WEB

This “WEB” volume describes the operating procedure for WEB.

Contents

This page is for editorial purpose only.

Chapter 1. Before Using Web

Precautions when restarting.

- If the array subsystem used for a remote side of TrueCopy remote replication/TrueCopy Extended Distance restarts in the status that TrueCopy remote replication/TrueCopy Extended Distance is enabled, the following phenomena occur.
  - The paths of TrueCopy remote replication/TrueCopy Extended Distance are both blocked. The notice of E-mail Alert Function, SNMP Agent Support Function, and TRAP occur at the time of the path blockade.
    Perform the notice and the check to the Failure Monitoring Department in advance.
    The path blockade automatically recovers after restarting.
  - When the status of the pair of TrueCopy remote replication/TrueCopy Extended Distance is PAIR or COPY, the pair changes to PSUE.
    If the Pair status of TrueCopy remote replication/TrueCopy Extended Distance is either PAIR or COPY, suspend the pairs before restarting the array subsystem.
- When Power Saving of the priced option is used, if you restart the subsystem after executing the spin-down and before completing it, the spin-down may fail because of the recognition processing of the host immediately after the subsystem starts.
  Check that there is no RAID Group whose power saving status is "Normal (command monitoring)" after executing the spin-down, and then restart the subsystem.
  If the spin-down fails, execute the spin-down again.
- If the NAS Unit is connected and the NAS service is in operation, ask the NAS Unit administrator for planned shutdown of the NAS Unit.
  After rebooting the array device, ask the NAS Unit administrator to reboot the NAS Unit and check the status of the FC path (Fibre Channel path). Refer to "Recovering from FC path errors" in "Hitachi NAS Manager User's Guide" to check the status of the FC path, and if there is a failure in the FC path, ask the NAS Unit administrator to recover the FC path.

1.1 The Operating Environment

The operating environment where is able to use Web is shown below.

Table 1.1.1 Operating Environment

No.	Item	Description	Remark
1	OS	Microsoft Windows 2000, XP, 2003, Vista, 2008, 7, Solaris 8, 9, 10, IRIX 6.5, AIX 5.1	When connecting with IPv6, we recommend Windows Vista 2008.
2	PC	Pentium 4 1 G Hz (2 G Hz or more is recommended), Memory 1 G bytes or more (2 G bytes or more is recommended)	—
3	WS	Turbo Sparc 170 M Hz, Memory 256 M bytes or more R10000 195 M Hz, Memory 128 M bytes or more	—
4	Disk requirement	• 60 M bytes, under ordinary maintenance work • 2.4 G bytes per one Controller, under Full Dump collection(*1) { Storing temporary file of Browser : 1.2 G bytes Storing Full Dump: 1.2 G bytes }	• Data compression tool is required for Full Dump. • Refer to "3.5.3 Collecting Full Dump" (WEB 03-0460) or "3.5.4 Collecting Full Dump (Full Dump(SnapShot/TCE))" (WEB 03-0500) for the capacity of Full Dump when it is uncompressed.

*1 : Full Dump collection may be requested by the Technical Support Center at the time of a tough failure.

1.2 Notices on (Restriction of) the Support Browser

In the case of Windows2003, because the strict data security is the default setting, the Web function cannot work.
In order to solve the above problem, change the setting of the browser as follows.

- Select [Tools] - [Internet Options …] - [Security] - [Custom Level …] - [Custom Setting Reset] of the browser in this order and select the setting of the security level from Medium or lower and click the "Reset" button.
  The making of the setting as Medium solves the problem. However, if you want to use Win2003 leaving the security level as High, make the following settings for the detailed items of the [Custom Level …].
  - Enable the [Active scripting] of the [Scripting].
  - Enable the [Allow META REFRESH] of the [Miscellaneous].
  - Enable the [File download] of the [Downloads].
  - Enable the [Run ActiveX controls and plug-ins] of the [ActiveX controls and plug-ins].

- In Windows Vista, Server 2008, the value that security is more strengthened than Windows Server 2003 is default, so that the WEB function does not operate as is.
  To solve this, change the browser setting as shown below.
  - Register is as the reliable WEB site from [Tool] – [Internet Option] – [Security] – [Reliable Site] – [Site].
- When entering IPv6 address in URL in Windows Vista, Server 2008, you need to put the IP address in square brackets ([ ]) and specify it as URL. (e.g.: http://[fe80::16]/).
- The WEB function operates normally in other Windows because the security level is being [Medium]. However, set the following items in [Settings] of [Tools] - [Internet Options …] - [Security] - [Custom Level …] to [Enable].
  - Enable the [Active scripting] of the [Scripting].
  - Enable the [File download] of the [Downloads].

- There may be a case where an operation is guarded, the setting for user authentication is required, or expected screen is not displayed depending on the setting of security.
  There is a precaution for the setting item of the browser(IE) of[Tools] -[Internet Options …] - [Security]- [Custom Level …]as follows.
  - When obtaing trace, a file saving screen is not displayed.
    In case of [ActiveX controls and plugin]-[Automatic prompting for ActiveX controls］is [Enable], the file saving screen is blocked when obtaining trace.
    In such case, please follow the explanation indicated there for operation.
    If you display a dialog with no block, [Enable] the [Automatic prompting for ActiveX controls]

• There may be a case where a new line is started in a window depending on a setting of the browser. In such a case, make the character size smaller.
< Method of character size change >
In the case of IE
Select “Middle” or smaller size for the “Character Size” in the “Display”.
In the case of Netscape
Select the “Reduction of Font Size” in the “Display” and keep it being selected until paragraphs become easy to be read.

- There may be a case where an empty dialog box is displayed during operation in the Maintenance mode. In such a case, close the window by clicking on the mark of “X” in the upper left corner of the dialog box, restart the browser, and then make a retry from the entry of the URL.
- When a window size is changed while a page is displayed by Netscape, the succeeding operation in the Refresh mode may not be done normally. In such a case, display the page over again by clicking the Re-Display button.
- In the case of using Netscape
  Memory cache: 1024 k bytes (default) or larger
  Disk cache: 7680 k bytes (default) or larger

< Method of cache size setting >
Select the “Edition”, “Setting”, “Details”, and “Cache” in this order.
Specify sizes of the memory cache and disk cache.

- When obtaining trace information etc. with Netscape, there are cases that a sub-screen to specify the file download destination does not automatically close.
  In such a case, press a close button at the upper right corner of the sub-screen to close the sub-screen after download complete.
- When using Netscape Navigator 7.x, select [Edit]-[Preference...]-[Advanced]-[HTTP Networking], and set “Use HTTP 1.0” in the “Direct Connection Options” and “Proxy Connection Options”. When this setting is not made, the summary window is not displayed correctly.
- When collecting Full Dump using Netscape Navigator 4.7x, pay attention to free space in PC because information to be downloaded won’t be compressed.

	Installed cache per Control Unit	Free Capacity needed on PC
RKM	1 G bytes (Minimum)	1,825 M bytes
	8 G bytes (Maximum)	6,187 M bytes
RKS	1 G bytes (Minimum)	1,461 M bytes
	4 G bytes (Maximum)	3,387 M bytes
RKH	2 G bytes (Minimum)	3,734 M bytes
	16 G bytes (Maximum)	12,087 M bytes
RKEXS/RKEXSA/RKEXSB/RKEXS8F	2 G bytes	2,103 M bytes

NOTE : When using IE 8.0, IE 9.0 or IE 10.0, the WEB window display may slow down and the collection of the trace from the WEB window may not complete. Uncheck the checkbox of “Enable SmartScreen Filter” in the Internet Options Advanced Settings. If the issue still occurs, please cancel the DNS Server’s settings of the PC's LAN.

1.3 The Characteristic of the Network Function

- LAN interface
  The connector for 10Base-T/100Base-TX, 1000 Base-T is equipped with the Controller. 10Base-T/100Base-TX, 1000 Base-T and half-duplex/full-duplex communication are selected automatically by the automatic negotiation function.

  NOTE : The fixed setting of the negotiation cannot be performed. Communicate by setting the device to be connected to the automatic negotiation.

- Network parameter

  The DF800 has the following network parameters, and the User management port of each Control Unit can be set or changed from the WEB browser or the Hitachi Storage Navigator Modular 2.

Network parameter		Description	Values set when shipped from the factory				Remark
			Control Unit #0		Control Unit #1		
			Maintenance port < Fixed IP >	User management port <Variable IP>	Maintenance port < Fixed IP >	User management port <Variable IP>	
IPv4	IP Address	The IP Address is changed/set up.	10.0.0.16	192.168.0.16	10.0.0.17	192.168.0.17	(*1)
	Subnet Mask	The Subnet Mask is changed/set up.	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	
	Default Gateway	The Default Gateway is changed/set up.	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	
	DHCP	Enable/Disable of the DHCP function is set up.	OFF	OFF	OFF	OFF	(*2)
IPv6	IP Address	The IP Address is changed/set up.	fe80::16	Automatic	fe80::17	Automatic	(*3)
	Subnet prefix	Set and change the length of the subnet prefix.	64	Automatic	64	Automatic	
	Default Gateway	The Default Gateway is changed/set up.	::	Automatic	::	Automatic	
	Automatic acquisition	Set Enabled/Disabled of the automatic acquisition function.	OFF	ON	OFF	ON	(*4)

*1 : The network connection is possible in the above IP Address (192.168.0.16) for the unchanging from the factory setting value. Please manage the IP Address after the change certainly, if the IP Address is changed from the IP Address of factory setting.

*2 : When DHCP mode is valid, IP address is obtained from the DHCP server.
When the DHCP server has not started up or DHCP function has been miss-set, obtaining the IP address fails and the device IP address remains to be “0.0.0.0”. (Hitachi Storage Navigator Modular 2 or Web cannot be used via LAN.) In this case, the device IP address can be obtained by starting up the DHCP server or setting DHCP function correctly if necessary.
When the IP address of this subsystem is acquired using the DHCP function, if the network address of the reserved IP address for the maintenance port is assigned as an IP address, the IP addresses of the port for the user control and the port for the maintenance may not operate normally because they compete.
Request the system administrator that the DHCP server does not assign IP address of “10.0.0.x”, “192.168.0.x”, “192.168.233.x”, “172.23.211.x”, “10.197.181.x” to the device.

*3 : The shipment setting is automatic acquisition for the IP address of the user management port of IPv6.
You can check the IP address allocated to the user management port by searching from Hitachi Storage Navigator Modular 2.
When changing the IP address of the shipment setting, please manage the changed IP address responsibly.

*4 : When the automatic acquisition is enabled (ON), the IP address is acquired from the RA delivery server.
When the RA delivery server is not started or the setting of the RA delivery function is incorrect, the IP address acquisition fails and the IP address of the subsystem remains as “::”. In such case, you can acquire the IP address correctly by starting the RA delivery server or set the RA delivery function correctly if needed.
When acquiring the IP address of this subsystem by using the RA delivery server, if the IP address duplicated by the reserved IP address for the user maintenance port is allocated, the IP addresses for the user management port and the maintenance port compete and they may not be operated normally.
In such case, request the system administrator so that the RA delivery server does not allocate “fe80::/10” as prefix of the IP address.

This page is for editorial purpose only.

- Manual change of network parameters of the Maintenance port
  When the User management port is set as the same network address as the Maintenance port, the communication cannot be made normally. Prepare five patterns of the network parameter fixed values to be used in the Maintenance port, and change the network parameter fixed values to be used in the Maintenance port manually by the network parameter of the User management port.
  The following can be set as the fixed values of the network parameters used in the Maintenance port.
  <In case of IPv4 Protocol>
  - 10.0.0.xxx
  - 192.168.0.xxx
  - 192.168.233.xxx
  - 172.23.211.xxx
  - 10.197.181.xxx

  <In case of IPv6 protocol>
  - fe80::xxx

  NOTE : • For the part of xxx, set 16 to CTL0 except when connecting the Maintenance port to the network (in that case, 17 is automatically set to CTL1).
  • For a Maintenance port, subnet mask and default gateway cannot be set. Thus a Maintenance port does not support the network including routers.
  • In case of IPv4 Protocol, when the network address of the LAN device, which is connected via the Gateway in the extension of the User management port, is the same as that of the Maintenance port, the communication cannot be made normally because of the conflict between them.
  In case of IPv6 protocol, when the IP address of the user management port becomes the same as the IP address of the maintenance port, they both compete and communication is not performed normally.
  Therefore, use a value other than the network address set to the maintenance port for the LAN device connected to the port for the user management via Gateway. Or change the IP address of the maintenance port to a value other than the network address of the LAN device connected via Gateway by Hitachi Storage Navigator Modular 2. (Refer to System Parameter “4.2 (4) Setting of Maintenance LAN” (SYSPR 04-0160).)

- Automatic change of network parameters of the Maintenance port (Only in case of IPv4 protocol)
  When setting the network parameters of the User management port, if “Maintenance port IP address automatic change mode” is enabled, the IP address of the Maintenance port is automatically changed as shown below according to the IP address value of the User management port to be set.
  - When setting the User management port of CTL0 to 10.xxx.xxx.xxx, the Maintenance port of CTL0 is 192.168.0.16.
  - When setting the User management port of CTL0 to other than 10.xxx.xxx.xxx, the Maintenance port of CTL0 is 10.0.0.16.
  - When setting the User management port of CTL1 to 10.xxx.xxx.xxx, the Maintenance port of CTL1 is 192.168.0.17.
  - When setting the User management port of CTL1 to other than 10.xxx.xxx.xxx, the Maintenance port of CTL1 is 10.0.0.17.

  When “Maintenance IP address automatic change mode” is disabled, it becomes the same operational specification as the manual change of the network parameters of the Maintenance port.

  NOTE : When the network address of the LAN device, which is connected via the Gateway in the extension of the User management port, is the same as that of the Maintenance port, the communication cannot be made normally because of the conflict between them.
  Therefore, use a value other than the network address set to the maintenance port for the LAN device connected to the port for the user management via Gateway. Or change the IP address of the maintenance port to a value other than the network address of the LAN device connected via Gateway by Hitachi Storage Navigator Modular 2. (Refer to System Parameter “4.2 (4) Setting of Maintenance LAN” (SYSPR 04-0160).)

1.4 Support Browser List

Table 1.1.2 Support Browser List

(○ : support × : not support)

No.	Platform	OS		Browser		Supported or not supported	Java Applet supported or not supported (*2) (*3)	Supported or not supported (IPv6)
		Type	Ver.	Type	Ver.(*1)			
1	WS	IRIX	6.5	Netscape Navigator	4.76(*4)	○	×	×
		Solaris	8, 9	Netscape Navigator	4.76(*4)	○	×	×
			10	Mozilla	1.7	○	×	○
		AIX	5.1	Mozilla	1.7	○	×	×
2	PC	Windows	2000	Internet Explorer	6.0	○	○	×
			XP	Internet Explorer	6.0, 7.0	○	○	×
			2003 (32 bit)	Internet Explorer	6.0, 7.0	○	○	×
			2003 (64 bit)	Internet Explorer	6.0	○	○	×
					6.0 (64 Bit)	○	×	×
			Vista	Internet Explorer	7.0, 9.0	○	○	○
					7.0 (64 Bit)	○	×	○
			2008	Internet Explorer	7.0, 9.0	○	○	○
					7.0 (64 Bit)	○	×	○
			7 (32 bit)	Internet Explorer	8.0, 9.0, 10.0	○	○	○
			7 (64 bit)	Internet Explorer	8.0, 9.0 (64 bit)	○	×	○
					10.0 (64 Bit)	○	○(*5)	○
		Windows	2000/XP	Netscape Navigator	7.1 (J)	○	×	×
					7.2 (E)	○	×	×
			2003	Netscape Navigator	7.1 (J)	○	×	×
					7.2 (E)	○	×	×
			Vista	Netscape Navigator	7.1 (J)	○	×	×
					7.2 (E)	○	×	×

*1 : Service Pack 1 is included. (except Internet Explorer 8.0, 9.0 and 10.0)

*2 : When installing the firmware, the Maintenance PC must be started by the OS from the drive C in order to prevent a problem of security from occurring.

*3 : Java Applet is used for the following cases.

- Firmware installation
- Host command trace download
- Online ENC firmware download
- Offline Drive Firmware download
- Online Drive Firmware download

*4 : Netscape Navigator 4.76 causes the following problems because the release is old. However, there is no problem in the operation.

- If you cancel in the file save window when saved by the simple trace collection, WEB may not be connected for a while. Leave the interval for about 20 minutes and connect it again.
- The java script error may occur in some windows, but there is no problem in the operation.
- Since the sub-window is closed soon in the initialization window of the SSL certificate and the complete window is not displayed, the initialization is completed normally.

*5 : The extended protection mode of the Internet options newly installed in Internet Explorer 10.0 should be disabled (default is disabled).

1.5 Displaying the Special Window

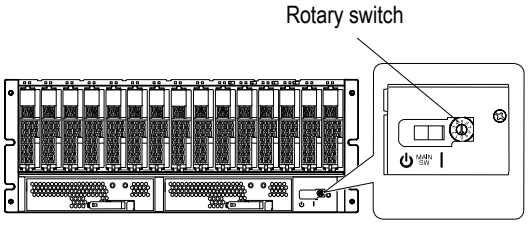
When the firmware version is 0862/A or more, displaying the special window needs to set the Rotary switch on the front side of the Control Unit and enter the URL.

Table 1.5.1 List of Special Window

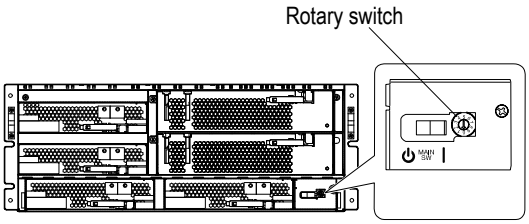
No.	Function	URL (following the device IP address)
1	SSL certificate Initialization Function	/sslc_init
2	Online Drive Firmware Replacement Function	/drvfirm_mnt

Change the setting of the Rotary switch according to the procedure shown below, and display the window by entering the URL on the WEB.

(1) Before the operation, write down the set value of the Rotary switch on a memo pad.



(a) Rackmount Model (RKM/RKS)

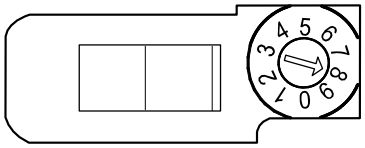


(b) Rackmount Model (RKH)

Rotary switch : Here shown is an instance that it is set to Local-mode.

Figure 1.5.1 Location of Rotary Switch

(2) Set the Rotary switch to the 8 before operating on the WEB.



(3) After ten seconds or longer pass from the step (2), display the window by entering the URL of the special window.

(4) After the WEB operation is terminated, return the setting of the Rotary switch to the value written in the step (1).

Chapter 2. The Normal Mode Operation Procedure

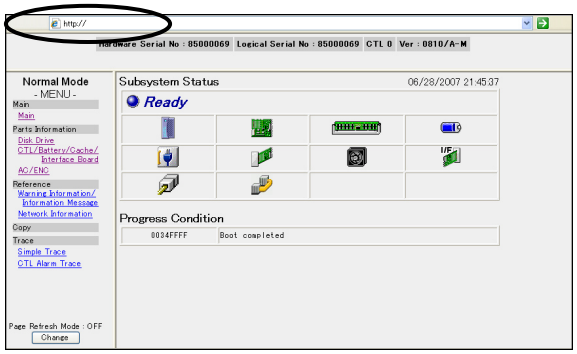
2.1 Transferring to the Normal Mode

For entering Normal mode, input IP address of Maintenance LAN connecter to which the LAN cable is connected into the [address] window of Web Browser.

Under dual system configuration, input one of IP addresses of LAN-Connecter for maintenance. The status of the devices (both Controllers) can be monitored from one controller.
If it is connected, the next screen is displayed.

NOTE : • Set the TCP/IP to “Disable DNS” because the connection takes a long time when the TCP/IP of the network is set to the condition in which the DNS is used. For the setting procedure, refer to the instruction manual of the PC to be used.

