

NOVASCALÉ

NovaScale R630 E1

User's Guide



REFERENCE
86 A1 38FA 00

NOVASCALÉ

NovaScale R630 E1

User's Guide

Hardware

June 2008

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

REFERENCE
86 A1 38FA 00

Proprietary Notice and Liability Disclaimer

The information disclosed in this document, including all designs and related materials, is the valuable property of NEC Computers and/or its licensors. NEC Computers and/or its licensors, as appropriate, reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use, and sales rights thereto, except to the extent said rights are expressly granted to others.

To allow for design and specification improvements, the information in this document is subject to change at any time, without notice. Reproduction of this document or portions thereof without prior written approval of NEC Computers is prohibited.

The Bull product(s) discussed in this document are warranted in accordance with the terms of the Warranty Statement accompanying each product. However, actual performance of each product is dependent upon factors such as system configuration, customer data, and operator control. Since implementation by customers of each product may vary, the suitability of specific product configurations and applications must be determined by the customer and is not warranted by Bull.

Trademarks

NEC ESMPRO, NEC DianaScope, NEC MWA, and ExpressBuilder are trademarks or registered trademarks of NEC Corporation.

NovaScale is a registered trademark of Bull SAS.

Adobe, and Adobe Acrobat are registered trademarks of Adobe Systems, Incorporated.

Microsoft, Microsoft Windows, Windows NT, Windows 95, Windows 98, Windows2000 and Windows Server 2003 are all registered trademarks of Microsoft Corporation.

MS-DOS is a registered trademark of Microsoft Corporation.

Intel and Xeon are registered trademarks of Intel Corporation.

All other product, brand, or trade names used in this publication are the trademarks or registered trademarks of their respective trademark owners.

Copyright © NEC Computers SAS 2006

Suggestions and criticisms concerning the form, content, and presentation of this manual are invited. A form is provided at the end of this manual for this purpose.

The information in this document is subject to change without notice. Bull will not be liable for errors contained herein, or for incidental or consequential damages in connection with the use of this material.

CONTENTS

CHAPTER 1	1-1
PRECAUTIONS FOR USE	1-1
WARNING LABELS	1-2
PRECAUTIONS FOR SAFETY	1-3
GENERAL.....	1-3
USE OF POWER SUPPLY AND POWER CORD.....	1-4
INSTALLATION, RELOCATION, STORAGE AND CONNECTION.....	1-5
CLEANING AND HANDLING OF INTERNAL DEVICES.....	1-7
DURING OPERATION.....	1-8
RACK-MOUNT MODEL.....	1-9
FOR PROPER OPERATION	1-10
DISPOSAL OF EQUIPMENT AND CONSUMABLES.....	1-11
IF SYSTEM TROUBLE IS SUSPECTED.....	1-12
ABOUT REPAIR PARTS.....	1-12
CHAPTER 2	2-1
GENERAL DESCRIPTION.....	2-1
STANDARD FEATURES.....	2-2
How the Operating System Sees the CPU Modules.....	2-6
How CPU MODULES APPEAR ON TASK MANAGER	2-6
NAMES AND FUNCTIONS OF COMPONENTS	2-7
FRONT VIEW.....	2-8
REAR VIEW.....	2-10
DVD-ROM DRIVE.....	2-12
CPU/IO MODULE.....	2-13
MOTHER BOARD	2-14
FT REMOTE MANAGEMENT CARD.....	2-15
LEDs	2-16
BASIC OPERATION	2-20
INSTALLING/REMOVING THE FRONT BEZEL.....	2-20
POWER ON	2-21
POWER OFF.....	2-21
POST CHECK.....	2-22
FLOPPY DISK DRIVE (OPTION).....	2-25
DVD-ROM DRIVE	2-27
CHAPTER 3	3-1
WINDOWS SETUP AND OPERATION.....	3-1
DISK OPERATIONS	3-2
DISK OPERATIONS USING THE RDR (RAPID DISK RESYNC) FUNCTION	3-2
REPLACING FAILED HARD DISK DRIVES	3-17
CHANGE DRIVE LETTER.....	3-20
DUPLEX LAN CONFIGURATION.....	3-21
OVERVIEW.....	3-21
RULES OF DUPLEX CONFIGURATION ON FAULT TOLERANT SERVER SERIES.....	3-22
CONFIGURING DUPLEX LAN.....	3-23
REMOVING DUPLEX/DUAL LAN.....	3-27
CHECKING THE DUPLICATING OPERATION OF MODULES	3-28
EVALUATE STARTUP AND STOP OF PCI MODULES.....	3-28
CONFIRM START AND STOP OF CPU MODULES	3-31
Fault Tolerant Server series SERVICE PROGRAM CONFIGURATION.....	3-33
CHAPTER 4	4-1
SYSTEM CONFIGURATION.....	4-1
SYSTEM BIOS –SETUP–.....	4-2
STARTING SETUP UTILITY	4-3
DESCRIPTION OF ON-SCREEN ITEMS AND KEY USAGE.....	4-4
CONFIGURATION EXAMPLES	4-6
MENU AND PARAMETER DESCRIPTIONS.....	4-8
SAS BIOS –ADAPTEC SAS/SATA CONFIGURATION UTILITY–.....	4-26
FORCED SHUTDOWN AND CLEAR	4-35
FORCED SHUTDOWN.....	4-35
Clear CMOS/Password.....	4-36
How to Clear Passwords.....	4-38

How to Clear THE BMC configuration	4-39
Remote Management function	4-40
NETWORK DEFAULT VALUES	4-40
SETTINGS ON THE SERVER	4-41
INITIAL SETTINGS ON THE SERVER	4-41
SETTING A MANAGEMENT PC	4-43
USING REMOTE MANAGEMENT	4-45
TROUBLESHOOTING	4-74
CHAPTER 5	5-1
INSTALLING AND USING UTILITIES	5-1
EXPRESSBUILDER	5-2
START MENU	5-2
AUTORUN MENU	5-4
Parameter File creator	5-5
PARAMETER FILE CREATOR	5-5
NEC ESMPRO Agent and Manager	5-12
OVERVIEW	5-12
NEC ESMPRO AGENT	5-19
NEC ESMPRO MANAGER	5-26
MAINTENANCE OF FAULT TOLERANT SERVER SERIES	5-42
NEC DianaScope	5-67
NOTES	5-67
Active Upgrade	5-68
INTRODUCTION	5-68
OVERVIEW	5-69
PREPARING FOR THE ACTIVE UPGRADE PROCESS	5-77
CONFIGURING THE ACTIVE UPGRADE PROCESS	5-93
PERFORMING THE UPGRADE	5-111
TROUBLESHOOTING	5-141
CHAPTER 6	6-1
MAINTENANCE	6-1
DAILY MAINTENANCE	6-2
CHECKING ALERT	6-2
CHECKING STATUS LEDs	6-2
MAKING BACKUP COPIES	6-3
CLEANING	6-3
SYSTEM DIAGNOSTICS	6-6
TEST ITEMS	6-6
STARTUP AND EXIT OF SYSTEM DIAGNOSTICS	6-6
OFF-LINE MAINTENANCE UTILITY	6-9
STARTING THE OFF-LINE MAINTENANCE UTILITY	6-9
FUNCTION OF MAINTENANCE TOOLS	6-11
RELOCATING/STORING THE Fault Tolerant Server series	6-13
TO THE ACCIDENT OF PCI MODULE	6-14
PROCEDURE TO CONFIRM	6-14
PROCEDURE TO RECOVER	6-15
PROCEDURE TO CHECK	6-17
CHAPTER 7	7-1
TROUBLESHOOTING	7-1
TO LOCATE THE ERRORS	7-2
ERROR MESSAGES BY LED INDICATION	7-3
POST ERROR MESSAGES	7-4
WINDOWS SERVER 2003, ENTERPRISE EDITION ERROR MESSAGES	7-8
SERVER MANAGEMENT APPLICATION ERROR MESSAGE	7-9
troubleshooting	7-10
PROBLEMS WITH FAULT TOLERANT SERVER SERIES	7-10
EVENT LOG	7-20
PROBLEMS WITH EXPRESSBUILDER	7-24
PROBLEMS WITH MASTER CONTROL MENU	7-25
PROBLEMS WITH PARAMETER FILE CREATOR	7-26
PROBLEMS WITH NEC ESMPRO	7-27
COLLECTING TROUBLE LOGS	7-33
COLLECTION OF EVENT LOGS	7-33
COLLECTION OF CONFIGURATION INFORMATION	7-34
COLLECTION OF DIAGNOSTIC INFORMATION BY DR. WATSON	7-34
COLLECTING THE MEMORY DUMP	7-35
CHAPTER 8	8-1

SYSTEM UPGRADE	8-1
SAFETY PRECAUTIONS	8-1
ANTI-STATIC MEASURES	8-2
Pre-upgrade verification.....	8-2
PREPARING YOUR SYSTEM FOR UPGRADE	8-3
3.5-INCH HARD DISK DRIVE	8-4
<i>INSTALLING 3.5-INCH HARD DISK DRIVE.....</i>	<i>8-5</i>
<i>REMOVING 3.5-INCH HARD DISK DRIVE</i>	<i>8-7</i>
<i>REPLACING 3.5-INCH HARD DISK DRIVE</i>	<i>8-8</i>
CPU/IO Module.....	8-9
<i>PRECAUTIONS</i>	<i>8-9</i>
<i>REMOVING CPU/IO MODULE</i>	<i>8-10</i>
<i>INSTALLING CPU/IO MODULE.....</i>	<i>8-13</i>
DIMM	8-14
<i>PRECAUTIONS</i>	<i>8-14</i>
<i>INSTALLING DIMM.....</i>	<i>8-15</i>
<i>REMOVING DIMM</i>	<i>8-17</i>
<i>REPLACING DIMM</i>	<i>8-19</i>
PROCESSOR (CPU)	8-20
<i>INSTALLING CPU.....</i>	<i>8-21</i>
<i>REMOVING CPU</i>	<i>8-23</i>
PCI BOARD	8-24
<i>INSTALLING PCI BOARD.....</i>	<i>8-26</i>
<i>REMOVING PCI BOARD</i>	<i>8-29</i>
<i>REPLACING PCI BOARD</i>	<i>8-29</i>
<i>SETUP OF OPTIONAL PCI BOARD.....</i>	<i>8-29</i>
APPENDIX A	A-1
SPECIFICATIONS.....	A-1
APPENDIX B.....	B-1
I/O PORT ADDRESSES.....	B-1



Keep this User's Guide handy for quick reference when necessary.

SAFETY INDICATIONS




To use Fault Tolerant Server series safely, follow the instructions in this User's Guide.

This guide explains components that pose a danger, types of dangers, and actions taken to prevent them; such components are labeled warning.

This guide and warning labels use “WARNING” and “CAUTION” to indicate a danger depending on the degree. These terms are defined as follows:

 WARNING	Indicates a danger that could lead to a death or serious injury.
 CAUTION	Indicates a danger that could lead to a burn, other injuries or damage to physical assets.


This guide uses the following three types of symbols to give indications and precautions against a danger. They are defined as follows:


	Indicates that there is a risk of danger. Each image symbolizes a particular type of danger. (Attention)
	Indicates what you must not do. Each image symbolizes a particular type of prohibition. (Prohibited actions)
	Indicates what you must do. Each image symbolizes a particular type of action necessary to avoid a danger. (Mandatory actions)

(Example)

Symbol to draw attention

Term indicating a degree of danger





High temperature.









Immediately after the power-off, system components such as hard disk are very hot. Wait the server to cool down completely before adding/removing some component.

Symbol indicating a prohibited action (may not always be indicated)







Description of a danger

SYMBOLS USED IN THIS USER'S GUIDE AND WARNING LABELS



Attention

	Indicates a risk of an electric shock.
	Indicates a risk of a personal injury due to heat.
	Indicates a risk of catching your fingers.
	Indicates a risk of a fire or smoke.
	Indicates a general precaution or warning that is not defined herein.
	Indicates a risk of losing eyesight due to laser beam.
	Indicates a risk of an explosion.
	Indicates a risk of a personal injury.

Prohibited actions

	Indicates a general prohibition that is not defined herein.
	Do not touch the indicated area. There is a risk of an electric shock or fire.
	Do not touch with wet hands. There is a risk of an electric shock.
	Keep from flame. There is a risk of a fire.
	Avoid using water or liquid nearby. If it spills on the equipment, there is a risk of an electric shock or fire.
	Do not disassemble, repair, or modify the equipment. There is a risk of an electric shock or fire.

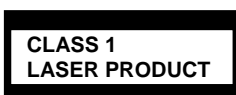
Mandatory actions

	Unplug the server. There is a risk of an electric shock or fire.
	Indicates a general action to take that is not defined herein. Make sure to follow the instructions.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.



This system is classified as a CLASS 1 LASER PRODUCT. This label is located on the internal DVD-ROM installed in your system.

NOTE: This product provides resistance against hardware faults with its redundant hardware modules. However, this does not mean complete fault-tolerance is assured. For example, there is a risk of system down when:

- A fatal fault occurs in software.
- Both modules within a redundant hardware pair break down.
- A fatal fault occurs in a non-redundant component, such as the clock generator circuitry or the interconnect backplane.
- The entire system is cut off from AC power.

Trademarks and Patents

EXPRESSBUILDER, NEC ESM PRO and NEC DianaScope are trademarks of NEC Corporation.

Microsoft, Windows, Windows Server, Windows NT, and MS-DOS are registered trademarks of Microsoft Corporation in the United States and other countries.

Intel and Pentium are registered trademarks of Intel Corporation.

AT is a registered trademark of International Business Machines Corporation in the United States and other countries.

Adobe, the Adobe logo, Acrobat, and the Acrobat logo are trademarks of Adobe Systems Incorporated.

Datalight is a registered trademark of Datalight, Inc. ROM-DOS is a trademark of Datalight, Inc.

Xeon is a trademark of Intel Corporation in the United States. DLT and DLTape are trademarks of Quantum Corporation in the United States.

Mozilla is a registered trademark of Mozilla Foundation.

Netscape is a registered trademark of Netscape Communications Corporation in the United States and other countries.

Java is a registered trademark of Sun Microsystems, Inc in the United States and other countries.

All other product, brand, or trade names used in this publication are the trademarks or registered trademarks of their respective trademark owners.

Microsoft Windows Server 2003 R2 Standard x64 edition operating system and Microsoft Windows Server 2003 R2 Enterprise x64 Edition operating system or Microsoft Windows Server 2003 Enterprise x64 Edition operating system are called Windows Server 2003 x64 Edition for short. Microsoft Windows Server 2003 R2 32-bit Standard Edition operating system, Microsoft Windows Server 2003 R2 32-bit Enterprise Edition operating system, Microsoft Windows Server 2003 Standard Edition operating system and Microsoft Windows Server 2003 Enterprise Edition operating system are called Windows Server 2003 for short. Microsoft Windows 2000 Server operating system, Microsoft Windows 2000 Advanced Server operating system and Microsoft Windows 2000 Professional operating system are called Windows 2000 for short. Microsoft Windows Vista Business operating system is called Windows Vista for short. Microsoft Windows XP Professional x64 Edition operating system is called Windows XP x64 Edition for short. Microsoft Windows XP Home Edition operating system and Microsoft Windows XP Professional operating system are called Windows XP for short. Microsoft Windows NT Server network operating system version 3.51/4.0 and Microsoft Windows NT Workstation operating system version 3.51/4.0 are called Windows NT for short. Microsoft Windows Millennium Edition Operating System is called Windows Me for short. Microsoft Windows 98 operating system is called Windows 98 for short. Microsoft Windows 95 operating system is called Windows 95 for short. Names used with

sample applications are all fictitious. They are unrelated to any existing product names, names of organizations, or individual names.

AVOCENT and DVC (DAMBRACKAS VIDEO COMPRESSION) are registered trademarks of US AVOCENT in the United States and other countries.

The ft remote management card, adopts the DVC technology of AVOCENT US.

The patent numbers for the DVC technology of AVOCENT US:

US Patent Number: 5,732,212/5,937,176/6,633,905/6,681,250/6,701,380 (other patents pending)

Taiwanese Patent Number: 173784

European Patent Number: 0 740 811

To prevent voltage sag:

This product may be affected by voltage sag caused due to lightning. To prevent voltage sag, you are recommended to use an AC uninterruptible power supply (UPS) unit.

Notes:

- (1) No part of this manual may be reproduced in any form without prior written permission of the manufacturer.
- (2) The contents of this manual are subject to change without prior notice.
- (3) The contents of this manual shall not be copied or altered without prior written permission of the manufacturer.
- (4) All efforts have been made to ensure the accuracy of all information in this manual. If you find any part unclear, incorrect, or omitted in this manual, contact the sales agent where you purchased this product.
- (5) The manufacturer assumes no liability arising from the use of this product, nor any liability for incidental or consequential damage arising from the use of this manual regardless of (4) above.

PREFACE

Welcome to the Fault Tolerant Server series.

Fault Tolerant Server series is a “fault-tolerant (ft)” server focusing on “high reliability” in terms of fault-tolerance, in addition to “high performance,” “scalability,” and “general versatility” provided by the series. In the event of trouble, its dual configuration will allow the system to instantaneously isolate the failed parts to assure non-stop running; operation will be moved smoothly from one module to the other, minimizing damage to it. You can use this Fault Tolerant Server series in a mission-critical system where high availability is required. By the use of Windows Server 2003 operating system, it also provides outstanding openness for general-purpose applications, etc.

To make the best use of these features, read this User's Guide thoroughly to understand how to operate Fault Tolerant Server series.

ABOUT THIS USER'S GUIDE

This User's Guide helps a user to properly setup and use the product.

Consult this guide to ensure safety as well as to cope with trouble during a system setup and daily operation.

Keep this manual handy.

This User's Guide is intended for users who have a good knowledge on the basic use of Windows operating systems and general I/O devices such as a keyboard and mouse.

How to Use This User's Guide

This guide consists of eight chapters and appendices. To help you find a solution quickly, the guide contains the following information:

For descriptions on setting up this product, see the separate volume "User's Guide (Setup)."

Read "Precautions for Use" first.

Before going on to main chapters, be sure to read "Precautions for Use." These precautions are very important for using the product safely.

Chapter 1 Precautions for Use

This chapter describes precautions necessary to use the product safely and properly. Be sure to read this chapter before using the product. It also provides information on user support. It will be helpful when you need maintenance service, support, etc.

Chapter 2 General Description

This chapter describes what you should know about the product: its component names, functions, operating procedures as well as handling of devices and other parts.

Chapter 3 Windows Setup and Operation

This chapter describes setup and operation specific to the product when it is on Windows.

Chapter 4 System Configuration

This chapter describes how to make settings of built-in basic input/output system. It also describes factory-shipped parameters.

Chapter 5 Installing and Using Utilities

This chapter describes features and operating procedures of a standard utility "EXPRESSBUILDER." It also describes procedures to install and operate various software programs contained in its DVD.

Chapter 6 Maintenance

This chapter describes maintenance procedures and use of maintenance tools. If you need to move the product for maintenance purposes, follow the steps provided in this chapter.

Chapter 7 Troubleshooting

If the product does not work properly, see this chapter before deciding that it is a breakdown.

Chapter 8 System Upgrade

This chapter describes procedures to add options and precautions. See also this chapter when you replace failed components.

Appendix A Specifications

This appendix lists specifications of the product.

Appendix B I/O Port Addresses

This appendix lists factory-assigned I/O port addresses.

Additional symbols

The following symbols are used throughout this User's Guide in addition to the caution symbols describe at the beginning.

IMPORTANT:	Important points or instructions to keep in mind when using the server or software
CHECK:	Something you need to make sure when using the server of software
TIPS:	Helpful information, something useful to know

Accessories

This product is shipped with various accessories. See the packing list to make sure everything is included and check the individual items. If some component is missing or damaged, contact your sales agent.

- Keep the accessories in a safe place. You will need them when you perform setup, addition of options, or replacement of failed components.
- To check EXPRESSBUILDER components, see the attached list.
- Be sure to fill out and mail the software registration card that is attached to your operating system.
- Make backup copies of included floppy disks, if any. Keep the original disks as the master disks; use these copies in operation.
- Improper use of an included floppy disk or DVD may alter your system environment. If you find something unclear, stop using them and contact your sales agent.

Chapter 1

Precautions for Use

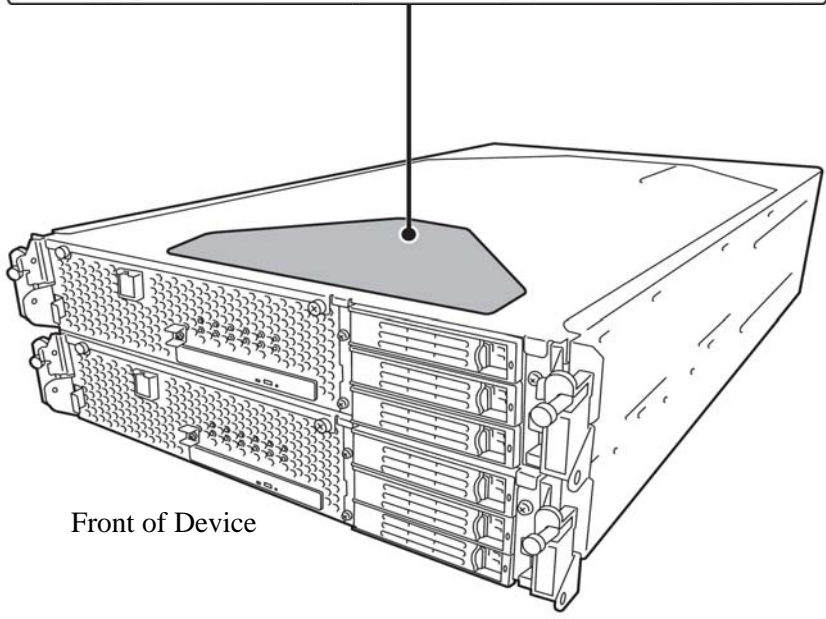
This chapter includes information necessary for proper and safe operation of the server.

WARNING LABELS

Warning label is placed in the certain part of the system so that the user stays alert to possible risks. Do not remove or damage the label.

If this label is missing, about to peel off, or illegible, contact your sales agent.

The figures below show the location of this label on the server.











Front of Device

PRECAUTIONS FOR SAFETY

This section provides precautions for using the server safely. Read this section carefully to ensure proper and safe use of the server. For symbol meanings, see "SAFETY INDICATIONS" described in the previous section.

General

 WARNING	
	<p>Do not use the equipment in an operation where human lives are involved or high reliability is required.</p> <p>This equipment is not intended for use and control in facilities/systems where human lives are involved or high reliability is required, including medical devices or nuclear, aerospace, transportation, and traffic control facilities. The manufacturer assumes no liability for any accidents or damage to physical assets resulting from the use of this equipment in such systems or facilities.</p>
	<p>Do not continue to use the equipment if you detect smoke, odor, or noise.</p> <p>If the equipment emits smoke, odor, or noise, immediately flip off the POWER switch, unplug the cord, and contact your sales agent. There is a risk of a fire.</p>
	<p>Do not insert a wire or metal object.</p> <p>Do not insert a wire or metal objects into a vent or disk drive slot. There is a risk of an electric shock.</p>
	<p>Do not use the equipment in an unsuitable place.</p> <p>Do not install a server rack in an unsuitable environment. Other systems also may be affected, and the rack may fall over to cause a fire or injuries. For details about installation environment and quake-resistant engineering, see the attached manual or contact your sales agent.</p>

 CAUTION	
 	<p>Prevent water or foreign objects from getting into the equipment.</p> <p>Do not let water or foreign objects (e.g., pins or paper clips) enter the equipment. There is a risk of a fire, electric shock, and breakdown. When such things accidentally enter the equipment, immediately turn off the power and unplug the cord. Contact your sales agent instead of trying to disassemble it yourself.</p>

Use of Power Supply and Power Cord

WARNING



Do not handle a power plug with a wet hand.
Do not plug/unplug a power cord with a wet hand.
There is a risk of an electric shock.



Do not connect the ground wire to a gas pipe.
Never connect the ground wire to a gas pipe.
There is a risk of a gas explosion.

CAUTION



Do not plug the attached cord in a nonconforming outlet.



Use a wall outlet with specified voltage and power type.
There is a risk of a fire or current leakage.
Avoid installing the equipment where you may need an extension cord. If the cord that does not meet the power specifications, there is a risk of overheating that could lead to a fire.



Do not plug multiple cords in a single outlet.

If the rated current is exceeded, there is a risk of overheating that could lead to a fire.



Do not plug the cord insecurely.

Insert the plug firmly into an outlet. There is a risk of heat or fire due to poor contact. If dust settles on the slots and it absorbs moisture, there is also a risk of heat or fire.



Do not use nonconforming power cords.



AC cord is to spend the thing of the next specifications.
You also have to observe the following prohibitions about handling and connecting interface cables.

- Do not pull on the cord.
- Do not pinch the cord.
- Do not bend the cord.
- Keep chemicals away from the cord.
- Do not twist the cord.
- Do not tread on the cord.
- Do not place any object on the cord.
- Do not use cords as bundled.
- Do not alter, modify, or repair the cord.
- Do not staple the cord.
- Do not use any damaged cord. (Replace it with a new one of the same specifications. For replacement procedures, contact your sales agent.)

Installation, Relocation, Storage and Connection

WARNING



Disconnect the power cord(s) before installing or removing the equipment.

Be sure to power off the equipment and unplug its power cords from the wall outlet before installation/relocation. All voltage is removed only when the power cords are unplugged.

CAUTION



Do not install or store the equipment in an unsuitable place.

Install or store the equipment in such a place as specified in this User's Guide. Avoid the following, or there is a risk of a fire.

- a dusty place
- a humid place located near a boiler, etc
- a place exposed to direct sunlight
- an unstable place



Be careful not to hurt your fingers.

Exercise great care not to hurt your fingers on the rail when you mount/dismount the equipment into/from the rack.



Do not use or store this product in corrosive environment.

Avoid the usage or storage of this product in an environment which may be exposed to corrosive gases, such as those including but not limited to: sulfur dioxide, hydrogen sulfide, nitrogen dioxide, chlorine, ammonia and/or ozone.

Avoid installing this product in a dusty environment or one that may be exposed to corrosive materials such as sodium chloride and/or sulfur.

Avoid installing this product in an environment which may have excessive metal flakes or conductive particles in the air.

Such environments may cause corrosion or short circuits within this product, resulting in not only damage to this product, but may even lead to be a fire hazard.

If there are any concerns regarding the environment at the planned site of installation or storage, please contact your sales agent.

⚠ CAUTION

Do not connect any interface cable with the power cord of the server plugged to a power source.



Make sure to power off the server and unplug the power cord from a power outlet before installing/removing any optional internal device or connecting/disconnecting any interface cable to/from the server. If the server is off-powered but its power cord is plugged to a power source, touching an internal device, cable, or connector may cause an electric shock or a fire resulted from a short circuit.



Do not use any non-designated interface cable.

Use only interface cables designated by the manufacturer; identify which component or connector to attach beforehand. If you use a wrong cable or make a wrong connection, there is a risk of short-circuit that could lead to a fire. You also have to observe the following prohibitions about handling and connecting interface cables:

- Do not use any damaged cable connector.
- Do not step on the cable.
- Do not place any object on the cable.
- Do not use the equipment with loose cable connections.
- Do not use any damaged cable.

Cleaning and Handling of Internal Devices

⚠ WARNING



Do not disassemble, repair, or alter the server.



Unless described herein, never attempt to disassemble, repair, or alter the equipment. There is a risk of an electric shock or fire as well as malfunction.



Do not look into the DVD-ROM drive.



The DVD-ROM drive uses a laser beam. Do not look or insert a mirror inside while the system is on. A laser beam is invisible; if your eyes are exposed to the laser beam, there is a risk of losing eyesight.



Do not detach a lithium battery yourself.

This equipment has a lithium battery. Do not detach it yourself. If the battery is exposed to fire or water, it could explode.

When the lithium battery is running down and the equipment doesn't work correctly, contact your sales agent. Do not disassemble replace or recharge the battery yourself.



Disconnect the power plug before cleaning the server.

Make sure to power off the server and disconnect the power plug from a power outlet before cleaning or installing/removing internal optional devices. Touching any internal device of the server with its power cord connected to a power source may cause an electric shock even if the server is off-powered.

Disconnect the power plug from the outlet occasionally and clean the plug with a dry cloth. Heat will be generated if condensation is formed on a dusty plug, which may cause a fire.

⚠ CAUTION



High temperature

Immediately after powering off the system, system components such as hard disk may be very hot. Wait for the server to cool down completely before adding/removing components.



Make sure to complete installation.

Firmly install all power cords, interface cables and/or boards. An incompletely installed component may cause a contact failure, resulting in fire and/or smoke.

⚠ CAUTION



Protect the unused connectors with the protective cap.



The unused power cord connectors are covered with the protective cap to prevent short circuits and electrical hazards. When removing the power cord connector from the internal devices, attach the protective cap to the connector. Failure to follow this warning may cause a fire or an electric shock.

During Operation

CAUTION



Do not pull out a device during operation.

Do not pull out or remove a device while it works. There is a risk of malfunction and injuries.



Do not touch the equipment when it thunders.

Unplug the equipment when it threatens to thunder. If it starts to thunder before you unplug the equipment, do not touch the equipment and cables. There is a risk of a fire or electric shock.



Keep animals away.



Animal's waste or hair may get inside the equipment to cause a fire or electric shock.



Do not place any object on top of the server.

The object may fall off to cause injuries, damage to hardware and/or a fire.



