the Port Number Used by the SVP

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.

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 “12.7 See the Port Number to be Used in the SVP”. 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 Windows command prompt on the SVP as Administrator.

3. 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.

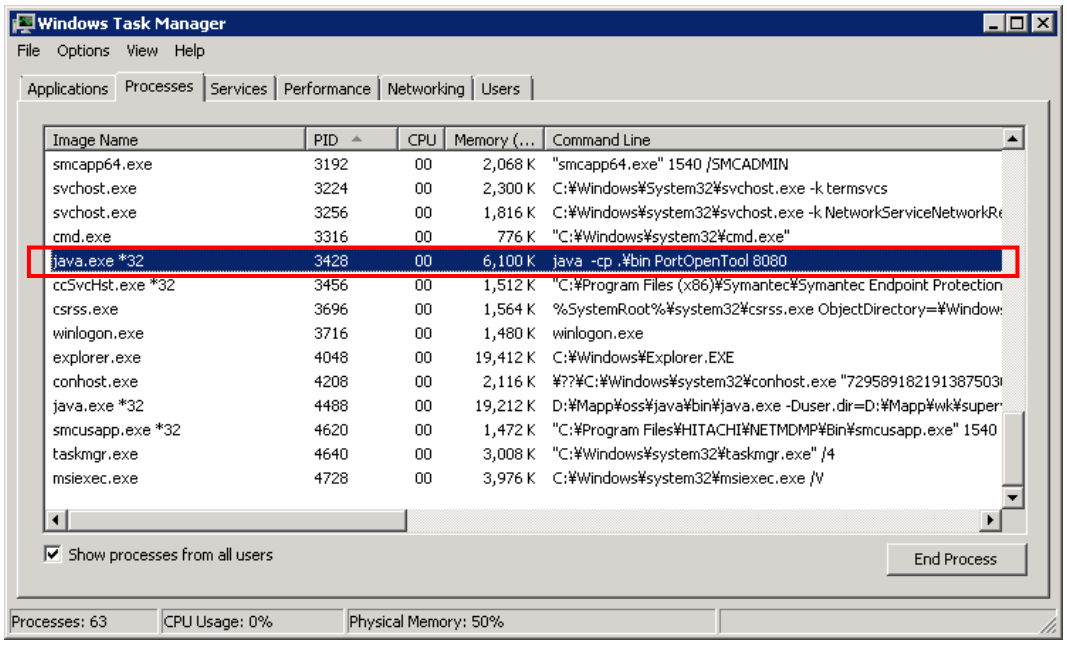
Example: When the port number 8080 is used by a different application

```
>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.

4. 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.

Copyright © 2015, 2017, Hitachi, Ltd.

13. Appendix

13.1 IP Addresses of Maintenance Ports and Internal Network

13.1.1 Maintenance Port Addresses

Select the maintenance port address of the model in which NAS Modules are installed in DW800 from Table 13-1 to Table 13-3. 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 13-1.
Select the host address, yy, from Table 13-2.
For the host address of each component, set the address by adding the corresponding value in Table 13-3 to yy that was selected from Table 13-2.

Table 13-1 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 13-2 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

Table 13-3 Each Component Host Address of Maintenance Port

No.	Component	CTL1	CTL2	Remarks
1	Storage System	+0	+1	
2	Unified Hypervisor	+2	+3	
3	NAS Platform	+4	+5	

Copyright © 2015, 2017, Hitachi, Ltd.

13.1.2 Internal Network Addresses

You can select the internal network address from Table 13-4 and the default value is set to (126.255...).

Table 13-4 Selections of Internal Network Addresses

No.	Selectable Network Address	Subnet Mask	Remarks
1	126.255 (Default)	255.255.0.0	Unusable when adding NAS Modules
2	10.1		
3	192.169		Unusable when adding NAS Modules
4	172.240		
5	10.198		
6	10.17		
7	10.97		
8	10.251		Default when adding NAS Modules
9	172.17		
10	172.31		
11	192.168		Unusable when the maintenance LAN network address is as follows • 192.168.0.0 • 192.168.233.0

Copyright © 2015, 2017, Hitachi, Ltd.

13.2 Port Number Used by Hitachi Command Suite

The Maintenance PC uses the following port number.
The following port number can be changed to a different one.
See "12. Changing/Initializing Port Numbers Used by the SVP" for the procedure.

Protocol	Port number	Applicable SVP software version
HTTP	80	All versions
HTTPS	443	All versions
RMI	51099	All versions
RMI (SSL)	5443	All versions
RMI	1099	All versions
RMI	51100	less than 83-03-01-xx/00
	51100-51355	83-03-01-xx/00 or later
RMI	11099	All versions
HTTP	8080	All versions
HTTP	8210	All versions
HTTP	9080	All versions
HTTP	9210	All versions
HTTP	8081	less than 83-03-01-xx/00
HTTP	48081-48336	83-03-01-xx/00 or later
HTTP	8211	less than 83-03-01-xx/00
HTTP	48411-48666	83-03-01-xx/00 or later

Copyright © 2015, 2017, Hitachi, Ltd.

13.3 Port Number Used by the Maintenance PC

Port number	Protocol	Software	Change port no: A or NA	Conflict with Maintenance PC
162	UDP	Device Manager	NA	None
427	TCP	Device Manager	NA	Available
1099	TCP	Hitachi Storage Navigator Modular 2 (SNM2 Server)	A	Available
2001	TCP	Device Manager	A	None
2443	TCP	Device Manager	A	None
5983	TCP	Device Manager	A	None
5988	TCP	Device Manager	A	None
5989	TCP	Device Manager	A	Available
20352	TCP	Tiered Storage Manager	A	None
22015-22018	TCP	Hitachi Command Suite common component	A	None
22019	TCP	Tuning Manager	A	None
22020	TCP	Tuning Manager	A	None
22023	TCP	Tuning Manager	A	None
22024	TCP	Tuning Manager	A	None
22025-22028	TCP	Hitachi Command Suite common component	A	None
22031-22034	TCP	Hitachi Command Suite common component	A	None
22098-22100	TCP	Host Data Collector	A	None
22104-22106	TCP	Host Data Collector	A	None
22110-22120	TCP	Host Data Collector	A	None
22286	TCP	Tuning Manager	A	None
22610	TCP	Compute Systems Manager	A	None
22611	TCP	Compute Systems Manager	A	None
22900-22999	TCP	Tuning Manager	NA	None
23015-23018	TCP	Hitachi Command Suite common component	A	None
23019-23024	TCP	Tuning Manager	A	None
23025	TCP	Device Manager (*1)	NA	None
23026	TCP	Device Manager (*1)	A	None
23031	TCP	Hitachi Command Suite common component (*1)	A	None
23032	TCP	Hitachi Command Suite common component (*1)	A	None
23052	TCP	Host Data Collector (*1)	A	None
23055	TCP	Device Manager	A	None
23450-23453	TCP	Hitachi Command Suite REST API	A	None
24220	TCP	Device Manager (*1)	A	None
24221	TCP	Tuning Manager	A	None
24222	TCP	Tuning Manager	A	None
24230	TCP	Device Manager	A	None
24235-24242	TCP	Hitachi Command Suite common component	A	None
24500	TCP	Tiered Storage Manager	A	None
31001-31002	UDP	Hitachi Command Suite REST API	NA	None
45001-49000	TCP	Hitachi Command Suite common component (*1)	A	Available

*1: The port number is not used by Hitachi Command Suite 8 or later.