• Make sure that the browser is set to the condition in which the proxy server is not used because the connection cannot be done if the proxy server is set to be used. To make sure the setting, refer to the instruction manual of the browser to be used.



2.2 Screen Outline

If the function of the Normal Mode is shown with the menu form and clicked, the proper function is executed. The main screen outline of the Normal Mode is shown below.

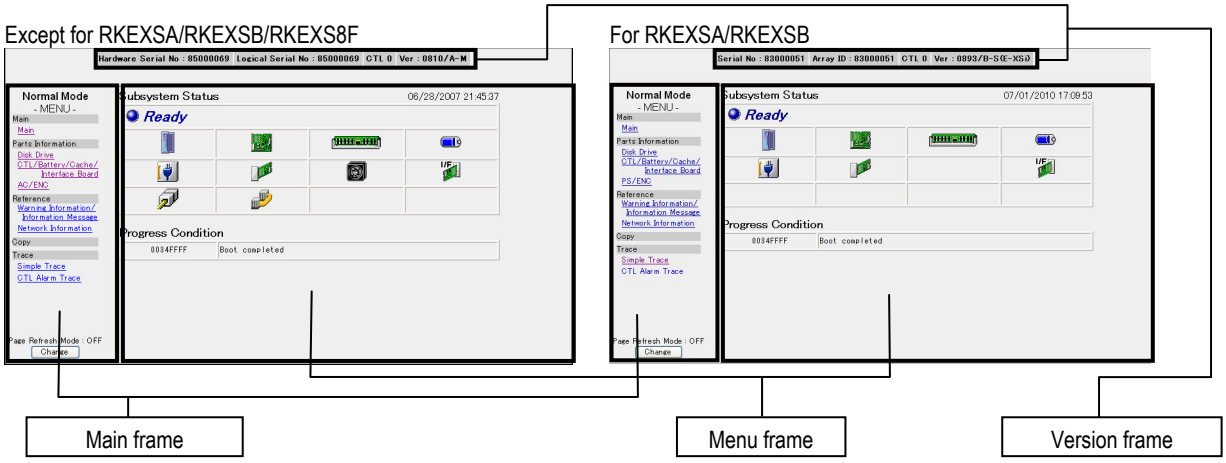


Figure 2.2.1 Main Screen Outline of the Normal Mode

(1) Version frame

- Web Title
  A Web title set by a user is displayed as it is. When it is not set, nothing is displayed.
- Serial No
  The subsystem serial number is shown.
- CTL
  Shows the number of the Controller to which the Web is connected.
- Ver
  The version of the firmware of the device is shown.
  When the unit is RKEXSA/RKEXSB, the (E-XSi) is displayed of right side of version frame.
  When the unit is RKEXS8F, the (E-XS) is displayed of right side of version frame.

(2) Menu frame

If the function of the Normal Mode is displayed with the menu frame and clicked, the proper function is executed.

- Main
  The Main screen of the Normal Mode is displayed.
- Disk Drive
  The status of the Disk Drive is displayed.
- CTL/Battery/Cache/Interface Board
  The status of the Control Unit, Cache Backup Battery, Cache Unit, and Interface Board are displayed.
- PS/ENC
  The status of the Power Unit and ENC Unit are displayed.
- Warning Information/Information Message
  The fault information that was detected during the device operation and the status of the device information are displayed.
- Network Information
  The LAN port number is displayed.
- Simple Trace
  A window for collecting the Simple trace is displayed.
- CTL Alarm Trace
  A window for collecting the CTL Alarm trace is displayed.
- Page Refresh Mode
  The mode for setting turning on or off of the automatic display function is displayed.
  When the [Change] button is clicked, the mode is changed to on or off.
  As the [OFF] display : This is not refreshed.
  As the [ON] display : The screen of the mainframe is refreshed every 5 seconds.
  The time of the latest refreshment (RTC) is displayed in the upper right part of the main frame.

NOTE : When the PC enters the suspension status during operation while the Page Refresh Mode is set to [ON], the Web may not operate correctly after the PC is released from the suspension status.
In the case where the Web is connected for the purpose of status monitoring, etc., set the power management of the PC so that the PC should not enter the suspension status.

(3) Main frame

- Subsystem Status
  The status of the device and the status of the exchange parts are displayed.
- Progress Condition
  The Progress Condition as the device booting is displayed.

2.3 Main Screen of the Normal Mode

The main screen of the Normal Mode is consisted of the Patrol Lamp, the summary of exchange parts status, the Progress Condition display box.
The Patrol Lamp shows the status of subsystem.

The “summary of exchange parts status” notifies replacement parts errors by turning the parts in red.
If the image of the part is clicked, the details information of the proper part are displayed.

The Main screen of the Normal Mode is shown below.

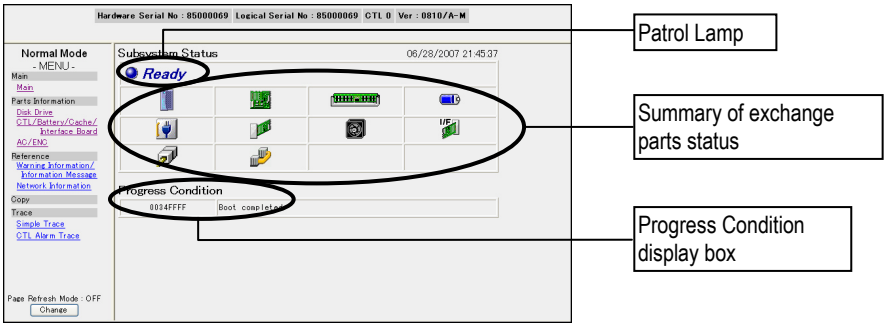


Figure 2.3.1 Main Screen of the Normal Mode

(1) Patrol Lamp

Monitoring the device, the status is displayed. The Status of the Patrol Lamp is shown below

Image	Status
Booting... Black	• During the start
Ready Blue	• Normal
Warning Yellow	• Warning status
Alarm Red	• Alarm status

(2) Display of Progress Condition

The Progress Condition as the device booting is displayed.

(3) Summary of Exchange Parts Status

The condition of the exchange parts is displayed. If the image of the part is clicked, the details of the proper part are displayed. The status of each exchange part is shown below.

Cache Backup Battery

Image	Status
 Blue	• Normal
 Red	• Cache Backup Battery error

Power Unit

Image	Status
 Blue	• Normal
 Red	• Power Unit error

ENC Unit

Image	Status
 Green	• Normal
 Red	• ENC Unit error

FAN Unit

Image	Status
 Black	• Normal
 Red	• FAN Unit error

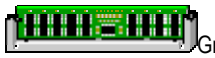
Disk Drive

Image	Status
 Blue	• Normal
 Red	• Disk Drive error

Control Unit

Image	Status
 Green	• Normal
 Red	• Control Unit error

Cache Unit

Image	Status
 Green	• Normal
 Red	• Cache Unit error

Host Connector

Image	Status
 Gray	• Normal
 Red	• Fault

Interface Board

Image	Status
 Green	• Normal
 Red	• Fault

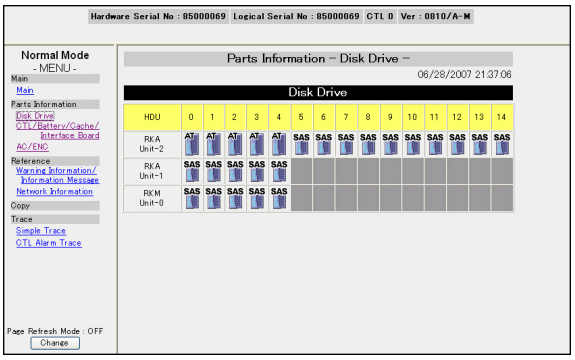
2.4 Display of Exchangeable Parts Status (Parts Information)

(1) Checking the status through an image

The display screen of exchange part status displays the status of the Disk Drive, Control Unit, Cache Unit, FAN Unit, Cache Backup Battery, Power Unit, ENC Unit, that are implemented. Furthermore, if no parts are implemented, the part status is not displayed and its status display area becomes gray. If the part concerned does not exist due to the integration of pats or cannot be implemented physically, the part status is not displayed and its status display area becomes black.

Also, the exchange part of abnormal status displays a red image. The Parts Information screen is shown below.

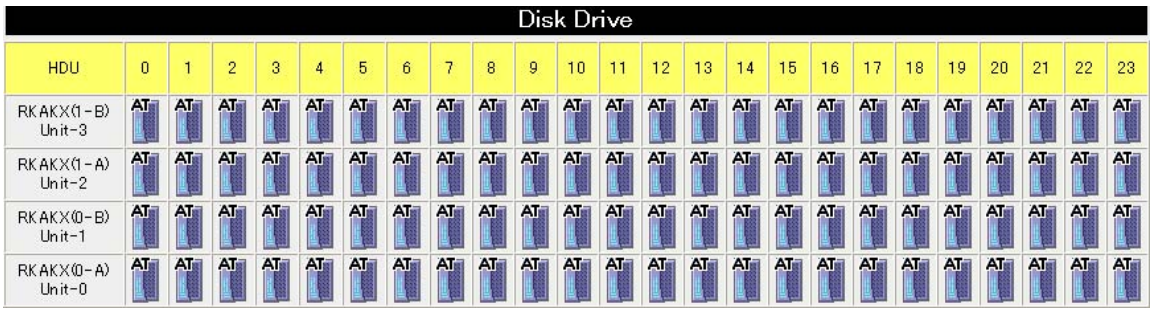
(a) Disk Drive



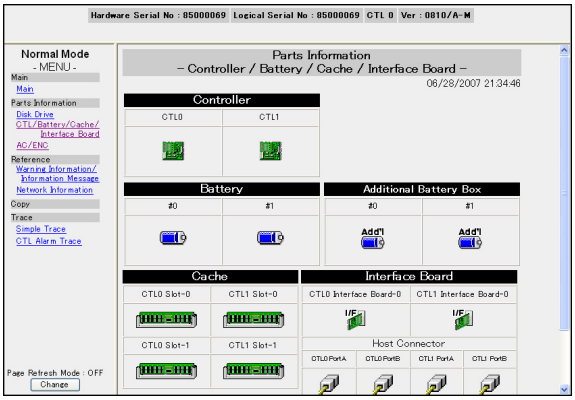
• Disk Drive

Image	Status
Blue	Normal
Red	Fault has occurred to the Disk Drive
Red and Black	Disk Drive port that the fault occurred is not implementing the Disk Drive
No display	Disk Drive is not implemented (Except for the status where the Disk Drive that the fault occurred was drawn out), or although a failure occurs in the Disk Drive, the Disk Drive type cannot be determined.

RKAKX is treated as two units, each of which contains 24 Disk Drives (19 Disk Drives when SAS/SAS(SED) drives are installed).
Seen from the front bezel side, the left side unit is called Unit A, and right side unit is called Unit B.
The label marked Unit A or Unit B is attached near the LED on the front bezel.
The unit number is assigned the running number of the RKAK, and the Unit A and Unit B of the RKAKX. (The unit number of Unit B is a number adding 1 to the unit number of Unit A.)
RKAKX (x-A) or RKAKX (x-B) (‡1) to be displayed indicates that the unit is Unit A or Unit B of the RKAKX.
When the RKAKX is mounted, the status shown below is displayed.



(b) CTL/Battery/Cache/Host Connector/Interface Board



• Control Unit

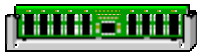
Image	Status
Green	Normal
Red	Shutdown of the Control Unit (Status where it is not implemented with the setting of the dual system configuration is included)
Yellow	Fault of the battery backup circuit
No display	Even the fault has not occurred without being implemented with the setting of single system configuration

‡1 : x(integer) is the running number of the RKAKX. The x is the same number in the Unit A and Unit B in pairs which compose the RKAKX.

• Cache Backup Battery

Image	Status
 Green	Normal
 Red	There is a fault or not implemented

• Cache Unit

Image	Status
 Green	Normal
 Red	Fault (Status where is not implemented and extracted the fault cache memory is included)
No display	It is not implemented and there is not a fault

• Host Connector

Image	Status
 Gray	Normal
 Red	Fault

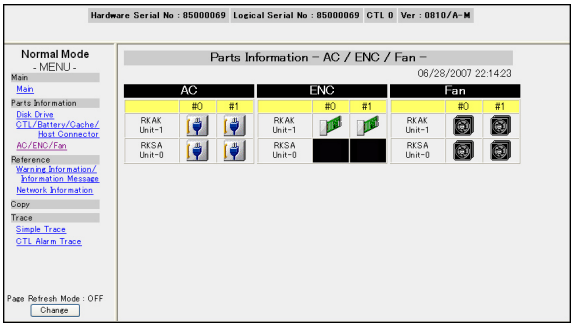
• Interface Board

Image	Status
 Green	Normal
 Red	Fault

• Additional Battery Box

Image	Status
 Green	Normal
 Red	There is a fault or not implemented

(c) AC/ENC/Fan



• Power Unit

Image	Status
Blue	Normal
Red	It is fault occurred or not implemented

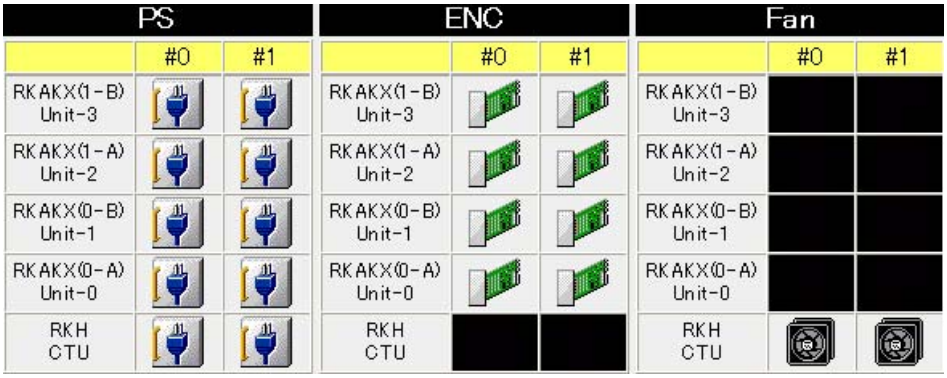
• ENC Unit

Image	Status
Green	Normal
Red	It is fault occurred or not implemented

• FAN Unit

Image	Status
Black	Normal
Red	There is a fault or not implemented

RKAKX is treated as two units, each of which contains 24 Disk Drives (19 Disk Drives when SAS/SAS(SED) drives are installed).
Seen from the front bezel side, the left side unit is called Unit A, and right side unit is called Unit B.
The label marked Unit A or Unit B is attached near the LED on the front bezel.
The unit number is assigned the running number of the RKAK, and the Unit A and Unit B of the RKAKX. (The unit number of Unit B is a number adding 1 to the unit number of Unit A.)
RKAKX (x-A) or RKAKX (x-B) [‡1] to be displayed indicates that the unit is Unit A or Unit B of the RKAKX.
When the RKAKX is mounted, the status shown below is displayed.



‡1 : x(integer) is the running number of the RKAKX. The x is the same number in the Unit A and Unit B in pairs which compose the RKAKX.

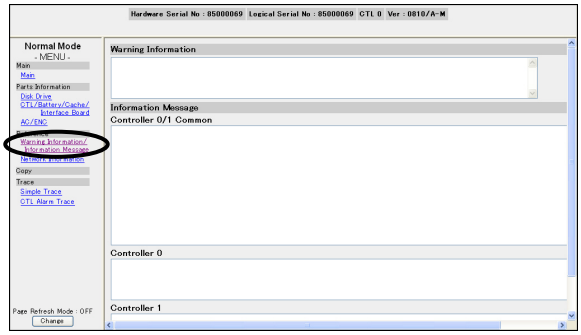
This page is for editorial purpose only.

(2) Procedure of the Status checking by messages

A warning message about the failed part is displayed.

Refer to Troubleshooting “4.3 Confirm Log Messages” (TRBL 04-0100) for the details of the warning messages.

When checking the status of a component through a message, a clicking on the “Warning Information” of the menu frame in the main window changes the screen to the one shown below and a detailed message explaining the component status is displayed.

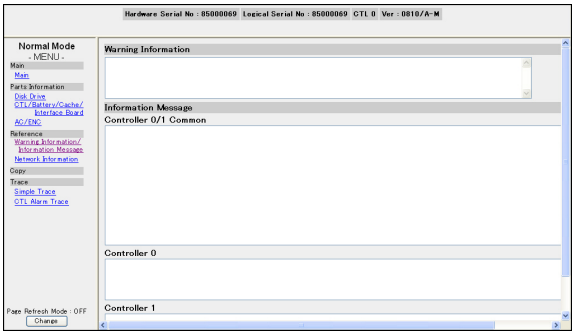


2.5 Information Message

The fault information and status information of the device that detected it in during the device operation are displayed.

The fault information and status information after the device booting are displayed in the Controller 0/1 Common box.
The fault information and status information as the device booting are displayed in the box of Controller 0 and Controller 1 every the controller.

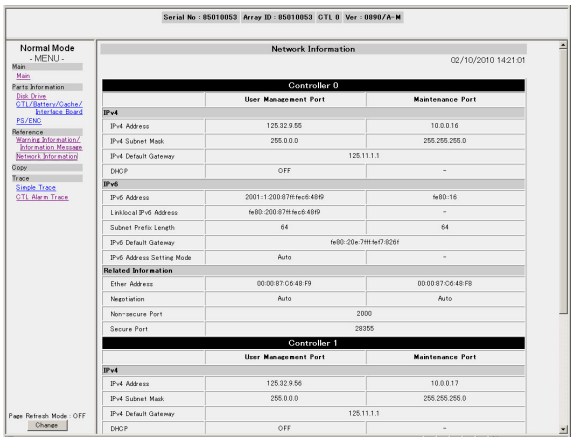
The Information Message screen is shown below.



2.6 Network Information

The set LAN Port Number is displayed.
Please click “LAN Port Number” of menu frame to enter into the LAN Port Number reference screen.

The LAN Port Number reference screen is shown below.



2.7 Collecting Simple Trace

This is a function to download current trace information.
To perform the down-load, a free capacity of approximately 40 M bytes is required in the PC.
Simple Trace needs to be collected from both controllers.

NOTE : When using IE 8.0, IE 9.0 or IE 10.0, the WEB window display may slow down and the collection of the trace from the WEB window may not complete. Uncheck the checkbox of "Enable SmartScreen Filter" in the Internet Options Advanced Settings. If the issue still occurs, please cancel the DNS Server's settings of the PC's LAN.