Do not leave the DVD tray ejected.

Dust may get in the equipment to cause malfunction. The ejected tray may also become a cause of injuries.

Rack-mount Model

CAUTION



Do not install the equipment on a nonconforming rack.

Install the equipment on a 19-inch rack conforming to the EIA standard. Do not use the equipment without a rack or install it on a nonconforming rack. The equipment may not function properly, and there is a risk of damage to physical assets or injuries. For suitable racks, contact your sales agent.



Do not attempt to install the server yourself.

To avoid a risk of injuries, users should not attempt to install the equipment into a rack. Installation should be performed by trained maintenance personnel.

< For Maintenance Personnel Only >



Do not install the equipment in such a manner that its weight is imposed on a single place.

To distribute the weight, attach stabilizers or install two or more racks. It may fall down to cause injuries.



Do not assemble parts alone.

It takes at least two people to mount doors and trays to a rack. You may drop some parts to cause a breakage or injuries.



Do not pull a device out of the rack if it is unstable.

Before pulling out a device, make sure that the rack is fixed (by stabilizers or quake-resistant engineering).



Do not leave two or more devices pulled out from the rack.

If you pull out two or more devices the rack may fall down. You can only pull out one device at a time.



Do not install excessive wiring.

To prevent burns, fires, and damage to the equipment, make sure that the rated load of the power branch circuit is not exceeded. For more information on installation and wiring of power-related facilities, contact your electrician or local power company.



Do not pull out a device from the rack during operation.

Do not pull out a device while it works. There is a risk of malfunction and injuries.

For Proper Operation

Observe the following instructions for successful operation of the server. Failure to observe them could lead to malfunction or breakdown.

- Do not use a cellular phone or pager around the equipment. Turn off your cellular phone or pager when you use the equipment. Their radio waves may cause the equipment to malfunction.
- Perform installation in a place where the system can operate correctly. For details, see the separate volume "User's Guide (Setup)."
- Before turning off the power or ejecting a disk, make sure that the access LED is off.
- When you have just turned off the power, wait at least 30 seconds before turning it on again.
- Once you have turned on the server, do not turn it off until the full screen logo appears.
- After plugging in the power cord, do not turn on the power of the equipment for 30 seconds.
- For safe operation, it is recommended to reboot the OS after duplication is completed.
- Before you move the equipment, turn off the power and unplug the cord.
- This server shall not assure reproduction of copy-protect CDs using reproduction equipment if such disks do not comply with CD standards.
- Clean the equipment regularly. (For procedures, see Chapter 6.) Regular cleaning is effective in preventing various types of trouble.
- Lightning may cause voltage sag. As a preventive measure, it is recommended to use UPS (uninterruptible power supply).

This equipment does not support the connection through an UPS serial port (RS-232C) or the control using PowerChute *Plus*.

- Check and adjust the system clock before operation in the following conditions:
 - After transporting the equipment
 - After storing the equipment
 - After the equipment halt under the conditions which is out of the guaranteed environment conditions (Temperature: 10 to 35°C, Humidity: 20 to 80%).

Check the system clock once in a month. It is recommended to operate the system clock using a time server (NTP server) if it is installed on the system which requires high level of time accuracy. If the system clock goes out of alignment remarkably as time goes by, though the system clock adjustment is performed, contact your sales agent.

- When you store the equipment, keep it under storage environment conditions (Temperature: -10 to 55°C, Humidity: 20 to 80%, non-condensing).
- If Fault Tolerant Server series, the built-in optional devices, and the media set for the backup devices (tape cartridges) are moved from a cold place to a warm place in a short time, condensation will occur and cause malfunctions and breakdown when these are used in such state. In order to protect important stored data and assets, make sure to wait for a sufficient period of time to use the server or components in the operating environment.

Reference: Length of the time effective at avoiding condensation in winter (more than 10°C differences between room temperature and atmospheric temperature)

Disk devices: Approximately 2-3 hours

Tape media: Approximately 1 day

- Make sure that the optional devices are attachable and connectable to the equipment. There is a risk of malfunctions that could lead to a breakdown of the equipment even if you could attach and connect.
- Make sure that your options are compatible with the system. If you attach any incompatible option, there is a risk of malfunction that could lead to a breakdown.
- It is recommended to use the manufacturer's genuine option products. Some competitors' products are compatible with this server. However, servicing for trouble or damage resulting from such a product will be charged even within the warranty period.

DISPOSAL OF EQUIPMENT AND CONSUMABLES

- When you dispose of the main unit, hard disk drives, floppy disks, DVDs, optional boards, etc., you need to observe your local disposal rules. Dispose the attached power cable along with the equipment to avoid being used with other equipment.

For details, ask your municipal office.


IMPORTANT:

For disposal (or replacement) of batteries on the motherboard, consult with your sales agent.

You are responsible for wiping out such data before disposal. Erase all data on the hard disk, backup data cartridges, floppy disks, or other writable media (such as CD-R and CD-RW); prevent your data from being restored and reused by a 3rd party. You need to exercise sufficient care to protect privacy and confidential information.

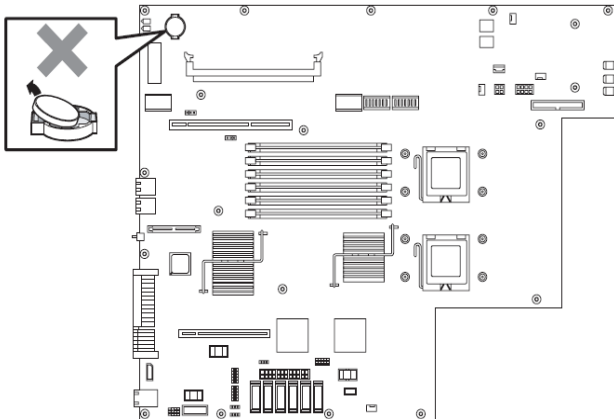
- Some of the system components have limited lifetime (e.g., cooling fans, built-in batteries, built-in DVD-ROM drive, floppy disk drive and mouse). For stable operation, it is recommended to replace them regularly. For lifetime of individual components and replacing procedures, ask your sales agent.

⚠ WARNING



Do not detach a lithium battery yourself.

This equipment has a lithium battery. Do not detach it yourself. If the battery is exposed to fire or water, it could explode.
RISK OF EXPLOSION IF BATTERY IS REPLACED WITH INCORRECT TYPE.
DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.
When the lithium battery is running down and the equipment doesn't work correctly, contact your sales agent. Do not disassemble, replace or recharge the battery yourself.



IF SYSTEM TROUBLE IS SUSPECTED

Before sending the equipment for repair, try the following:

1. Check if its power cord and connection cables are attached correctly.
2. See “Error Messages” in Chapter 7 to check if there is a relevant symptom. If yes, take measures as instructed.
3. Certain software programs are required for operation of Fault Tolerant Server series. Check if these programs are properly installed.
4. Use a commercially available anti-virus program to check the server.

If the problem isn't solved by the above actions, stop using the server and consult with your sales agent. In this case, check LED indications of the server and alarm indications on the display, which will serve as helpful information at the time of repair.

ABOUT REPAIR PARTS

The minimum duration of holding repair parts of this equipment may be different for each country, so contact your sales representatives.

Advice for Your Health

Prolonged use of a computer may affect your health. Keep in mind the following to reduce stresses on your body:

Sit in a good posture

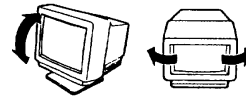
Sit on your chair with your back straight. If the desk height is appropriate, you will slightly look down at the screen and your forearms will be parallel to the floor. This “good” work posture can minimize muscle tension caused by sedentary work.

If you sit in a “bad” posture—for example, sit round-shouldered or with your face too close to the display—you may easily suffer fatigue or have your eyesight affected.



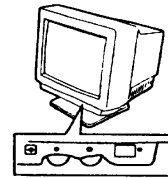
Adjust the installation angle of Display

Most types of displays allow you to adjust the angle vertically and horizontally. This adjustment is very important to prevent the reflection of light as well as to make the screen more comfortable to see. Without this adjustment, it is difficult to maintain a “good” work posture and may get tired soon. Be sure to adjust the angle before using the display.



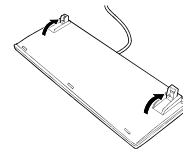
Adjust Brightness and Contrast

Displays allow you to adjust brightness and contrast. Optimum brightness and contrast vary depending on the individual, age, brightness of the room, etc; you need to make an adjustment accordingly. If the screen is too bright or too dark, it is bad for your eyes.



Adjust the installation angle of Keyboard

Some types of keyboards allow you to adjust the angle. If you adjust the angle to make the keyboard more comfortable to use, you can greatly reduce stresses on your shoulders, arms, and fingers.



Clean the Equipment

Cleanliness of the equipment is very important not only for reasons of appearance but also from the viewpoints of function and safety. Especially, you need to regularly clean the display, which gets unclear due to the accumulation of dirt.

Take a break when you get tired

If you feel tired, you are recommended to refresh yourself by taking a short break or doing a light exercise.



This page is intentionally left blank

Chapter 2

General Description

This chapter describes what you need to know to use the Fault Tolerant Server series. Refer to this chapter when you want to know about certain components and how to operate them.

STANDARD FEATURES

The Fault Tolerant Server series is the server that has hardware for two servers.

High performance

- Quad-Core Intel® Xeon™ Processor (2.00GHz/3.00GHz)
- High-speed Ethernet interface (1000Mbps/100Mbps/10Mbps supported)
- High-speed disk access (SAS (Serial Attached SCSI))

Expandability

- Three slots
 - Low Profile (PCI-X bus, 133MHz) x 1
 - Full Size (PCI-X bus, 133MHz) x 1
 - Full Height (PCI-Express x 4 lane) x 1
- Large capacity memory (max: 24 GB)
- USB interface

High-reliability

- Memory monitoring feature (1-bit error correction/ 2-bit error detection)
- Bus parity error detection
- Error notification
- BIOS password feature

Management Utilities

- NEC ESM PRO

Ready-to-use

- Quick cableless connection: hard disk, CPU/IO module

Fault-tolerant Feature

- Redundant modules achieved within a system
- Higher hardware availability by isolation of failed module

Various Features

- Graphic accelerator "ES1000" supported
- DVD Combo

Self-diagnosis

- Power On Self-Test (POST)
- Test and Diagnosis (T&D) Utility

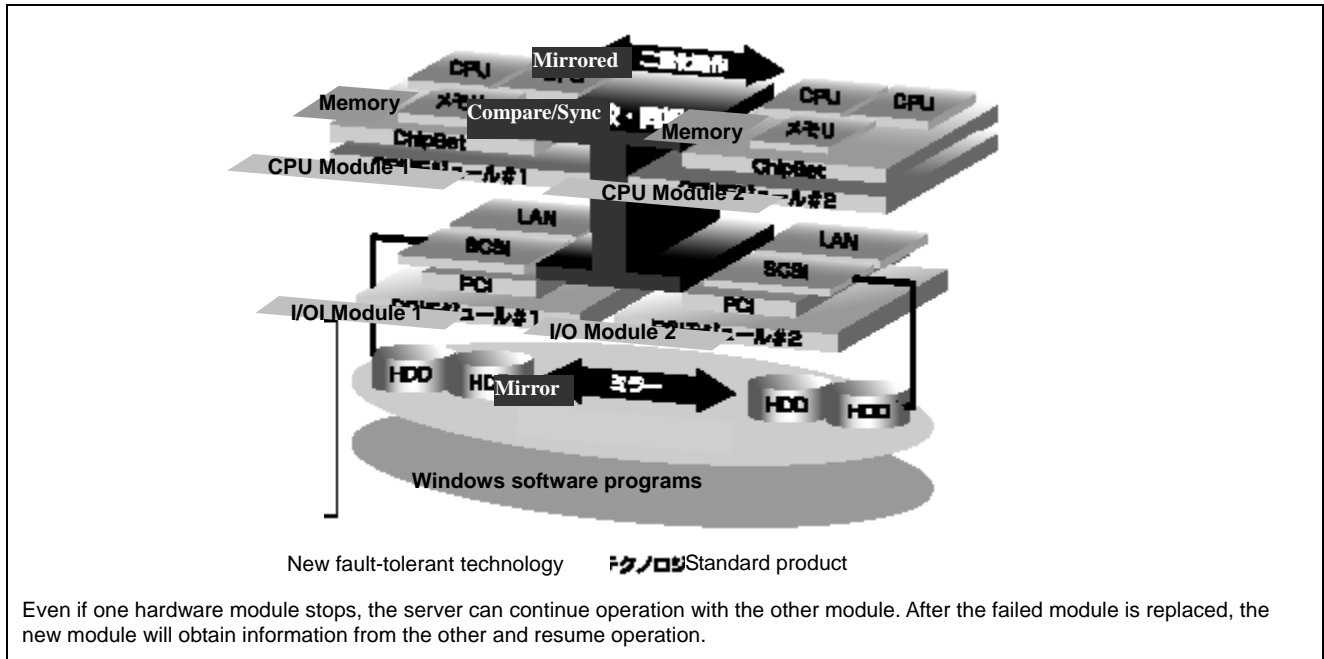
Maintainability

- Off-line Maintenance Utility

Easy and Fine Setup

- EXPRESSBUILDER (system setup utility)
- SETUP (BIOS setup utility)

Hardware modules work while synchronizing and comparing with each other. Even if one hardware module stops, the server can continue its operation as the service with the other hardware module.



Fault Tolerant Server series is a highly fault-tolerant Windows server that achieves continuous computing operations, data storage mirror, and continuous network connection. It allows you to run Windows Server 2003-based applications.

Fault Tolerant Server series achieves continuous computing operations for the Windows server and server-based applications with its redundant CPU processing and redundant memory. It assures data redundancy through duplication of server data on an independent storage system. These features eliminate server downtime that is usually caused by network disconnection or trouble with the I/O controller, Ethernet adapter or disk drive, and support operation of the network and server applications continuously. While being transparent to application software, Fault Tolerant Server series achieves high fault-tolerance.

Fault Tolerant Server series detects status changes, errors and other events and notifies the Windows Event Log of these events. If you use an alarm notification tool, you can configure Fault Tolerant Server series to notify you when certain events occur.

NEC ESMPRO is installed on the system as a server management solution. NEC ESMPRO, a GUI-based management tool, allows you to monitor, view, and configure Fault Tolerant Server series. This tool also supports both local and remote management of Fault Tolerant Server series.

Fault Tolerant Server series mainly provides the following advantages:

- **Highly fault-tolerant processing and I/O subsystems**
Fault Tolerant Server series use redundant hardware and software to assure server operation even if one module suffers trouble with its processor, memory, I/O (including trouble related to the I/O controller), disk drive, or Ethernet adapter.
- **Continuous network connection**
Fault Tolerant Server series maintains continuous network connection by detecting any trouble with the network adapter, connection, etc. If trouble occurs, the standby network connection will take over all network traffic processing and thus securely maintain the network system connection of Fault Tolerant Server series without losing network traffic or client connection.
- **Support of multiple network connections**
Since Fault Tolerant Server series can support multiple Ethernet connections, you can add network redundant control or network traffic control.
- **Industry standard hardware platform**
Fault Tolerant Server series uses IA (Intel Architecture)-based system hardware.
- **No need to modify applications**
You can run Windows Server 2003-compliant applications on Fault Tolerant Server series. Thus, unlike other highly fault-tolerant products, special API or scripts are not necessary.
- **Automatic mirroring**
Fault Tolerant Server series automatically maintains data as the current data.
- **Automatic detection and notification of faults**
Fault Tolerant Server series detects and sorts out all events such as general status changes and faults, and notifies Windows Event Log of these events.
- **Transparent migration**
Fault Tolerant Server series constantly monitors events. If trouble occurs on Fault Tolerant Server series' server module, it will transparently use a redundant module of the failed module. This feature maintains data and user access without losing application service.
- **Automatic reconfiguration**
When the failed module restarts after the trouble is corrected, Fault Tolerant Server series will perform reconfiguration automatically, and if necessary, resynchronize the affected modules. Reconfiguration can include CPU processing (e.g., CPU memory), server's operating system (and related applications), and system data stored on the hard disks. In most cases, Fault Tolerant Server series automatically restores redundancy of the server modules after recovery.

- Local and remote management

Fault Tolerant Server series uses NEC ESMPRO as a server management tool. This tool uses a GUI that enables monitoring and setting of Fault Tolerant Server series. NEC ESMPRO can be used both locally and remotely on work station PCs or server PCs.

- Event notification function

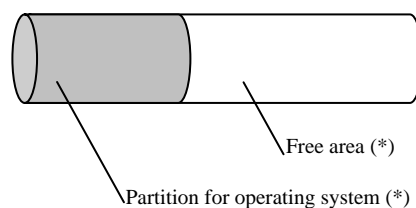
When trouble or other events are detected on Fault Tolerant Server series, they will be notified to Windows Event Log and saved. Therefore, you can view the log items locally or remotely by a usual Windows procedure. Since an Fault Tolerant Server series events use unique IDs, they are easy to distinguish.

- In-service repairing

You can repair or replace a failed module even if Fault Tolerant Server series is operating.

- Partition structure

On this server model, the first logical drive will be the following state when the setup by EXPRESSBUILDER is complete.



* The size varies depending on the specification at setup.

CHECK:

The partition for operating system is not mirrored at the time of EXPRESSBUILDER setup completion. Mirror the partition separately.

- Windows OS and media

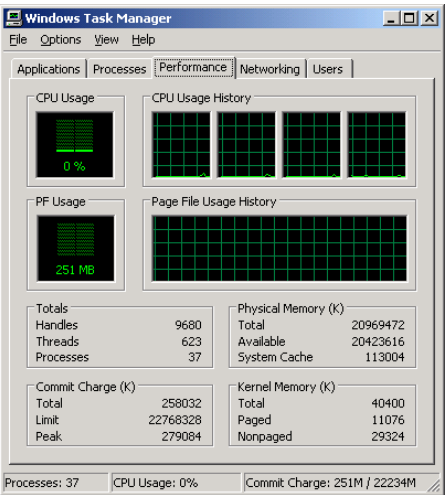
The Windows OS media used on Fault Tolerant Server series are not specifically processed for it. The standard operating methods of Windows are same as general.

HOW THE OPERATING SYSTEM SEES THE CPU MODULES

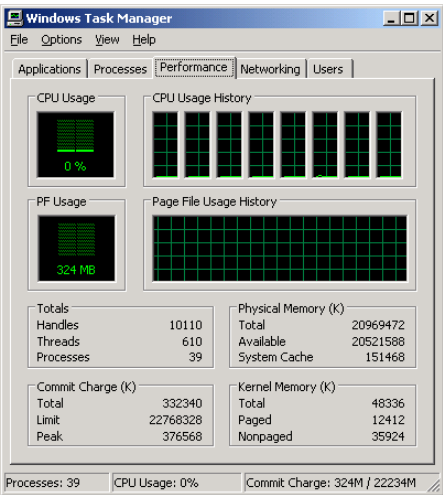
On Fault Tolerant Server series, the CPU modules are redundantly configured and all processors installed on this server are shown.

How CPU modules appear on Task Manager

CPU's are displayed as many as there are.



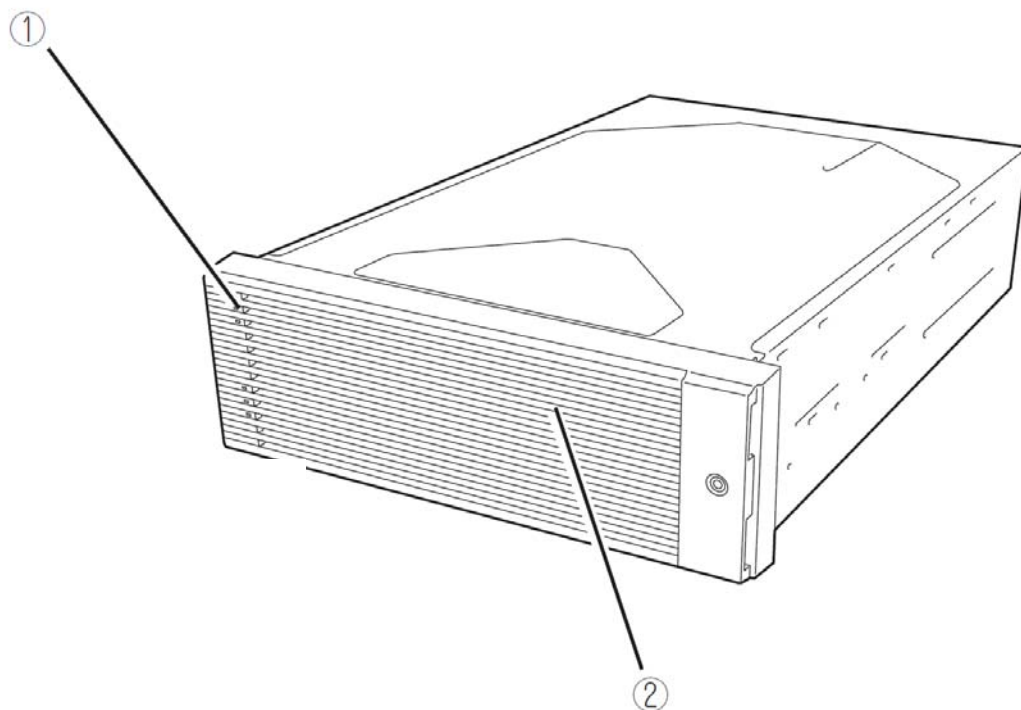
System with one CPU (Quad-Core)



System with two CPUs (Quad-Core)

NAMES AND FUNCTIONS OF COMPONENTS

Names and functions of components are shown below:



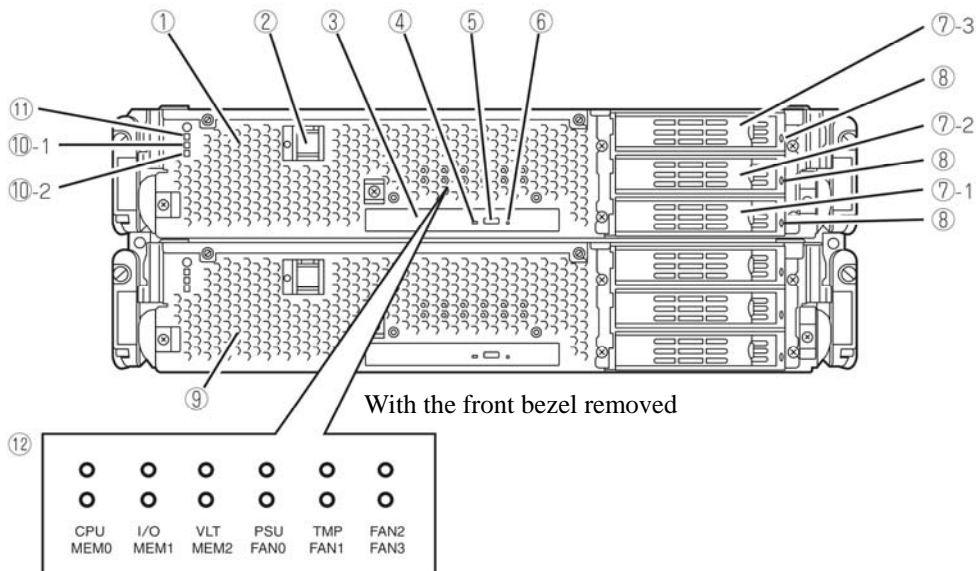
(1) LEDs

For more information see the description on the front view (page 2-8).

(2) Front bezel

The cover to protect devices in the front.

Front View



(1) CPU/IO module 0

This is a module with a set of CPU (processor), memory (DIMM), PCI board, cooling fan unit, and hard disk drive.

(2) POWER switch

This switch is used to power on/off the server. The in-built LED illuminates for the primary CPU/IO module, showing that it is primary. (The secondary POWER LED (off) cannot be used. If the switch is pressed once, the server is powered on. If the switch is pressed again, the server is powered off. If the switch is pressed for more than 4 seconds, the server is forcibly shut down.

(3) DVD-ROM drive

This device is used to read data from DVDs and CD-ROMs.

(4) DISK ACCESS LED

This LED illuminates when the set optical disks are accessed.

(5) Tray eject button

This button ejects the tray.

(6) Forcible eject hole

This is the hole for forcibly eject by inserting a metal pin.

(7) Hard disk drive bay

This is the bay to mount the hard disk drive. The number after the parenthesized number indicates a slot number.

(8) CPU/IO module DISK ACCESS LED (green/amber)

This LED illuminates in green when the internal hard disk drives are accessed. If any internal hard disk drive is failing, the LED illuminates in amber.

(9) CPU/IO module 1

This is a module with a set of CPU (processor), memory (DIMM), PCI board, cooling fan unit, and hard disk drive.

(10)-1 CPU/IO module status LED 1 (amber)

This LED indicates the status of the CPU/IO module. When the module is successfully running, the LED is powered off. If a module has a problem, the LED illuminates in amber.

(10)-2 CPU/IO module status LED 2 (green)

This LED indicates the status of the CPU/IO module. When both of the CPU/IO modules are running, the LED illuminates in green. When one of the modules is running, the LED blinks in green or is powered off.

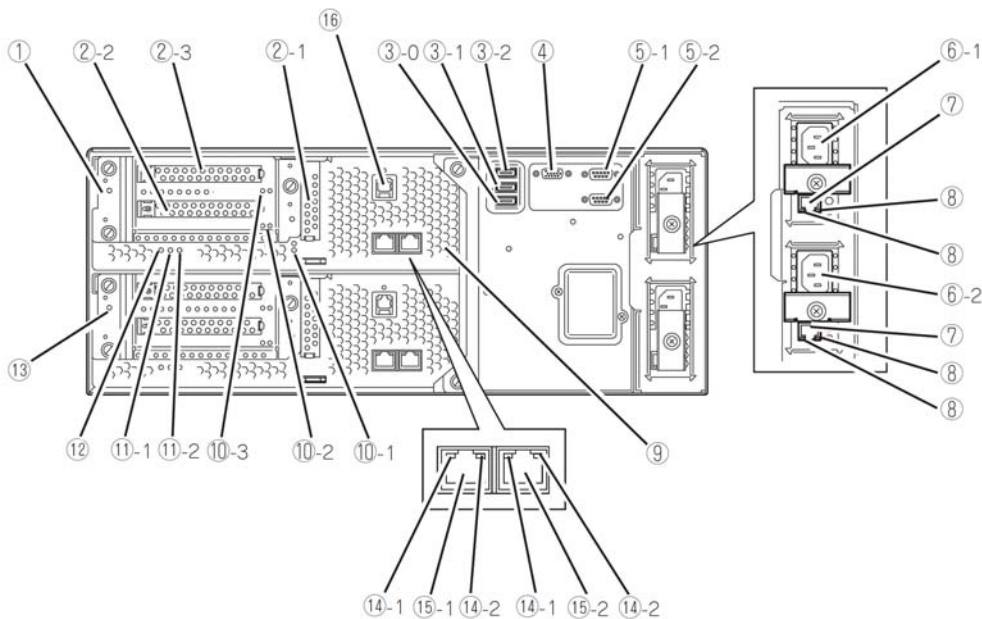
(11) CPU/IO module POWER LED (green)

When the power is turned on, the LED illuminates in green.

(12) EXPRESSSCOPE LEDs (amber)

This LED indicates the fault status of the designated modules. If a module has a problem, the LEDs illuminate in amber.

Rear View



(1) CPU/IO module 0

This is a module with a set of CPU (processor), memory (DIMM), PCI board, and cooling fan unit.

(2)-1, 2 PCI slots 1, 2, 3

(2)-1: A Low Profile type PCI board is mounted on this slot (64 bit 133MHz 3.3V PCI).

(2)-2: A Full Size and Full Height PCI-Express board is mounted on this slot (x8 socket x4 lane).

(2)-3: A Full Size and Full Height PCI board is mounted on this slot (64bit 100MHz 3.3V PCI-X).

(3)-0, 1, 2 USB connector 0, 1, 2

These connectors attach USB2.0-interface-supported devices.

(4) Monitor connector

This is used to attach a display device.

(5)-1, 2 serial port 1, 2 connector

This is used to attach a serial interface connector.

This is not supported with this server model.

(6)-1 AC inlet A connector

A power cord is connected to this socket (for the CPU/IO module 0). If you want make the CPU/IO module 0 primary, connect a power cord to this inlet first.

(6)-2 AC inlet B connector

A power cord is connected to this socket (for the CPU/IO module 1). If you want to make the CPU/IO module 1 primary, connect a power cord to this inlet first.

(7) LAN connector (VTM)

This is not used with this server model.

(8)-1 LINK/ACT LED (VTM)

This is not used with this server model.

(8)-2 Speed LED (VTM)

This LED indicates the transfer speed of LAN(VTM).

(9) DUMP (NMI) switch

This switch executes a memory dump.

Press the DUMP switch on the primary CPU/IO module, whose POWER LED has been blinking, for four to eight seconds.

(10)-1, 2 PCI slot status LEDs (Slot 1, 2, 3)

These LEDs display the status of the PCI slot. The status is shown by the display combination of the 2 LEDs (Refer to the chart on p 2-19).

(11)-1 CPU/IO module status LED 1 (amber)

This LED indicates the status of the CPU/IO module. When the module is successfully running, the LED is powered off. If a module has a problem, the LED illuminates in amber.

(11)-2 CPU/IO module status LED 2 (green)

This LED indicates the status of the CPU/IO module. When both modules are operating, the LED illuminates in green. When one module is operating, the LED blinks in green or is powered off.

(12) CPU/IO module POWER LED (green)

This LED illuminates in green when the system is powered on.