The first file name during the collection is as follows:

(i) When the firmware version is 0897/H or more;
Serial number and the trace collection starting time
(year/month/day/hour/minute/seconds) are added to the first file name.
smpl_trc0_xxxxxxxx_YYYYMMDDhhmmss_0E.dat

xxxxxxxx	: Trace collection serial number
YYYYMMDDhhmmss	: Trace collection starting time (year/month/day/hour/minute/seconds)

- The first file name when the collection from Control Unit #0 fits in a file
  "smpl_trc0_xxxxxxxx_YYYYMMDDhhmmss_0E.dat"
- The first file name when the collection from Control Unit #1 fits in a file
  "smpl_trc1_xxxxxxxx_YYYYMMDDhhmmss_0E.dat"
- The first file names when the collection from Control Unit #0 fits in two files
  "smpl_trc0_xxxxxxxx_YYYYMMDDhhmmss_0S.dat"
  "smpl_trc0_xxxxxxxx_YYYYMMDDhhmmss_1E.dat"
- The first file names when the collection from Control Unit #1 fits in two files
  "smpl_trc1_xxxxxxxx_YYYYMMDDhhmmss_0S.dat"
  "smpl_trc1_xxxxxxxx_YYYYMMDDhhmmss_1E.dat"
- The first file names when the collection from Control Unit #0 fits in three files
  "smpl_trc0_xxxxxxxx_YYYYMMDDhhmmss_0S.dat"
  "smpl_trc0_xxxxxxxx_YYYYMMDDhhmmss_1C.dat"
  "smpl_trc0_xxxxxxxx_YYYYMMDDhhmmss_2E.dat"
- The first file names when the collection from Control Unit #1 fits in three files
  "smpl_trc1_xxxxxxxx_YYYYMMDDhhmmss_0S.dat"
  "smpl_trc1_xxxxxxxx_YYYYMMDDhhmmss_1C.dat"
  "smpl_trc1_xxxxxxxx_YYYYMMDDhhmmss_2E.dat"

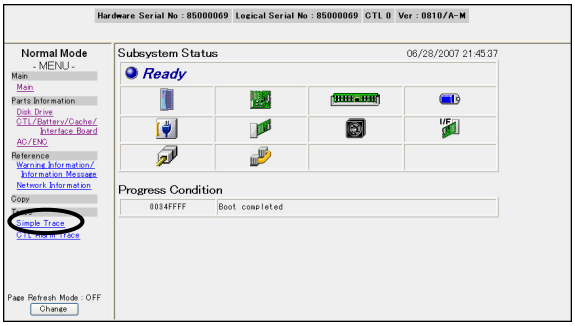
(ii) When the firmware version is 0890/A or more and less than 0897/H;

- The first file name when the collection from Control Unit #0 fits in a file
  “smpl_trc0_0E.dat”
- The first file name when the collection from Control Unit #1 fits in a file
  “smpl_trc1_0E.dat”
- The first file names when the collection from Control Unit #0 fits in two files
  “smpl_trc0_0S.dat”
  “smpl_trc0_1E.dat”
- The first file names when the collection from Control Unit #1 fits in two files
  “smpl_trc1_0S.dat”
  “smpl_trc1_1E.dat”
- The first file names when the collection from Control Unit #0 fits in three files
  “smpl_trc0_0S.dat”
  “smpl_trc0_1C.dat”
  “smpl_trc0_2E.dat”
- The first file names when the collection from Control Unit #1 fits in three files
  “smpl_trc1_0S.dat”
  “smpl_trc1_1C.dat”
  “smpl_trc1_2E.dat”

(iii) When the firmware version is less than 0890/A;

- The first file name during the collection from Control Unit #0
  “smpl_trc0.dat”.
- The first file name during the collection from Control Unit #1
  “smpl_trc1.dat”.

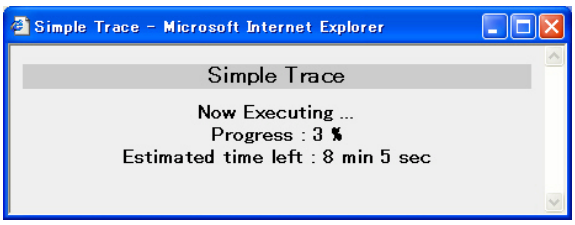
(1) Click “Simple Trace” in the menu frame.



(2) When the “Simple Trace” is clicked, the following window is displayed.

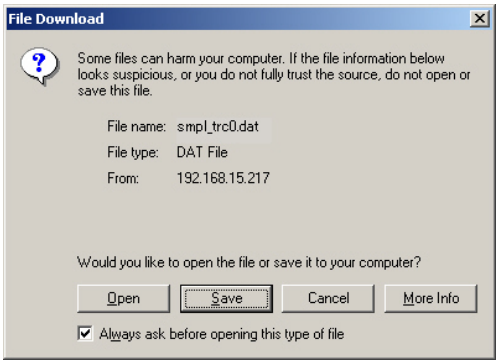
(3) When the [OK] button is clicked, the following window is displayed.

NOTE : If the window update (e.g.: pressing F5 key) is performed in this window, the automatic update stops and so that the trace collection does not make progress. When the automatic update stops due to the window update, close this window and, after 20 minutes or more elapse, perform the simple trace collection again.

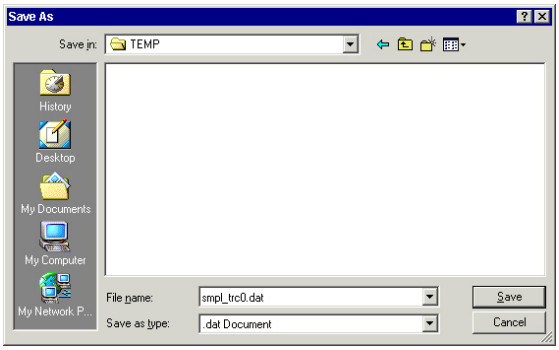


(4) The following window is displayed. Click the [Download] button.

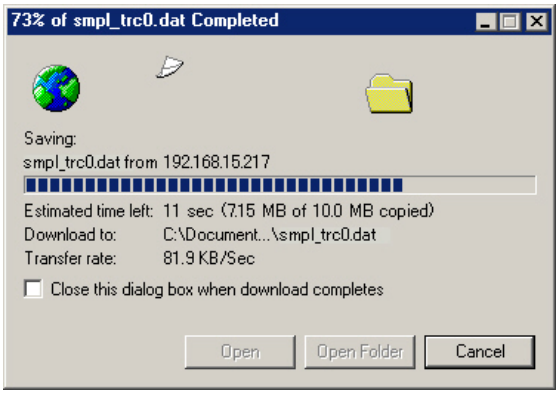
(5) Please click [Save], if it is continued. Please click [Cancel], if it is stopped.



(6) If the following window is displayed. Please click [Save] after file name is setting, if it is continued.(‡1) Please click [Cancel], if it is stopped.



(7) The following window is displayed during execution download.

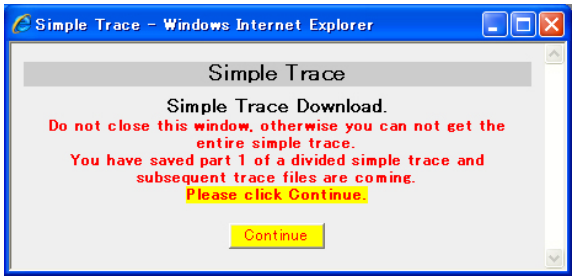


(8) When the downloading completes, the progress indicating message window is closed.

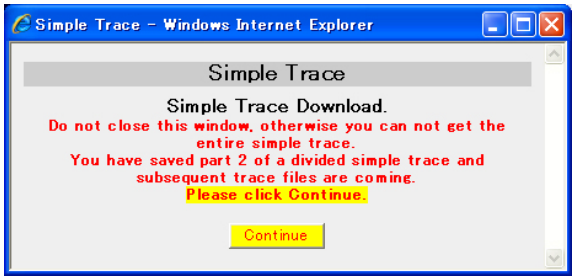
(9) If all traces cannot be collected, the following window is displayed.
Click the [Continue], and then collect traces in the next file beginning from the step (4).

NOTE : When performing an array boot or simple trace collection from the same Control Unit in the same array in the window shown below without clicking the [Continue], a error window is displayed, and the trace cannot be collected.

When all the traces can't be collected on the first time.



When all the traces can't be collected on the second time.

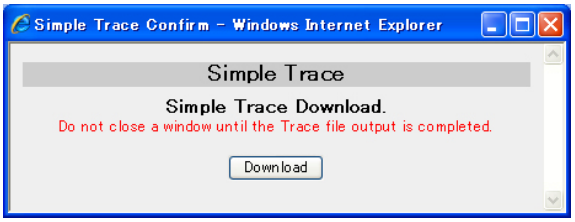


‡1 : There may be a case where the first file name is given as "smpl_trc0xxxx.dat.dat" depending on the setting of the PC. In this case, ".dat" is deleted or any other name.

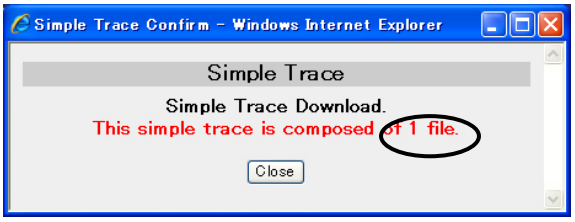
(10) The following window appears when all traces are collected.
Click the [Close] button.

NOTE : When the firmware version is 0890/A or more, verify that the number of files described in the window is the same as the number of the files actually collected.

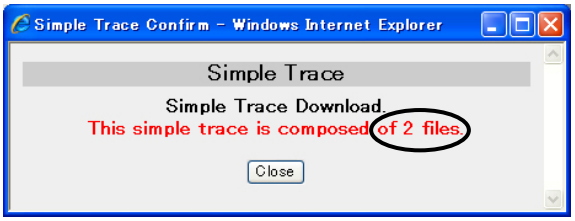
• When the firmware version is less than 0890/A



• When the firmware version is 0890/A or more
When all traces can be collected in one file



When all traces can be collected in two files



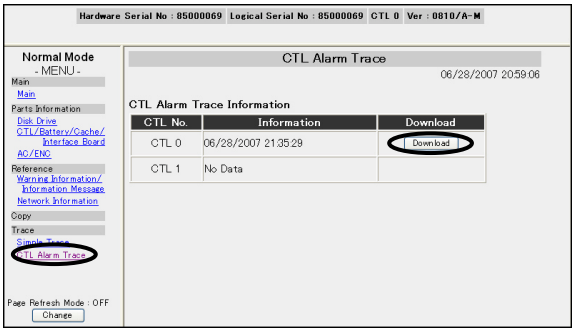
2.8 Collecting CTL Alarm Trace

Through the CTL Alarm Trace collection, detailed information (the CTL Alarm Trace) on the immediately Controller blockade stored in the Controller is collected. It may not be collected depending on the types of the failures which cause the controller blockade.

NOTE : When the Control Unit to be connected to WEB is blocked, the WEB connection may not be performed for ten minutes usually (for the maximum of 60 minutes) from the time when the Control Unit was blocked because the CTL alarm trace is being created.

Since the above-mentioned CTL Alarm Trace information is taken over from the blocked Control Unit to the replaced Control Unit, it can be collected after the Control Unit is recovered from the failure. Even after the collection, the information remains until the controller blockade trace is rewritten in the next controller blockade. If the Control Unit is blocked while collecting the CTL Alarm Trace may not be collected normally. Therefore, in this case, collect the CTL Alarm Trace again.
For collecting the CTL Alarm Trace, disk space of 520 M bytes per one Control Unit is required. (260 M bytes for temporary data and 260 M bytes for Full Dump data)
Collect CTL Alarm Trace from each Control Unit.
In order to distinguish from which Control Unit it is collected, store the collected data in different directories or with different file names.
The method of collecting the CTL Alarm Trace is shown below.

(1) Click “CTL Alarm Trace” in the menu frame.
The CTL Alarm Trace Information window is displayed when the CTL alarm trace information is present.

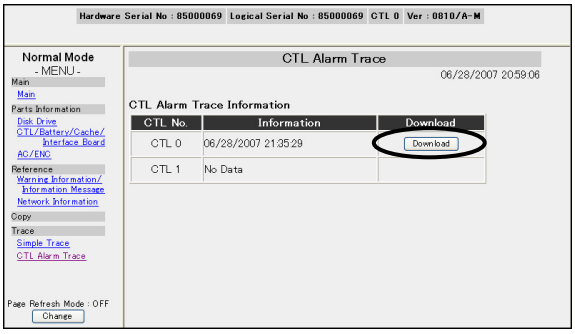


The following is displayed as contents of the information.

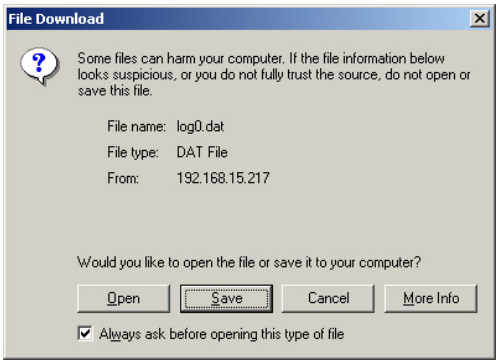
[Not Ready] .....: A status in which the trace area is not established in the subsystem
[Not Data] .....: A status in which the CTL Alarm trace information is not present or being generated
[MM/DD/20XY hh:mm:ss] .....: A status in which the CTL alarm trace information is present

NOTE : When “Not Ready” or “No Data” is displayed on the description of “Information”, or when the date of the information is different from that of the collection of this time, the CTL alarm trace may not be collected normally. Connect the Maintenance PC to the LAN port of the blocked Control Unit, and collect the simple trace.
If simple trace cannot be obtained through detached Controller, connect the Maintenance PC to the Controller at the opposite side, and collect the simple trace.

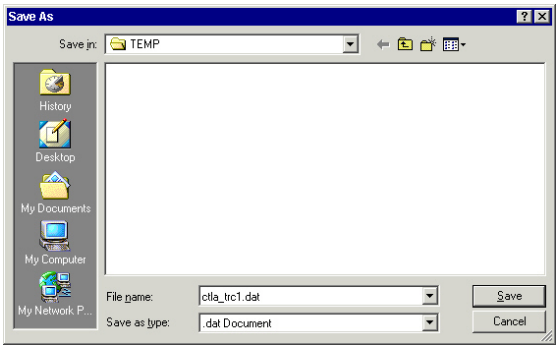
(2) To download the CTL Alarm trace information, press the “Download” button on the Control Unit side to be collected in “CTL Alarm Trace information”.



(3) The following window is displayed. Please click [Save], if it is continued. Please click [Cancel], if it is stopped.

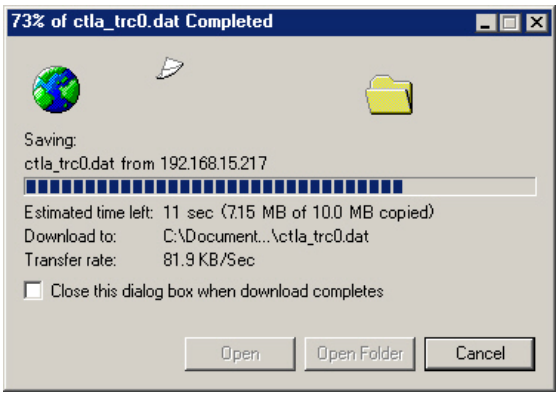


(4) If the following window is displayed. Please click [Save] after file name is setting, if it is continued.(‡1) Please click [Cancel], if it is stopped.



‡1 : There may be a case where the default file name is given as “ctla_trc0.dat..dat” depending on the setting of the PC. In this case, “.dat” is deleted or any other name.

(5) The following window is displayed during execution download.



(6) When the downloading completes, the progress indicating message window is closed.

2.9 Host Command Trace Download

The following conditions are necessary to download the host command trace.
The host command trace information is required to analyze by executing the performance measurement.
If the host command trace exceeds a certain range, the new information is overwritten, so that the old information is deleted and cannot be analyzed.
This function is to collect the command information from the host in the Maintenance PC at a maximum.

Use this function only when the performance analysis is required. Do not use it normally.

- The READY LED (green) on the Front Bezel lights on.
- For Firmware "1.3 Preparation for Installation of Firmware" (FIRM 01-0020) is performed and the Maintenance PC is set up.

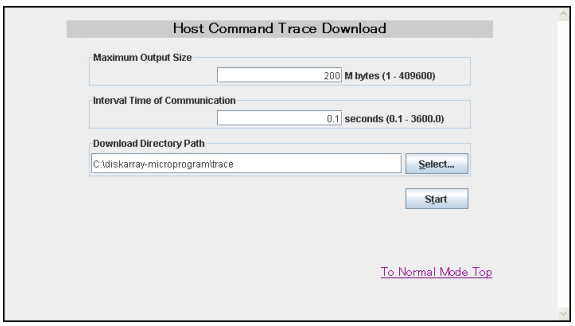
The data size of the host command trace that can be downloaded is affected by environments of the service PC and a LAN.
Therefore, it is recommended to do the downloading in the following environment.

- The downloading is done through the LAN port for maintenance.
- The LAN interface used by the Maintenance PC is 100Base-TX or the superior.

Incidentally, the size of the data that can be downloaded varies depending on the load of I/O's issued to the disk array system

(1) Display in the host command trace download window.
Enter "http://(IP address)/hcmd_trc" in the [Address] of the Web browser.
In the case of the dual system configuration, enter an IP address of any one of the control units. (Only the information of the input IP address is collected. If the information for both Control Units is required, start two Web browsers.)
A [User Name] and a [Password] may be requested at the time of Web connection or Web operation. In that case, input "maintenance" for the [User Name] and "hosyu9500" for the [Password].

(2) Input of “Maximum Output Size”, “Interval Time of Communication” and “Download Directory Path”.



[Maximum Output Size] : Check the empty drive space of the Maintenance PC and input the maximum output size (the initial value is 200 M bytes).

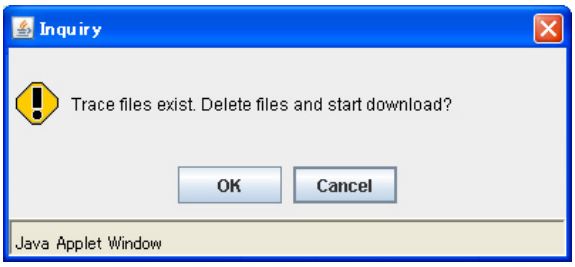
[Interval Time of Communication] : Input the interval time of downloading the host command trace (the initial value is 0.1 second).

[Download Directory Path] : Input the folder which stores the host command trace (the initial value is “C:\diskarray-microprogram\trace” and the folder can be selected by pressing the [Select] button).

- It is required to create the storage folder beforehand.
- The folder can be created only in the “C:\diskarray-microprogram” folder.
- The collected host command trace is divided into two or more files “hcmdtrc$p#_xxxxx.trc” ($: Control Unit number, #: port number, and xxxxx: following number) and output. When collecting the host command trace two or more times, create the folder in every case.

(3) Click the [Start] button to start the download.

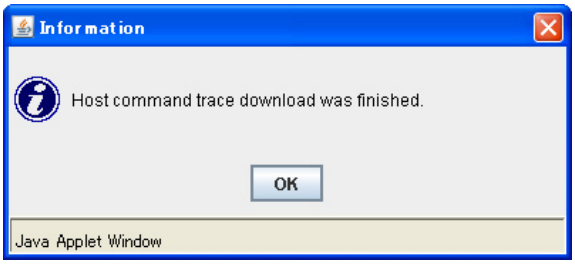
(4) The following window is displayed when the stored file exists.



Click the [OK] button.
Click [Cancel] if stopping it.

(5) The following window is displayed when executing the download.

(6) The following window is displayed when the download is completed.



If the [OK] button is clicked, the host command trace download window is displayed.

- Standard of the host command trace collection
  When collecting the host command trace, make the following a standard and set it.
  If the empty drive space of the host decreases, the system becomes unstable. Therefore, set the host command trace collection after checking the empty space.
  Also, when the command issue from the host exceeds the collectable IOPS, all the host commands are not collected.

$$\text{Required disk capacity (M bytes)} = \frac{\text{Host command trace collection time (second)}}{\text{Interval time of communication (second)}} \times 76.8 \text{ (k bytes)}$$

Table 2.12.1 Required Disk Capacity for Host Command Trace Collection (M bytes)

Communication interval (second) and the collectable IOPS / Collection time (second)	0.1 6000	0.2 3000	0.5 1200
1	0.8	0.4	0.2
10	7.7	3.8	1.5
60	46.1	23.0	9.2

The collection time and the disk capacity vary depending on the issue interval of the command from the host.

This page is for editorial purpose only.

Chapter 3. The Maintenance Mode Operation Procedure

3.1 Transferring to the Maintenance Mode

The method of making the subsystem enter the maintenance mode varies depending on the lighting status of the READY LED (green) and ALARM LED (red) on the front bezel (RKH/RKM/RKS).

- Do not make the work when the READY LED (green) on the Front Bezel is blinking at high speed. When it is high-speed blinking, the ENC firmware is being downloaded. Make the work after making sure that the READY LED (green) lights on after the maximum of 30 to 50 minutes (RKH: for the maximum of 40 to 60 minutes).
- Do not work when the WARNING LED (orange) on the front of the Basic Chassis is blinking at high speed. While this WARNING LED (orange) is blinking at high speed, the update of the flash program or the automatic download of the ENC firmware at the time of turning the power on in the single controller configuration is being executed. Perform the work after checking that this WARNING LED (orange) goes out in the maximum of 30 to 85 minutes, and the READY LED (green) on the front of the Basic Chassis lights up.
- When the READY LED (green) is on, proceed to the procedure starting from the step (2).
- When the ALARM LED (red) is on, wait for three minutes after making sure of the lighting of it, proceed to the procedure starting from the step (2).
- Also proceed to the procedure starting from the step (1) in the case where the READY LED (green) and ALARM LED (red) do not come on after waiting for ten minutes when the power is turned on.

(1) Make sure that the WARNING LED (orange) is not blinking fast. If it is blinking fast, wait for a while (80 seconds at the longest). It will cease to blink fast. There is no problem if it blinks slowly (at intervals of one second).

(2) Changing to the maintenance mode.

NOTE : In the subsystem where the Power Saving of the priced option is used, when RAID group whose power saving status is "Normal (command monitoring)" exists, do not change to the Maintenance Mode. Change to the Maintenance Mode after completing the spin-down, or have the user perform the spin-down or spin-up instruction, and then change to the Maintenance Mode after there is no RAID group whose power saving status is "Normal (command monitoring)".

• Single Controller

Press the RST SW of the single Control Unit. (While pressing RST SW, the RST LED (orange) is on.) Use a tool with a thin tip (a precise screwdriver, etc.) because the hole of RST SW is small (3 mm in diameter).

• Dual Controller

(a) Press the RST SW of the Control Unit #0. (While pressing RST SW, the RST LED (orange) is on.) Use a tool with a thin tip (a precise screwdriver, etc.) because the hole of RST SW is small (3 mm in diameter).

(b) Wait for a while (about ten seconds) and check that the ALM LED (red) of the Control Unit lights up. Within ten seconds after the ALM LED (red) lights up, press the RST SW of the other Control Unit.
When the ALM LED (red) of the Control Unit #0 does not go out in spite of the above operation, turn off the main switch and disconnect the power cable, and then connect the power cable and turn on the main switch without pulling out or inserting the Control Unit. After that, return to step (1) and execute the procedure over again.

NOTE : Because the Control Unit is shutdown status for the Maintenance Mode, the command from the host is impossible execution. Rebooting of the Control Unit is required for the return.

When ALM LED (red) on Control Unit#0 turns off and READY LED (green) on Front Bezel turns off, it transfers to Maintenance mode.

(c) Start the setting after making sure that the subsystem has entered the Ready status.

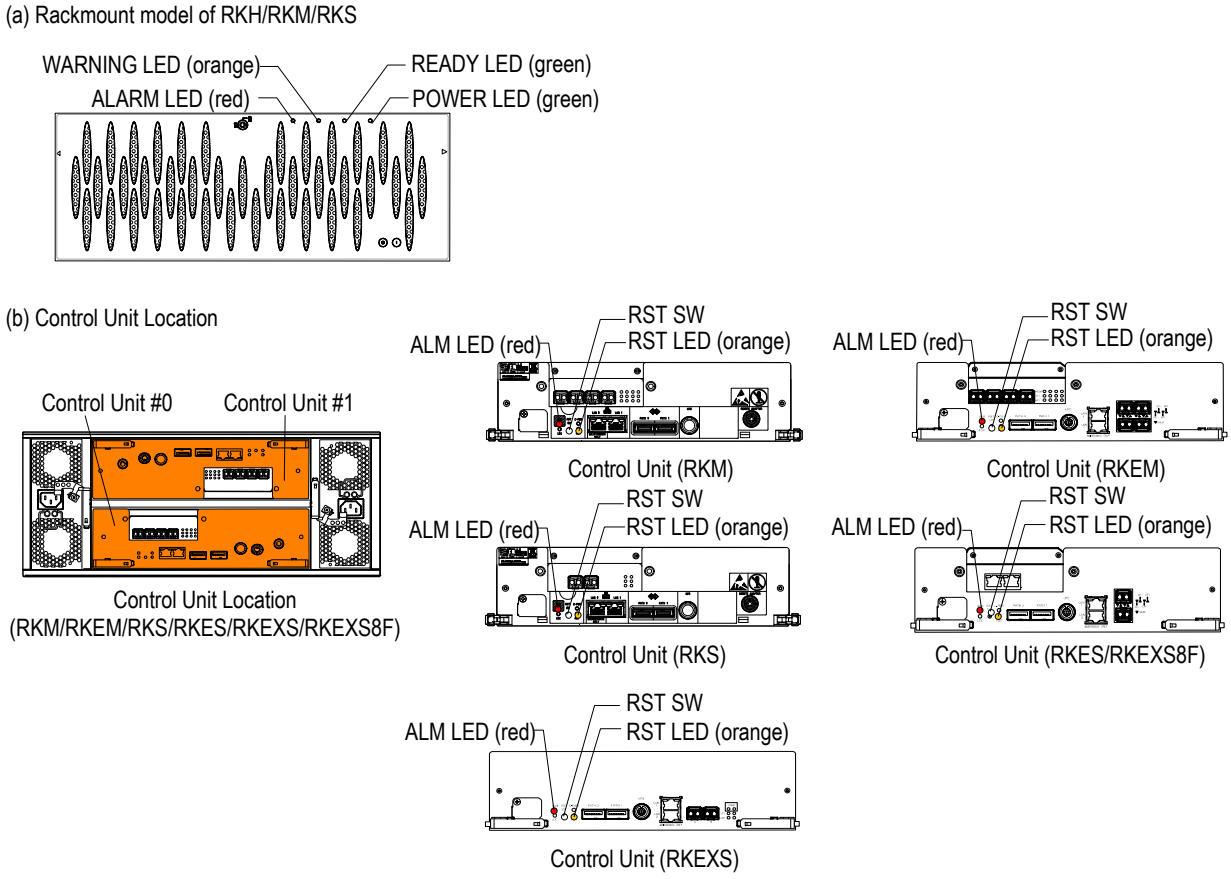


Figure 3.1.1 Indication Position

NOTE : • Set the TCP/IP to “Disable DNS” because the connection takes a long time when the TCP/IP of the network is set to the condition in which the DNS is used. For the setting procedure, refer to the instruction manual of the PC to be used.

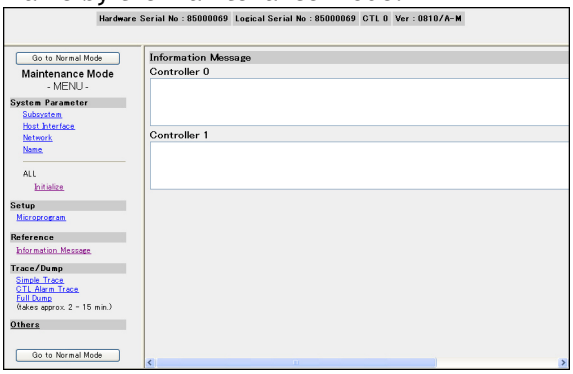
• Make sure that the browser is set to the condition in which the proxy server is not used because the connection cannot be done if the proxy server is set to be used. To make sure the setting, refer to the instruction manual of the browser to be used.

(3) Please input the IP Address of the Control Unit where it was connected with the network to the browser. Please input the page by the update button of the browser if it has already been connected with WEB.

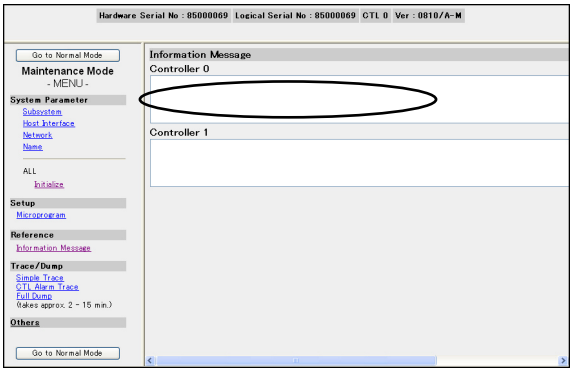
NOTE : The contents that were set up with “System Parameter” and the firmware that was installed with “Setup” come into effect after the rebooting of the Control Unit.

A [User Name] and a [Password] may be requested at the time of Web connection or Web operation. In that case, input “maintenance” for the [User Name] and “hosyu9500” for the [Password].

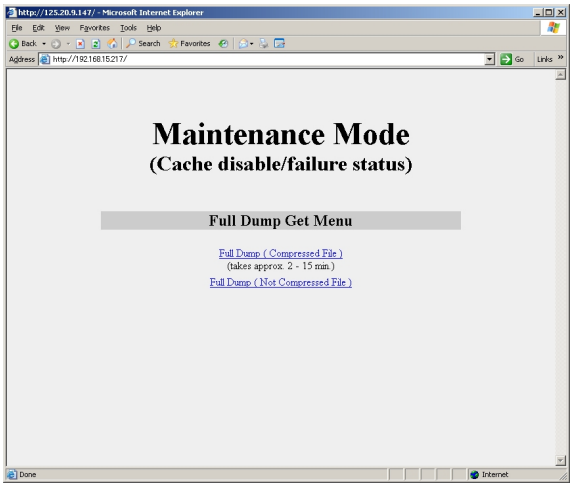
(4) Usually, the following window is displayed in the browser.
For RKEXSA/RKEXSB in the nomal mode of web, the (E-XSi) is not displayed of right side of version frame by the maintenance mode.
For RKEXS8F in the nomal mode of web, the (E-XS) is not displayed of right side of version frame by the maintenance mode.



When this window is displayed in the browser, check if the “Series No” and the “CTL number”, which are displayed in the upper part of the window, match with the device number and the CTL number of the subsystem to be connected to WEB. The WEB connection in the maintenance mode is completed when these are matched. If not matched, the specification of the IP address at the WEB connection is incorrect. Enter the correct IP address of the Control Unit to be connected to WEB in the browser again.

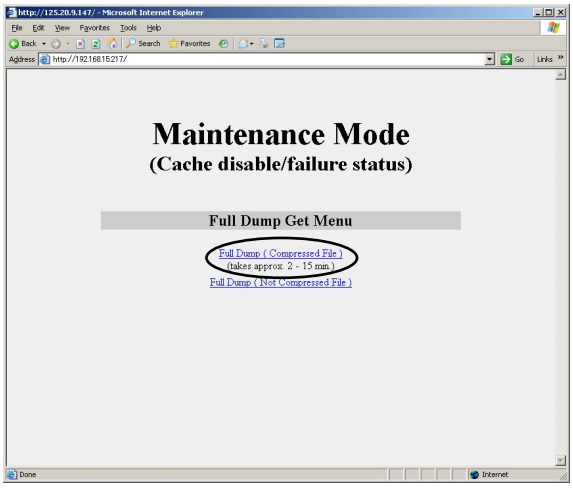


Also, when the Cache memory access failure occurs, in the Control Unit connected to WEB, the following window is displayed in the browser. At this time, refer to “3.1.1 WEB Operation in the Maintenance Mode During the Cache Memory Access Failure” (WEB 03-0050).



3.1.1 WEB Operation in the Maintenance Mode During the Cache Memory Access Failure

The message display and the setting operation do not function during the Cache memory access failure. Select “Full Dump (Compressed File)” on the window, and collect Full Dump. And then, contact the Technical Support Center.



* The time displayed on the window changes by the model or the status of the subsystem.

Also, connect WEB to the other Control Unit, and continue the maintenance work for the dual Control Unit system.

3.2 Reference/Setting of the System Parameter and Initialize

System Parameter is being classified to the following group and selecting each group executes the reference/setting and Initialize.

(1) Subsystem
Reference and setting of the system parameter regarding the Subsystem is executed (refer to "3.2.1 Subsystem" (WEB 03-0070)).

(2) Host Interface
Reference and setting of the system parameter regarding the host interfacing are executed (refer to "3.2.2 Host Interface" (WEB 03-0120)).

(3) Network
Reference and setting of the system parameter regarding the network are executed (refer to "3.2.3 Network" (WEB 03-0160)).

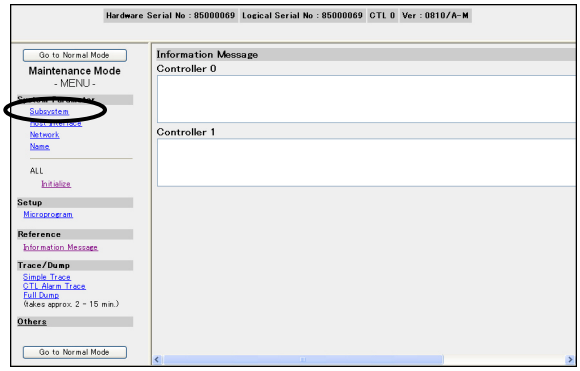
(4) Name
Reference and setting of the system parameter such as the Vendor ID, Product ID, Controller Name are executed (refer to "3.2.4 Name" (WEB 03-0210)).

(5) ALL
The system parameter information is initialized. (refer to "3.2.5 ALL" (WEB 03-0250)).

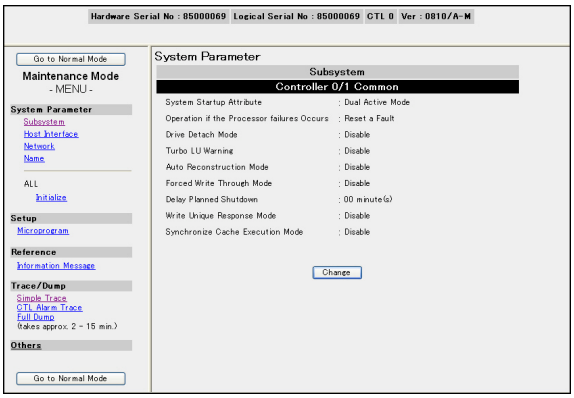
3.2.1 Subsystem

This function sets up/refer to the item regarding the Subsystem in the device.

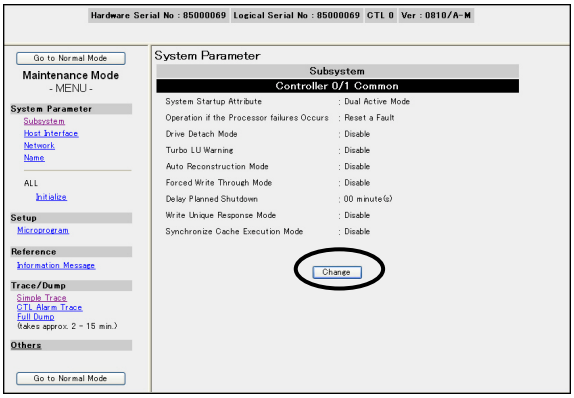
(1) Please click “Subsystem”.



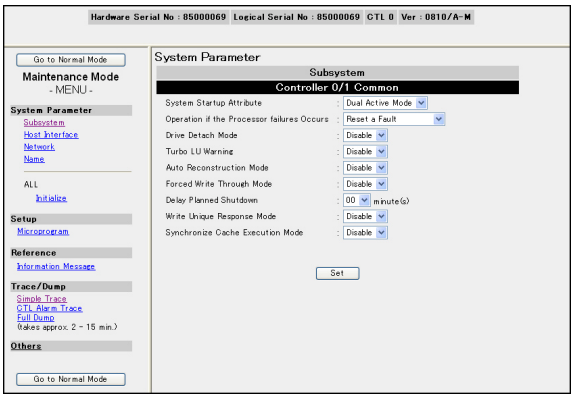
(2) The present setting value (the current value) is displayed.



(3) Please click [Change] for the setting.
Please click [Back] of the browser for the unsetting.



(4) Please select the item that is set up from the pull-down menu of the corresponding item that is set up. At this time, please set up the item that is set up all.



Explanation with regard to each item

[Controller 0/1 Common]

- System Startup Attribute
  The System Operation Attribute is designated.
  [Single Mode] : This is Single controller configuration.
  [Dual Active Mode] : This is Dual controllers configuration.

- Operation if the Processor failures Occurs
  The operation as the processor fault occurrence is designated.
  [Reset a Fault] : A fault is reset.
  [Shutdown the System] : The controller is shutdown.

- Drive Detach mode
  The Drive Shutdown Mode is designated.
  [Enable] : The Drive Shutdown Mode is effectively.
  [Disable] : The Drive Shutdown Mode is ineffectively.

- Turbo LU Warning
  Suppression of the R/W command operation regarding the LU concerned for the case where the Turbo LU Residence function becomes ineffective is set.
  [Enable] : The operation is suppressed.
  [Disable] : The operation is not suppressed

- Auto Reconstruction Mode
  The Auto Reconstruction Mode (Data restoration to a spare drive to be done when a drive is pulled out) is designated.
  [Enable] : The Auto Reconstruction Mode is effectively.
  [Disable] : The Auto Reconstruction Mode is ineffectively.

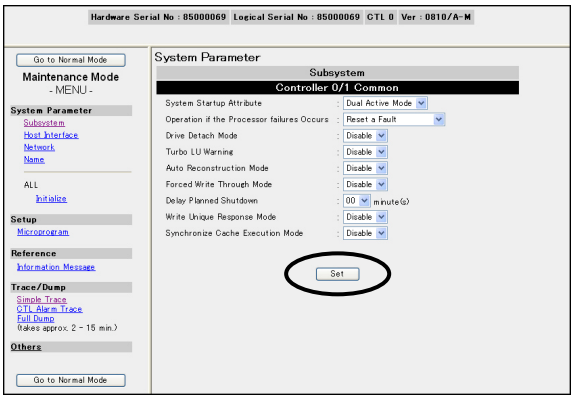
- Forced Write Through Mode
  The Forced Write Through Mode is designated.
  [Enable] : The Forced Write Through Mode is effectively.
  [Disable] : The Forced Write Through Mode is ineffectively.

- Delay Planned Shutdown
  The Delay Planned Shutdown (Time from the power switch turning off to the deliberate shutdown) is designated. 00 to 60 minute

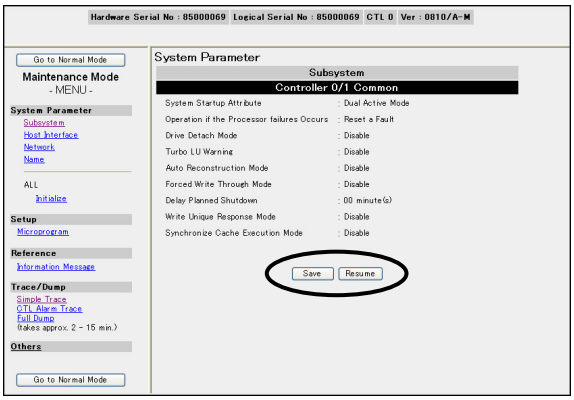
- Write Unique Response Mode
  Specify this when setting the Write Unique Response Mode.
  [Enable] : The Write Unique Response Mode is effectively.
  [Disable] : The Write Unique Response Mode is ineffectively.

- Synchronize Cache Execution Mode
  This is specified when the Synchronize Cache command is executed.
  [Enable] : The Synchronize Cache Execution Mode is effectively.
  [Disable] : The Synchronize Cache Execution Mode is ineffectively.

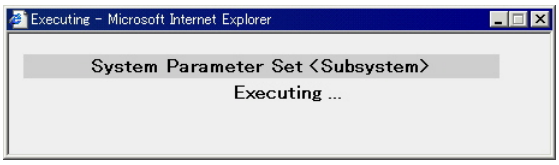
(5) Please click [Set] after setting completion.



(6) The screen that confirms the following setting contents is displayed.
Please click [Save] if the setting is correct. Please click [Resume] if the setting contents are changed.



(7) If [Resume] is clicked, it returns to the setting window of before. If [Save] is clicked, the following window is displayed.



(8) The following window is displayed at the later time for a while.
Please click [OK], if the setting is continued. Please click [Cancel], if the setting is stopped.
If [Cancel] was clicked, the system parameter is not set up.

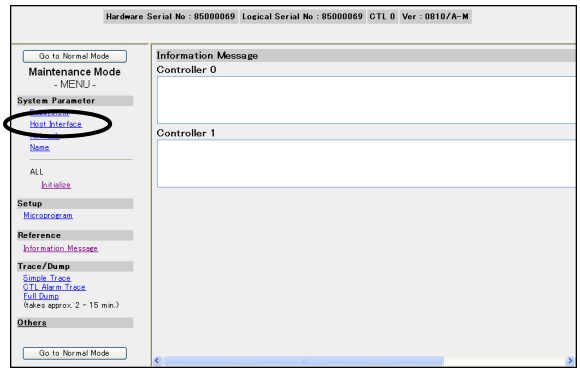
(9) If [OK] is clicked, the following window is displayed.