(13) CPU/IO module 1

This is a module with a set of CPU (processor), memory (DIMM), PCI board, and cooling fan unit.

(14)-1 LINK/ACT LED

This LED indicates the access status of the LAN connector.

(14)-2 Speed LED

This LED indicates the transfer speed of the LAN connector.

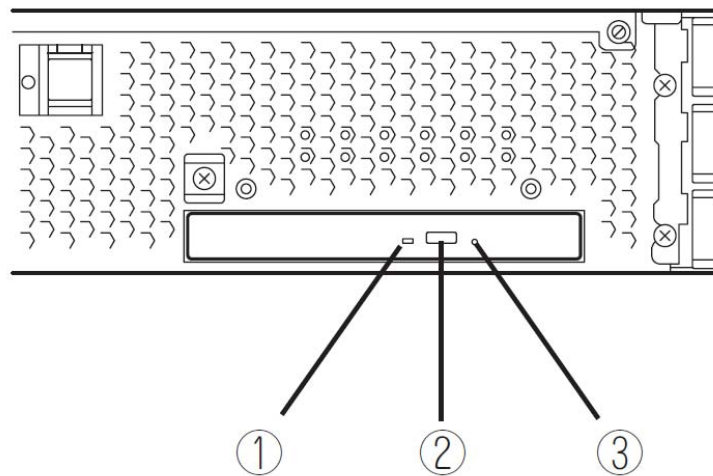
(15)-1, 2 LAN connector 1, 2

These connectors support 1000BASE-T/100BASE-TX/10BASE-T. These are connected to the network system on LAN.

(16)-F-MRC connector

A management device is connected to this connector.

DVD-ROM drive



(1) Status LED

The LED that illuminates while accessing the loaded DVD/CD-ROM

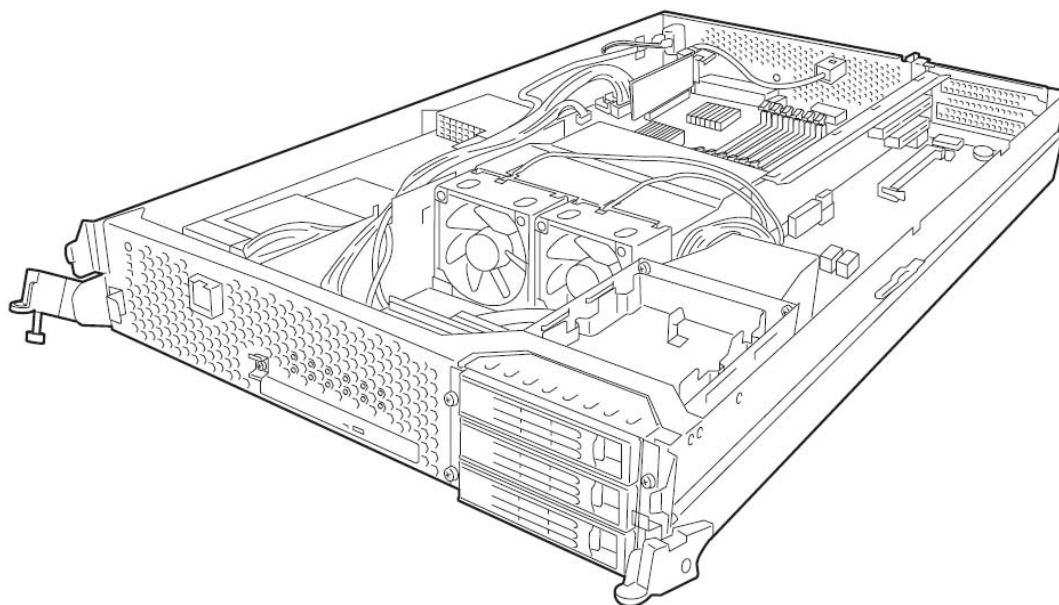
(2) Tray eject button

The button to eject the tray.

(3) Manual release hole

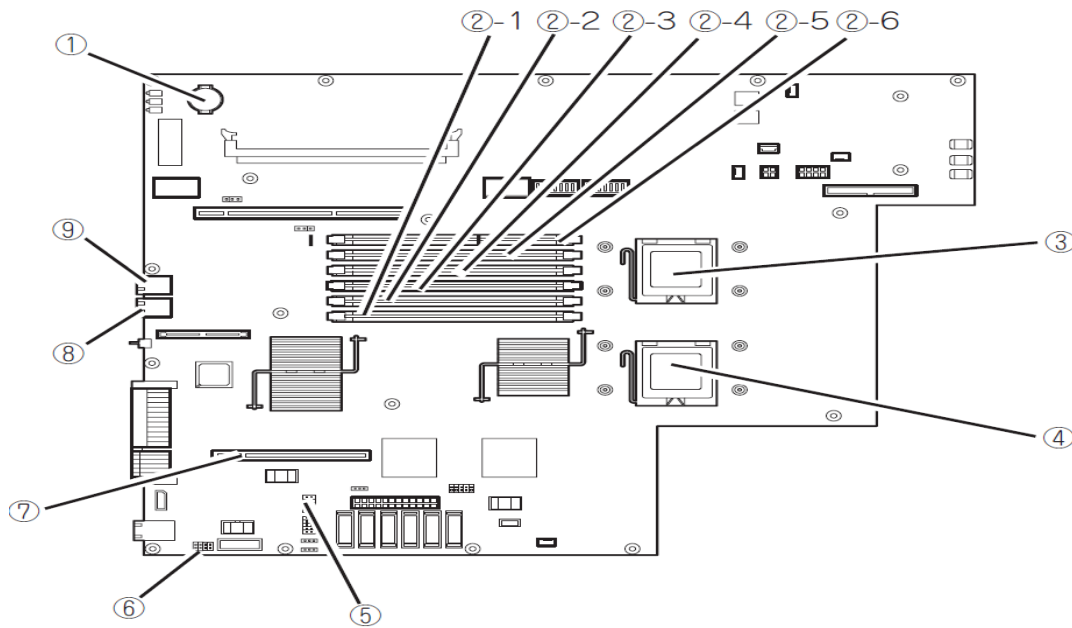
When the eject button does not work, insert a metal pin into this hole to forcefully eject the tray.

CPU/IO Module



CPU/IO module

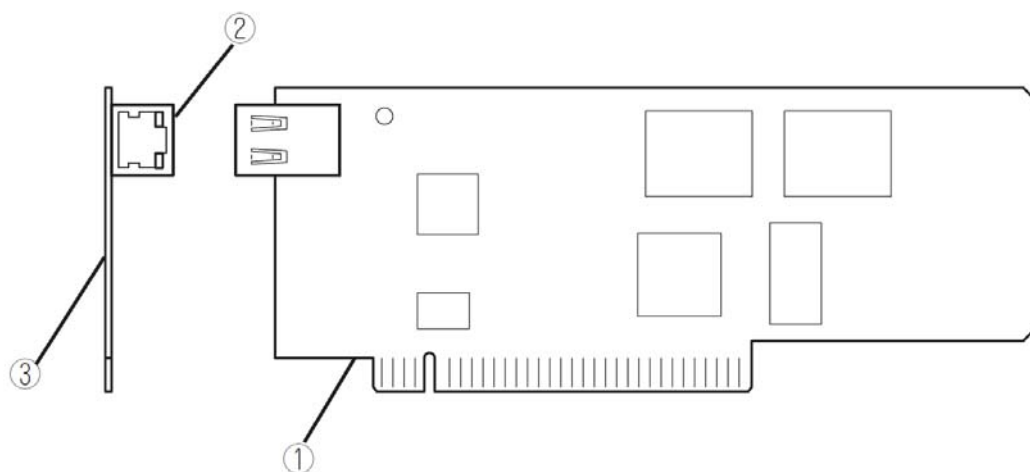
Mother Board



CPU/IO module mother board

- (1) **Lithium battery**
- (2) **DIMM slot ((2)-1 from the bottom)**
 - (2)-1 DIMM CH0 Slot 0
 - (2)-2 DIMM CH0 Slot 1
 - (2)-3 DIMM CH0 Slot 2
 - (2)-4 DIMM CH1 Slot 0
 - (2)-5 DIMM CH1 Slot 1
 - (2)-6 DIMM CH1 Slot 2
- (3) **Processor 0 socket (CPU0)**
- (4) **Processor 1 socket (CPU1)**
- (5) **Jumper switch for clearing CMOS/password**
- (6) **Jumper switch for clearing BMC configuration**
- (7) **F-RMC card slot**
- (8) **LAN 2 connector**
- (9) **LAN 1 connector**

ft Remote Management Card



- (1) Attaching to servers.
This is a card edge part touching to the F-RMC slot inside of the server.

IMPORTANT:

Do not mount this card on other slots or devices in order to avoid a fault.

- (2) Management LAN port
This port can be connected to network system, and supports 100Mbps/10Mbps. The port can't be connected to phone line. The port is also used when managing the server with the management software NEC DianaScope attached on this device.

IMPORTANT:

Communication mode on the management LAN port cannot be manually set or changed because the mode is fixed as auto negotiation mode.

Please set the link partner side (switch/hub) as auto negotiation mode.

- (3) MAC address
On the back side of the management card, a seal is labeled with MAC address printed.
The MAC address can also be confirmed on the server's BIOS Setup screen.

LEDs

POWER LED

The POWER switch of the CPU/IO module has an in-built LED. If the AC power is supplied, the LED of the primary POWER switch illuminates (only the primary POWER switch functions). Also, the CPU/IO module has the POWER LED to show the status of the module power status.

CPU/IO Module POWER LED

LED indication	Description	Action
Not on	Power supply is off.	Check that the status LED 1 on both CPU/IO modules is powered off, and then press the POWER LED to power on the system.
On	Power supply is on.	

CPU/IO Module Status LED 1, 2

There are two kinds of LEDs that indicate the module status on the front and back sides of the CPU/IO module. The display combination of the two LEDs indicates the CPU/IO module status.

Status LED1	Status LED2	Description	Action
Not on	Not on	Power supply is off.	
	Blinking in green	When the system is starting, the initialization process is performed.	Wait for a while; the LED will illuminate in green.
		If the OS is running, duplex configuration is not made for one of the components in the CPU/IO modules.	Check that the cable is firmly connected. If the LED does not illuminate in green after a while, record the status LED status, and contact a maintenance service company.
	Green	The device is duplexed and running normally.	
Amber	Not on	After the AC power is supplied, the device running in the standby power mode is being initialized.	Wait for a while. The status LED 1 will be powered off, and the POWER switch will be enabled.
		When the system is starting, the initialization process is performed.	Wait for a while; the status LED 1 is powered off.
		When the OS is running, the CPU/IO module has a problem.	Check that the cable is firmly connected. If the LED does not illuminate in green after a while, record the status LED status, and contact a maintenance service company.

PCI Slot status LED 1, 2

There are two kinds of LEDs that indicate the PCI slot status on the back of the CPU/IO module. The PCI slot status is indicated by the display combination of the two LEDs.

Status LED1	Status LED2	Description	Action
Not on	Not on	Power supply is off.	
		When the system is starting, the initialization process is performed.	Wait for a while; the LED illuminates in white.
	Blinking in white	If the OS is running, and it is in the Simplex mode, the PCI slot of the other CPU/IO module is degenerated.	Check that the cable is firmly connected. If the LED does not illuminate in white after a while, record the status LED status, and contact a maintenance service company.
	White	If the PCI slot status LED 2 of the other CPU/IO module is on, the device is successfully running in the Duplex mode.	
		If the PCI slot status LED 2 of the other CPU/IO module is blinking, the cable may be disconnected, the option PCI board of the slot has a problem, or the CPU/IO module itself has a problem.	Check that the cable is connected securely. If the PCI slot status LED 2 of the other CPU/IO module does not illuminate white, record the status of the status LED, and call your maintenance service company.
Amber	Not on	When the system is starting, the initialization process is performed.	Wait for a while; the status LED 1 is powered off.
		When the OS is running; 1) The optional PCI board of the slot has a problem. 2) The CPU/IO module has a problem.	Check that the cable is firmly connected. If the LED does not illuminate in white after a while, record the status LED status, and contact a maintenance service company.

Hard Disk Drive LED

Hard Disk LED	Description	Action
Not on	The disk is in the idle state.	
Green	Accessing the disk	
Amber	Disk failure	Contact a maintenance service company.
Blinking in amber (Illuminate in green when accessing the disk)	The mirror of the disk is disconnected.	Perform mirroring.
Blinking in green and amber in turn	The hard disk drive configuration (rebuild) is on going.	Wait for a while; the LED blinks in green after rebuild finishes. If the rebuild fails, the LED illuminates in amber.

Access LED on the DVD-ROM drive

This LED illuminates when the installed DVD or CD-ROM is being accessed.

LAN Connector LED

- LINK/ACT LED

The LINK/ACT LED shows the status of a standard network port. It is green if power is supplied to the main unit and hub, and they are connected correctly ("LINK"). It blinks green while the network port sends or receives data (ACT).

When the LED does not illuminate during "LINK," check the condition and connection of network cables. If there is nothing wrong with the cables, a defect is suspected in the network (LAN) controller. In this case, contact your sales agent.

- Speed LED

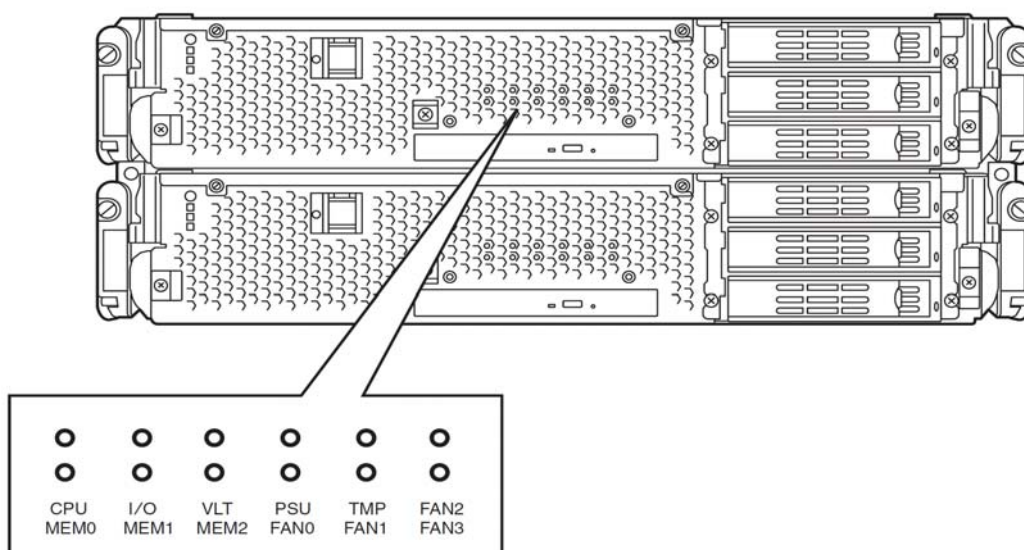
This LED indicates the network interface of the communication mode used by a network port.

1000BASE-T and 100BASE-TX are the supported LAN port types. When this LED illuminates in amber, the port is operating on 1000BASE-T; when in green, 100BASE-TX; and when not illuminate, 10BASE-T.

EXPRESSSCOPE

Corresponding EXPRESSSCOPE LEDs (amber) illuminate when modules have failures.

The LEDs on the upper line correspond to the upper names, and the LEDs on the lower line correspond to the lower names.



CPU (CPU module error LED)

Amber LED illuminates when failure occurs on CPU of CPU/IO module.

I/O (I/O module error LED)

Amber LED illuminates when failure occurs on I/O of CPU/IO module.

VLT (Power error LED)

Amber LED illuminates when electric voltage failure occurs in CPU/IO module.

MEM0 (Memory slot 0 error LED)

Amber LED illuminates when failure occurs on the memory slot 0 of CPU/IO module.

MEM1 (Memory slot 1 error LED)

Amber LED illuminates when failure occurs on the memory slot 1 of CPU/IO module.

MEM2 (Memory slot 2 error LED)

Amber LED illuminates when failure occurs on the memory slot 2 of CPU/IO module.

PSU (Power supply unit error LED)

Amber LED illuminates when failure occurs on the power supply unit of CPU/IO module.

TMP (Abnormal temperature LED)

Amber LED illuminates when temperature in CPU/IO module becomes abnormal.

FAN0 (Fan 0 error LED)

Amber LED illuminates when failure occurs on the cooling fan for CPU0 of CPU/IO module.

FAN1 (Fan 1 error LED)

Amber LED illuminates when failure occurs on the cooling fan for CPU1 of CPU/IO module.

FAN2 (Fan 2 error LED)

Amber LED illuminates when failure occurs on the disk cooling fan of CPU/IO module.

FAN3 (Fan 3 error LED)

Amber LED illuminates when failure occurs on the power supply unit's fan of CPU/IO module.

BASIC OPERATION

This section describes basic operation procedures of Fault Tolerant Server series.

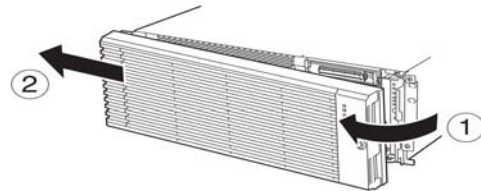
Installing/removing the front bezel

When you power on/off the server, handle the DVD-ROM drive, or remove/install a hard disk drive or CPU/IO module, remove the front bezel.

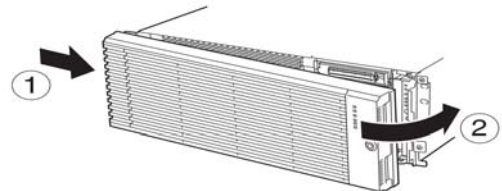
IMPORTANT:

The front bezel can only be removed by unlocking the lock with the security key attached.

- (1) Insert the product-accessory security key into the key slot and push lightly. Turn the key to the left to unlock.
- (2) Hold the right edge of the front bezel and pull it forward.
- (3) Slide the front bezel to take the tab off the frame and remove the front bezel.



When attaching the front bezel, hook the left tab into the server's frame first, then push forward on the right side.



Power ON

To power on Fault Tolerant Server series, press the POWER switch (the one whose in-built LED is illuminating). Follow the steps below to turn on the power.

1. Power on the display unit and other peripheral devices connected to the server.

CHECK:

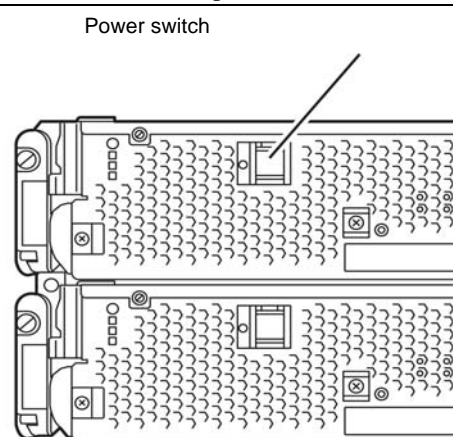
If the power cord is connected to a power controller like a UPS, make sure that it is powered on.

2. Remove the front bezel.
3. Press the power switch located on the front of the front panel.

After a while, a full screen logo will appear on the screen.

IMPORTANT:

Do not turn off the power before you see the full screen logo and a character below the logo.



While the full screen logo is displayed on the screen, Fault Tolerant Server series is performing a power-on self test (POST) to check itself. For details, see “POST Check” described later in this chapter. Upon the completion of POST, Windows Server 2003 will start.

CHECK:

If the server finds errors during POST, it will interrupt POST and display the error message. See Chapter 7.

Power OFF

Follow the steps below to turn off the power. If Fault Tolerant Server series is plugged to a UPS, see manuals included with the UPS or the application that controls the UPS.

1. Perform a normal shutdown from Windows Server 2003.

The system will be powered off automatically. (Note: the POWER switch on the primary side will remain illuminating when AC power is supplied.)

2. Power off all peripheral devices.

POST Check

POST (power-on self test) is a self-test function stored on the motherboard of Fault Tolerant Server series.

When you power on the server, POST will start automatically to check the motherboard, ECC memory modules, CPU/IO modules, keyboard, mouse, etc. It also shows startup messages for various BIOS setup utilities.

According to the factory default settings, the full screen logo appears on the display while POST is being performed. (To view details of POST, press **Esc**.)

TIPS:

- You can view POST details from the beginning without the need to press **Esc** when the BIOS menu is displayed: select [System Configuration] - [Advanced], and set [Boot-time Diagnostic Screen] to “Enabled” (see Chapter 4).
 - You can view the test items and details from a management PC where NEC ESMPRO Manager is installed.
-

You do not always need to check POST details. You will need to check messages when:

- You install a new Fault Tolerant Server series.
- A failure is suspected.
- You hear several beeps between the time of the power-on and OS start-up.
- The display unit shows an error message.

Flow of POST

This section walks you through how POST is performed.

1. When you power on the system, one selected CPU/IO module will start up.
POST will be performed on this selected CPU/IO module.
2. Memory check starts.
A message appears at the upper left of the screen to show that the basic and expanded memories are being counted. The memory check may take a few minutes to complete depending on the server's memory size. Likewise, it may take about one minute for the screen to appear when the server is rebooted.
3. The server starts processor check, IO check, and initialization.
Several messages appear: they show the ID of the selected CPU/IO modules, information on the processor, detection of the keyboard and mouse, etc.
4. A message appears at the lower left of the screen, prompting for startup of the BIOS setup utility "SETUP."

Press <F2> to enter SETUP

You will need to start it when you want to modify the configuration for using the server. Unless this message appears together with an error message, you do not need to start the utility to modify the configuration. (If you wait for a few seconds, POST will go on automatically.)

To start the SETUP utility, press **F2** while the above message is displayed. For setting and parameter functions, see the section of BIOS setup.

When SETUP is completed, the server will reboot itself automatically and perform POST.

5. A message appears prompting for startup of SAS BIOS setup utility.
When a built-in SAS controller is detected, a message will appear prompting for startup of SAS BIOS setup utility. (If you wait for a few seconds, POST will go on automatically.)
If you press **Ctrl + A**, the SAS BIOS setup utility will start. However, you usually do not need to use the setup utility. For setting and parameter functions, see "SAS BIOS" (page 4-33).
When SETUP is complete, the server will reboot automatically and perform POST from the start again.

6. The screen shows the ID numbers of the connected disk drive.
7. Upon completion of POST, the password entry screen appears prior to OS startup.
The password entry screen will appear after the normal termination of POST only if you have set a password in the BIOS setup utility "SETUP."
You can enter a password up to three times. If you enter an incorrect password three times, the startup will be unsuccessful. In this case, turn off the power and then turn it on again after waiting 30 seconds to boot the server.

IMPORTANT:

Do not set a password before installing the OS.

8. Upon completion of POST, the OS will start up.

Behavior at Occurrence of Error

If POST or OS startup does not finish normally, the server will reboot itself automatically.

At the time of reboot, it will select the other CPU/IO module and run POST or OS startup.

In this manner, the server retries POST or OS startup with different combinations of CPU/IO modules. If POST does not finish normally with any combinations, the server will stop with the state of DC OFF or Post end with an error message displayed.

While performing retries, the server displays or registers the error types.

For details of error messages, see Chapter 7 “Troubleshooting.”

POST Error Messages

When the server detects an error during POST, it will notify you of the occurrence in the following manners:

- Displays an error message on the display unit.

These notification methods are described in “POST Error Messages” (Page 7-4).

IMPORTANT:

Before you contact your sales agent, write down the error messages. They will serve as helpful information at the time of maintenance.

CPU/IO Module Status

The CPU/IO module (0 or 1) started first is managed as primary, and the module started later is managed as secondary. If one CPU/IO module is disconnected because of the failure and others, the other module becomes primary.

The CPU/IO module to be started first is selected depending on the primary/secondary status of modules when the server was shut down the last time.

The following devices are connected to the primary CPU/IO module by the hardware switch, although those can be connected to both CPU/IO modules 0 and 1. When one CPU/IO module is disconnected because of a failure, those are switched to the other module automatically and continue operating.

- VGA (display)
- USB device (keyboard, mouse, floppy disk drive)

TIPS:

As for DVD-ROM drive, the DVD-ROM drive of both CPU/IO modules 0 and 1 can be accessed. If one CPU/IO module is disconnected because of the failure, only the DVD-ROM of the other module can be accessed

IMPORTANT:

- If the floppy disk drive is connected, the drive letter may change from A to B by switching CPU/IO modules. Changing of the drive letter does not affect the operation of the server. If the drive letter is changed, access the floppy disk drive with the changed drive letter.
 - The drive letter of the DVD-ROM drive is allocated again automatically. The letter which is not used is allocated to the drive in the order of D to Z. If you want to set the fixed drive letter to the DVD-ROM, specify the drive letter which is not allocated in the order of D to Z after setting the hard disk drive letter.
-

Floppy Disk Drive (Option)

If you want to use a floppy disk drive with this server, connect the USB FDD UNIT, which are available optionally to a USB connector.

This server supports 3.5-inch 2HD (1.44 MB) and 2DD (720KB) floppy disks.

IMPORTANT:

- When using a USB floppy disk drive, the access to the floppy disk is delayed on rare occasions if the display graphic load is high because a moving picture is being played. In such a case, retry the operation with the floppy disk inside the floppy disk drive.
 - The drive letter of the USB floppy disk may be displayed as B instead of A. This does not affect the operation of the server. Use B drive for the floppy disk drive.
-

Insert/Remove Floppy Disk

Before inserting a floppy disk into the drive, make sure that Fault Tolerant Server series is on (the POWER LED illuminates).

Insert a floppy disk into the drive firmly until it snaps in place. The eject button of the drive is then raised slightly.

CHECK:

- You cannot use 1.2 MB-formatted disks.
 - If you insert an unformatted disk, you will see a message that the disk cannot be read or that needs formatting. To format a floppy disk, see your OS manual.
 - If you power on or restart Fault Tolerant Server series with a floppy disk left in the drive, the server will access the floppy disk to start the system. Unless a system exits on the FD, the server will be unable to start.
-

To remove a floppy disk from the drive, press the eject button.

CHECK:

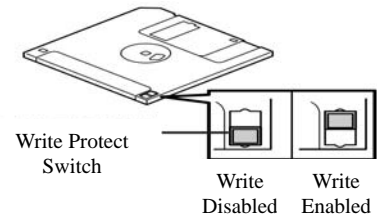
- Before removing a floppy disk, make sure that the floppy disk access LED is off. If you eject a floppy disk while the LED is on, the stored data could be damaged.
 - When using a USB floppy disk drive, the access to the floppy disk is delayed on rare occasions if the display graphic load is high because a moving picture is being played. In such a case, retry the operation with the floppy disk inside the floppy disk drive.
-

Use of Floppy Disk

You may need to store important data on floppy disks. Since the floppy disk is a very delicate medium, you must handle it with extra care:


- Push the floppy disk gently into place.
- Attach the label on a proper position.
- Do not use a pencil or ballpoint pen to write on the floppy disk.
- Do not open the protective shutter.
- Do not use the floppy disk in a dusty place.
- Do not place anything on the floppy disk.
- Do not leave the floppy disk in a place that is subject to direct sunlight or high temperatures (e.g., near a heater).
- Keep away from cigarette smoke.
- Do not leave the floppy disk near water or chemicals.
- Keep away from magnetic objects.

- Do not clip disks. Be careful not to drop.
- Store floppy disks in a protective case where they are kept away from magnetic waves or dust.
- To prevent data from being erased accidentally, the floppy disk has a write-protect notch. When the disk is write-protected, you can read data, but you cannot write the data or format the disk. It is recommendable to write-protect floppy disks that contain important data except when you write data to the floppy disk. To write-protect a 3.5-inch floppy disk, slide the write-protect notch located on its back.
- The floppy disk is a very delicate storage medium. Dust or changes in temperature could cause data to be lost. Data loss could also be caused by faulty operation and computer trouble. To avoid such possible data loss, it is recommendable to back up important data regularly. (Be sure to make back-up copies of the floppy disks that are included with Fault Tolerant Server series.)



DVD-ROM drive

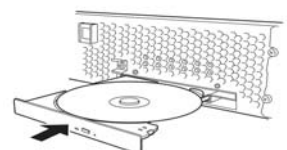
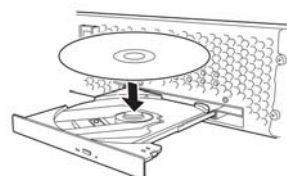
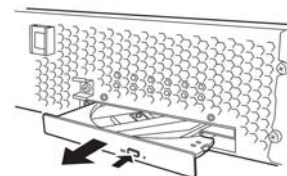
Fault Tolerant Server series has a DVD-ROM drive on the front panel. It is a device used to read data from an optical disk (compact disc read-only memory). Compared to a floppy disk, an optical disk allows for larger volume and fast data readout.

⚠ CAUTION	
	<p>Observe the following instructions to use the server safely. There are risks of a burn, injury, or damage to physical assets. For details, see “PRECAUTIONS FOR SAFETY” in Chapter 1.</p> <ul style="list-style-type: none"> ■ Do not leave the DVD-ROM drive tray ejected.

Insert/Remove DVD-ROM

Follow the steps below to set an optical disk.

1. Before you insert an optical disk, make sure that the server is powered on. When the server is powered on, the LED illuminates in green.
2. Press the tray-eject button located in the front of the DVD-ROM drive. The tray is then ejected.
3. Hold the optical disk with its signaling side facing the tray.
4. As shown in the figure on the right, place the optical disk on the tray and press lightly on the center to lock.
5. Push the front side of the tray gently to the drive-closed position.