(10) If the following window is displayed at the later time for a while, the setting is completion.
If [OK] is clicked, it returns to the menu.

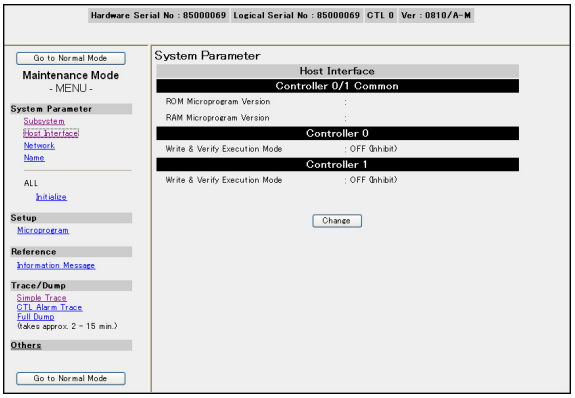
3.2.2 Host Interface

This function sets up/refer to the item regarding the host interfacing of the device.

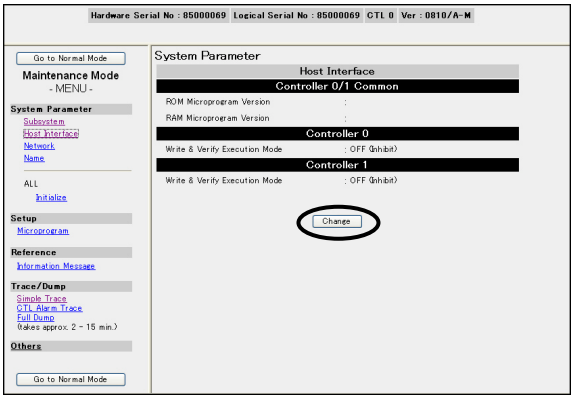
(1) Please click “Host Interface”.



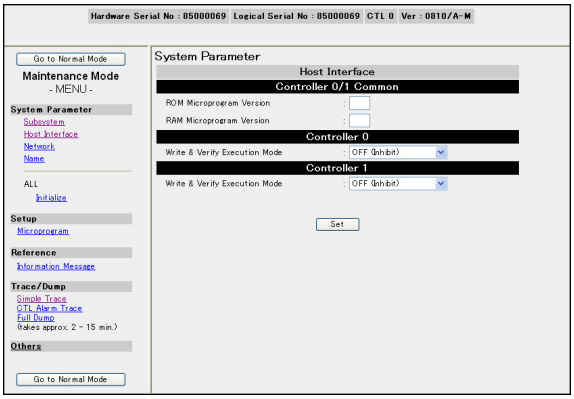
(2) The present setting value (the current value) is displayed.



(3) Please click [Change] for the setting.
Please click [Back] of the browser for the unsetting.



(4) Please select the item that is set up from the pull-down menu of the corresponding item that is set up. At this time, please set up the item that is set up all.



Explanation with regard to each item

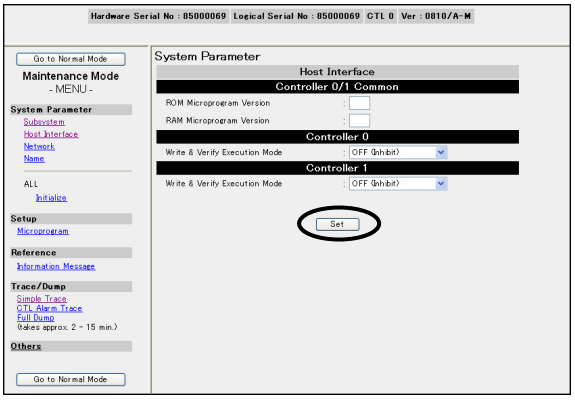
[Controller 0/1 Common]

- ROM Microprogram Version :
  The response value of Product Revision Level (ROM Microprogram Version) in the Inquiry command is shown.
- RAM Microprogram Version :
  The response value of Product Revision Level (RAM Microprogram Version) in the Inquiry command is shown.

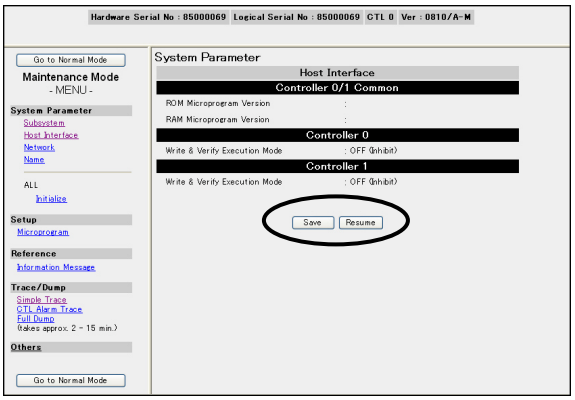
[Controller]

- Write & Verify Execution Mode
  The operations inside the Write & Verify command from the host are shown.
  [ON (Does not inhibit)] : The Write & Verify are executed.
  [OFF (Inhibit)] : This is executed and replace to the Write.

(5) Please click [Set] after setting completion.



(6) The screen that confirms the following setting contents is displayed.
Please click [Save] if the setting is correct. Please click [Resume] if the setting contents are changed.



(7) If [Resume] is clicked, it returns to the setting window of before. If [Save] is clicked, the following window is displayed.

(8) The following window is displayed at the later time for a while.
Please click [OK], if the setting is continued. Please click [Cancel], if the setting is stopped.
If [Cancel] was clicked, the system parameter is not set up.

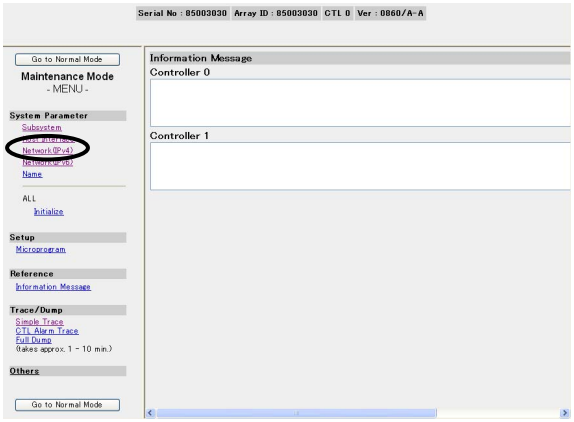
(9) If [OK] is clicked, the following window is displayed.

(10) If the following window is displayed at the later time for a while, the setting is completion. If [OK] is clicked, it returns to the menu.

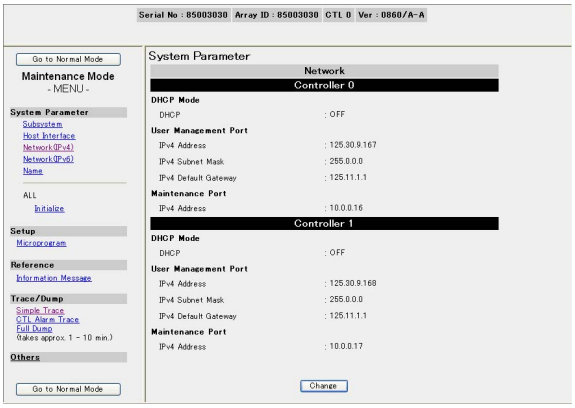
3.2.3 Network

This function sets up/refer to the item regarding the network (Setting the user management LAN port) of the device.

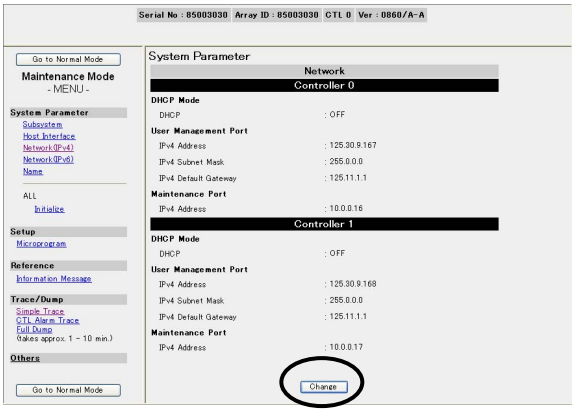
(1) Please click “Network (IPv4)”.



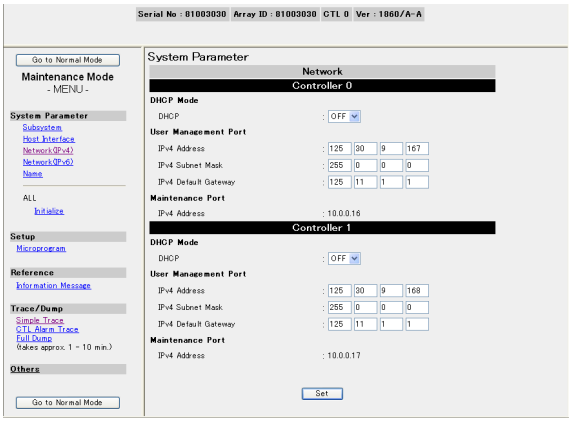
(2) The current IPv4 address setting value (current value) is displayed.



(3) Please click [Change] for the setting.
Please click [Back] of the browser for the unsetting.



(4) Please set up/select the corresponding item that is set up from the pull-down menu or input them.
At this time, please set up the item that is set up all.



Explanation with regard to each item

[Controller 0]/[Controller 1]

- DHCP Mode

  DHCP : The DHCP function (‡1) is specified.

  [OFF] : Invalid the DHCP mode.

  [ON] : Valid the DHCP mode.

- User Management Port

  IPv4 Address : Sets the IPv4 ADDRESS.

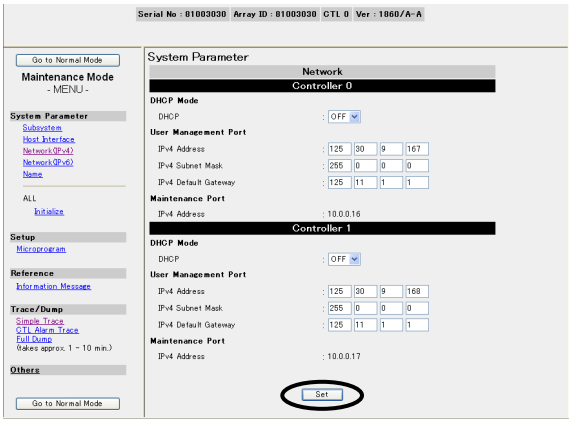
  IPv4Subnet Mask : Sets the IPv4 Subnet Mask.

  IPv4Default Gateway : Sets the IPv4 Default Gateway.

- Maintenance Port

  IPv4 Address(‡2) : The IPv4 address of the maintenance port, which is currently set, is displayed. It cannot be changed.

(5) Please click [Set] after setting completion.

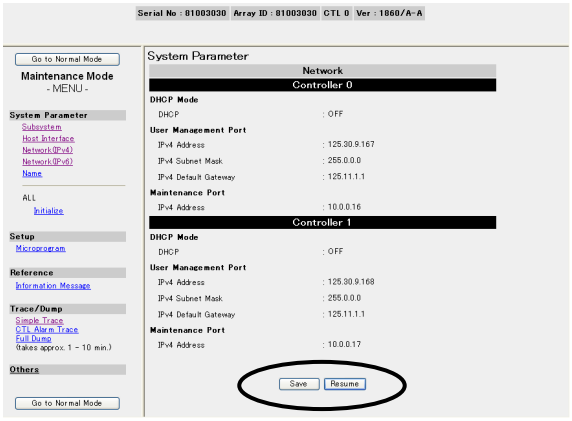


‡1: When DHCP mode is valid, IP address is obtained from the DHCP server.
When the DHCP server has not started up or DHCP function has been miss-set, obtaining the IP address fails and the device IP address remains to be “0.0.0.0”. (Hitachi Storage Navigator Modular 2 or WEB cannot be used via LAN.)
In this case, the device IP address can be obtained by starting up the DHCP server or setting DHCP function correctly if necessary.
In the configuration which uses this subsystem as an external Disk Drive of the DHCP server, when the IP address of this subsystem is acquired using the DHCP function, if the network address of the reserved IP address for the maintenance port is assigned as an IP address, the IP addresses of the port for the user control and the port for the maintenance may not operate normally because they compete.
Request the system administrator that the DHCP server does not assign IP address of “10.0.0.x”, “192.168.0.x”, “192.168.233.x”, “172.23.211.x”, “10.197.181.x” to the device.

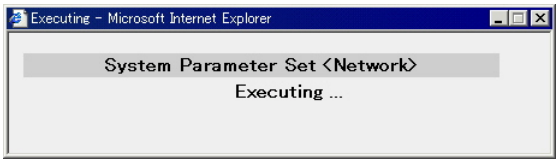
‡2: The IP address with the same network address as the displayed IP address of the maintenance port cannot be set. Also, set up the network after restarting the subsystem and setting the IP address of the maintenance port (refer to System Parameter “4.2 (4) Settig of Maintenance LAN” (SYSPR 04-0160)) when the IP address of the maintenance port is displayed as “0.0.0.0”.

‡3: IPv6 address cannot be set on WEB (reference only). When setting IPv6 address, set it from Hitachi Storage Navigator Modular 2.

(6) The screen that confirms the following setting contents is displayed.
Please click [Save] if the setting is correct. Please click [Resume] if the setting contents are changed.

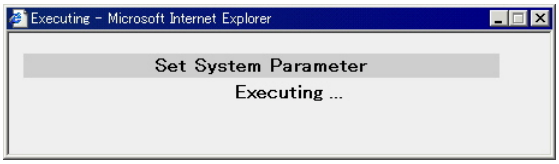


(7) If [Resume] is clicked, it returns to the setting window of before. If [Save] is clicked, the following window is displayed.



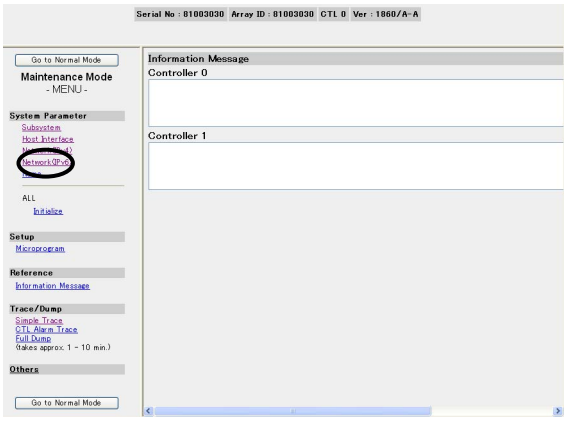
(8) The following window is displayed.
Please click [OK], if the setting is continued. Please click [Cancel], if the setting is stopped.
If [Cancel] was clicked, the system parameter is not set up.

(9) If [OK] is clicked, the following window is displayed.

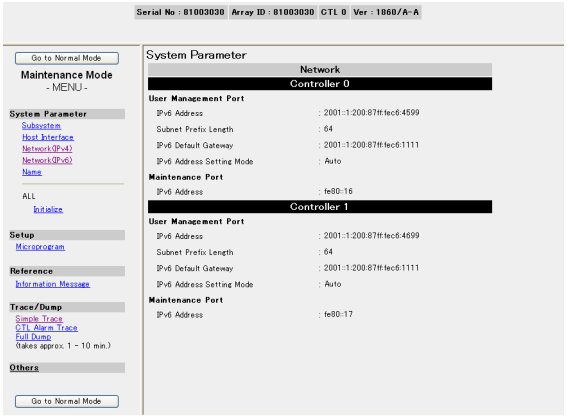


(10) If the following window is displayed at the later time for a while, the setting is completion.
If [OK] is clicked, it returns to the menu.

(11) Click “Network (IPv6)”.



(12) The current IPv6 address setting value (current value) is displayed.

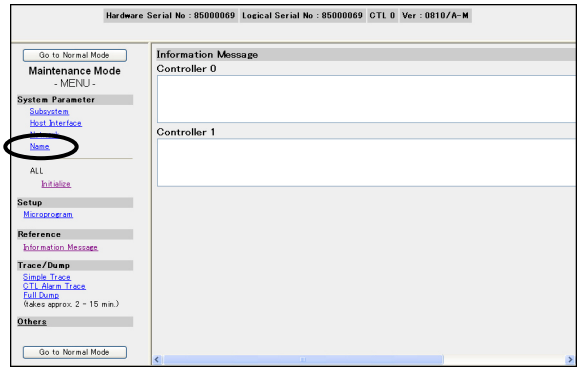


NOTE : IPv6 address cannot be set on WEB (reference only). When setting IPv6 address, set it from Hitachi Storage Navigator Modular 2.

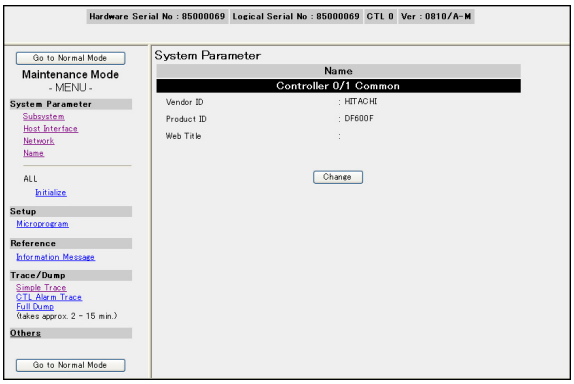
3.2.4 Name

This function can set up/refer to the item of the vendor name, model name etc. of the device.

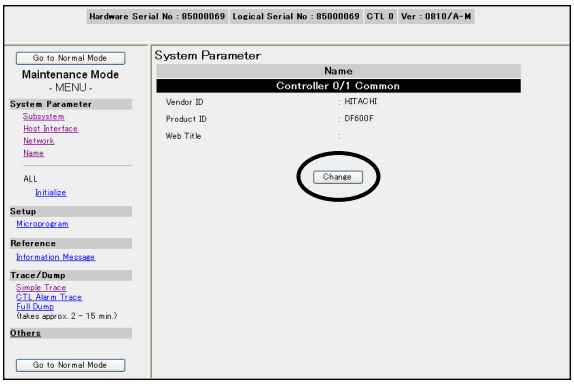
(1) Please click “Name”.



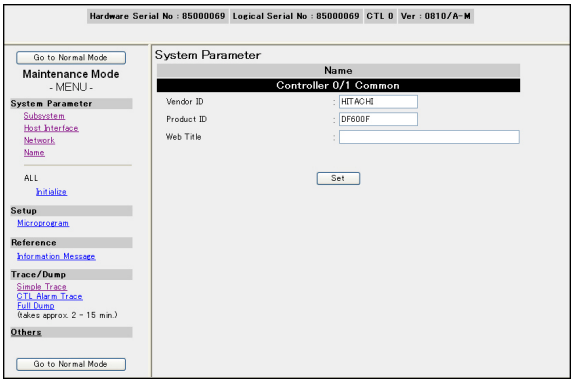
(2) The present setting value (the current value) is displayed.



(3) Please click [Change] for the setting.
Please click [Back] of the browser for the unsetting.



(4) Please set up/select the corresponding item that is set up from the pull-down menu or input them.
At this time, please set up the item that is set up all.