IMPORTANT:

If you hear noise while running the DVD-ROM drive, reset the optical disk.

To remove the optical disk, press the tray-eject button as you did in setting the optical disk.

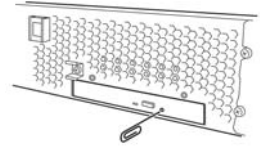
When the access LED illuminates in green, it indicates the optical disk is being accessed. Make sure the access LED is not illuminating in green before you press the tray-eject button.

Press the locking part in the center of the tray and pick the optical disk gently. When you have removed the optical disk, push the tray to the drive-closed position.

When you cannot eject a DVD/CD-ROM

When you cannot eject the optical disk from the server even by pressing the eject button, follow the steps below to eject it:

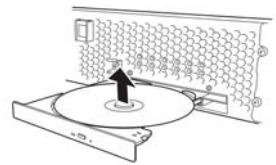
1. Press the POWER switch to power off this server (i.e. the POWER LED is off).
2. Use a metal pin of about 1.2 mm in diameter and 100 mm long (alternatively, you can use a fairly large paper clip after straightening). Insert it gently into the manual release hole located at the low front side of the server until the tray is ejected.



IMPORTANT:

- Do not use a toothpick, plastic pin, or other breakable objects.
 - If you cannot eject the optical disk by following the steps above, contact your sales agent.
-

3. Hold the tray and pull it out.
4. Take out the optical disk.
5. Push the tray back.



Handling optical disks

Observe the following when you use an optical disk on Fault Tolerant Server series:

- As for a disk such as a noncompliant “copy-protected CD,” we shall not guarantee that you can use a CD player to play it with this server.
- Be careful not to drop the optical disk.
- Do not bend or place anything on the optical disk.
- Do not attach labels on the optical disk.
- Do not touch the signal side (blank side).
- Place the optical disk gently on the tray with the printed side up.
- Do not scratch, or use a pencil or ballpoint pen to write on the optical disk.
- Keep away from cigarette smoke.
- Do not leave the optical disk in a place that is subject to direct sunlight or high temperatures (e.g., due to a heater).
- If the optical disk becomes dirty with dust or fingerprints, wipe it gently from its center to edge with a dry soft cloth.
- When you clean the optical disk, use the cleaner expressly meant for it. Do not use a record cleaner (spray), benzine, or thinner.
- Store the optical disk in a protective case when not in use.

Chapter 3

Windows Setup and Operation

This chapter describes setup procedures to make Fault Tolerant Server series ready for use. CPU/IO module has a processor function part and IO function part. In utilities in this chapter, the processor function part is referred to as CPU module and IO function part PCI module.

DISK OPERATIONS

This section explains the disk operation by the RDR (Rapid Disk Resync) function.

Fault Tolerant Server series duplicates disks to secure data by using “Rapid Disk Resync (RDR) function”. This section describes operations such as configuration of dual settings to disks and replacement of disks.

IMPORTANT:

On the disks containing OS, do not create a partition other than the system partition,

Create a data disk partition after configuring the RDR.

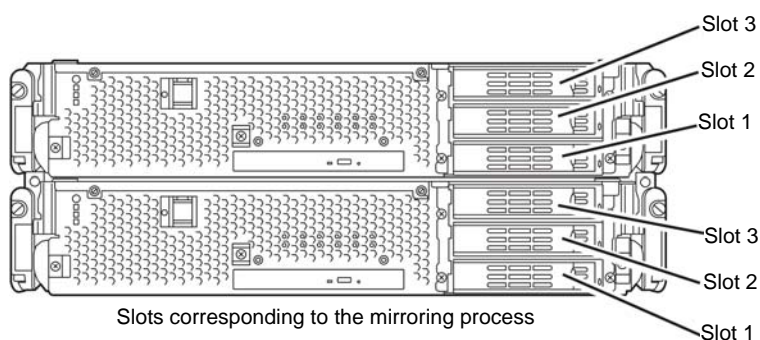
Disk Operations Using the RDR (Rapid Disk Resync) Function

RDR (Rapid Disk Resync)

RDR function of ft control software secures reliability by making disks duplexed per disk. Duplexing disks by the RDR function enables the disks to be resynchronized in a short period of time when their mirror has been broken due to causes such as PCI module replacement.

Setting RDR to disks duplicates the disks of paired slots as shown in the figure below and Windows (ex. Disk Management and Device Manager) recognizes paired disks as a single virtual disk.

[Corresponding slots]



Corresponding slots
PCI module 0 Slot 1 ⇔ PCI module 1 Slot 1
PCI module 0 Slot 2 ⇔ PCI module 1 Slot 2
PCI module 0 Slot 3 ⇔ PCI module 1 Slot 3

Note: In the above table, the PCI module names correspond to the following modules:

PCI module (for CPU/IO module 0): PCI module 0

PCI module (for CPU/IO module 1): PCI module 1

[Cautions for using the RDR function]

1. RDR can be set only to the disks inserted into the built-in slots of Fault Tolerant Server series.
2. Be sure to specify RDR to all disks inserted to the built-in slots and make duplex settings.
3. RDR can be set only to basic disks.
If a span volume or stripe volume is needed, make settings of RDR to a basic disk and then change the disk to a dynamic disk from [Disk Management].
4. The disks to set RDR must have the same capacity and must be new or physically formatted.
(For physical format, refer to “SAS BIOS” in Chapter 4 and perform Format Disk using Disk Utilities.)
5. If the system is shut down (or restarted) while the mirror is broken, or a long time (30 minutes or longer) has passed after the mirror is broken, the mirror resynchronization target will be the entire disk.
For example, if the mirroring has been broken due to a PCI module failure, when you shut down the system and

replace the PCI module in such a state, the entire area of the disk needs to be resynchronized.

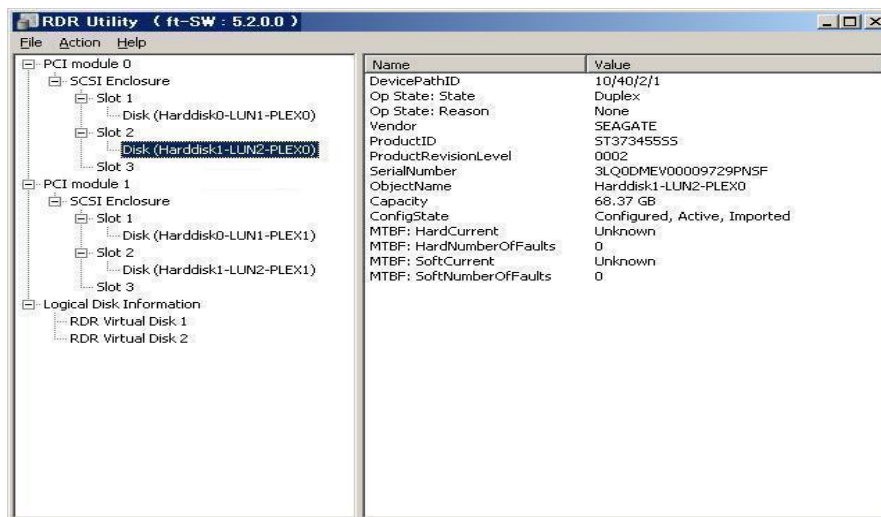
6. You must insert a new disk or replace a disk while the server is powered on.
7. Create a data disk partition after configuring the RDR. If you create a data disk partition before configuring the RDR, the partition's drive letters may be deleted when the RDR is configured.

Configuring and Removing Duplexed Setting of Disks by the RDR Function

This section describes how to make disks duplex and how to remove the settings by using the RDR function. To use the RDR function, use [RDR Utility].

About RDR Utility

- Starting RDR Utility
From [Start], select [All Programs] then [RDR] and click [RDR Utility] to start [RDR Utility].
- Screen



[Left pane]

The tree shows disks inserted to the built-in slots and virtual disks (RDR Virtual Disks) created by RDR. Right-click a disk on the tree to display the menu for setting RDR. By looking at the tree, you can know which disk corresponds to which disk of the Windows' [Disk Management] and whether RDR is set to the disk.

For example, in the case of the disk highlighted in the figure above:

Disk (Harddisk1 - LUN2 - PLEX0)

(1) (2) (3)

- (1) Corresponds to the number of Windows' [Disk Management]. In this example, this disk is the Disk1 on [Disk Management].
- (2) Corresponds to the number of a virtual disk created by RDR setting. In this example, this disk is a disk which makes up the RDR Virtual Disk 2 (only appears for disks with RDR setting).
- (3) This section appears only for disks with RDR setting.

[Right pane]

The properties of the disk selected in the left pane is shown.

In the figure above, the properties of the disk inserted to the Slot 2 of the PCI module 0.

IMPORTANT:

The [RDR Utility] display is not updated automatically. Therefore, update it by clicking [Refresh] from [Action] on the menu or pressing **F5** after performing operations to disk such as inserting/removing a disk, specifying/removing the RDR setting.

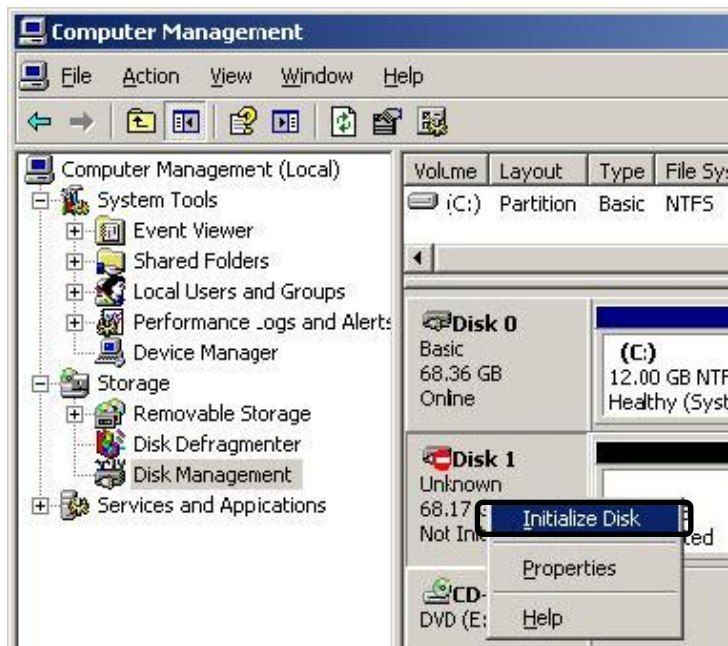
Making disks duplex by RDR

The following describes the procedure to set duplex configuration to disks by RDR. In this example, the disks of the Slot 2 of the PCI modules 0 and 1 are duplexed.

1. Insert a new disk to a built-in slot.
(In this example, a disk is inserted to the Slot 2 of the PCI module 0.)
2. From [Start], select [Control Panel] then [Administrative Tools] and start [Computer Management]. On the tree in the left pane, click [Disk Management].
If the inserted disk is indicated as [Not Initialized] in the right pane, right-click the disk and initialize it.

IMPORTANT:

When a disk is inserted or initialized, a popup window asking for rebooting the system may be displayed, but there is no need to reboot it. Select [No] and close the popup window.



3. Start RDR Utility.

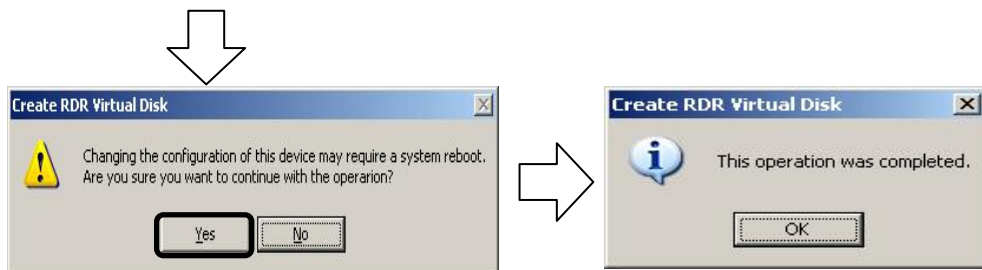
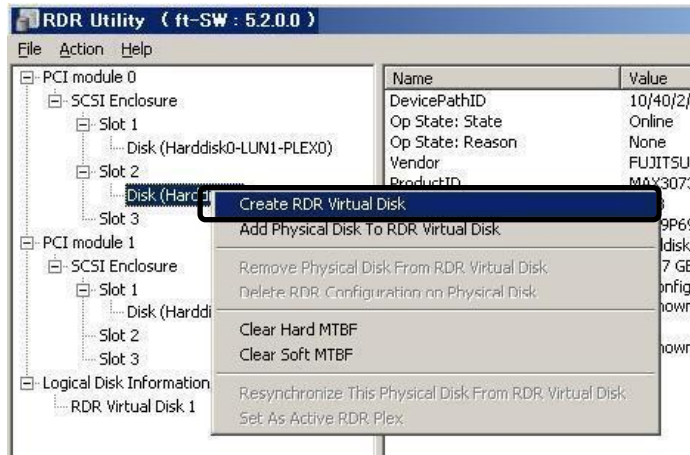
IMPORTANT:

- If the inserted disk does not appear on the tree, from the menu of RDR Utility, select [Action] and click [Refresh] or press **F5** to update the display after awhile.
 - The display of RDR Utility is not updated automatically. Therefore, update it every time after you perform disk operations described below.
-

4. On the left tree of RDR Utility, right-click a disk to set RDR and click [Create RDR Virtual Disk].

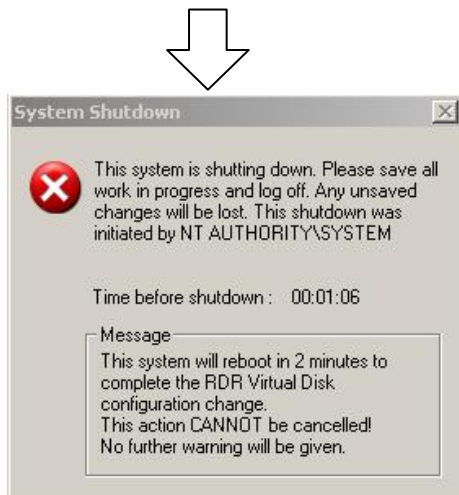
IMPORTANT:

Depending on the disk condition, RDR setting may take some time and RDR Utility may pause for a few minutes. There is no error, so wait until the process is completed.



IMPORTANT:

If RDR is specified to a disk which contains the system partition or partition which cannot be unmounted, the following pop-up message appears. If you click [Yes], the system is restarted in two minutes automatically. Go on to 5. when the system is restarted.



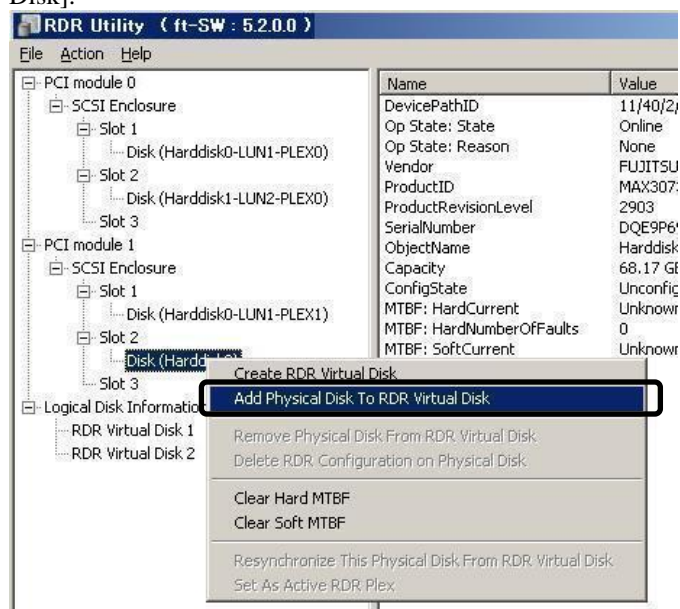
5. Insert a disk to set duplex configuration into the corresponding slot.
(In this example, a disk is inserted into the Slot 2 of the PCI module 1.)

IMPORTANT:

- When a disk is inserted, a popup window asking for rebooting the system may be displayed, but there is no need to reboot it. Select [No] and close the popup window.
- For a disk to be inserted, use a new or physically formatted disk which has the same capacity as the synchronization source. If such a disk is not used, disks are not duplicated successfully.

For physical format, see “SAS BIOS – Adaptec SAS/SATA Configuration Utility –” in Chapter 4 “System Configuration” and perform Format Disk with Disk Utilities. When performing Format Disk, on BIOS Setup Utility, click [Server], [Monitoring Configuration] and disable [Option ROM Scan Monitoring]. For how to set up, see “SYSTEM BIOS – SETUP –” on Chapter 4 “System Configuration.”

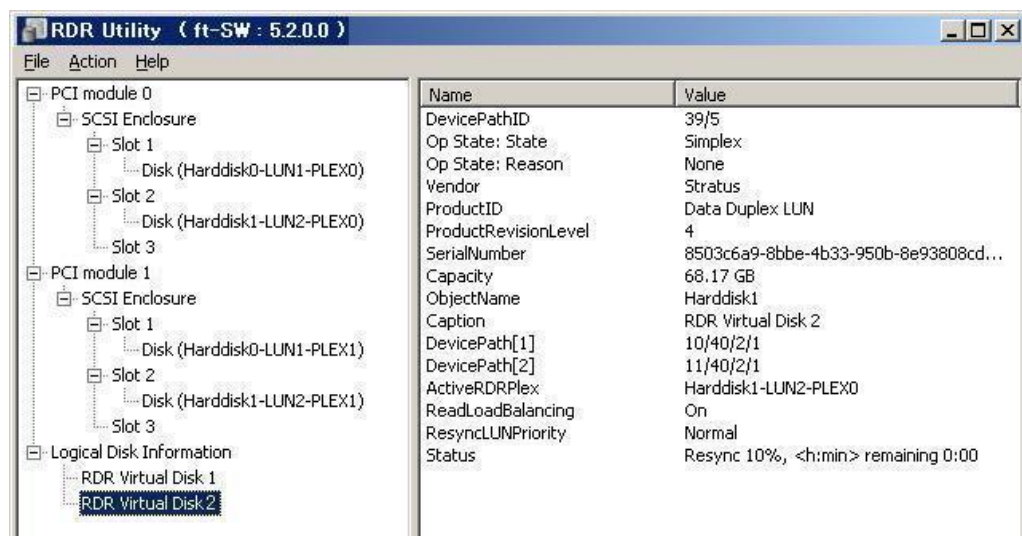
6. On the left tree of RDR Utility, right-click a disk to set RDR and click [Add physical Disk To RDR Virtual Disk].



7. Confirm that synchronizing disks are started and the DISK ACCESS LEDs and the display of RDR utility change as shown below:

■ Synchronizing

	DISK ACCESS LED	RDR Utility	
		Op State: State	Status
Source disk	Amber (Blinking)	Simplex	
Destination disk	Amber (Blinking)	Syncing	
RDR Virtual Disk		Simplex	Resync x percent (x=0, 4, 8, ..., 96)

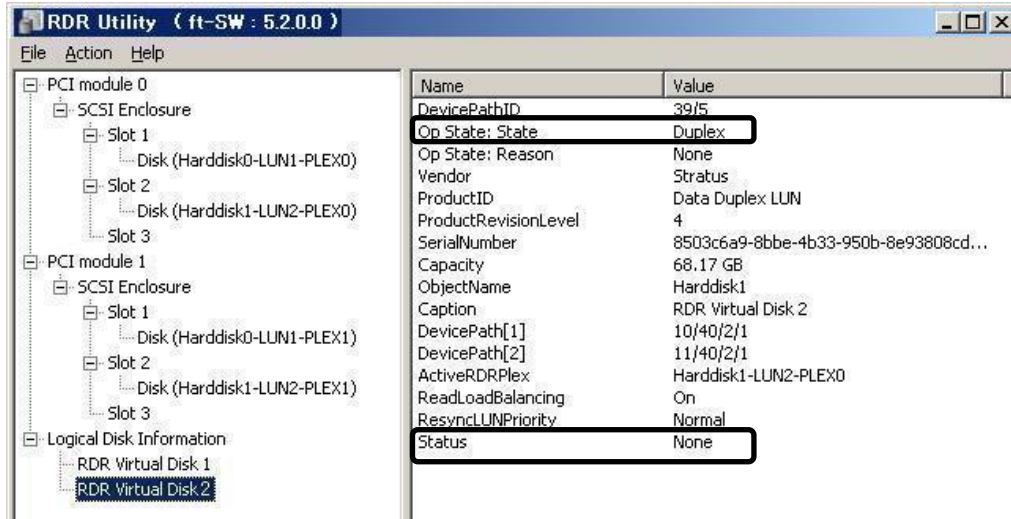


IMPORTANT:

- The time required for synchronization varies depending on the partition size on the disk.
For 18GB partition, it takes about 20 minutes.
If there is no partition, synchronization may complete in a short period and the disk may become synchronized after RDR is set.
- If the system is rebooted during synchronization, the process cannot be completed. Do not restart the system until the synchronization is completed.

■ Synchronization completed

	DISK ACCESS LED	RDR Utility	
		Op State: State	Status
Source disk	Green (Blinking)	Duplex	
Destination disk	Green (Blinking)	Duplex	
RDR Virtual Disk		Duplex	None



IMPORTANT:

- When a new partition is created on the disk where RDR is configured, the created partition area is synchronized automatically.
- When the system is halted without shutting down Windows properly, for example, by pressing the power button, the entire area of the synchronized disks will be resynchronized after the system is restarted.

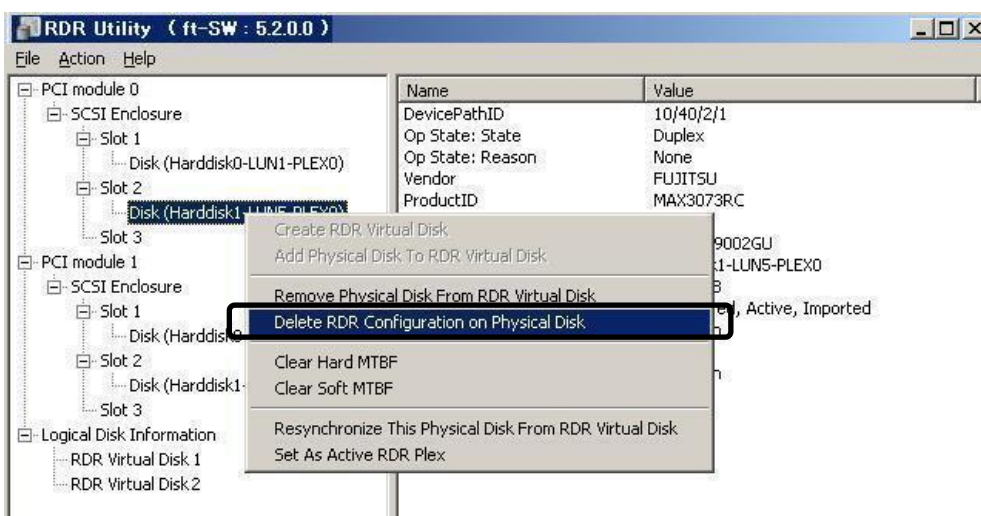
Removing duplex configuration of RDR disks

This section describes how to remove duplex configuration from the disk with RDR setting.
In the example below, the duplication setting of the disks in the Slot 2 of the PCI modules 0 and 1 is removed.

IMPORTANT:

- After executing the command, RDR settings will be cancelled but other data will remain.
- You cannot release the duplex setting of the following disks:
 - Disk containing page files
 - Dynamic disk
- The display of RDR Utility is not updated automatically. Therefore, update it every time you check the status of disks by clicking [Refresh] from [Action] on the menu or pressing **F5**.

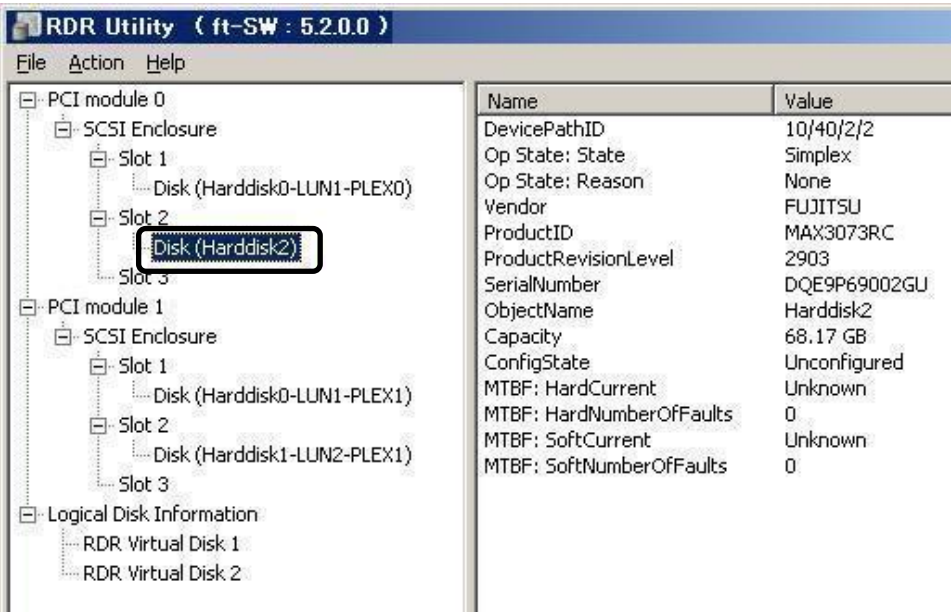
1. Start the RDR Utility, right-click a disk you want to cancel RDR from the tree in the left pane, and select [Delete RDR configuration on Physical Disk].



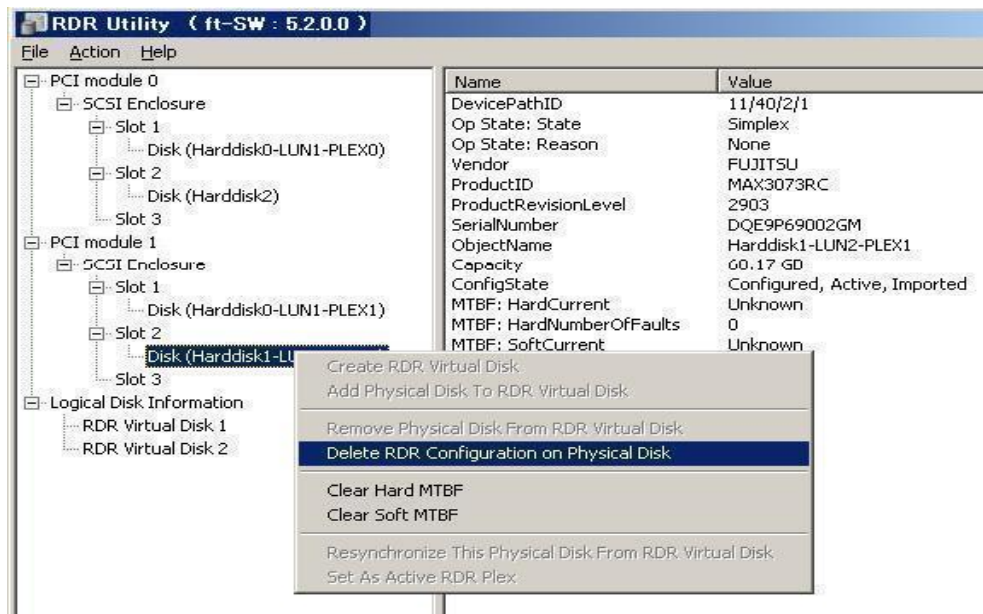
2. Click [Yes].



3. Confirm that RDR of the disk is cancelled.

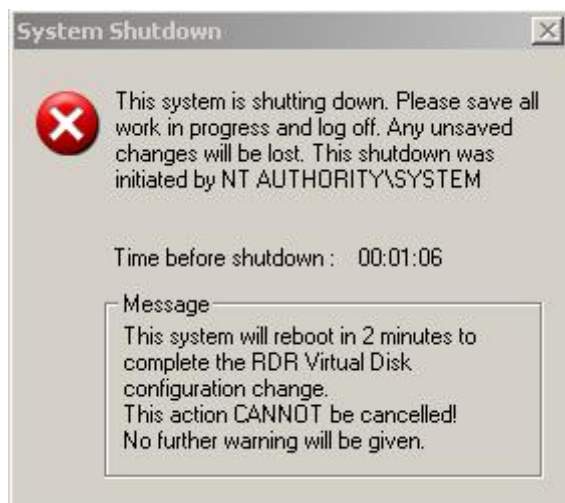


4. Cancel the disk of the corresponding slot in the same manner.



IMPORTANT:

- Cancelled disk may not be displayed properly on [Disk Management] after the RDR is cancelled. If this is the case, execute the following:
 1. Exit [Disk Management].
 2. Open [Computer Management] – [Service] and execute “Virtual Disk Service (vds).”
 3. Open [Disk Management].
- A partition on the disk where the RDR setting is removed is not assigned a drive letter. To use the partition, assign a drive letter using [Disk Management].
- If the disk contains a partition which cannot be unmounted, the OS needs to be restarted when canceling RDR. In that case, the following pop-up message appears. If you click [Yes], the OS is restarted automatically after two minutes:



Other functions of RDR Utility

<Commands for physical disks>

Remove Physical Disk From RDR Virtual Disk

All data including RDR settings on a physical disk can be deleted.

IMPORTANT:

- After executing the command, the physical disk becomes an empty basic disk without RDR settings.
 - This command can only be executed to physical disks in Duplex/Syncing state.
-

1. Start RDR Utility and right-click a target disk on the tree in the left pane, and click [Remove Physical Disk from RDR Virtual Disk].
2. In the [Remove Physical Disk From RDR Virtual Disk] dialog box, click [Yes].
3. In the [Remove Physical Disk From RDR Virtual Disk] dialog box, click [OK].

Clear Hard MTBF

When a hardware failure occurs to a disk, the mean time between failures (MTBF) is counted and the value is saved. In RDR Utility, the value is displayed at [MTBF: HardCurrent] and [MTBF:HardNumberOfFaults].

These MTBF values can be cleared by the [Clear Hard MTBF] command.

1. Start RDR Utility and right-click a target disk on the tree in the left pane, and click [Clear Hard MTBF].
2. In the [Clear Hard MTBF] dialog box, click [OK].

Clear Soft MTBF

When a software failure occurs to a disk, the mean time between failures (MTBF) is counted and the value is saved. In RDR Utility, the value is displayed at [MTBF: SoftCurrent] and [MTBF:SoftNumberOfFaults].

These MTBF values can be cleared by the [Clear Soft MTBF] command.

1. Start RDR Utility and right-click a target disk on the tree in the left pane, and click [Clear Soft MTBF].
2. In the [Clear Soft MTBF] dialog box, click [OK].

Resynchronize This Physical Disk From RDR Virtual Disk

Disks whose synchronization by RDR is cancelled for reasons including a failure can be resynchronized.

1. Start RDR Utility and right-click a target disk in the left pane and click [Resynchronize This Physical Disk From RDR Virtual Disk].
2. In the [Resynchronize This Physical Disk From RDR Virtual Disk] dialog box, click [OK].
3. Confirm that the resynchronization starts and the status of disks changes as shown below:

■ Resynchronizing

	DISK ACCESS LED	RDR Utility	
		Op State: State	Status
Source disk	Amber (Blinking)	Simplex	
Destination disk	Amber (Blinking)	Syncing	
RDR Virtual Disk		Simplex	Resync x percent (x=0, 4, 8, ..., 96)

■ Synchronization completed

	DISK ACCESS LED	RDR Utility	
		Op State: State	Status
Source disk	Green (Blinking)	Duplex	
Destination disk	Green (Blinking)	Duplex	
RDR Virtual Disk		Duplex	None

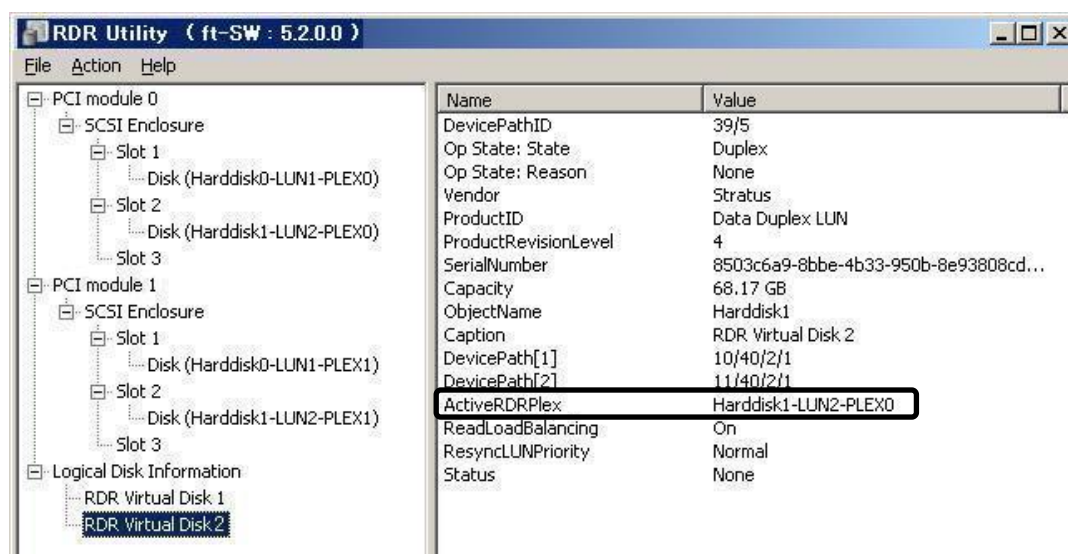
Set As Active RDR Plex

A physical disk can be set as “Active RDR Plex” by a command.

Active RDR Plex is the disk on which data reading process is performed when Load Balancing of RDR Virtual Disk is off.

1. Start RDR Utility and right-click a target disk in the left pane and click [Set As Active RDR Disk].
2. In the [Set As Active RDR Plex] dialog box, click [OK].

Active RDR Plex can be viewed from [Active RDR Plex] of RDR Virtual Disk. (In the image below, the disk in the slot 2 of PCI module 0 is set to Active RDR Plex among physical disks constructing RDR Virtual Disk 2.)



Commands for RDR Virtual Disk

Verify RDR Virtual Disk

Whether the synchronization by RDR is performed normally can be checked.

1. Start RDR Utility and right-click [RDR Virtual Disk x] in the left pane and click [Verify RDR Virtual Disk].
2. In the [Verify RDR Virtual Disk] dialog box, click [OK].
The progress of verification can be viewed using RDR Utility.

	Verifying	Verification completed
[Status] of RDR Virtual Disk x	Verify x percent (x=0, 4, 8, ..., 96)	None

TIPS:

- The verification process is automatically performed every 1 week.
 - The time required for verification depends on the disk size and load.
-

Stop Verifying RDR Virtual Disk

Verification of RDR virtual disk in progress can be stopped.

1. Start RDR Utility and right-click [RDR Virtual Disk x] in the left pane and click [Stop Verify RDR Virtual Disk].
2. In the [Stop Verify RDR Virtual Disk] dialog box, click [OK].

Set Resync Priority

Priority of synchronization by RDR can be specified. By changing the priority, I/O load during synchronization can be reduced.

1. Start RDR Utility, right-click [RDR Virtual Disk x] in the left pane and click [Set Resync Priority].
2. When a dialog box appears, select Low, Normal or High (a default is Normal) and click [OK].
3. In the [Set Resync Priority] dialog box, click [OK].

Set RDR LUN Load Balancing

On or off of load balancing can be specified.

When the load balancing is on (default), the read process is performed alternately from two physical disks forming the RDR Virtual Disk to improve performance. When it is off, the read process is performed from the physical disk specified as Active RDR Plex.

1. Start RDR Utility, right-click [RDR Virtual Disk x] in the left pane to change the priority and click [Set RDR LUN Load Balancing].
2. When a dialog box appears, select On or Off (a default is On) and click [OK].
3. In the [Set RDR LUN Load Balancing] dialog box, click [OK].

Replacing Failed Hard Disk Drives

The following describes how to locate and replace the failed hard disk. The failed hard disk should be replaced with the server powered on.

How to Locate Failed Disks

1. From [Start], select [All Programs], [RDR] and click [RDR Utility] to start RDR Utility.
2. From the tree on the left pane of [RDR Utility], select each disk and check the values of [MTBF: Current] and [MTBF:NumberOfFaults] in the right pane.

TIPS:

For RDR Utility, see “About RDR Utility” on page 3-3.

[Description of each MTBF value]

Property name	Description	Normal value*
MTBF: HardCurrent	Mean time between hardware failures.	Unknown
MTBF: SoftCurrent	Mean time between software failures.	Unknown

* The normal value denotes the value of when no error has occurred.

If either of the values is different from the normal value, the disk has an error.

Procedures to Replace Failed Disks

This section describes a procedure for replacing a disk when a failure occurs to a disk that is duplicated by the RDR function.

IMPORTANT:

The display of RDR Utility is not updated automatically. Therefore, update it every time you check the status of disks by clicking [Refresh] from [Action] on the menu or pressing **F5**. Do not update RDR Utility frequently immediately after inserting a disk.

Here, an example that a failure of the disk in slot 2 of the PCI module 0 is determined as described in “How to Locate Failed Disks” is explained.

1. From [Start], click [All Programs], point to [RDR], and select [RDR Utility] to start RDR Utility.
2. Remove the disk in the slot 2 of the PCI module 0.
3. Insert a new disk to the slot 2 of the PCI module 0.
RDR is automatically set to the inserted disk and synchronization starts.

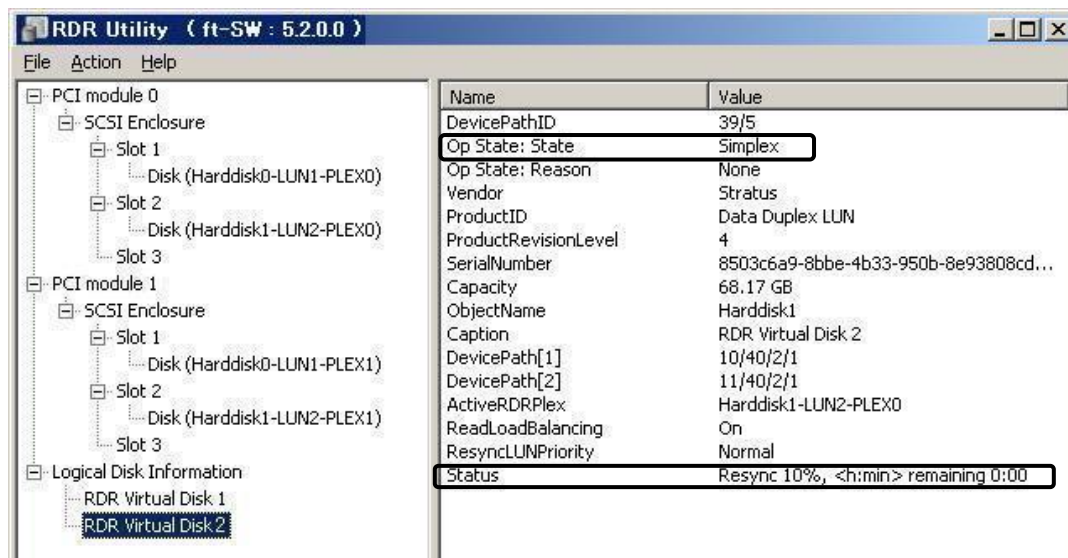
IMPORTANT:

- For a disk to be inserted, use a new or physically formatted disk which has the same capacity as the disk of the corresponding slot (in this example, the disk in slot 2 of the PCI module 0)
- When a disk is inserted, a popup window asking for rebooting the system may be displayed, but there is no need to reboot it. Select [No] and close the popup window.
- Insert the replacement disk after waiting for 15 seconds or more after removing a disk.
- Inserted disk may not be configured to RDR automatically. If this occurs, right click on the inserted disk in the left tree on [RDR Utility] and click [Add Physical Disk To RDR Virtual Disk] to start synchronizing.

4. Confirm that the DISK ACCESS LEDs and the display of RDR Utility change as shown below:

■ Synchronizing

	DISK ACCESS LED	RDR Utility	
		Op State: State	Status
Source disk	Amber (Blinking)	Simplex	
Destination disk	Amber (Blinking)	Syncing	
RDR Virtual Disk		Simplex	Resync x percent (x=0, 4, 8, ..., 96)

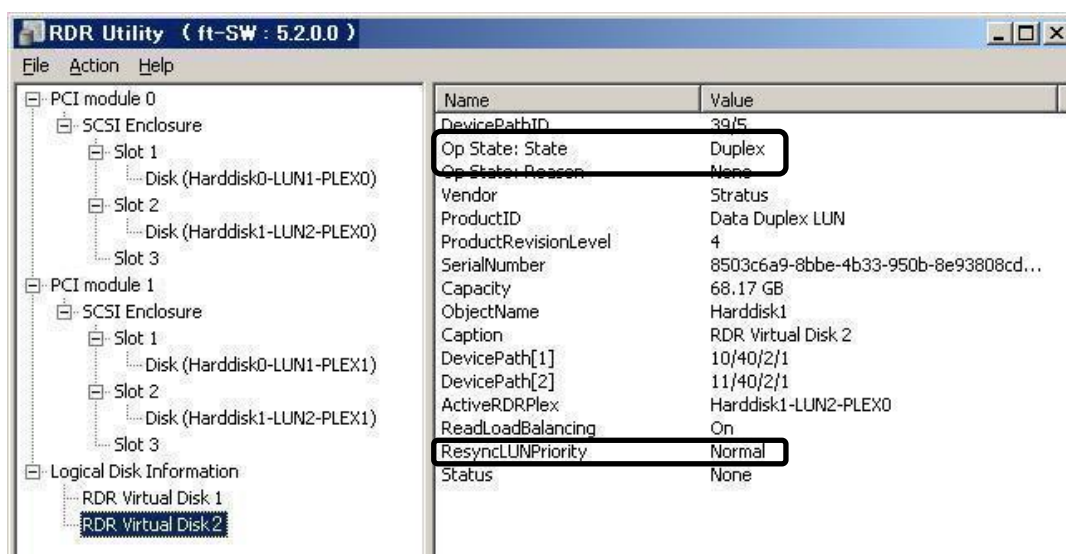


IMPORTANT:

- The time required for synchronization varies depending on the partition size on the disk.
For 18GB partition, it takes about 20 minutes.
If there is no partition, synchronization may complete in a short period of time and the disk may become synchronized after RDR is set.
- If the system is rebooted during synchronization, the process cannot be completed. Do not restart the system until the synchronization is completed.

■ Synchronization completed

	DISK ACCESS LED	RDR Utility	
		Op State: State	Status
Source disk	Green (Blinking)	Duplex	
Destination disk	Green (Blinking)	Duplex	
RDR Virtual Disk		Duplex	None



CHANGE DRIVE LETTER

To add, change or delete drive letters, follow the steps below. Before making any changes, thoroughly read the Fault Tolerant Server series-specific precautions and general precautions for Windows.

1. Select [Start] - [Control Panel] - [Administrative Tools] and open [Computer Management].
2. In the console tree of [Computer Management], click [Disk Management].
3. Right-click a target partition, logical drive or volume and click [Change Drive Letter and Paths...].
4. Perform one of the following:
 - To assign a drive letter, click [Add...], a drive letter to use, then [OK].
 - To change a drive letter, click the drive letter to change, [Change...], a drive letter to use, then [OK].
 - To delete a drive letter, click the drive letter to delete then [Remove].

IMPORTANT:

<Fault Tolerant Server series-specific precautions>

- When connecting an optional floppy disk drive, drive letters may change from A to B by switching CPU/IO modules. This does not affect the operation of the server. Use B drive as the floppy disk drive.

<General precautions for Windows>

- Drive letter of system volume or boot volume cannot be changed.
 - Up to 26 drive letters can be used on a computer. "A" and "B" are drive letters for floppy disk drives. Generally, hard disk drives are assigned "C" to "Z", but for network drives, drive letters are assigned in a reverse order ("Z" to "C").
 - Because many of Windows programs refer to specific drive letters, cautions are required for assigning drive letters. For example, the Path environment variable specifies a program name and a specific drive letter.
 - For performing the procedure above, you need to be a member of Backup Operators group or Administrators group, or you need to have appropriate authorization.
-

DUPLEX LAN CONFIGURATION

The Fault Tolerant Server series builds a duplex LAN configuration by using “Stratus emb-EB 2-Port Gigabit Adapter,” mounted as standard on the CPU/IO module and the extended PCI slot “NEC MT Gigabit Adapter”, “NEC MF Gigabit Adapter,” and “Stratus U 575 Dual Port Copper Gigabit Adapter.”

Overview

The duplex LAN configuration is of three types as described below:

■ **Adapter Fault Tolerance (AFT)**

Adapter Fault Tolerance (AFT) is a feature that places more than one LAN controller on the same LAN (same segment), and automatically switches the process of the primary controller to the backup controller when any trouble occurred on the primary.

■ **Adaptive Load Balancing (ALB)**

Adaptive Load Balancing (ALB) is a feature that connects more than one LAN controller to the same hub and enhances the throughput by operating packet transmission from the server.

Receive Load Balancing (RLB) is enabled by default. Disable RLB. When RLB is enabled the network duplex configuration may fail.

■ **Switch Fault Tolerance (SFT)**

Switch Fault Tolerance (SFT) is a feature that provides the network availability because the fail-over target (standby) adapter takes over the MAC address/L3 address when failure occurs on adapter/cable/connecting switch, as two adapters are connected to corresponding two switches. One is allocated to the primary adapter and the other is allocated to the standby adapter. On the network, the primary adapter communicates.

Regarding the path redundancy, you need to construct the environment both on the ft server and the switch devices. Spanning Tree Protocol (SPT) function is required to construct the path redundancy on the switch devices.

When you construct the environment, you need to set the switch priority in order to maintain the path to the primary adapter after the path information is updated if a switch on the path is broken. In addition, you need to set the priority to use the secondary adapter's switch if the primary adapter's switch is broken.

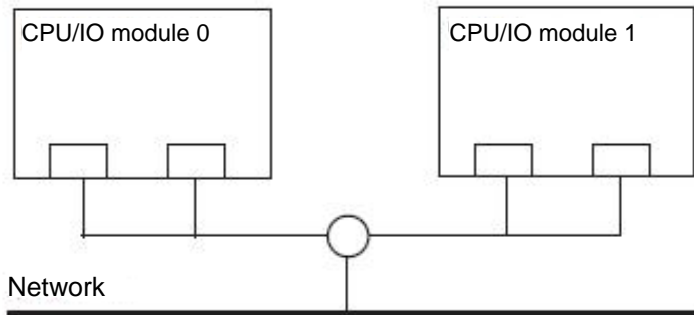
The other modes, “Static Link Aggregation” and “IEEE 802.3ad Link Aggregation,” do not contribute to enhancement against a fault. When a fault occurs, the communication performed on the controller with the fault is not taken over by the backup controller but lost.

Rules of Duplex Configuration on Fault Tolerant Server series

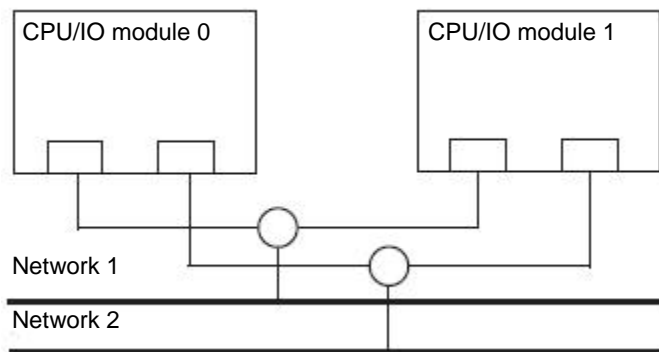
Be sure to make the setting of duplex network configuration on the server.

When building duplex configuration, be sure to use at least one adapter of CPU/IO module 0 and of 1 individually.

Example1) Configure the duplex network which enhances the service life by using all adapters.



Example 2) Configure the duplex network which corresponds to multiple LAN connection.



Configuring Duplex LAN

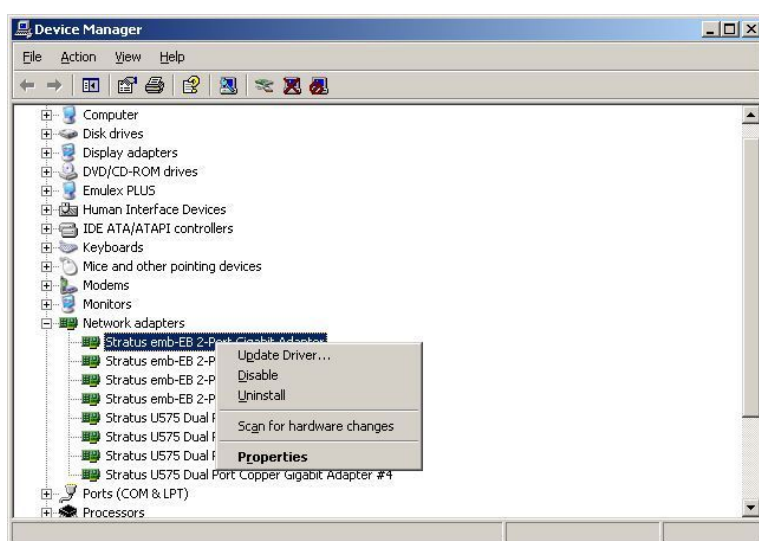
This section describes how to configure duplex LAN.

The following explains how to configure duplex/dual LAN regarding to the example shown in “Rules of Duplex Configuration on Fault Tolerant Server series.”

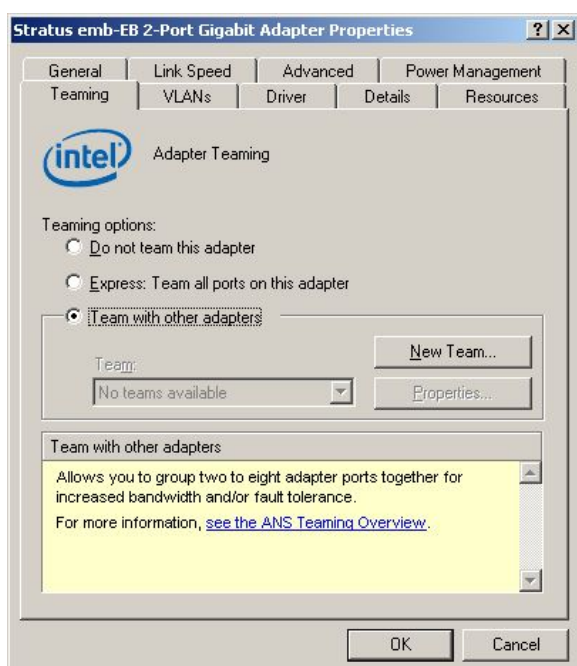
IMPORTANT:

Log on as "Administrator" or a member of the group "Administrators."

1. Start [Device Manager].
2. Select a target Network Adapter. Right-click on it and select [Properties] from the menu displayed to show the properties dialog box.



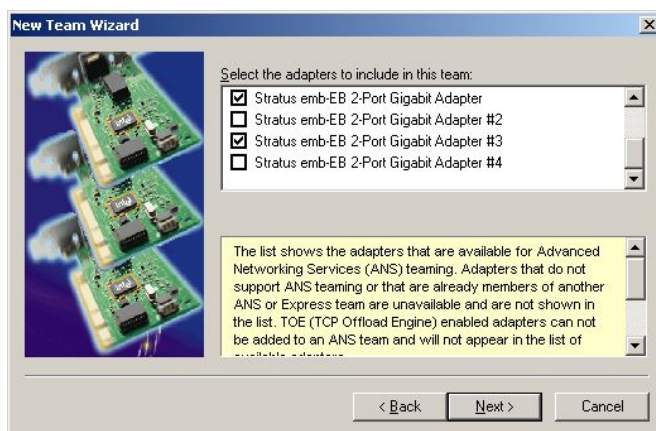
3. Select the [Teaming] tab on the properties dialog box. Select the [Team with other adapters], and then click the [New Team...] button.



4. Enter the team name and click [Next].

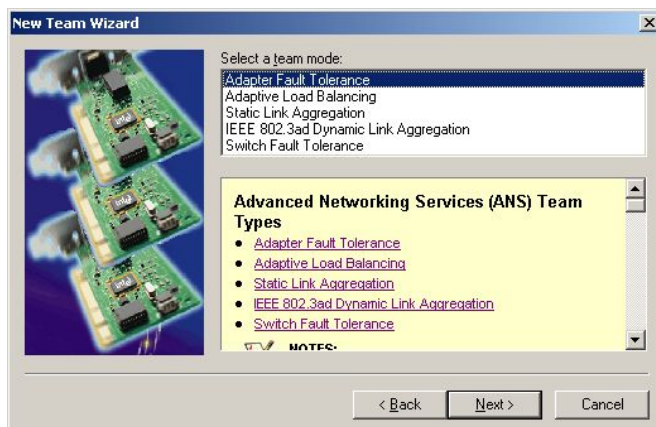


5. Select the adapters to include in the team and click [Next].

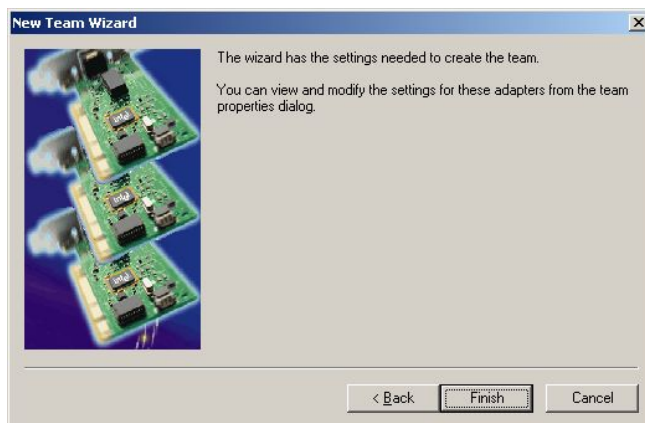


6. Select [Adapter Fault Tolerance] or [Adaptive Load Balancing] or [Switch Fault Tolerance] as a team mode (Usually select [Adapter Fault Tolerance]).

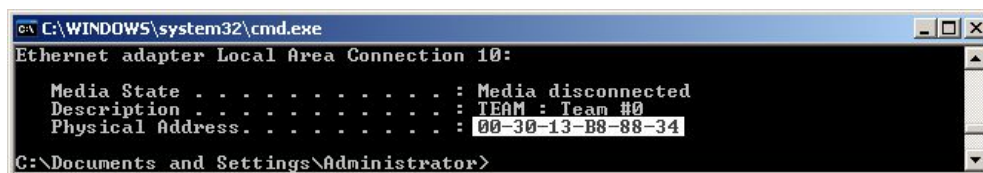
Click [Next].



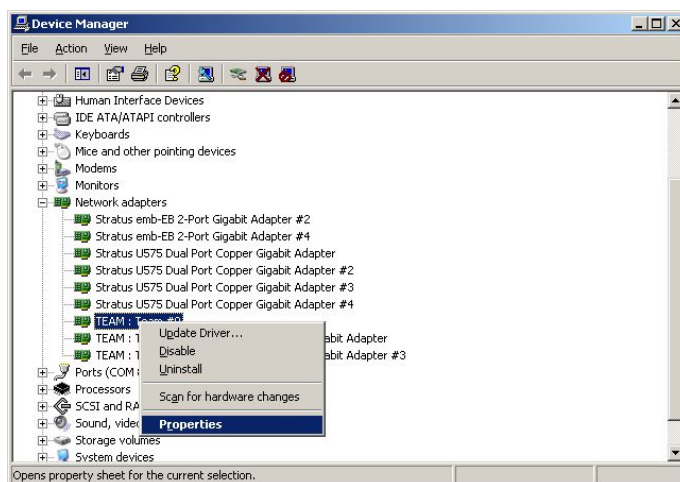
7. Click [Finish].



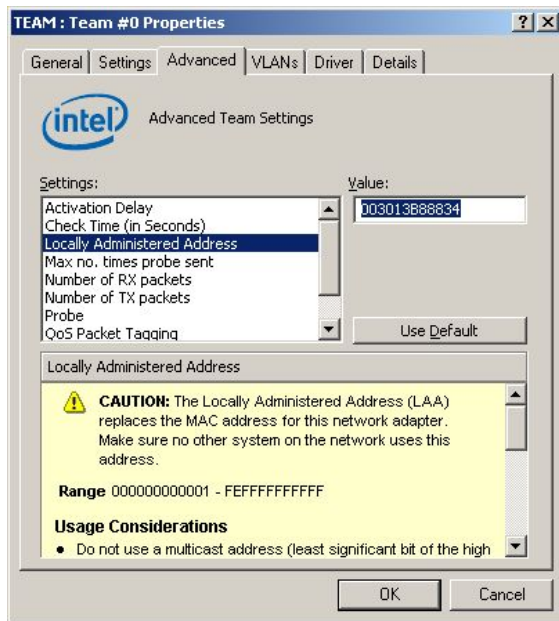
8. Start Command prompt to check the physical MAC address set on ipconfig/all.



9. Select the Team Adapter you have set. Right-click on it and select [Properties] from the menu displayed to show the properties dialog box.



10. Select the [Advanced] tab on the properties dialog box. Select [Locally Administered Address] from the [Settings] list box, and then enter the MAC address of a Team Adapter, which you have checked, in the [Value] text box. Click [OK].



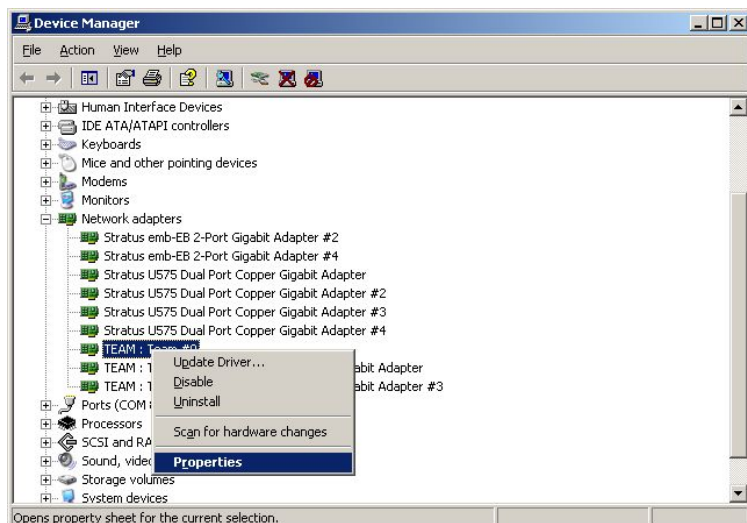
Removing Duplex/Dual LAN

This section describes how to remove duplex/dual LAN.