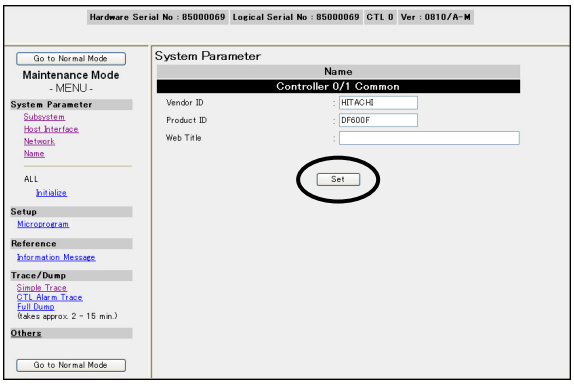


Explanation with regard to each item

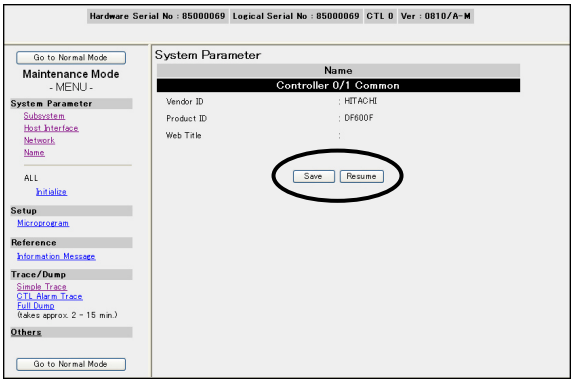
[Controller 0/1 Common]

- Vendor ID
  The vendor name that is reported with the Inquiry command is set up.
- Product ID
  The model name that is reported with the Inquiry command is set up.
- Web Title
  Sets the Web Title.

(5) Please click [Set] after setting completion.



(6) The screen that confirms the following setting contents is displayed.
Please click [Save] if the setting is correct. Please click [Resume] if the setting contents are changed.



(7) If [Resume] is clicked, it returns to the setting window of before. If [Save] is clicked, the following window is displayed.

(8) Please click [OK], if the setting is continued. Please click [Cancel], if the setting is stopped. If [Cancel] was clicked, the system parameter is not set up.

(9) If [OK] is clicked, the following window is displayed.

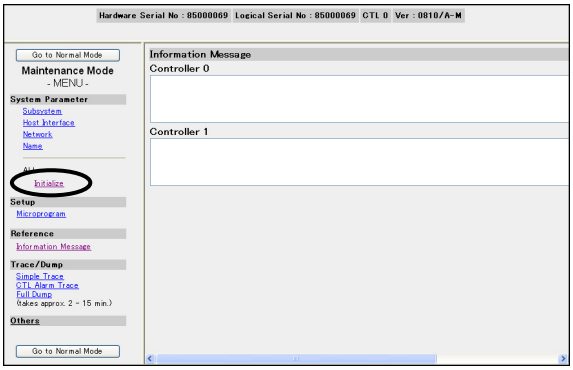
(10) If the following window is displayed at the later time for a while, the setting is completion. If [OK] is clicked, it returns to the menu.

3.2.5 ALL

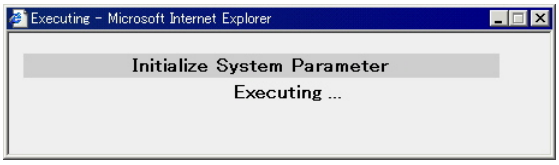
(1) Initialize

This function sets up the system parameter information of the device to the initial state.
If this function was executed, the resetting of the system parameter becomes needed, because the system parameter becomes the initial state.

(a) Please click “Initialize”.

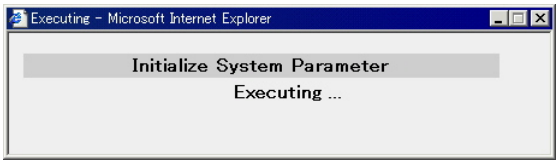


(b) If [Initialize] is clicked, the following window is displayed.



(c) If the following confirmation message is displayed for a while. Please click [OK], if it is continued.

(d) If [OK] is clicked, the following window is displayed.



(e) The system parameter becomes the initial state, the following window is displayed.
If [OK] is clicked, it returns to the menu.

3.3 Setup

3.3.1 Microprogram

This function installs firmware of the subsystem. There are two types of installation as shown below.

- Update installation ..... To install the firmware with configuration information and system parameters taken over
- Initial setting up ..... To install the firmware with configuration information and system parameters cleared

When the version of the firmware is downgraded, click “Others” of the menu frame beforehand and display the “Others” window, and then check “Down Grade Check” of the displayed main frame for [Disable]. Change “Current” to “Disable” of “Down Grade Check” by clicking the [Change] button. (Refer to “3.6 Others” (WEB 03-0530).)

(1) Set Up for the Maintenance PC

(a) Outline

Set up the Maintenance PC before installing the firmware. The setting up is completed when the installer stored in the CD-ROM of the firmware is executed. Outline of the setting up is shown below

- Installation of the JRE 6 update 10
- Creating the "C:\diskarray-microprogram\microprogram" folder and setting the security

(b) Prerequisites for setting up of a Maintenance PC

Prerequisites concerning the user ID of Windows are as follows.

- The user ID of Windows at the time when the firmware is installed in the Maintenance PC must be identical with that at the time when a maintenance work is done.
- The user ID mentioned above must be defined not with full size Japanese characters but with half size alphabetic characters and/or numerals.

A prerequisite of a drive for booting the OS of the Maintenance PC

- The drive for booting the OS must be the c drive.

(c) Java error codes displayed at the time of update installation and actions for coping with them.

When the PC does not satisfy the prerequisite shown in Item (b) Prerequisites for setting up of a Maintenance PC. Details of the Java errors and actions for coping with them are shown below.

If the message code of the Java error that occurred does not exist in Table 3.3.1, refer to Message "Chapter 7. Web Error Messages" (MSG 07-0000).

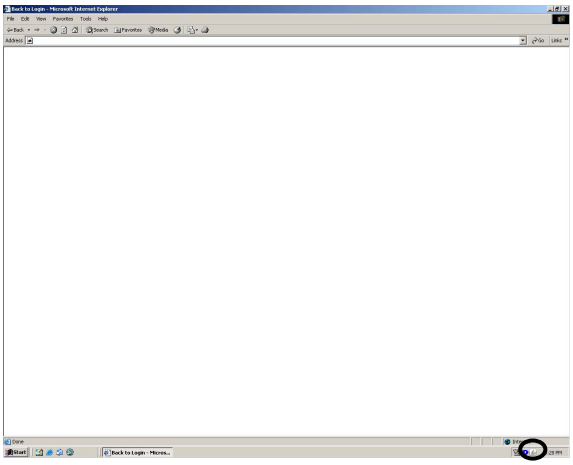
Table 3.3.1 Java Error Codes

Message code	Message text	Time when the error occurs/ Cause estimated	Action for coping with the error
1216	Access to the property information was rejected. Confirm the setup of the security policy.	Time when the error occurs • The error occurs immediately after the [Select] key is pressed when the firmware is selected. Cause estimated • A drive for booting the OS is not the c drive. • The user name of Windows at the time when the firmware was installed in the Maintenance PC is not identical with that at the time when the firmware is updated, or two-byte characters (full size characters or Japanese characters) are used to define the user name	① Check if the drive for booting the OS is the c drive. (Refer to the (c) (i) Method for checking the drive for booting the OS (WEB 03-0300).) In the case of the dual boot, boot Windows using the c drive and perform the installation again. ② Check if the user name of Windows at the time when the firmware is installed in the Maintenance PC is identical with that at the time when the firmware is updated and if two-byte characters (such as full size characters and Japanese characters) are not used. If an illegal specification has been made, perform the logon over again using an appropriate user name and perform the installation again after connecting the browser.
1219	An error occurred during the communication with the subsystem. Confirm the subsystem status and the LAN environment.	Time when the error occurs • The error occurs when the resource for the LAN cannot be ensured. Cause estimated • The error occurs because the resource (memory) of the Maintenance PC is insufficient.	① Reboot the subsystem and the Maintenance PC and quit unnecessary application programs. Make sure that the subsystem is in the Ready status, place the subsystem in the Maintenance mode, and perform the installation again. ② If the error recurs in spite of the operations above, replace the Maintenance PC and perform the installation over again from the beginning. Use a Maintenance PC whose memory capacity is as large as possible.

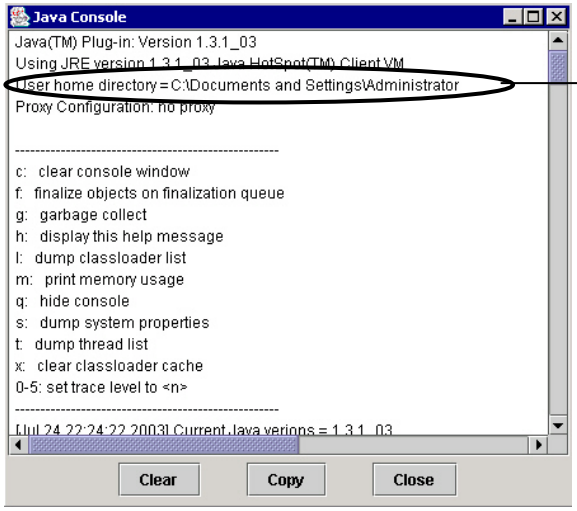
(i) Method for checking the drive for booting the OS

A method for checking the boot drive when the Java message (message code: 1216) is issued is shown below.

① Right-click [: Java Icon] on the task tray at the lower right of the service PC window, and click [Open Console].



② Since the JavaConsole window opens, make sure that the [User Home Directory] is the c drive (=C: *****…).



If "=C:***** …" is displayed here, the boot drive is the c drive.

(d) Procedure for setting up the Maintenance PC

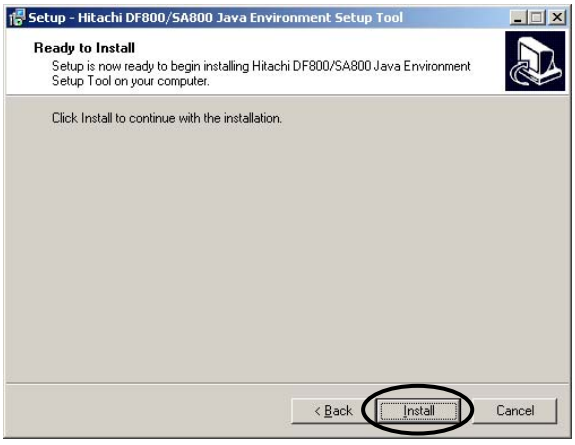
NOTE : When using Windows Vista, Server 2008, the Hitachi DF800/SA800 Java Environmental Construction Tool Version 2.0 or more and JRE 6 Update10 are required (JRE 6 Update10 is included in the DF800/SA800 Java Environmental Construction Tool Version 2.0 or more).

(i) When JRE 6 or JRE of other version than JRE 6 Update10 is installed in the service PC, the firmware may not be replaced normally. If JRE 6 or JRE of other version than JRE 6 Update10 is installed, be sure to uninstall the JRE, and then install the Hitachi DF800/SA800 Java Environmental Construction Tool.
Open [Setting] – [Control Panel] from the start menu of Windows, and delete the JRE by "Addition and Deletion of Applications" to uninstall the JRE.

(ii) Install the "DF800JSetup10e.exe" for firmware installation. (You can get "DF800JSetup10e.exe" from maintenance tools CD-ROM)

(iii) The initial window of the setting up appears.
The confirmation window is displayed. Click the [Next] button.

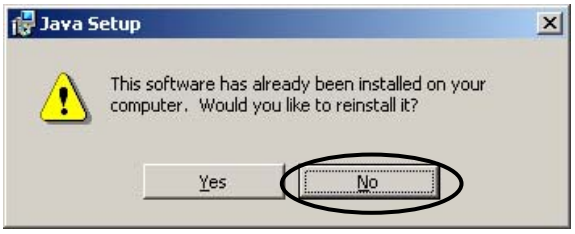
(iv) Start the installation.
Preparation for the installation is completed. The confirmation window is displayed. Click the [Install] button.



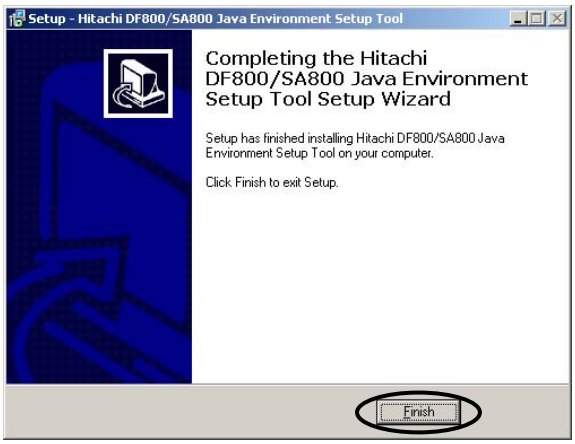
(v) Install JRE 6.
The confirmation window is displayed. Check the license agreement and click the [Accept] button.

(vi) Click the [Finish] button.

(vii) When JRE 6 or JRE 6 Update10 is already installed, the next window is displayed. Click the [No] button, and go to the next step.



(viii) The setting up is completed. Press the [Finish] button.



This page is for editorial purpose only.

(e) Notes

(i) Note that the settings of the security policy file is changed when the Maintenance PC is set up.

(ii) Do not change a name of the unified version directory(‡1) or directory in a stratum under the unified version directory. The firmware becomes unable to be installed if the directory name is changed.

‡1 : For the unified version directory, refer to "3.3.1 (2) Hierarchy of Firmware Storage Directories" (WEB 03-0340).

(2) Hierarchy of Firmware Storage Directories

The firmware is stored as the compression format (zip file) in the CD-ROM for firmware installation. Since the firmware (zip file) is stored under "program\microprogram" in the CD-ROM for firmware installation, store the ZIP file from the CD-ROM under the directory "C:\diskarray-microprogram\microprogram" and unzip it.

Table 3.3.2 CD-ROM Directory Hierarchy

First stratum	Second stratum	Third stratum
manual	HostInst	Manual file
	UG	
program	Microprogram	Firmware zip file
	DF800JSetup10e.exe (Java setup file)	-

The hierarchical structure of firmware storage ZIP file (08xxx.zip) directories is shown in Table 3.3.3.

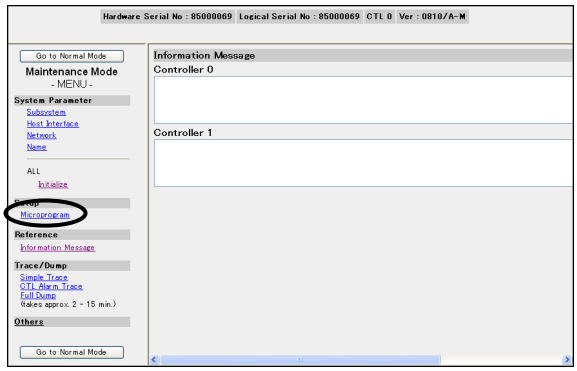
Table 3.3.3 ZIP File Directory Hierarchy

First stratum	Second stratum	Third stratum	Fourth stratum
Unified version (Example: 0810A)	DF800EH	disk 01 - disk X	Firmware file
		fmins	
	DF800EM	disk 01 - disk X	Firmware file
		fmins	
	DF800ES	disk 01 - disk X	Firmware file
		fmins	
	DF800EXS	disk 01 - disk X	Firmware file
		fmins	
	DF800M	disk 01 - disk X	Firmware file
		fmins	
	DF800S	disk 01 - disk X	
		fmins	
	DF800H	disk 01 - disk X	
		fmins	
	drvfirm	DKR2F-VIPERAP	Drive firmware file
		:	
	ENC	ENC Firmware file	–

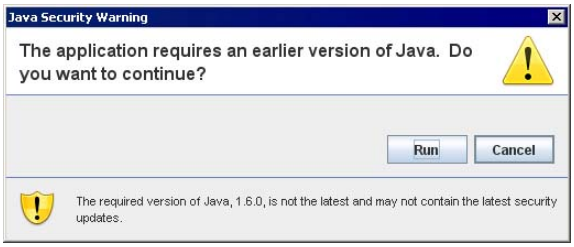
(3) Installation Procedure

NOTE : When using Windows Vista, Server 2008, the firmware may not be replaced normally depending on the authority of the user who is logging in. Execute it by the administrator authority.

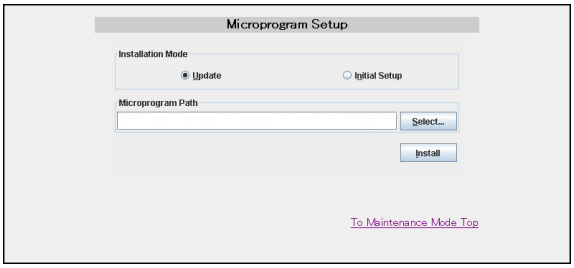
(a) Click “Microprogram”.



(b) When JRE 6 and JRE 6 Update10 are installed in the service PC at the same time, the following window may be displayed. Click [Cancel] here, and continue the operation with the JRE 6 Update10 (it is executed by JRE 6 if “Execute” is clicked, but this is not recommended because it may not be operated normally depending on the execution environment).



(c) When the Java is started, the following window is displayed.

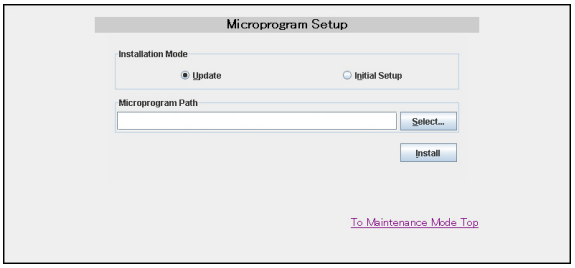


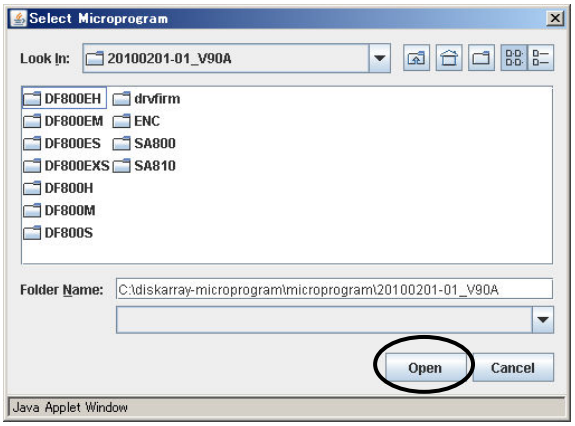
(d) Select the installation type in the “Install Mode”.

- Update····· Update installation
- Initial Setup····· Initial setting up

In the Firmware Path field, specify the Unified version directory(‡1) in which the firmware to be installed is stored.
When the “Select” button is clicked, the “Select Microprogram” window is displayed. Select the Unified version directory in which the firmware is stored and click the “Open” button.

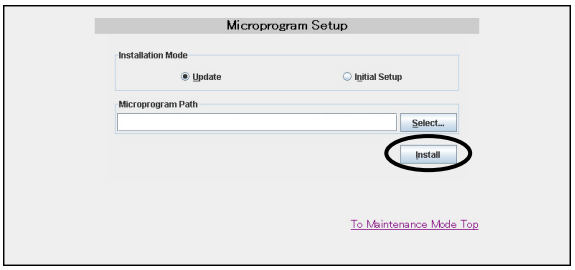
NOTE : If the window is not displayed, the JRE 1.6 may have not been installed or the installation of it may have failed.
Perform the installation of the JRE 1.6 (See “3.1.1 (1) Set Up for the Maintenance PC” (WEB 03-0280).) again.



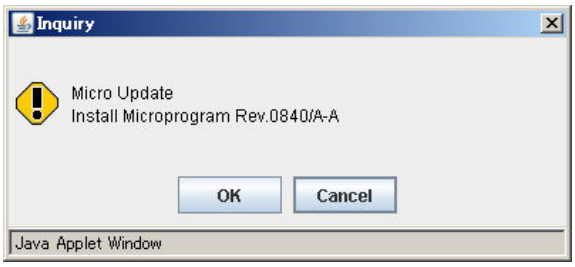


‡1 : For the unified version directory, refer to “3.3.1 (2) Hierarchy of Firmware Storage Directories” (WEB 03-0340).

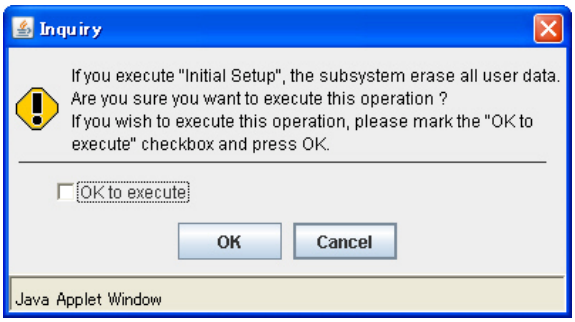
(e) Press the [Install] button.



(f) A dialog box for confirming whether to execute the installation is displayed. Press the [OK] button when you want to install or [Cancel] when you want to abort.



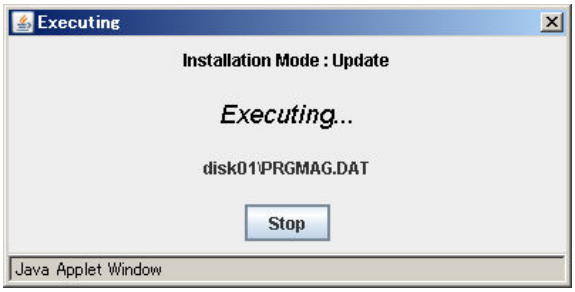
(g) The following dialog box is displayed when the firmware has already been installed in the subsystem in the case where the initial setting up is specified.



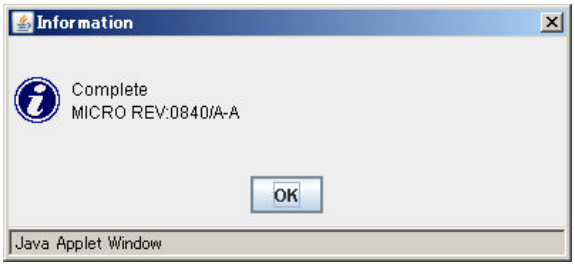
(h) When you want to continue the installation, press the [OK] button. When you want to abort the installation, press the [Cancel] button.

(i) When the installation is started, the following dialog box showing that the installation is in progress is displayed. The installation type and a name of a file being processed is displayed in the dialog box. When you abort the installation, press the [Stop] button.

NOTE : When a LAN failure, etc. occurred and the processing of WEB terminated abnormally before the window in the procedure (j) was displayed, execute the new installation procedure again from the beginning.



(j) When the installation is completed, the completion window is displayed. Click the [OK] button.

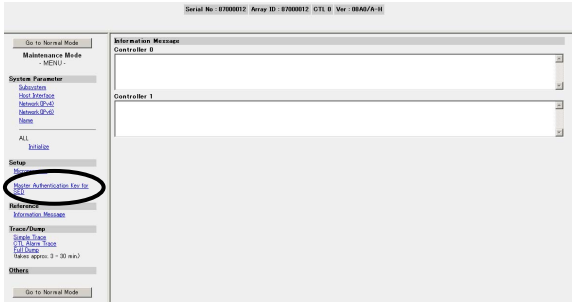


3.3.2 Master Authentication Key for SED

This function restores the Master Authentication Key for SAS(SED) drive.

NOTE : When restoring the master authentication key, restore only either one of the Control Units.
If the Control Unit #0 and the Control Unit #1 are accessed respectively and restored at the same time, the Control Units cannot be restored.

(1) Click the “Master Authentication Key for SED”.



(2) The restoring execution window is displayed. Enter the password and the backup file for restoration.
Store the backup file under “C:\” or “C:\diskarray-microprogram”.
Do not change the backup file name.

[Input password] : Enter the password specified when the master authentication key was backed up.

NOTE : Inquiring of the customer about the password before entering the password.

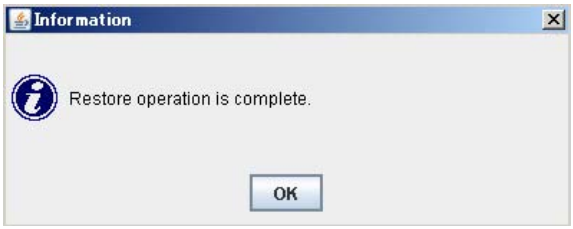
[Select Backup File] : Specify the backup file for restoring.

NOTE : Specify the file by clicking the [Select] button.

(3) Check the description you inputted, and then click the [Start] button to execute the restoration.

(4) The execution confirmation window is displayed. Click the [OK] button.

(5) Click the [OK] button.

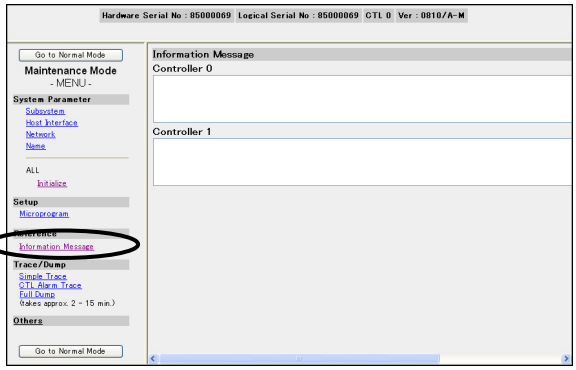


3.4 Reference

3.4.1 Information Message

If the abnormality occurred to the array device, this function displays the fault information.

The fault information of Controller # 0 is displayed in “Information Message” and the fault information of Controller # 1 is displayed in “Information Message”.



3.5 Trace/Dump

3.5.1 Collecting Simple Trace

This is a function to download current trace information.
To perform the down-load, a free capacity of approximately 40 M bytes is required in the PC.
Simple Trace needs to be collected from both controllers.

NOTE : When using IE 8.0, IE 9.0 or IE 10.0, the WEB window display may slow down and the collection of the trace from the WEB window may not complete. Uncheck the checkbox of "Enable SmartScreen Filter" in the Internet Options Advanced Settings. If the issue still occurs, please cancel the DNS Server's settings of the PC's LAN.

The first file name during the collection is as follows:

(i) When the firmware version is 0897/H or more;
Serial number and the trace collection starting time
(year/month/day/hour/minute/seconds) are added to the first file name.
smpl_trc0_xxxxxxxx_YYYYMMDDhhmmss_0E.dat

xxxxxxxx	: Trace collection serial number
YYYYMMDDhhmmss	: Trace collection starting time (year/month/day/hour/minute/seconds)

- The first file name when the collection from Control Unit #0 fits in a file
  "smpl_trc0_xxxxxxxx_YYYYMMDDhhmmss_0E.dat"
- The first file name when the collection from Control Unit #1 fits in a file
  "smpl_trc1_xxxxxxxx_YYYYMMDDhhmmss_0E.dat"
- The first file names when the collection from Control Unit #0 fits in two files
  "smpl_trc0_xxxxxxxx_YYYYMMDDhhmmss_0S.dat"
  "smpl_trc0_xxxxxxxx_YYYYMMDDhhmmss_1E.dat"
- The first file names when the collection from Control Unit #1 fits in two files
  "smpl_trc1_xxxxxxxx_YYYYMMDDhhmmss_0S.dat"
  "smpl_trc1_xxxxxxxx_YYYYMMDDhhmmss_1E.dat"
- The first file names when the collection from Control Unit #0 fits in three files
  "smpl_trc0_xxxxxxxx_YYYYMMDDhhmmss_0S.dat"
  "smpl_trc0_xxxxxxxx_YYYYMMDDhhmmss_1C.dat"
  "smpl_trc0_xxxxxxxx_YYYYMMDDhhmmss_2E.dat"
- The first file names when the collection from Control Unit #1 fits in three files
  "smpl_trc1_xxxxxxxx_YYYYMMDDhhmmss_0S.dat"
  "smpl_trc1_xxxxxxxx_YYYYMMDDhhmmss_1C.dat"
  "smpl_trc1_xxxxxxxx_YYYYMMDDhhmmss_2E.dat"

(ii) When the firmware version is 0890/A or more and less than 0897/H;
- The first file name when the collection from Control Unit #0 fits in a file
  "smpl_trc0_0E.dat"
- The first file name when the collection from Control Unit #1 fits in a file
  "smpl_trc1_0E.dat"

- The first file names when the collection from Control Unit #0 fits in two files
  “smpl_trc0_0S.dat”
  “smpl_trc0_1E.dat”
- The first file names when the collection from Control Unit #1 fits in two files
  “smpl_trc1_0S.dat”
  “smpl_trc1_1E.dat”
- The first file names when the collection from Control Unit #0 fits in three files
  “smpl_trc0_0S.dat”
  “smpl_trc0_1C.dat”
  “smpl_trc0_2E.dat”
- The first file names when the collection from Control Unit #1 fits in three files
  “smpl_trc1_0S.dat”
  “smpl_trc1_1C.dat”
  “smpl_trc1_2E.dat”

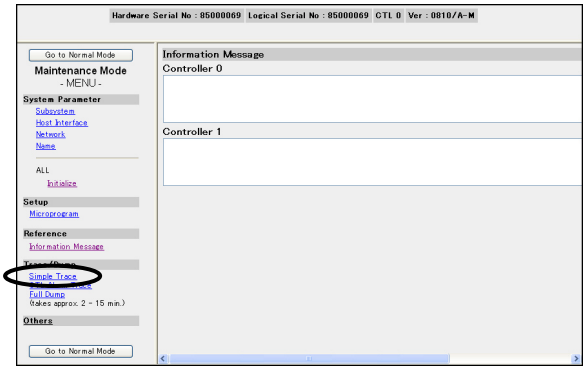
(iii) When the firmware version is less than 0890/A;

- The first file name during the collection from Control Unit #0
  “smpl_trc0.dat”.
- The first file name during the collection from Control Unit #1
  “smpl_trc1.dat”.

(1) Clear the cache of the browser in the following procedure before collecting the Simple Trace so that the old data collected last time is not saved.

- In the case of Internet Explorer, select the [Tools], [Internet Options], [General], [Temporary Internet files], and [Delete Files] in this order.
- In the case of Netscape, select the [Edit], [Preferences], [Cache], and [Clear Cache] in this order.

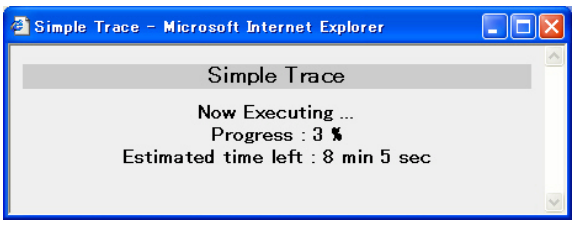
(2) Click “Simple Trace” in the menu frame.



(3) When the “Simple Trace” is clicked, the following window is displayed.

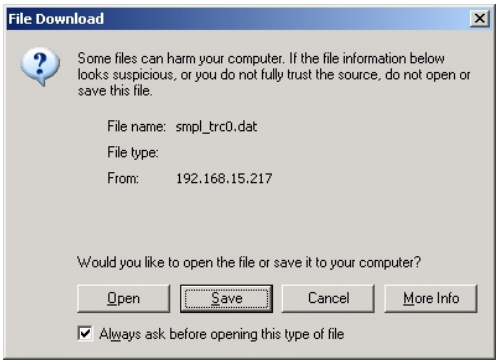
(4) When the [OK] button is clicked, the following window is displayed.

NOTE : If the window update (e.g.: pressing F5 key) is performed in this window, the automatic update stops and so that the trace collection does not make progress. When the automatic update stops due to the window update, close this window and, after 20 minutes or more elapse, perform the simple trace collection again.

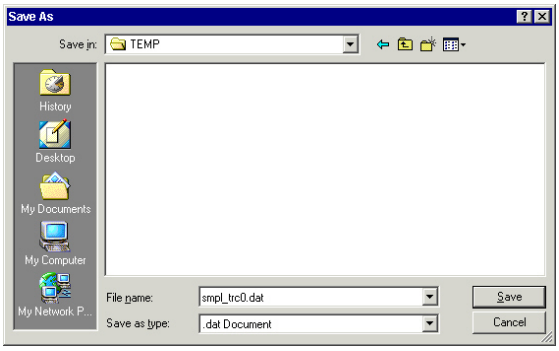


(5) The following window is displayed. Click the [Download] button.

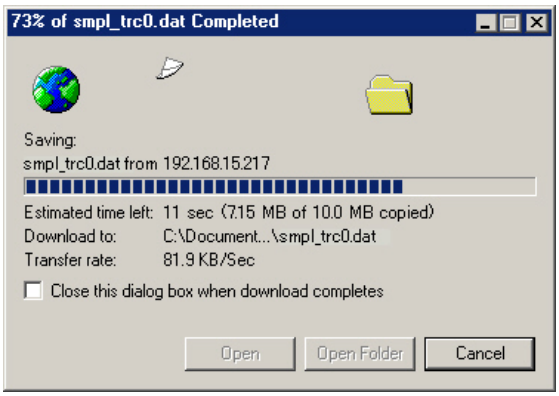
(6) Please click [Save], if it is continued. Please click [Cancel], if it is stopped.



(7) If the following window is displayed. Please click [Save] after file name is setting, if it is continued.(‡1) Please click [Cancel], if it is stopped.



(8) The following window is displayed during execution download.



(9) When the downloading completes, the progress indicating message window is closed.

(10) If all traces cannot be collected, the following window is displayed.
Click the [Continue], and then collect traces in the next file beginning from the step (4).

NOTE : When performing an array boot or simple trace collection from the same Control Unit in the same array in the following window without clicking the [Continue], a error window is displayed, and the trace cannot be collected.

When all the traces can't be collected on the first time.

When all the traces can't be collected on the second time.

‡1 : There may be a case where the first file name is given as "smpl_trc0xxxx.dat..dat" depending on the setting of the PC. In this case, ".dat" is deleted or any other name.

(11) The following window appears when all traces are collected.
Click the [Close] button.

NOTE : When the firmware version is 0890/A or more, verify that the number of files described in the window is the same as the number of the files actually collected.

- When the firmware version is less than 0890/A

- When the firmware version is 0890/A or more
When all traces can be collected in one file

When all traces can be collected in two files

3.5.2 Collecting CTL Alarm Trace

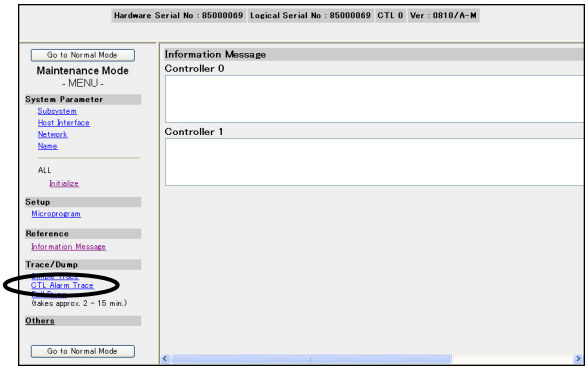
Through the CTL Alarm Trace collection, detailed information (the CTL Alarm Trace) on the immediately Controller blockade stored in the Controller is collected. It may not be collected depending on the types of the failures which cause the controller blockade.

NOTE : When the Control Unit to be connected to WEB is blocked, the WEB connection may not be performed for ten minutes usually (for the maximum of 60 minutes) from the time when the Control Unit was blocked because the CTL alarm trace is being created.

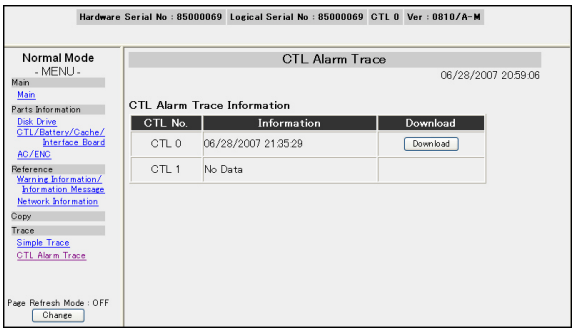
Since the above-mentioned CTL Alarm Trace information is taken over from the blocked Control Unit to the replaced Control Unit, it can be collected after the Control Unit is recovered from the failure. Even after the collection, the information remains until the controller blockade trace is rewritten in the next controller blockade. If the Control Unit is blocked while collecting the CTL Alarm Trace may not be collected normally. Therefore, in this case, collect the CTL Alarm Trace again.
For collecting the CTL Alarm Trace, disk space of 520 M bytes per one Control Unit is required. (260 M bytes for temporary data and 260 M bytes for Full Dump data)
Collect CTL Alarm Trace from each Control Unit.
In order to distinguish from which Control Unit it is collected, store the collected data in different directories or with different file names.
The method of collecting the CTL Alarm Trace is shown below.

(1) Clear the cache of the browser in the following procedure before collecting the CTL Alarm Trace so that the old data collected last time is not saved.
- In the case of Internet Explorer, select the [Tools], [Internet Options], [General], [Temporary Internet files], and [Delete Files] in this order.
- In the case of Netscape, select the [Edit], [Preferences], [Cache], and [Clear Cache] in this order.

(2) Click “CTL Alarm Trace” in the menu frame.
The CTL Alarm Trace Information window is displayed when the CTL alarm trace information is present.



(3) To download the CTL Alarm trace information, press the “Download” button on the Control Unit side to be collected in “CTL Alarm Trace information”.(‡1)



The following is displayed as contents of the information.

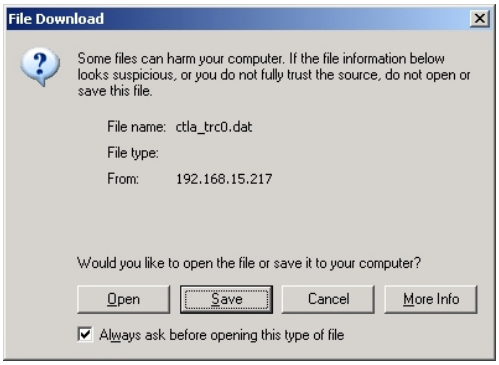
[Not Ready] ..... : A status in which the trace area is not established in the subsystem

[Not Data] ..... : A status in which the CTL Alarm trace information is not present or being generated

[MM/DD/20XY hh:mm:ss] . : A status in which the CTL alarm trace information is present

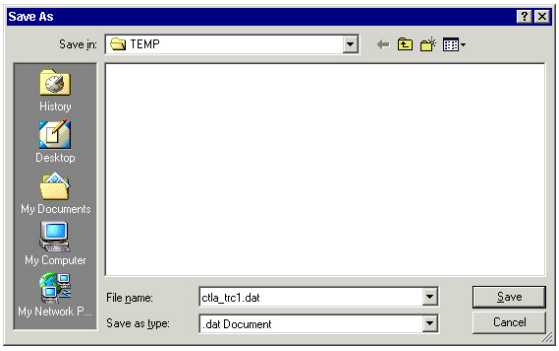
NOTE : When “Not Ready” or “No Data” is displayed on the description of “Information”, or when the date of the information is different from that of the collection of this time, the CTL alarm trace may not be collected normally. Therefore, collect the simple trace.
If simple trace cannot be obtained through detached Controller, connect the Maintenance PC to the Controller at the opposite side, and collect the simple trace.

(4) The following window is displayed. Please click [Save], if it is continued. Please click [Cancel], if it is stopped.

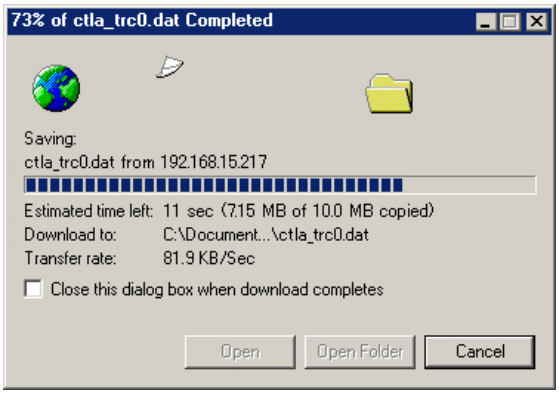


‡1 : An error message may be displayed. If it is displayed, click [OK], and collect the CTL Alarm Trace again after waiting for a while.

(5) If the following window is displayed. Please click [Save] after file name is setting, if it is continued. Please click [Cancel], if it is stopped.



(6) The following window is displayed during execution download.