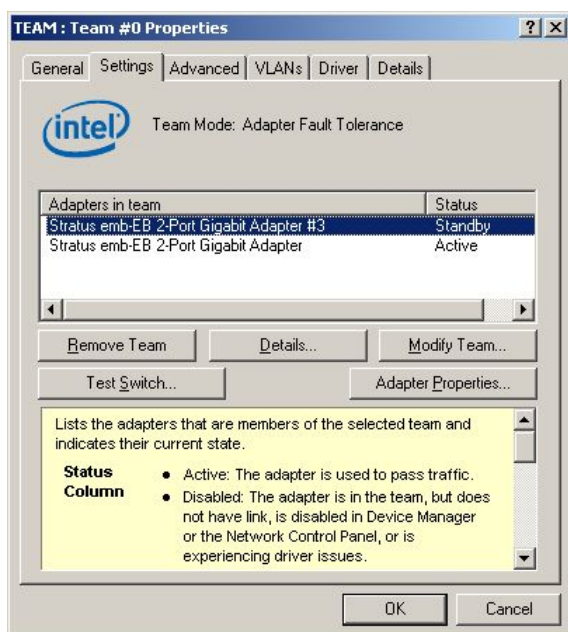
IMPORTANT:

Log on as "Administrator" or a member of the group "Administrators."

1. Start [Device Manager].
2. Select the Team Adapter of which you want to remove duplex/dual LAN. Right-click on it, and then select [Properties] from the menu displayed to show the properties dialog box.



3. Select the [Settings] tab in the properties dialog box and click the [Remove Team] button.



4. The confirmation dialog box appears. Click [Yes] button.



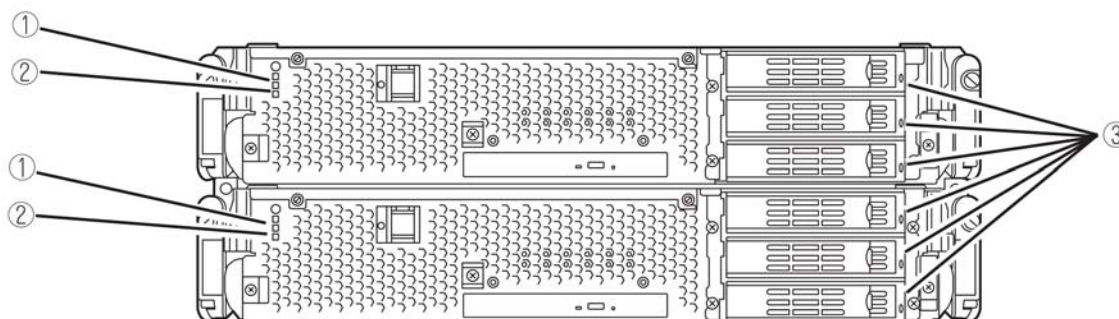
CHECKING THE DUPLICATING OPERATION OF MODULES

This section describes how to check if the system runs properly after system installation or reinstallation. CPU/IO module has a processor function part and IO function part. Each part is monitored and managed by the module. In this section, the processor function part is referred to as CPU module and IO function part PCI module.

Evaluate Startup and Stop of PCI Modules

This section describes how to confirm the continuous system operation by failover after stopping the primary PCI module.

1. Check which is the primary PCI module.
The PCI module with the POWER switch illuminated is the primary module.
2. Check whether the PCI modules are duplicated.
To check if the PCI modules are duplicated, see the CPU/IO modules' status LEDs.



[Indications of the status LEDs when PCI modules are duplicated]

	LED	Primary	Secondary
1	CPU/IO module status LED1	-	-
2	CPU/IO module status LED2	Green	Green
3	DISK ACCESS LED	Green blinking	Green blinking

* The numbers in the table correspond to the numbers in the above figure.
The DISK ACCESS LED (3) lights when the hard disk drive is accessed.

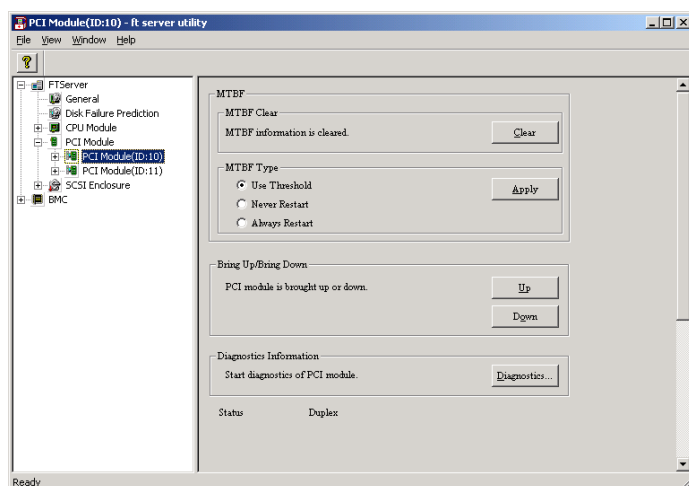
3. Stop the operation of a PCI module using the ft server utility.

Select [Start] - [All Programs] - [NEC ESMPRO Agent] - [ft server utility] to start the ft server utility.

Then, from the ft server utility, select [PCI Module] and then the primary PCI module (*) from the [FTServer] tree on the left pane, and click [Down] of [Bring Up/Bring Down].

* As for the primary PCI module (*), if the PCI module 0 is primary select [PCI Module(ID:10)]. If the PCI module 1 is primary, select [PCI Module (ID:11)].

When you stop the operation of the primary PCI module, a failover occurs and the secondary PCI module becomes the primary module.



The following events or changes occur when stopping the primary PCI module and the module fails over:

- The screen temporarily blacks out and then displayed again.
- The following message will appear from the taskbar:
Windows - FT Orphaning: A disk that is part of a fault-tolerant volume can no longer be accessed.
* The message denotes that the mirror volumes of the hard disk stored in the disconnected PCI module are released.
* The message will not appear if disks are duplicated by the RDR function.
- Indications of PCI modules' status LEDs change as follows:

[Indications of status LEDs]

LED		Secondary*	Primary*
1	CPU/IO module status LED1	Amber	-
2	CPU/IO module status LED2	-	Green blinking
3	DISK ACCESS LED	-	Amber or Green blinking (when the disk is accessed, this LED illuminates in green)

* The primary and secondary modules after failover

4. Restart the PCI module.

From the ft server utility, click [Up] of [Bring Up/Bring Down] to the PCI module which was stopped in the step 3, and the PCI module will be started. Once the PCI module is started, PCI module diagnosis, mirror volume duplication and PCI module duplication are performed.

IMPORTANT:

If BrightStor ARCserve 2000 or Backup Exec is installed, the tape will not be recognized due to the failover of the PCI module. Thus be sure to stop the services before starting the PCI module.

1. Start [Services] from [Administrative Tools] of [Control Panel].
 2. Select a service of backup software.
 3. Choose "Stop" from the "Action" menu.
 4. Repeat 2 and 3 for all services of the backup software.
-

The PCI modules' status LEDs changes as shown below:

[Indications of the status LEDs]

Immediately after the PCI module startup until the completion of diagnosis

	LED	Secondary	Primary
1	CPU/IO module status LED1	-	-
2	CPU/IO module status LED2	-	Green blinking
3	DISK ACCESS LED	-	Amber or Green blinking (when the disk is accessed, this LED illuminates in green)



When duplication of disks is started after the completion of PCI module diagnosis

* The status of LEDs varies depending on the method of disk duplication.

	LED	Secondary	Primary
1	CPU/IO module status LED1	-	-
2	CPU/IO module status LED2	Green blinking	Green blinking
3	DISK ACCESS LED	Amber or Green blinking (when the disk is accessed, this LED illuminates in green)	Amber or Green blinking (when the disk is accessed, this LED illuminates in green)



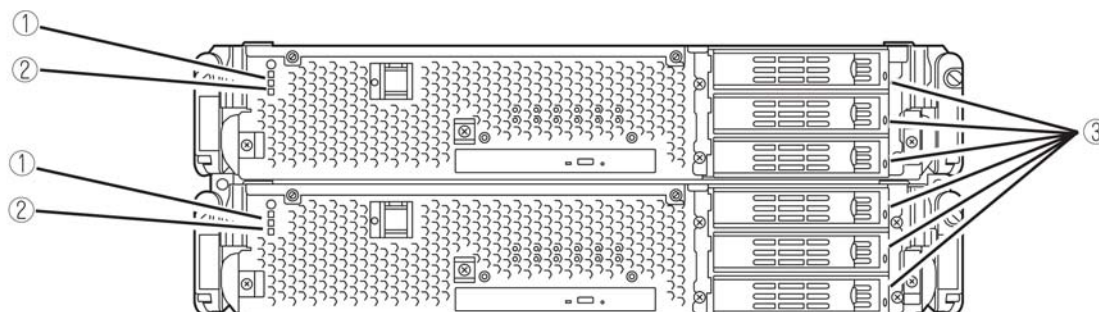
After the completion of disk duplication and when the PCI modules are duplicated

	LED	Secondary	Primary
1	CPU/IO module status LED1	-	-
2	CPU/IO module status LED2	Green	Green
3	DISK ACCESS LED	Green blinking	Green blinking

Confirm Start and Stop of CPU Modules

This section describes how to confirm the continuous system operation after stopping one of the CPU modules.

1. Confirm that the CPU modules are duplicated.
To check if the CPU modules are duplicated, see the status LEDs of the CPU modules.

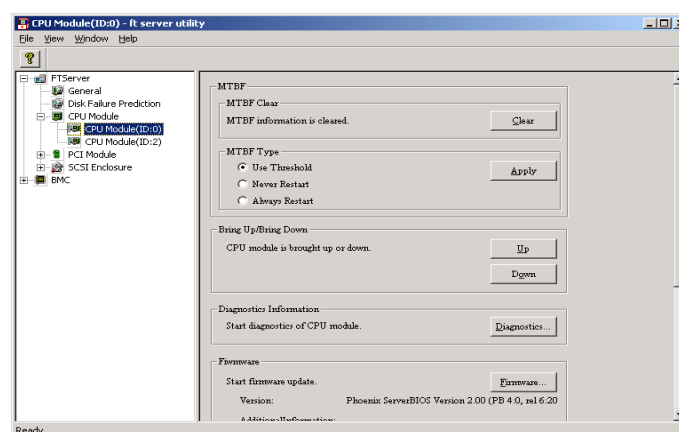


[Indications of status LEDs when CPU modules are duplicated]

LED		CPU module 0 (Operating)	CPU module 1 (Operating)
1	CPU/IO module status LED1	-	-
2	CPU/IO module status LED2	Green	Green
3	DISK ACCESS LED	Green blinking	Green blinking

2. Use the ft server utility to stop the operation of a CPU module to remove.
From [Start], select [All Programs], [NEC ESMPRO Agent] then [ft server utility] to start the ft server utility. Then, from the ft server utility, select [CPU Module] then the CPU module to stop (*) from the [FTServer] tree on the left pane, and click [Down] of [Bring Up/Bring Down].

* As for the CPU module to stop, select [CPU Module(ID:0)] to stop CPU module 0, select [CPU Module(ID:1)] to stop CPU module 1.



When you stop the operation of a CPU module, the indications of the status LEDs change as follows. Below denotes that the only one CPU module is operating.

[Indications of status LEDs]

LED		CPU module 1 (Stopped)*	CPU module 2 (Operating)
1	CPU/IO module status LED1	Amber	-
2	CPU/IO module status LED2	-	Green blinking
3	DISK ACCESS LED	Green blinking	Green blinking

- As an example, the indications of when CPU module 0 is stopped are shown.

3. Press the start button of the CPU module stopped by ft server utility.
 In the ft server utility, select the stopped CPU module and click [Up] of [Bring Up/Bring Down].
 Once the CPU module is started, hardware diagnosis and then synchronization of memory (memory copy) are performed, and the duplication process is completed.
 Note that the system is paused temporarily for copying memory during memory synchronization.

[Indications of status LEDs during diagnosis]

LED		CPU module 0 (Started)	CPU module 1 (Operating)
1	CPU/IO module status LED1	-	-
2	CPU/IO module status LED2	-	Green blinking
3	DISK ACCESS LED	Green blinking	Green blinking



[Indications of status LEDs after completion of duplication]

LED		CPU module 0 (Operating)	CPU module 1 (Operating)
1	CPU/IO module status LED1	-	-
2	CPU/IO module status LED2	Green	Green
3	DISK ACCESS LED	Green blinking	Green blinking

IMPORTANT:

After duplication is completed, the status of memory will be checked.

Wait until this process ends to perform the next step (evaluation of start and stop of PCI and CPU modules).
 When the process is complete, the following event log will be output:

Source: srabid

Type: Information

Event ID: 4137

Description: Memory consistency check has completed memory scan.

Fault Tolerant Server series SERVICE PROGRAM CONFIGURATION

Fault Tolerant Server series achieves the duplex system using the following service programs, in addition to dedicated drivers.

Service program names shown in [Services]:

- Stratus ER Service
- ftSys eService
- ftSys Maintenance and Diagnostics (MAD)
- ftSys RPC Provider
- ftSys SSN
- Windows Management Instrumentation
- SNMP Service
- Alert Manager Main Service
- ESMFSService
- ESMCommonService
- ESRAS Utility Service
- ESMLANSERVICE
- ESMPS
- Virtual Disk Service (vds)

The above programs are necessary for the Fault Tolerant Server series operation. Do not stop these services.

When minimizing the number of operating service programs temporarily is required, the following service programs may be stopped:

Services that can be stopped:

- ESRAS Utility Service
- ftSys RAS

Services required to keep operating

- Stratus ER Service
- ftSys eService
- ftSys Maintenance and Diagnostics (MAD)
- ftSys RPC Provider
- ftSys SSN
- Windows Management Instrumentation
- SNMP Service
- Alert Manager Main Service
- ESMFSService
- ESMCommonService
- ESMLANSERVICE
- ESMPS
- Virtual Disk Service (vds)

Make sure to restart the operations of stopped service programs immediately after the backup processes are completed.

This page is intentionally left blank.

Chapter 4

System Configuration

This chapter describes Basic Input Output System (BIOS) configuration.

When you install the Fault Tolerant Server series for the first time or install/remove optional devices, thoroughly read this chapter for better understanding and correct setups.

SYSTEM BIOS –SETUP–

The SETUP utility is provided to make basic hardware configuration for the server. This utility is pre-installed in the flash memory of the server and ready to run.

The server is configured with the correct parameters using the SETUP utility and shipped in the best conditions. Thus, you do not need to use the SETUP utility in most cases. However, you might wish to use the SETUP utility in the cases described below.

IMPORTANT:

- The SETUP utility is intended for system Administrator use only.
 - The SETUP utility allows you to set a password. The server is provided with two levels of password: Supervisor and User. With the Supervisor password, you can view and change all system parameters of the SETUP utility. With the User password, system parameters available for viewing and changing are limited.
 - Do not set any password before installing the OS.
 - The server contains the latest version of the SETUP utility. Dialog boxes appearing on your SETUP utility, thus, may differ from descriptions in this User's Guide. If you find anything unclear, see the online help or ask your sales agent.
-

Starting SETUP Utility

Powering on the server starts POST (Power On Self-Test) and displays its check results. If the full screen logo is displayed, press **Esc**.

After a few seconds, either of the following messages appears at bottom left on the screen depending on your system configuration.

Press <F2> to enter SETUP

Press <F2> to enter SETUP or Press <F12> to boot from Network

You may see either of the following messages at bottom left on the screen when POST terminates.

Press <F1> to resume, <F2> to SETUP

Press **F2** to start the SETUP utility and display its Main menu.

If you have previously set a password with the SETUP utility, the password entry screen appears. Enter the password.

Enter password:[]

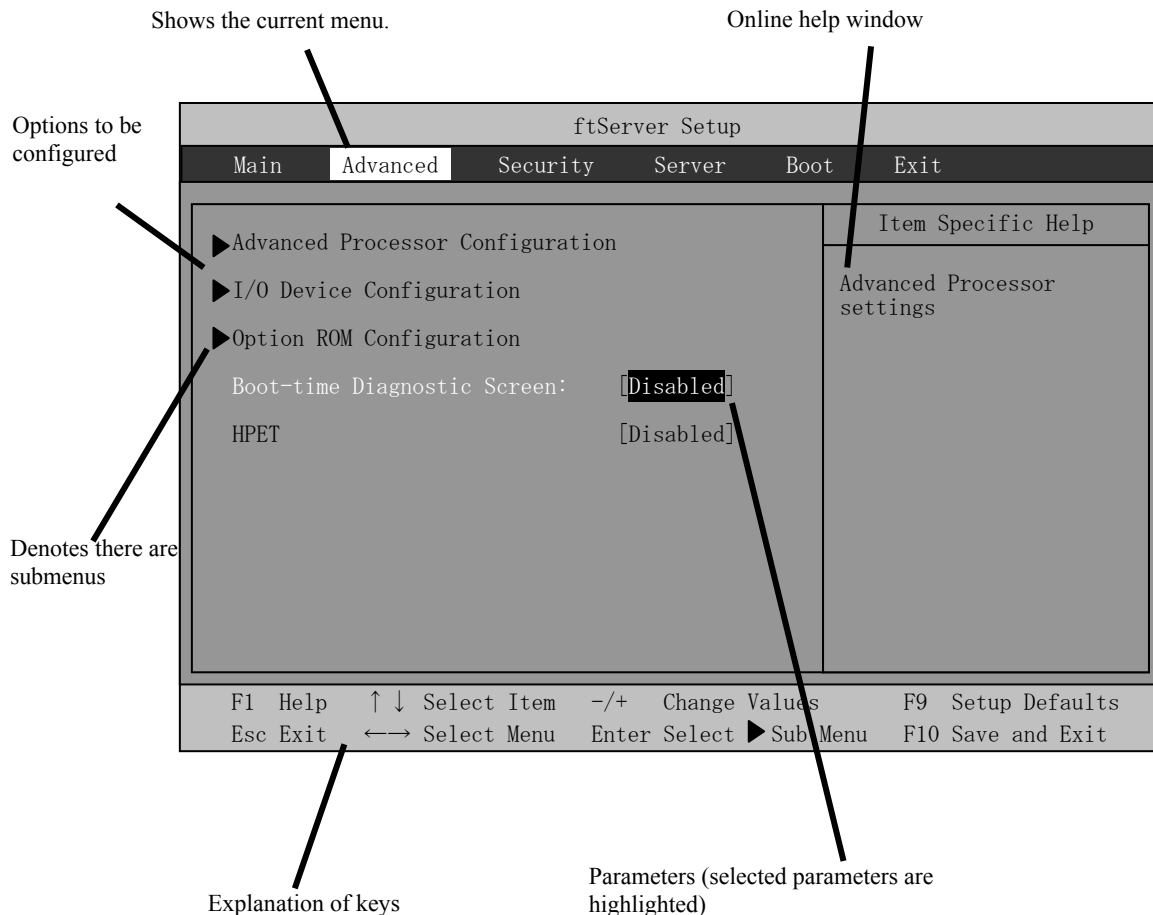
Up to three password entries will be accepted. If you fail to enter the password correctly for three consecutive times, the server halts. (You can no longer proceed.) Power off the server.

TIPS:

The server is provided with two levels of password: Supervisor and User. With the Supervisor password, you can view and change all system configurations. With the User password, the system configurations you can view or change are limited.

Description of On-Screen Items and Key Usage

Use the following keyboard keys to work with the SETUP utility. (Key functions are also listed at the bottom of the screen.)



- Cursor** (↑, ↓): Selects an item on the screen. The highlighted item is currently selected.
- Cursor** (←, →): Selects the Main, Advanced, Security, System Hardware, Boot, or Exit menu.
- : Changes the value (parameter) of the selected item to the previous value.
- +**: Changes the value (parameter) of the selected item to next value.
- Enter**: Displays a submenu or chooses the selected parameter.
- Esc**: Displays the previous screen.
- F1**: Press **F1** when you need help on SETUP operations. The help screen for SETUP operations appears. Press **Esc** to return to the previous screen.
- F9**: Shows the following:

```

      Setup Confirmation
Load default configuration now?
      [Yes]      [No]
  
```

If you select "Yes" and then press the **Enter** key, all items in the setup are set to default values. If you select "No" and then press either the **Enter** or **Esc** key, the status before pressing the **F9** key is restored.

F10:

Shows the following:

Setup Confirmation Save Configuration changes and exit now? [Yes] [No]

If you select "Yes" and then press the **Enter** key, the setup will complete with all changes you have made saved. If you select "No" and then press either the **Enter** or **Esc** key, the status before pressing the **F10** key is restored.

Configuration Examples

The following describes examples of configuration required to use software-link features or for system operations.

UPS

To link power supply with the UPS

- To power on the server when power is supplied from the UPS
Select [Server] - [AC-LINK] - [Power On].
- To keep the server off-powered even when power is supplied from the UPS if the POWER switch was used to power off
Select [Server] - [AC-LINK] - [Last State].
- To keep the server off-powered even when power is supplied from the UPS
Select [Server] - [AC-LINK] - [StayOff].

Keyboard

To set Num Lock

Select [Advanced] - [I/O Device Configuration] - [NumLock]

Security

To set passwords on the BIOS level

Select [Security] - [Set Supervisor Password] and enter a password.

Select [Security] - [Set User Password] and enter a password.

Set Supervisor password first, then User password.

Optional PCI-related devices

To enable Option ROM of the PCI card (option) installed on the server

Select [Advanced] - [Option ROM Configuration] - [PCI Slot n (...)] - [Enabled].

n: Slot number to install the board

Boot

To change the boot order of devices connected to the server

Select [Boot] and specify the boot order.

To display POST check results

Select [Advanced] - [Boot-time Diagnostic Screen] - [Enabled].

You can also press **Esc** while the full-screen logo is on the screen to display POST check results.

To control from the HW console

- Remote operation via Serial
Select [Server] - [Console Redirection], and make necessary settings.

Remote Wakeup

To enable remote wake on LAN

Select from LAN: [Advanced] - [Advanced Chipset Control] - [Wake on LAN] - [Enabled].

Memory

To check the installed memory (DIMM) status:

Select [Advanced] - [System Memory] and [Extended Memory] and check the status indications.

Saving the Configuration Data

To save the BIOS configuration data

Select [Exit] - [Exit Saving Changes]

To discard changes to the BIOS configuration data

Select [Exit] - [Exit Discarding Changes]

To restore the default BIOS configuration data (the data may differ from the factory preset)

Select [Exit] - [Load Setup Defaults].

Menu and Parameter Descriptions

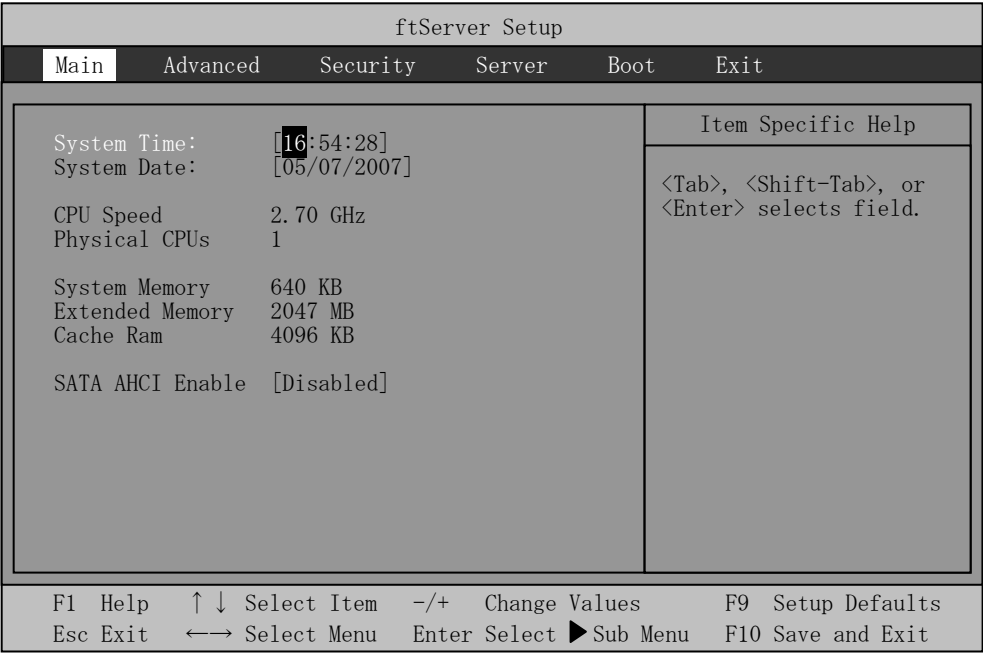
The SETUP utility has the following six major menus:

- Main
- Advanced
- Security
- Server
- Boot
- Exit

To configure detailed settings of functions, select a submenu from the above menus.
Below describes configurable functions and parameters and the factory settings displayed in the screen for each menu.

Main

Start the SETUP utility to display the Main menu.
When you select a menu with the “▶” mark and press the **Enter** key, its submenu appears.
<Example>



Available options in the Main and descriptions are listed below.

Option	Parameter	Description
System Time	HH:MM:SS	Specify the system time.
System Date	MM/DD/YYYY	Specify the system date.
CPU Speed	XXXX MHz	Displays the processor clock frequency.
Physical CPUs	X	Displays the number of processor installed.
System Memory	XXXX KB	Displays the size of system memory.
Extended Memory	XXXX MB	Displays the size of extended memory.
Cache Ram	XXXX KB	Displays the capacity of LS cache.
SATA AHCI Enable	[Disabled] Enabled	Specify whether or not to enable AHCI mode.

[] factory default

IMPORTANT:

Check and adjust the system clock before operation in the following conditions.

- After transporting the equipment
- After storing the equipment
- After the equipment halt under the conditions which is out of the guaranteed environment conditions (Temperature: 10 to 35°C, Humidity: 20 to 80%).

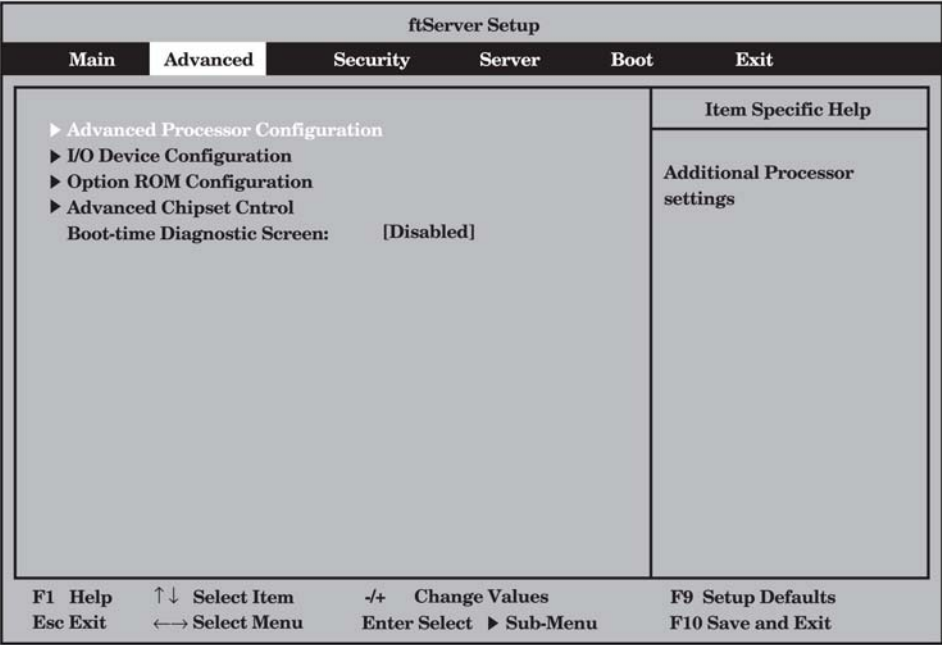
Check the system clock once in a month. It is recommended to operate the system clock using a time server (NTP server) if it is installed on the system which requires high level of time accuracy. If the system clock goes out of alignment remarkably as time goes by, though the system clock adjustment is performed, contact your sales agent.

Do not change "SATA AHCI" as "Enabled." The BIOS version may become unable to display on the ft Server Utility.

Advanced

Move the cursor onto “Advanced” to display the Advanced menu.

There is no configurable item on the Advanced menu screen below. Display each sub menu and make settings on the sub menu screen. Select an option with the “▶” mark and press **Enter** to display its submenu.



See the table below for setup options on the screen.

Option	Parameter	Description
Boot-time Diagnostic Screen	[Disabled] Enabled	Specify whether to display the Power On Self-Test (POST) screen at start-up. If “Disabled” is selected, the full screen logo appears while POST is in progress. (To display POST check results, press Esc .)

[]: factory default

Advanced Processor Configuration

When you select “Advanced Processor Configuration” in the Advanced menu, the following screen appears.

ftServer Setup	
Main	Advanced
<div> <div>Security</div> <div>Server</div> <div>Boot</div> <div>Exit</div> </div>	
<div> <div>Advanced Processor Configuration</div> <div>Item Specific Help</div> </div>	
<div> <div>Execute Disable Bit: [Enabled]</div> <div>Intel(R) Virtualization Tech. [Enabled]</div> <div>PECI Interface: [Enabled]</div> </div>	
<div> <div>F1 Help ↑ ↓ Select Item -/+ Change Values F9 Setup Defaults</div> <div>Esc Exit ← → Select Menu Enter Select ► Sub Menu F10 Save and Exit</div> </div>	

Refer to the table below for information on options.

Option	Parameter	Description
Execute Disable Bit	[Enabled] Disabled	Specify whether or not to enable Execute Disable Bit feature.
Intel(R) Virtualization Tech	[Enabled] Disabled	Specify whether or not to enable Intel Virtualization Technology feature.
PECI Interface	[Enabled] Disabled	Specify whether or not to enable Platform Environment Control Interface feature.

[]: factory default

I/O Device Configuration

When you select “I/O Device Configuration” in the Advanced menu, the following screen appears. If you select a menu with the “►” mark and press **Enter**, its submenu appears.

ftServer Setup		
Main	Advanced	Security Server Boot Exit
I/O Device Configuration		Item Specific Help
Serial Port1:	[Enabled]	Configure Serial Port 1 using options: [Disabled] No configuration [Enabled] User configuration [Auto] BIOS or OS chooses configuration NOTE: Serial Port 1 may not be routed to the Modem if a VTM is present.
Base I/O address:	[3F8/IRQ 4]	
Serial Port 1 Connection:	[Serial Connector]	
Serial Port2:	[Enabled]	
Base I/O address:	[2F8/IRQ 3]	
Serial Port2 Sharing	[Disabled]	
Keyboard Features:		
NumLock:	[Off]	
F1 Help ↑ ↓ Select Item -/+ Change Values F9 Setup Defaults		
Esc Exit ← → Select Menu Enter Select ► Sub Menu F10 Save and Exit		

Refer to the table below for information on options.

Option	Parameter	Description
Serial Port 1	Enabled [Disabled] Auto	Specify whether or not to enable Serial Port 1.
Base I/O address	[3F8/IRQ4] 2F8/IRQ3 3E8/IRQ4 2E8/IRQ3	Specify the I/O address and IRQ of Serial Port 1.
Serial Port 1 Connection	[Serial Connector] Internal Modem	Specify Serial Connector or Internal Modem for Serial Port 1 connection.
Serial Port 2	Enabled [Disabled] Auto	Specify whether or not to enable Serial Port 2.
Base I/O address	3F8/IRQ4 [2F8/IRQ3] 3E8/IRQ4 2E8/IRQ3	Specify the I/O address and IRQ of Serial Port 2.
Serial Port 2 Sharing	Enabled [Disabled]	Specify whether or not to use Serial Port 2 in BMC.
Keyboard Features		Display only.
NumLock	AUTO On [Off]	Specify whether or not to enable NumLock at system startup.

[]: factory default

Option ROM Configuration

When you select “Option ROM Configuration” in the Advanced menu, the following screen appears.

ftServer Setup	
Main	Advanced
<div> <div>Option ROM Configuration</div> <div>Item Specific Help</div> </div>	
Embedded SAS Option ROM: [Enabled] Embedded PXE#1 Option ROM: [Enabled] Embedded PXE#2 Option ROM: [Enabled]	Enables Embedded SAS Option ROM to boot from the device. Default state: ENABLED
F1 Help ↑↓ Select Item -/+ Change Values F9 Setup Defaults Esc Exit ←→ Select Menu Enter Select ► Sub Menu F10 Save and Exit	

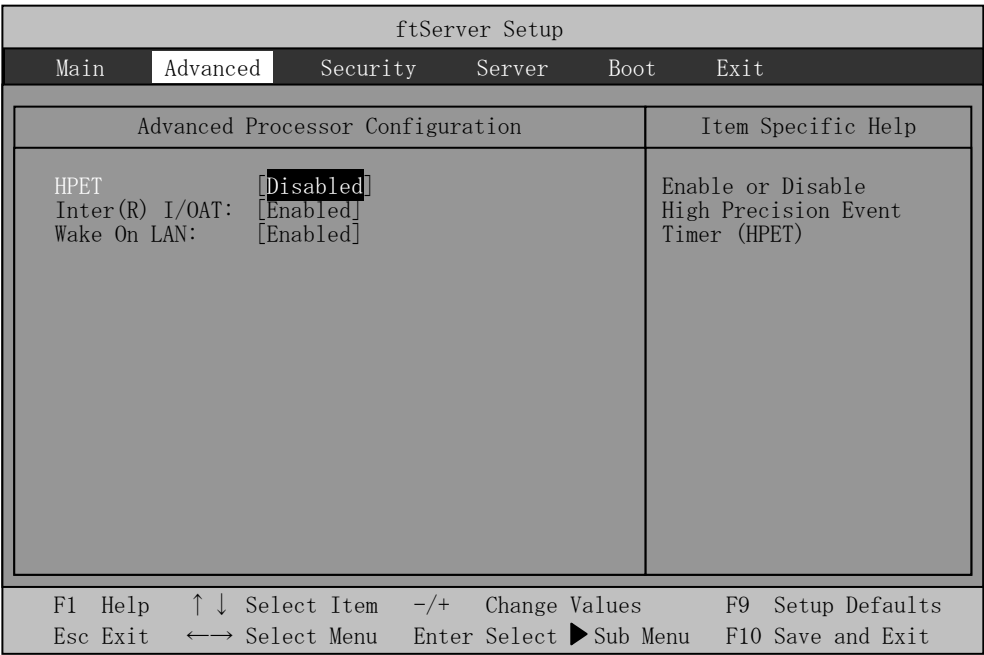
Refer to the table below for information on options.

Option	Parameter	Description
PCI Slot 1 (onboard) Option ROM	Enabled [Disabled]	If “Enabled” is selected, the extended ROM of the PCI card installed on PCI Slot 1 is initialized. Note: this option is displayed only when a PCI card is installed.
PCI Slot 2 (lower) Option ROM	Enabled [Disabled]	If “Enabled” is selected, the extended ROM of the PCI card installed on PCI Slot 2 is initialized. Note: this option is displayed only when a PCI card is installed.
PCI Slot 3 (upper) Option ROM	Enabled [Disabled]	If “Enabled” is selected, the extended ROM of the PCI card installed on PCI Slot 3 is initialized. Note: this option is displayed only when a PCI card is installed.
Embedded SAS Option ROM	[Enabled] Disabled	If “Enabled” is selected, SAS extended ROM embedded in the motherboard is initialized.
Embedded PXE#1 Option ROM	[Enabled] Disabled	If “Enabled” is selected, the extended ROM of LAN #1 embedded in the motherboard is initialized.
Embedded PXE#2 Option ROM	[Enabled] Disabled	If “Enabled” is selected, the extended ROM of LAN #2 embedded in the motherboard is initialized.

[]: factory default

Advanced Chipset Control

When you select “Advanced Chipset Control” in the Advanced menu, the following screen appears.



Refer to the table below for information on options.

Option	Parameter	Description
HPET	[Enabled] Disabled	Specify whether or not to enable High Precision Timer feature.
Intel(R) I/OAT	[Enabled] Disabled	Specify whether or not to enable Intel(R) I/OAcceleration Technology feature.
Wake On LAN	[Enabled] Disabled	Specify whether or not to enable network remote power-on feature.

[]: factory default

IMPORTANT:

Under Wake On LAN environment

When you disconnect either or both of the AC cables on the server and the Alternate Current supply is stopped, the Wake On LAN function becomes unavailable on the next system launch after the electricity supply starts. You need to connect the cables to both equipments to supply the electricity, and press the power switch to start the system.

On the OS, go to [Start] - [Management Tool] - [Computer Management] and select the Device Manager. Double click [Stratus emb-EB 2-Port Gigabit Adapter #n] under the network adapter, then select the following option from [Power Management] tab:

Wake On Magic Packet from power off state

Security

Move the cursor onto “Security” to display the Security menu.

ftServer Setup					
Main	Advanced	Security	Server	Boot	Exit
Supervisor Password Is: Unset User Password Is: Unset Set Supervisor Password [Enter] Set User Password [Enter] Password on boot [Disabled]		Item Specific Help Supervisor Password controls access to the setup utility.			
F1 Help ↑ ↓ Select Item -/+ Change Values F9 Setup Defaults Esc Exit ← → Select Menu Enter Select ► Sub Menu F10 Save and Exit					

Select “Set Supervisor Password” or “Set User Password” and press **Enter** to display the following pop-up screen. The screen below shows when “Set Supervisor Password” is selected.

Set a password on this pop-up screen. Enter a password of up to seven alphanumeric characters and symbols from the keyboard.

ftServer Setup					
Main	Advanced	Security	Server	Boot	Exit
Supervisor Password Is: Unset User Password Is: Unset Set Supervisor Password [Enter] Set User Password [Enter] Password		Item Specific Help Supervisor Password controls access to the setup utility.			
<div style="border: 1px solid black; padding: 5px; margin: 10px auto; width: 80%;"> <div style="border: 1px solid black; padding: 5px; text-align: center;">Set Supervisor Password</div> <div style="border: 1px solid black; padding: 5px;"> Enter New Password [] Confirm New Password [] </div> </div>					
F1 Help ↑ ↓ Select Item -/+ Change Values F9 Setup Defaults Esc Exit ← → Select Menu Enter Select ► Sub Menu F10 Save and Exit					

IMPORTANT:

- User password setup is not available before Supervisor password setup.
 - Do not set any password before installing the OS.
 - If you forget your password, contact your sales agent.
-

See the table below for setup options on the screen.

Option	Parameter	Description
Supervisor Password Is	Unset Set	Indicates Supervisor password setup status (view only).
User Password is	Unset Set	Indicates User password setup status (view only).
Set Supervisor Password	[Enter]	Press Enter to display the supervisor password entry screen. This option is available only when you log into the SETUP utility with the supervisor password.
Set User Password	[Enter]	Press Enter to display the user password entry screen. With a user password, accessing the SETUP menus is restricted.
Password on boot	[Disabled] Enabled	Specify whether to request a password entry at boot-up. User password setup is required beforehand.

[]: factory default

IMPORTANT:

If you have logged in SETUP by using the Supervisor Password, you can check and change all settings. If you have logged in SETUP by using User Password, you can see the settings but cannot make changes on the settings except System Time, System Date and User Password of Main.

Server

Move the cursor onto [Server] to display the Server menu.

The following describes options you can configure in the Server menu and their functions. Select an option with the “►” mark and press **Enter** to display its submenu.

Refer to the table below for information on options.

ftServer Setup	
Main	Advanced Security Server Boot Exit
► System Management ► Console Redirection ► Event Log Configuration ► Monitoring Configuration Post Error Pause: [Enabled] AC-LINK: [Last State] Power On Delay Time: [180]	Item Specific Help Additional setup menu to view server management features.
F1 Help ↑ ↓ Select Item -/+ Change Values F9 Setup Defaults Esc Exit ← → Select Menu Enter Select ► Sub Menu F10 Save and Exit	

Option	Parameter	Description
Post Error Pause	Disabled [Enabled]	Set whether or not to pause POST at the end of POST if an error has occurred during POST execution.
AC LINK	Stay Off [Last State] Power On	Specify the AC LINK feature by selecting the status of the power supply unit of the server when the AC power supply restarts. (See the following table for details.)
Power ON Delay Time	[180]-255(s)	Configure the DC ON delay time if AC LINK is set to “Power On” or “Last State” (unit: second).

[]: factory default

The table below lists how selections for “AC LINK” determine the power status of the server when the power supply to the server restarts.

State before powered off	Parameter		
	Stay Off	Last State	Power On
In service	Off	On	On
Out of service (DC power: Off)	Off	Off	On
Forced shutdown *	Off	Off	On

* Pressing the POWER switch for over four seconds shuts down the power to the server.

System Management

Select “System Management” on the Server menu and press **Enter** to display the following screen.

⟨Example⟩

ftServer Setup	
Main	Advanced Security Server Boot Exit
System Management	Item Specific Help
BIOS Version: 2.1:44 Board Part #: 243-632791 Board Serial #: 113108030768 System Part #: XXXXX-XXX System Serial #: 9072543618 Chassis Part #: 243-535509 Chassis Serial #: 01 BMC Device ID: 26 BMC Device Rev: 01 BMC Firmware Rev: 0E.25 SDR Rev: SDR Version 00.10 PIA Rev: 01.10 ASIC Rev: 2023 SMM Rev: 00.25	All items on this menu cannot be modified in user mode. If any items require changes, please consult your system Supervisor.
F1 Help	↑ ↓ Select Item -/+ Change Values F9 Setup Defaults
Esc Exit	← → Select Menu Enter Select ► Sub Menu F10 Save and Exit

See the table below for setup options on the screen.

Option	Parameter	Description
BIOS Version	—	Displays the BIOS version.
Board Part Number	—	Displays the board information.
Board Serial Number	—	Displays the board information.
System Part Number	—	Displays the system information.
System Serial Number	—	Displays the system information.
Chassis Part Number	—	Displays the chassis information.
Chassis Serial Number	—	Displays the chassis information.
BMC Device ID	—	Displays the BMC information.
BMC Device Revision	—	Displays the BMC information.
BMC Firmware Revision	—	Displays the BMC information.
SDR Revision	—	Displays the revision of SDR (sensor device information).
PIA Revision	—	Displays the PIA (plat form information) revision.
ASIC Rev	—	Displays the firmware information of the fault-tolerant chipset.
SMM Rev	—	Displays the firmware information of System Management.
CPU0 BMC MAC Address	—	Displays MAC Address of the CPU/IO Module0-mounted BMC if the ft management card is implemented.
CRU1 BMC MAC Address	—	Displays MAC Address of the CPU/IO Module1-mounted BMC if the ft management card is implemented.\

[]: factory default

Console Redirection

Select “Console Redirection” on the Server menu and press **Enter** to display the following screen.

ftServer Setup					
Main	Advanced	Security	Server	Boot	Exit
Console Redirection			Item Specific Help		
Com Port Address [Disabled]			If enabled, it will use a port on the motherboard.		
Baud Rate [19.2K]					
Console Type [PC ANSI]					
Flow Control [CTS/RTS]					
Console connection: [Direct]					
Continue C.R. after POST: [Off]					
F1 Help ↑ ↓ Select Item -/+ Change Values F9 Setup Defaults Esc Exit ← → Select Menu Enter Select ► Sub Menu F10 Save and Exit					

See the table below for setup options on the screen.

Option	Parameter	Description
Com Port Address	[Disabled] Serial Port1 Serial Port2	Select a serial port.
Baud Rate*	9600 [19.2K] 38.4K 57.6K 115.2K	Select a port rate used for the interface with a hardware console to be connected.
Console Type*	VT100 VT100, 8bit PC-ANSI, 7bit [PC-ANSI] VT100+ VT-UTF8	Select a console type.
Flow Control*	None XON/XOFF [CTS/RTS]	Select a flow control method.
Console Connection	[Direct] Via modem	Select a connector.
Continue C.R. after POST	[Off] On	Specify whether or not to continue Console Redirection after OS is loaded.

[]: factory default

ftServer Setup			
Main	Advanced	Security	Server
Event Log Configuration		Item Specific Help	
Clear Online Event Logs	[Press Enter]	The system event log will be cleared if selecting "YES" .	
Clear Offline Event Logs	[Press Enter]		
F1 Help	↑ ↓ Select Item	-/+ Change Values	F9 Setup Defaults
Esc Exit	← → Select Menu	Enter Select ► Sub Menu	F10 Save and Exit

Option	Parameter	Description
Clear Online Event Logs	[Press Enter]	To clear event logs of the working module, press the Enter key and select “Yes.”
Clear Offline Event Logs	[Press Enter]	To clear event logs of the stand-by module, press the Enter key and select “Yes.”

Monitoring Configuration

Select “Monitoring Configuration” on the Server menu and press **Enter** to display the following screen.

ftServer Setup					
Main	Advanced	Security	Server	Boot	Exit
Monitoring Configuration		Item Specific Help			
FRB-2 Timer [Enabled] PCI Enumeration Monitoring: [Enabled] PCI Enumeration Monitoring Timeout: [180] Option ROM Scan Monitoring: [Enabled] Option ROM Scan Monitoring Timeout: [300] OS Boot Monitoring: [Enabled] OS Boot Monitoring Timeout: [600] POST Pause Monitoring: [Enabled] POST Pause Monitoring Time-out [180]		Disables/enables the FRB-2 Timer.			
F1 Help ↑ ↓ Select Item -/+ Change Values F9 Setup Defaults Esc Exit ← → Select Menu Enter Select ► Sub Menu F10 Save and Exit					

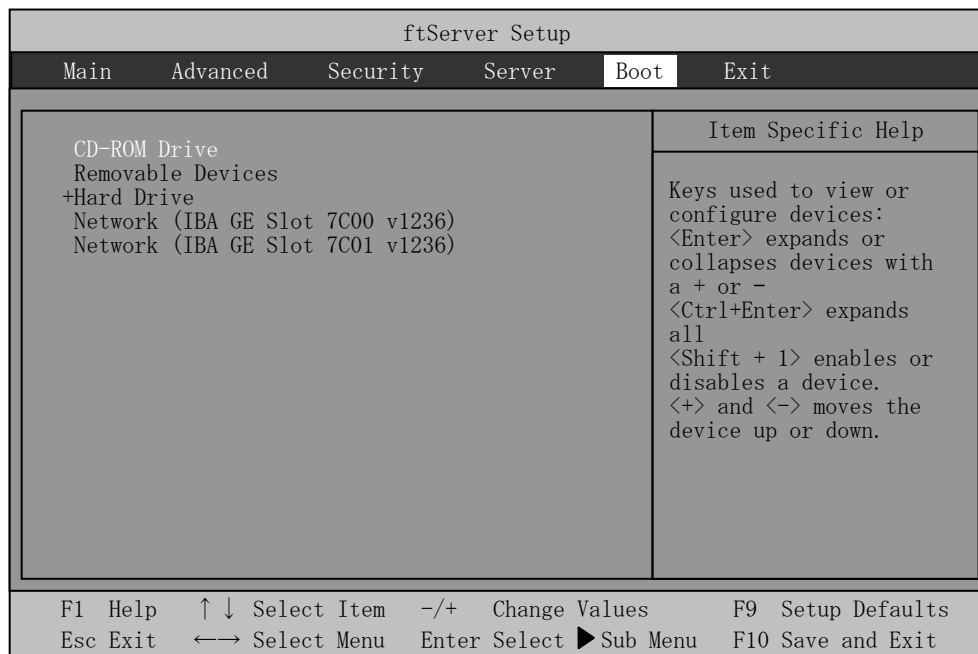
Option	Parameter	Description
FRB-2 timer	Disabled [Enabled]	Select whether or not to enable the FRB-2 timer.
PCI Enumeration Monitoring	Disabled [Enabled]	Select whether or not to enable the function to monitor PCI Device scan.
PCI Enumeration Monitoring Timeout	60-[180]-1200	Set the timeout for PCI Device scan. (unit: second)
Option ROM Scan Monitoring	Disabled [Enabled]	Select whether or not to enable the function to monitor the extended ROM scan.
Option ROM Monitoring Timeout	60-[300]-1200	Set the timeout of the extended ROM scan. (unit: second)
OS Boot Monitoring	Disabled [Enabled]	Select whether or not to enable the function to monitor OS boot-up. If you are starting up from an OS with no NEC ESMPRO Agent installed, disable this option. If you use Disaster Recovery Option for ARCServe, select [Disabled].
OS Boot Monitoring Timeout	60-[600]-1200	Set the timeout at OS boot-up. (unit: second)
POST Pause Monitoring	Disabled [Enabled]	Set whether or not to enable the POST monitoring function during boot pause. (unit: second)
POST Pause Monitoring Time-out	60-[180]-1200	Set the time for POST monitoring during boot pause. (unit: second)

[]: factory default

Boot

Move the cursor onto “Boot” to display the Boot menu.

The server searches for the boot device according to the order specified in this menu and use the software to boot the system if found.



You can change the boot device order using ↑ or ↓ and + or -. Move the cursor to select the device by ↑ or ↓, and then change the priority using + or -.

IMPORTANT:

Move to set “CD-ROM Drive” above “Hard Drive” when you boot the EXPRESSBUILDER.

Exit

Move the cursor onto “Exit” to display the Exit menu.

ftServer Setup			
Main	Advanced	Security	Server Boot Exit
Exit Saving Changes Exit Discarding Changes Load Setup Defaults Discard Changes Save Changes		Item Specific Help Exit System Setup and save your changes to CMOS.	
F1 Help ↑ ↓ Select Item -/+ Change Values F9 Setup Defaults Esc Exit ← → Select Menu Enter Select ► Sub Menu F10 Save and Exit			

The following describes each option on the Exit menu:

Exit Saving Changes

Select this option to save the current configuration data into the CMOS (non-volatile memory) and exit the SETUP utility.

Select “Exit Saving Changes” to display the screen below. Select “Yes” to save the current configuration data into the CMOS (non-volatile memory) and exit the SETUP utility. The server will automatically restart the system.

ftServer Setup	
Main	Advanced Security Server Boot Exit
Exit Saving Changes Exit Discarding Changes Load Setup Defaults Discard Changes Save Changes	Item Specific Help Exit System Setup and save your changes to CMOS.
<div style="border: 1px solid black; padding: 10px; margin: 10px auto; width: 60%;"> <p style="text-align: center;">Setup Confirmation</p> <p>Save configuration changes and exit now?</p> <p style="text-align: center;"> <input checked="" type="button" value="[Yes]"/> <input type="button" value="[No]"/> </p> </div>	
Space Select Enter Accept	

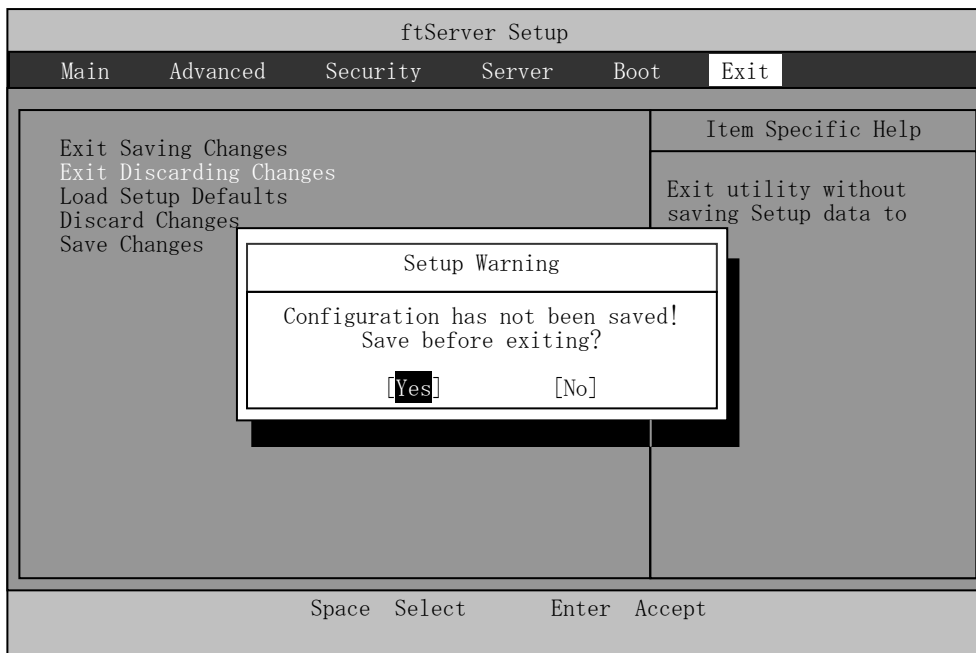
Exit Discarding Changes

Select this option to exit the SETUP utility without saving the current configuration data into the CMOS (non-volatile memory).

If you select “Yes” here, the “SETUP Warning” dialogue box appears.

If you select “No” in the “SETUP Warning” dialogue box, you can exit SETUP without saving the changes you have made.

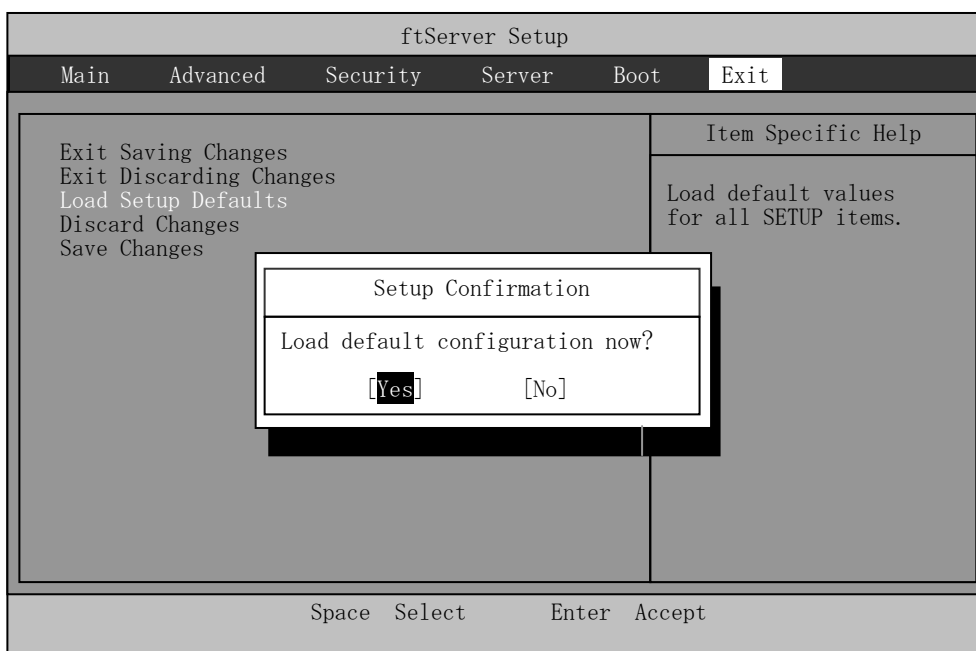
If you select “Yes” in the dialogue box, you can exit SETUP with the changes you have made saved in CMOS. The server reboots automatically.



Load Setup Defaults

Select this option if you want to reset all values in SETUP to default (factory-set values). When you select Load Setup Defaults, the dialogue box as shown below appears.

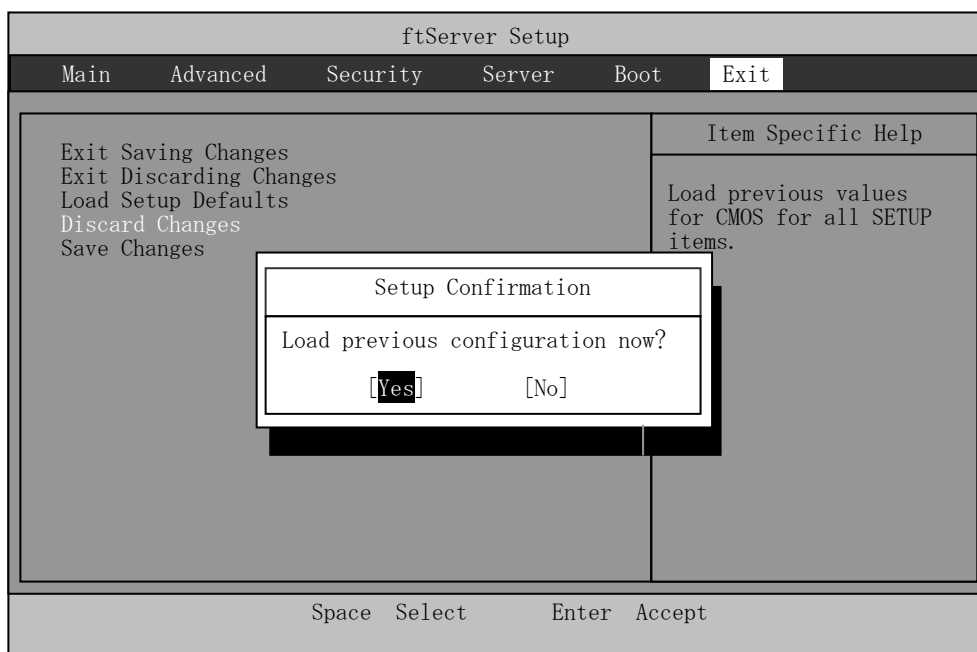
If you select “Yes” in the dialogue box, default values are restored. If you select “No”, you will see the Exit menu screen.



Discard Changes

Select this option if you want to restore previous values before saving values in CMOS. When you select “Discard Changes”, you will see the dialogue box as shown below.

If you select “Yes” in the dialogue box, changes you have made are discarded and previous settings are restored.



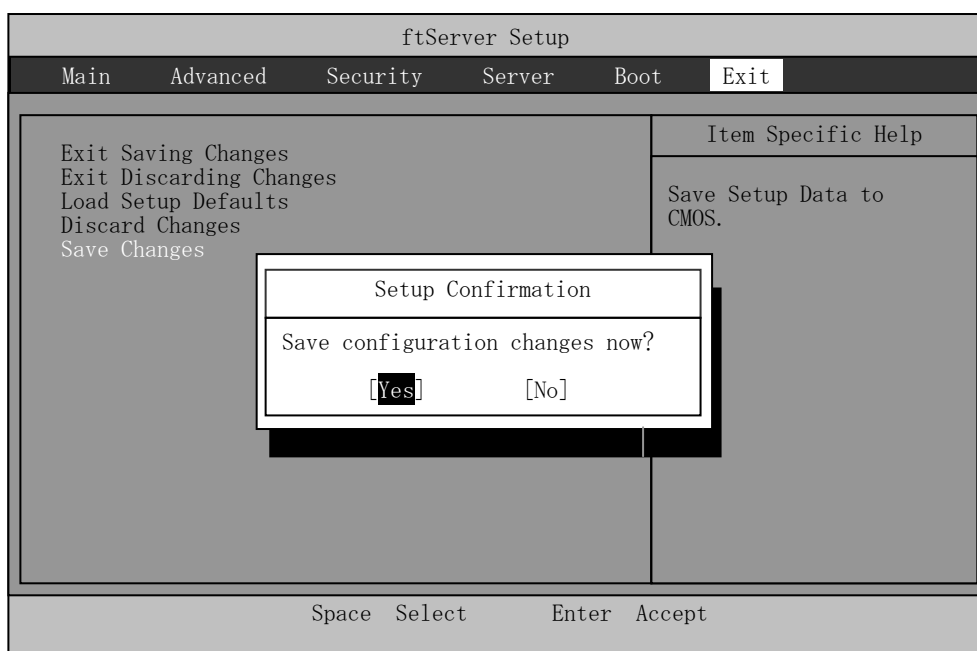
IMPORTANT:

The default value and the factory default value differ partially. If you want to bring the value back to the default, verify all the value you want to make changes.