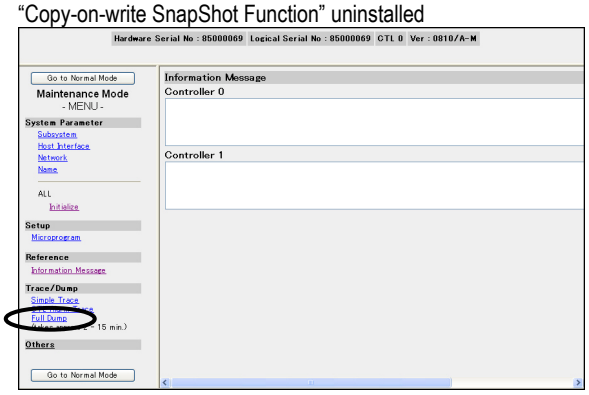


(7) When the downloading completes, the progress indicating message window is closed.

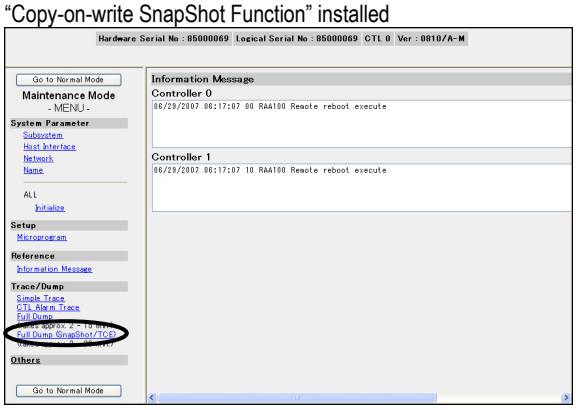
3.5.3 Collecting Full Dump

This function (Full Dump) is to download the logging information of the subsystem. The menu frame differs whether the priced optional feature, "Copy-on-write SnapShot Function", is installed or not.

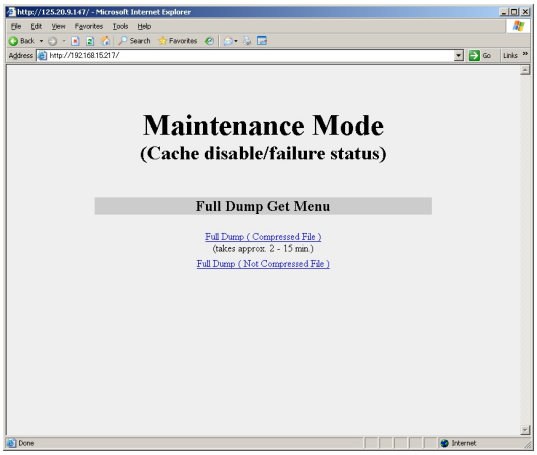
"Copy-on-write SnapShot Function" uninstalled



"Copy-on-write SnapShot Function" installed



The cache memory access failure occurs when the following window is displayed. Refer to "3.1.1 WEB Operation in the Maintenance Mode During the Cache Memory Access Failure" (WEB 03-0050).



When Copy-on-write SnapShot Function is installed, the information downloaded by this function (Full Dump) does not include the information in Copy-on-write SnapShot.
Collect Full Dump from each Control Unit.

In order to distinguish from which Control Unit it is collected, store the collected data in different directories or with different file names.
To download, the following free capacity size is needed on PC.

• When Copy-on-write SnapShot Function is not installed

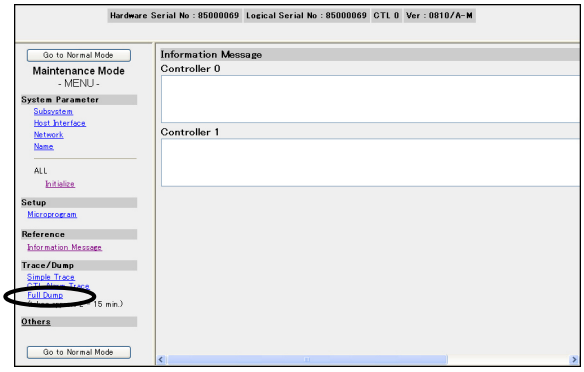
	Installed cache per Control Unit	Free Capacity needed on PC	
		no compression	compression (*1)
RKM	1 G bytes (Minimum)	1,725 M bytes	173 M bytes
	8 G bytes (Maximum)	2,091 M bytes	210 M bytes
RKS	1 G bytes (Minimum)	1,161 M bytes	117 M bytes
	4 G bytes (Maximum)	1,339 M bytes	134 M bytes
RKH	2 G bytes (Minimum)	3,234 M bytes	324 M bytes
	16 G bytes (Maximum)	3,895 M bytes	390 M bytes
RKEXS/RKEXSA/RKEXSB/RKEXS8F	2 G bytes	1,220 M bytes	112 M bytes

*1 : The value with compression has described the value when the compression rate is 10% as a standard.

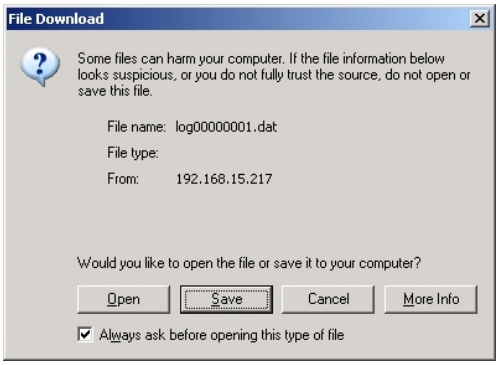
NOTE : When this function is used, the menu other than Logging Data comes not to use it. Please enter into the Maintenance Mode again by the reset switch of the Controller, once again, if other menus are used, after this function was used.

(1) Clear the cache of the browser in the following procedure before collecting the Full Dump so that the old data collected last time is not saved.
- In the case of Internet Explorer, select the [Tools], [Internet Options], [General], [Temporary Internet files], and [Delete Files] in this order.
- In the case of Netscape, select the [Edit], [Preferences], [Cache], and [Clear Cache] in this order.

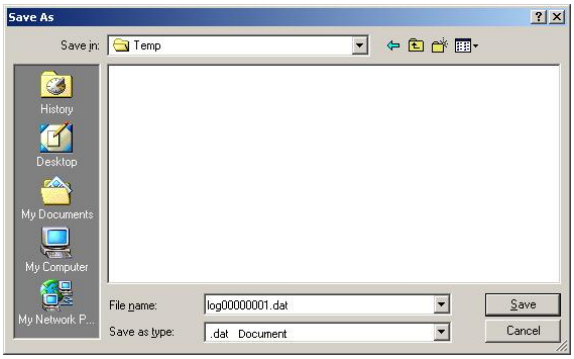
(2) Please click “Full Dump”.



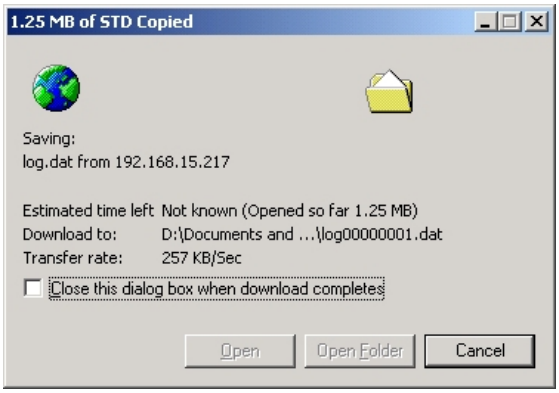
(3) The following window is displayed. Please click [Save], if it is continued. Please click [Cancel], if it is stopped.



(4) If the following window is displayed. Please click [Save] after file name is setting, if it is continued.(‡1) Please click [Cancel], if it is stopped.



(5) The following window is displayed during execution download.
There is no problem although it is displayed that the presumption remaining time is uncertain.



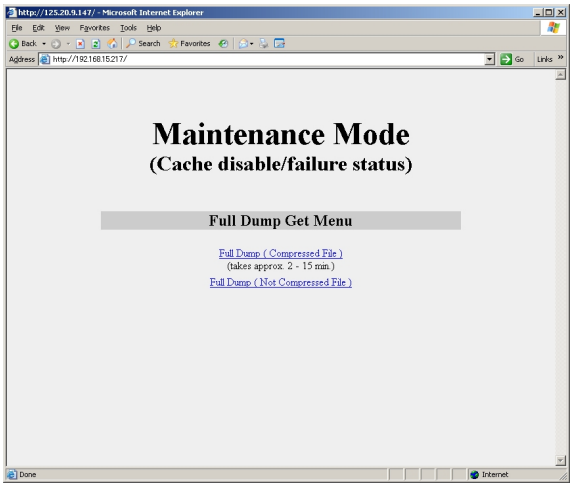
(6) When the downloading completes, the progress indicating message window is closed.

‡1 : There may be a case where the default file name is given as “logx.dat.dat” depending on the setting of the PC. In this case, “.dat” is deleted or any other name. (x: Controller serial numbers)

3.5.4 Collecting Full Dump (Full Dump (SnapShot/TCE))

This function (Full Dump(SnapShot)) is effective only when the priced optional feature, “Copy-on-write SnapShot Function” or “TrueCopy Extended Distance Function”, is installed. If not, this menu frame may not be displayed.

The cache memory access failure occurs when the following window is displayed. Refer to “3.1.1 WEB Operation in the Maintenance Mode During the Cache Memory Access Failure” (WEB 03-0050).



This function (Full Dump(SnapShot)) downloads the logging information of the subsystem. The downloaded information includes the information in Copy-on-write SnapShot.
Collect Full Dump from each Control Unit.
In order to distinguish from which Control Unit it is collected, store the collected data in different directories or with different file names.
To download, the following free capacity size is needed on PC.

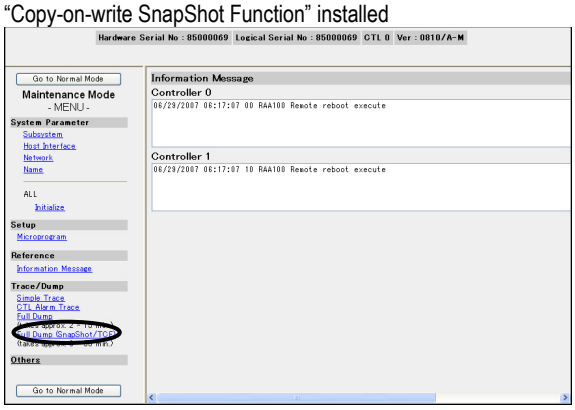
	Installed cache per Control Unit	Free Capacity needed on PC	
		no compression	compression (*1)
RKM	1 G bytes (Minimum)	1,825 M bytes	183 M bytes
	8 G bytes (Maximum)	6,187 M bytes	619 M bytes
RKS	1 G bytes (Minimum)	1,461 M bytes	147 M bytes
	4 G bytes (Maximum)	3,387 M bytes	339 M bytes
RKH	2 G bytes (Minimum)	3,734 M bytes	374 M bytes
	16 G bytes (Maximum)	12,087 M bytes	1,209 M bytes
RKEXS/RKEXSA/RKEXSB/RKEXS8F	2 G bytes	1,220 M bytes	112 M bytes

*1 : The value with compression has described the value when the compression rate is 10% as a standard.

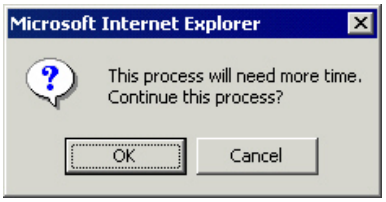
NOTE : When this function is used, the menu other than Logging Data comes not to use it. Please enter into the Maintenance Mode again by the reset switch of the Controller, once again, if other menus are used, after this function was used.

(1) Please click “Full Dump(SnapShot)” or “Full Dump(SnapShot/TCE)”.

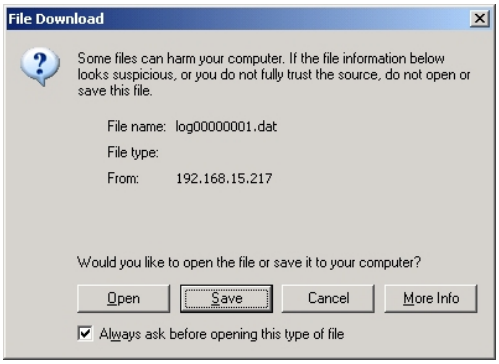
“Copy-on-write SnapShot Function” installed



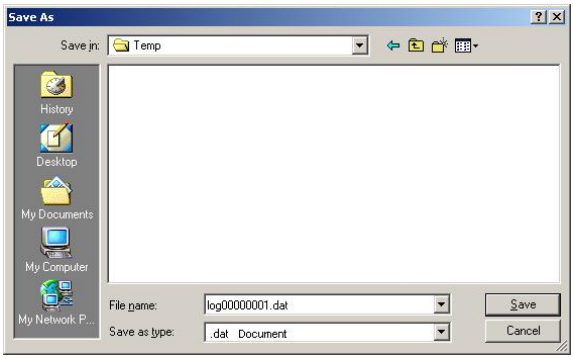
(2) The following window is displayed. Please click [OK], if it is continued. Please click [Cancel], if it is stopped.



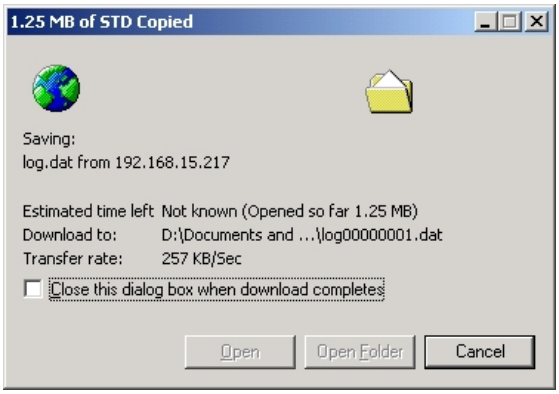
(3) The following window is displayed. Please click [Save], if it is continued. Please click [Cancel], if it is stopped.



(4) If the following window is displayed. Please click [Save] after file name is setting, if it is continued.(‡1) Please click [Cancel], if it is stopped.



(5) The following window is displayed during execution download.
There is no problem although it is displayed that the presumption remaining time is uncertain.



(6) When the downloading completes, the progress indicating message window is closed.

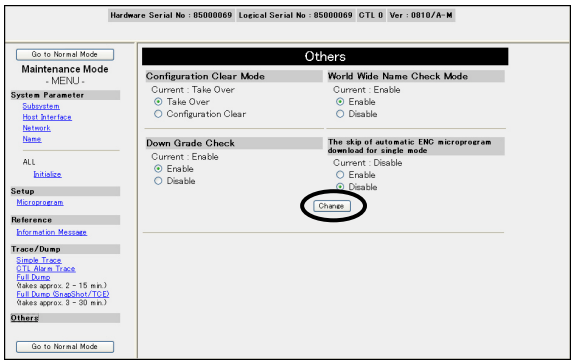
‡1 : There may be a case where the default file name is given as “logx.dat.dat” depending on the setting of the PC. In this case, “.dat” is deleted or any other name. (x: Controller serial numbers)

3.6 Other

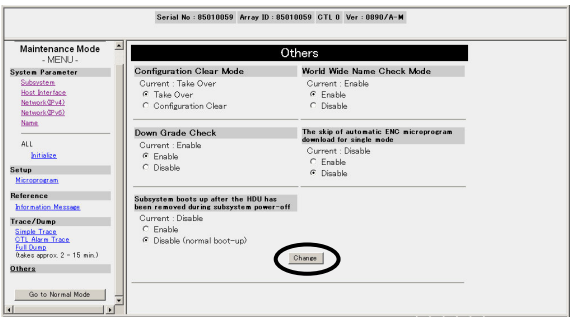
The others are set up.
The contents that were set up in this function are not taken over and not step over the PS-OFF/ON.

(1) Please confirm the setting value of each item and click the check box of the item that the setting contents are changed. Please click [Change], if the setting contents are updated.

Firmware is less than Ver.0890.



Firmware is Ver.0890 or more.



Explanation with regard to each item

- Configuration Clear Mode
  The transfer information initialization as the booting is designated.
  [Take Over] : Transfer booting (default).
  [Configuration Clear] : Default booting.
- World Wide Name Check Mode
  The World Wide Name Check Mode as the booting is designated.
  [Enable] : The WWN Check is executed (default).
  [Disable] : The WWN Check is not executed.
- Data Down Grade Check Mode
  It specifies whether to make the check of the version downgrade of the firmware enable or disable when performing the update installation of the firmware by using WEB.
  [Enable] : Guard the version downgrade of the firmware (default).
  It is specified usually when the version of the firmware is updated.
  [Disable] : The version downgrade of the firmware is not checked.
  It is specified before the update installation is performed when the version of the firmware is downgraded.
- The skip of automatic ENC microprogram download for single mode
  It skips or specifies the automatic ENC firmware download in case the subsystem is set to the single mode.
  [Enable] : It skips the automatic ENC firmware download.
  [Disable] : It does not skip the automatic ENC firmware download (default).

- Subsystem boots up after the HDU has been removed during subsystem power-off[‡1] :
  When starting the subsystem from the maintenance mode, if the subsystem is not Ready, it specifies whether to permit the removal or not.
  [Enable] : The removal of the Disk Drive is not checked.
  [Disable] : The removal status of the Disk Drive is checked d (default).

(2) Please confirm that the setting value was updated.

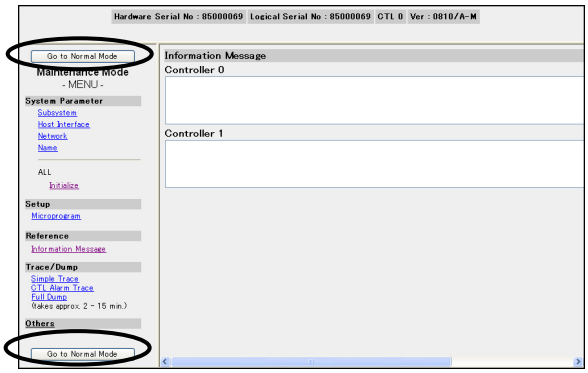
‡1 : It is supported from the microprogram Ver.0890/A

This page is for editorial purpose only.

3.7 Return Method to the Normal Mode

The method that returns from the Maintenance Mode to the Normal Mode is shown.

(1) Please click [Go To Normal Mode]. The button of [Go To Normal Mode] is in the top and down on the menu window. Please select either button.



(2) The following window is displayed during execution. Do not click the ☒ while the window is displayed(‡1).

(3) If the following confirmation message is displayed for a while. Please click [OK], if it is continued.

(4) The following window remains displayed during execution. Whether you click the [OK] or [Cancel] in the confirmation message window of (3), do not click the ☒ while the following window is displayed(‡1).

‡1 : If you click the ☒, reenter the Maintenance Mode, and then click the [Go To Normal Mode] again.

(5) If the return to the Usually Mode completes, the array device becomes the Ready status. Please confirm that the READY LED of the device entire surface is lighted. (Usually Controller recovers in about four minutes. (about five minutes in case of the RKH))
Check that the READY LED (green) on the front of the Basic Chassis lights up, and the ALARM LED (red) and the WARNING LED (orange) go out(‡1). The READY LED (green) may blink at high speed (for the maximum of 30 to 50 minutes, or 40 to 60 minutes in case of the RKH) or the WARNING LED (orange) may blink at high speed (for the maximum of 30 to 85 minutes) before the READY LED (green) on the front of the Basic Chassis lights up.

(6) Check that the start message and the end message of the drive firmware automatic download are displayed. When the drive firmware version of the disk drive is new, the start message and completion message of the drive firmware automatic download are not displayed.
When the message indicating the abnormal termination is displayed, perform the maintenance according the recovery method in the message code (refer to Firmware "1.6 (4) Checking the start message and end message of the automatic download (FIRM 01-0890)").

‡1 : When it is blinking at low speed, perform the maintenance according to the recovery method of the message referring to the Information Message on WEB. If the subsystem is in the Warning status when the Information Message on WEB was referred to, the WARNING LED (orange) on the front of the Basic Chassis lights up, and if the subsystem is not in the Warning status, the WARNING LED (orange) goes out.