Save Changes

Select this option if you want to save changes you have made in CMOS (non-volatile memory) without exiting SETUP. When you select the Save Changes, you will see the dialogue box as shown below.

If you select “Yes” in the dialogue box, changes you have made are saved in CMOS (non-volatile memory).



SAS BIOS –Adaptec SAS/SATA Configuration Utility–

Adaptec SAS/SATA Configuration utility makes settings of the built-in SAS controller on a motherboard. You can start it up by simple key operation during POST execution without using any special startup disk.

IMPORTANT:

- Because the server is installed with the latest version of the *SCSISelect* utility, your screen display may be different from the one described in this guide. For information on options different from those described in this guide, refer to the online help or ask your service agent.
- When you start this utility, select [Server], [Monitoring Configuration], [Option ROM Scan Monitoring], and [Disabled]. If [Enabled] is selected, system may reboot while you are making settings. However, set [Option ROM Scan Monitoring] to [Enabled] after making settings.

Starting and Quitting the Adaptec SAS/SATA Configuration utility

The following section describes the procedures from starting the Adaptec SAS/SATA Configuration utility to quitting the utility.

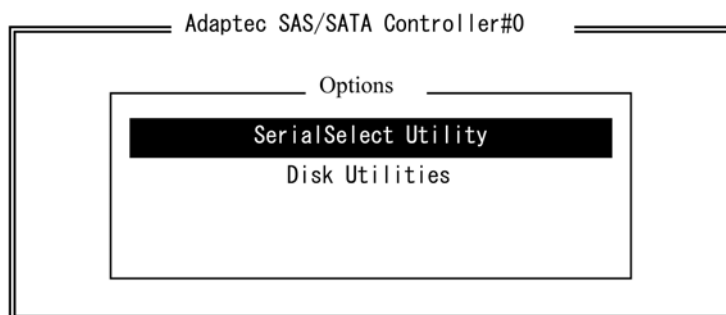
1. Power on the server.

The following message appears on the screen during POST execution.

```
Adaptec Serial Attached SCSI (SAS) BIOS Vx.x-x
(C) 1998-2006 Adaptec, Inc. All Rights Reserved.
◀◀◀ Press <CTRL><A> for Adaptec SAS/SATA Configuration Utility! ▶▶▶
```

2. Press and hold down the **Ctrl** key and press the **A** key.

The Adaptec SAS/SATA Configuration utility starts up with the “Main” menu displayed.



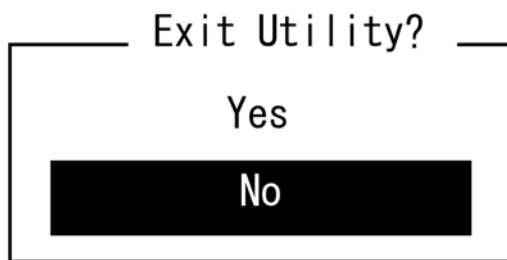
3. Select a menu in the “Options”, and then press the **Enter** key.

If you want to make settings of the adapter, select “SerialSelect Utility.”

If you want to format or verify the hard disk drive connected to the adapter, select “Disk Utility.”

For more information, see the explanation below.

4. To quit, press the **Esc** key until you see the closing message. (If any changes have been made, the message asking you whether or not to save the changes is displayed. Select Yes (save the changes) or No (discard the changes)).



Parameter and Description

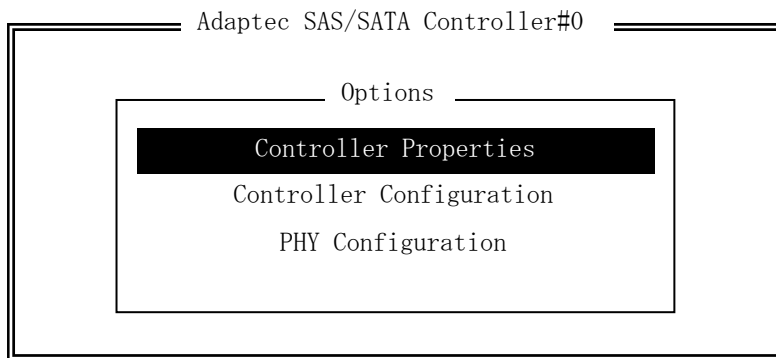
Adaptec SAS/SATA Configuration utility has two types of menu.

- SerialSelect Utility
- Disk Utilities

You can set features that are more detailed by selecting a submenu from these menus. The following describes the features and parameters that can be set in each menu and factory settings displayed on the screen.

SerialSelect Utility

The following screen is displayed when you select “SerialSelect Utility” in the “Options” menu.



Select an item using the UP and DOWN ARROW keys and press **Enter**. The following describes the menu and parameters.

Tips:

You do not need to specify the parameters. The following is described for reference.

Controller Properties

The following screen is displayed when “Controller Properties” is selected in the menu.

Adaptec SAS/SATA Controller#0

Controller Information

```

PCI Slot:Bus:Device:Function..... 0:A:0:0
Interrupt (IRQ) Channel..... 7
I/O Port Address..... 8000
Device ID..... 041E
Controller Serial number.....
Controller WWN..... 50030130F0B13700
          
```

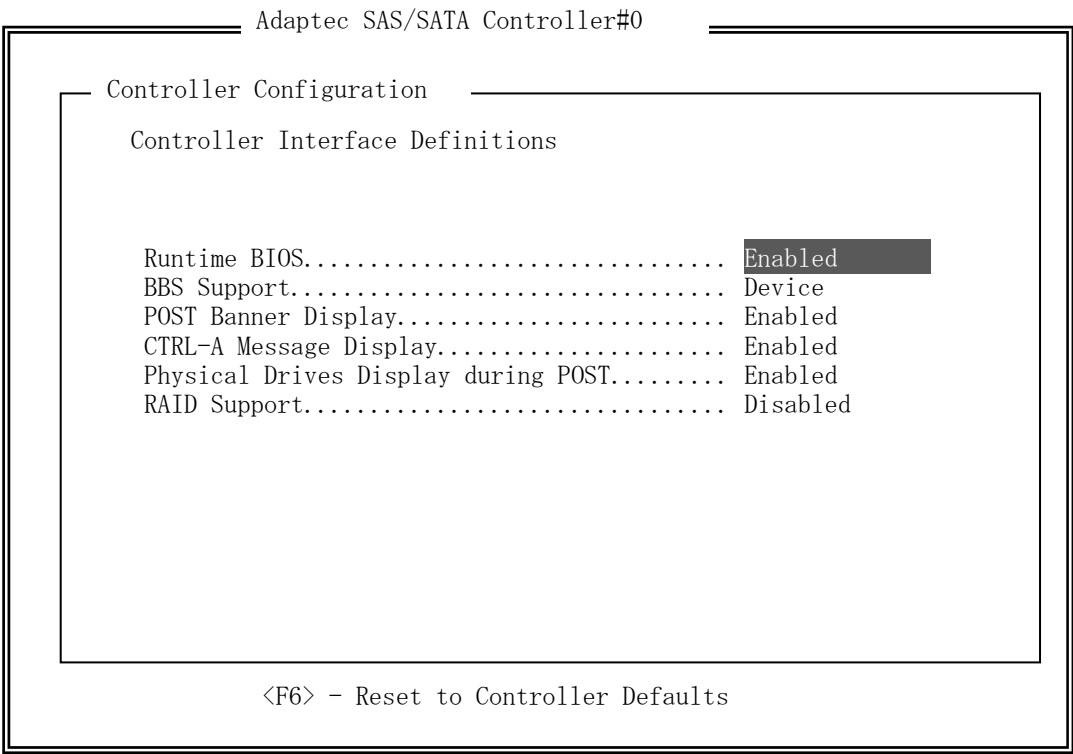
See the following table for each item.

Item	Parameter	Description
PCI Slot Bus: Device:Function	—	Displays the storage device bus on the SAS controller.
Interrupt(IRQ) Channel	—	Displays the interrupt.
I/O Port Address	—	Displays the I/O port device.
Device ID	—	Displays the device ID.
Controller Serial Number	—	Displays the controller serial number.
Controller WWN	—	Displays the controller WWN.

[]: factory default

Controller Configuration

The following screen is displayed when “Controller Configuration” is selected in the menu.



See the following table for each item.

Item	Parameter	Description
Runtime BIOS	[Enabled] Disabled Disabled:Scan bus	Controls the BIOS status at the POST. If [Enabled] is selected, the controller can be operated as a boot device by SAS controller BIOS. If [Disabled] is selected, other appropriate SAS controllers operate as boot devices.
BBS Support	[Device] Controller	If the setting of BBS support is set to [Device], the boot device connected to SAS controllers is registered to the boot menu of system BIOS. If BBS support is set to [Controller], only SAS controllers are registered to the BIOS boot menu.
POST Banner Display	[Enabled] Disabled	If [Enabled] is selected, Adaptec banner, the version, and copyright are displayed. If [Disabled] is selected, Adaptec banner, the version, and copyright are not displayed.
CTRL-A Message Display	[Enabled] Disabled	If [Enabled] is selected, the message "Press <CTRL><A> for Adaptec SAS/SATA Configuration Utility!" is displayed in SAS controller BIOS during the POST. Even if this option is set to [Disabled], the utility can be started by pressing CTRL+A after the BIOS title of SAS controllers is displayed.
Physical Drivers Display During Post	[Enabled] Disabled	If [Enabled] is selected, connected physical devices are displayed during the system POST. However, depending on the device display, the time that it takes to complete entire POST can become a few seconds longer.
RAID Support	Enabled [Disabled]	Do not set to [Enabled] since RAID is not supported.

[]: factory default

1. Press **F6** to return to the initial value.
2. To quit, press **Esc** until you see the closing message (If any changes have been made, the message asking you whether or not to save the changes is displayed.).
3. When the closing message is displayed, select [Yes] to quit SerialSelect Utility and restart the system by pressing any key. The changes made in SerialSelect Utility are enabled after the system is restarted.

PHY Configuration

The following screen is displayed when “PHY Configuration” is selected in the menu.

SAS Device Configuration

SAS Port ID	#0	#1	#2	#3	#4	#5	#6	#7
-------------	----	----	----	----	----	----	----	----

PHY Rate (Gb/s)	Auto	Auto	Auto	Auto	Auto	Auto	Auto	Auto
SAS Address ... 50030130F0B13700	0	0	0	0	0	0	0	0

<F6> - Reset to Defaults

See the following table for each item

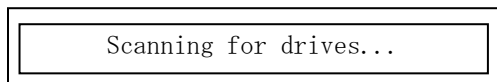
Item	Parameter	Description
PHY Rate	[Auto]	Data transfer rate between SAS controller and devices. The initial value is set to [Auto]. SAS card adjusts the rate if necessary.
	1.5	
	3.0	
SAS Address	0-F	Specifies the last digit of a 64-bit SAS address of the SAS controller, device, and each port using a globally unique worldwide name (WWN) identifier.

[]: factory default

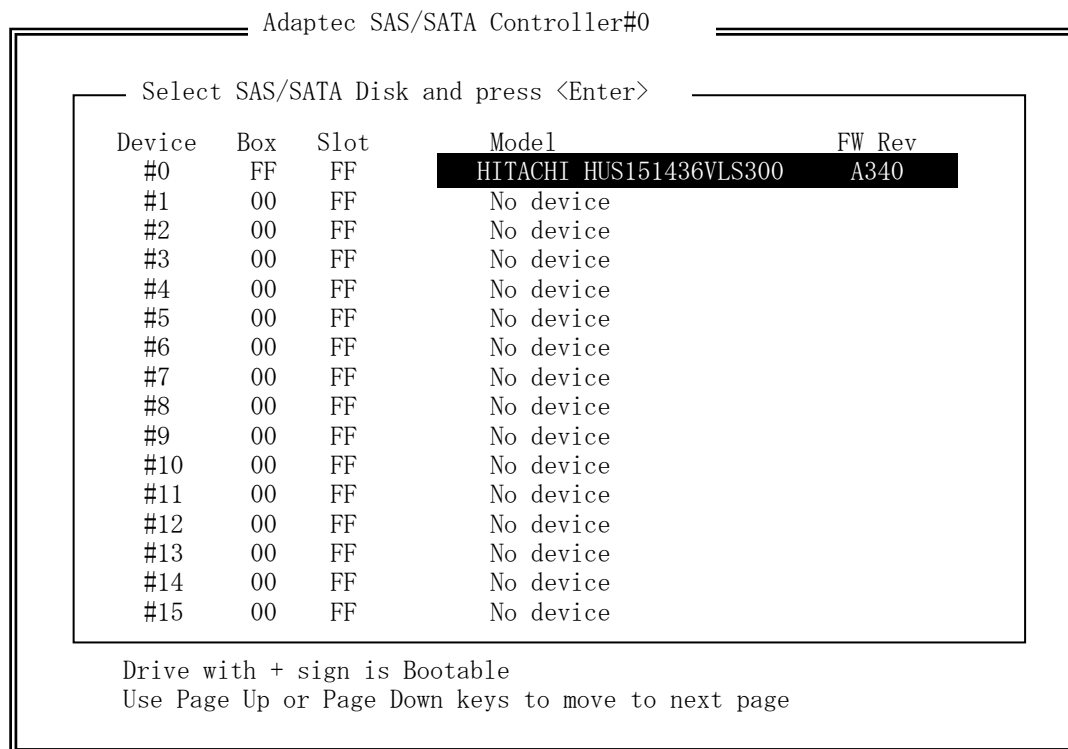
1. Press **F6** to return to the initial value.
2. To quit, press **Esc** until you see the closing message (If any changes have been made, the message asking you whether or not to save the changes is displayed.).
3. When the closing message is displayed, select [Yes] to quit SerialSelect Utility and restart the system by pressing any key. The changes made in SerialSelect Utility are enabled after the system is restarted.

Disk Utilities

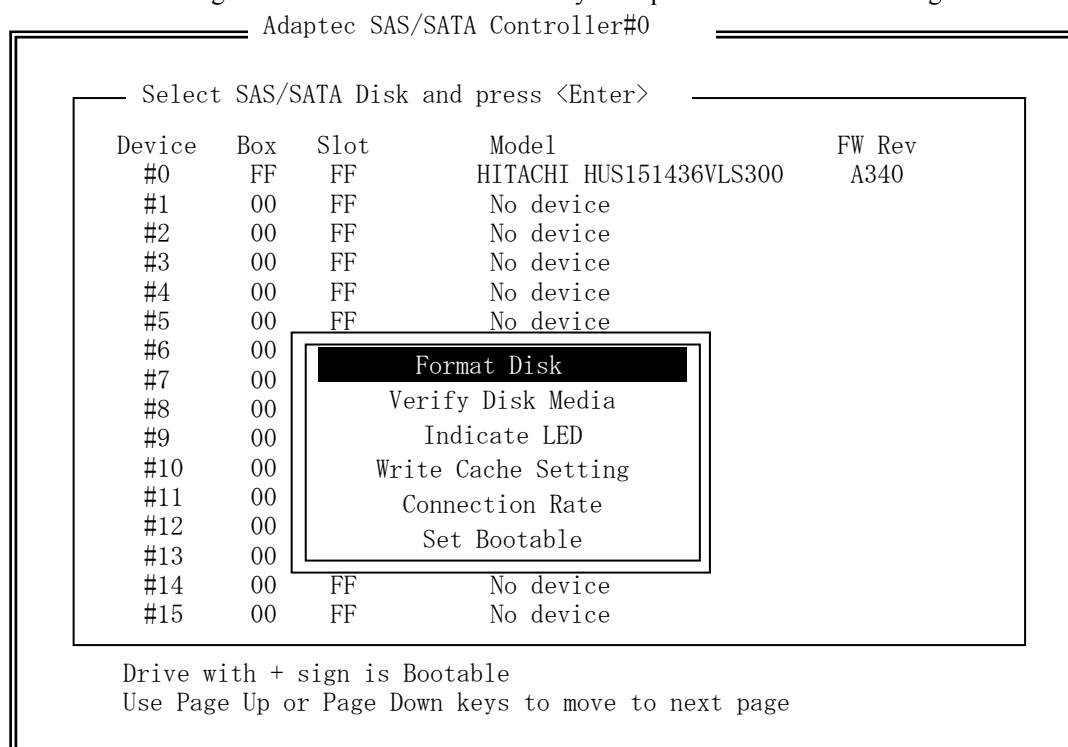
The following screen is displayed when “Disk Utilities” is selected in the menu.



The following screen is displayed after a while.



Select an item using the UP and DOWN ARROW keys and press **Enter**. The following menu will appear.



See the following table for each item.

Item	Parameter	Description
Format Disk	—	<p>Low-level format is simulated by writing entire disk to zero.</p> <hr/> <p>TIPS: Low-level format is performed to the disk drive at factory. You do not need to perform low-level format again.</p> <hr/> <p>IMPORTANT: All the data on the disk is deleted. Back up your data before performing this operation.</p> <hr/>
Verify Disk Media	—	Check for errors by scanning the disk drive media
Indicate LED	—	Flash the LED on the selected disk drive.
Write Cache Setting	Enabled [Disabled]	Enable/Disable Write Cache.
Connection Rate	[Auto] 1.5Gb/s 3.0Gb/s	The data transfer rate of disk drive. The initial value is set to [Auto]. You do not need to change it.
Set Bootable	Enabled [Disabled]	Set the disk drive to the bootable disk drive. You do not need to change it.

[]: factory default

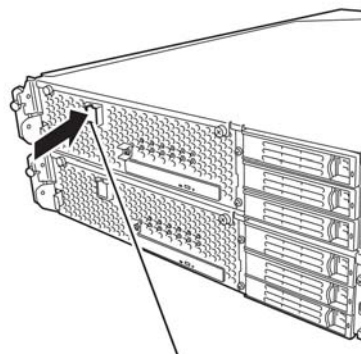
FORCED SHUTDOWN AND CLEAR

Read this section if your server does not operate as expected, or if you want to return all setup values to those made at shipment.

Forced Shutdown

Use this function when an OS command does not shut down the server, the POWER switch does not turn off the server, or resetting does not work.

Press and hold the POWER switch on the primary server for over 4 seconds. The power is forcibly turned off. To turn on the power back again, wait approximately 30 seconds after the forced shutdown.



Press it for over 4 seconds.

CLEAR CMOS/PASSWORD

With the pre-installed SETUP utility, you can set desired passwords to protect data stored on the server from unauthorized user access. If you forget the password, you can clear them by following the procedure described in this section.

You can also use the same procedure to clear the CMOS data in the server.

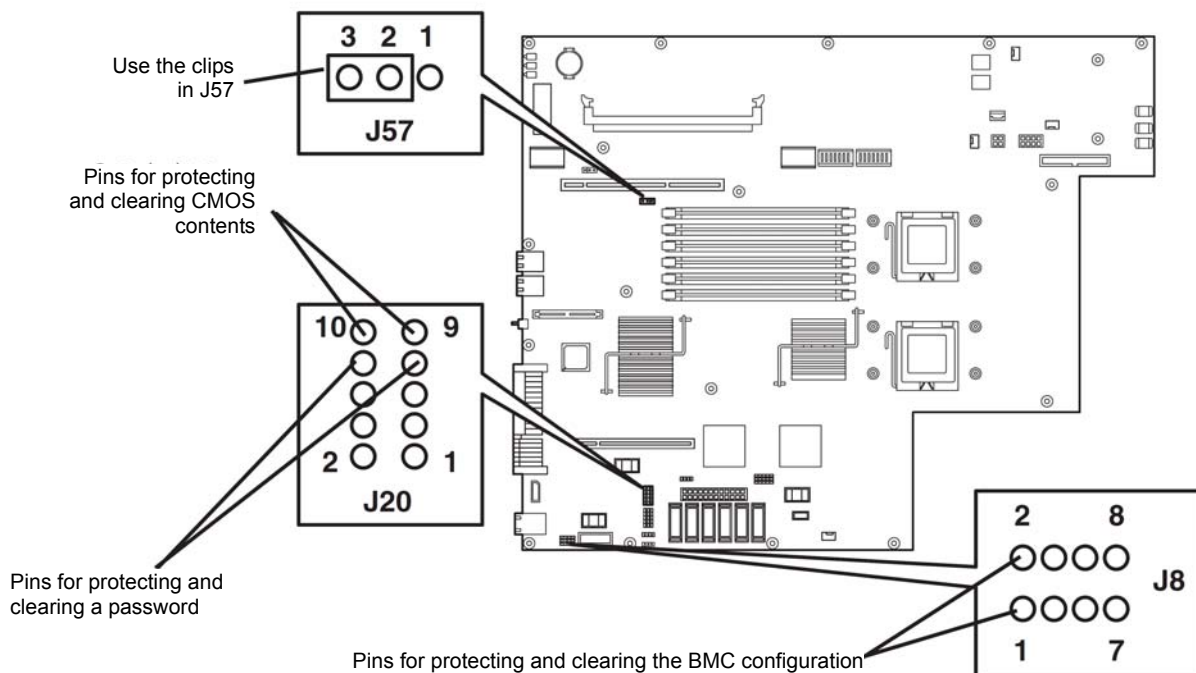
IMPORTANT:

- Clearing the CMOS data restores the factory settings.
 - To clear the password or CMOS data, power off the server.
-

To clear the password or the CMOS data, use configuration jumper pins (jumper switches) located inside of the server. The jumper switches are found on the motherboard in a CPU/IO module. See the figure below.



IMPORTANT:

Do not change any other jumper switch settings. Any improper change may cause the server to fail or malfunction.



- Pins for protecting/clearing the password
 - Short-circuiting the two pins: Clears the password
 - Opening the two pins: Protects the password (factory preset)
- Pins for protecting/clearing the CMOS data
 - Short-circuiting the two pins: Clears the CMS data
 - Opening two pins: Protects the CMOS data (factory preset)
- Pins for protecting/clearing the BMC configuration
 - Short-circuiting the two pins: Clears the BMC configuration
 - Opening two pins: Protects the BMC configuration (factory preset)

The following describe the clearing procedure.

 WARNING	
	<p>Observe the following instructions to use the server safely. There are risks of death or serious personal injury. See “PRECAUTIONS FOR SAFETY” in Chapter 1.</p> <ul style="list-style-type: none"> ■ Do not disassemble, repair, or alter the server.

How to Clear CMOS

1. Power off the Fault Tolerant Server series and unplug the both power cords.
2. Remove the both CPU/IO modules (0 and 1) from the Fault Tolerant Server series (see “Removing CPU/IO Module” on page 8-11).
3. Make setting of jumper switch for clearing CMOS of CPU/IO module 0.
Remove the clips from the jumper pins (J57) 2-3 and place them on the jumper pins (J20) 9-10 on the CPU/IO Module 0.
4. Connect only the power cord of the CPU/IO module 0 and press the POWER switch to power on.
5. When POST is completed after the startup, press the POWER switch to power off, and then disconnect the power cord from the outlet.
6. By referring to “Removing CPU/IO Module” on page 8-11, remove the CPU/IO module 0 from the server.
7. Restore the previous CMOS clear jumper switch settings. Remove the jumper pins (J20) 9-10 of the CPU/IO module 0 and install them on the jumper pins (J57) 2-3.
8. By referring to “Installing CPU/IO Module” on page 8-14, install the CPU/IO module 0 on the server.
9. Reconnect only the power cord of the CPU/IO module 0 and press the POWER switch to power on.
10. After the startup, press the **F2** key during POST to start BIOS SETUP.
11. Make settings in SETUP as you desire and then save the settings by selecting “Exit”→ “Exit Saving Changes.” Switch the power off and disconnect the power cord from the outlet.
12. Clear CMOS for the CPU/IO module 1 by following the steps 3 to 12.
13. By referring to “Installing CPU/IO Module” on page 8-14, connect both CPU/IO modules to the device.
14. Connect both power cords.

HOW TO CLEAR PASSWORDS

1. Power off Fault Tolerant Server series and unplug the both power cords.
2. Remove the both CPU/IO modules (0 and 1) from the Fault Tolerant Server series (see “Removing CPU/IO Module” on page 8-11).
3. Make setting of jumper switch for clearing the password of CPU/IO module 0.
Remove the clips from the jumper pins (J57) 2-3 on CPU/IO module 0 and place them on the jumper pins (J20) 7-8 on the CPU/IO module 0.
4. Mount the CPU/IO module 0 to Fault Tolerant Server series (see “Installing CPU/IO Module” on page 8-14).
5. Connect the power cord of CPU/IO module 0 only, and then press the POWER switch to power on.
6. When POST is completed after the startup, press the POWER switch to power off, and then disconnect the power cord from the outlet.
7. By referring to “Removing CPU/IO Module” on page 8-11, remove the CPU/IO module 0 from the server.
8. Reset the jumper switch setting.
Remove the clips from the jumper pins (J20) 7-8 and place them on the jumper pins (J57) 2-3 on the CPU/IO module 0.
9. Clear password for the CPU/IO module 1 by following the steps 3 to 8.
10. By referring to “Installing CPU/IO Module” on page 8-14, install both CPU/IO modules on the server.
11. Connect both power cords.

HOW TO CLEAR THE BMC CONFIGURATION

1. Power off Fault Tolerant Server series and unplug the both power cords.
2. Remove the both CPU/IO modules (0 and 1) from the Fault Tolerant Server series (see “Removing CPU/IO Module” on page 8-11).
3. Make setting of jumper switch for clearing the BMC configuration of module 0.
Remove the clips from the jumper pins (J57) 2-3 on CPU/IO module 0 and place them on the jumper pins (J20) 7-8 on the CPU/IO module 0.
4. Mount the CPU/IO module 0 to Fault Tolerant Server series (see “Installing CPU/IO Module” on page 8-14).
5. Connect the power cord of CPU/IO module 0 only, and then press the POWER switch to power on.
6. When POST is completed after the startup, press the POWER switch to power off, and then disconnect the power cord from the outlet.
7. By referring to “Removing CPU/IO Module” on page 8-11, remove the CPU/IO module 0 from the server.
8. Reset the jumper switch setting.
Remove the clips from the jumper pins (J20) 7-8 and place them on the jumper pins (J57) 2-3 on the CPU/IO module 0.
9. Clear password for the CPU/IO module 1 by following the steps 3 to 8.
10. By referring to “Installing CPU/IO Module” on page 8-14, install both CPU/IO modules on the server.
11. Connect both power cords.

REMOTE MANAGEMENT FUNCTION

Both models of the Fault Tolerant Server are equipped with the optional card, the ft Remote Management Card on the server. By connecting to a network via their management LAN port, BMC (Baseboard Management Controller), an LSI for system management, installed on the server allows remote monitoring and controlling of the server such as keyboard, video and mouse (KVM) control over management network.

Network Default Values

The following are default values to connect the server to a network.

IP Address	: 192.168.1.1
User Name	: administrator
Password	: (None)
Host Name	: ARMCXXXXXXXXXXXX

- The host name above is the host name used for auto registering with a DNS server using DHCP functions. XXXXXXXXXXXXXXX is the MAC address assigned to each management card. The MAC address can be found on the label attached to the rear of the card or [Server] – [System Management] – [CRU0 BMC MAC Address]/[CRU1 BMC MAC Address] on the BIOS Set UP screen.

IMPORTANT:

- The communication mode on the management LAN board is fixed as auto negotiation mode; it cannot be changed manually. At the same time, set the communication on the link partner side as auto negotiation mode.
 - The default IP address of the management LAN is 192.168.1.1 for both CPU/IO module #0 and CPU/IO module #1. Therefore, the servers are unable to connect network simultaneously without changing this IP address. In order to enable the network connections simultaneously, specify different IP address for each CPU/IO module.
 - To ensure security, change values for host name, password and IP address according to your network environment.
-

Settings on the Server

The following describes the setting procedure.

CHECK:

The resolution and refresh rate of the screen that can be displayed on a remote KVM console are 1024x768, 75Hz and smaller respectively. If values larger than these are set, the remote screen does not display any data. If a great value is set for the number of colors on the screen for the server, the remote may not show colors accurately. Connecting this card to a network where broadcast occurs frequently may affect remote control performance.

Initial Settings on the Server

1. If information specific to the server has not been written in, the following message informing you that the server-specific information is not written is displayed while the full screen logo is displayed, and the startup processing of the server is paused.

If this message is not displayed, the remote management function does not need to be initialized. If it is displayed, the remote management function needs to be initialized in order to monitor devices into details.

H/W Configuration of BMC is corrupted.

!! Update BMC H/W Configuration by configuration tool !!

!! Refer to BMC configuration manual !!

The message above may appear in a different screen during POST with the full screen logo is shown and paused. In that case, press the **Esc** key to display the diagnosis screen to check whether or not the above message is shown. If a different error message is shown, refer to Chapter 7 “Troubleshooting.”

2. How to make initial settings

Either wait for a while after the above message is shown or press the **F1** key to precede POST. Start up the “EXPRESSBUILDER”DVD and select “initialize RNESte Management Card” from the Tool menu. By doing so, information specific to each server will be written in.

When writing the information is completed, the following message appears. Press any key to reboot the server for use.

Programming complete, reboot server for normal operation.

Strike a key when ready...

TIPS:

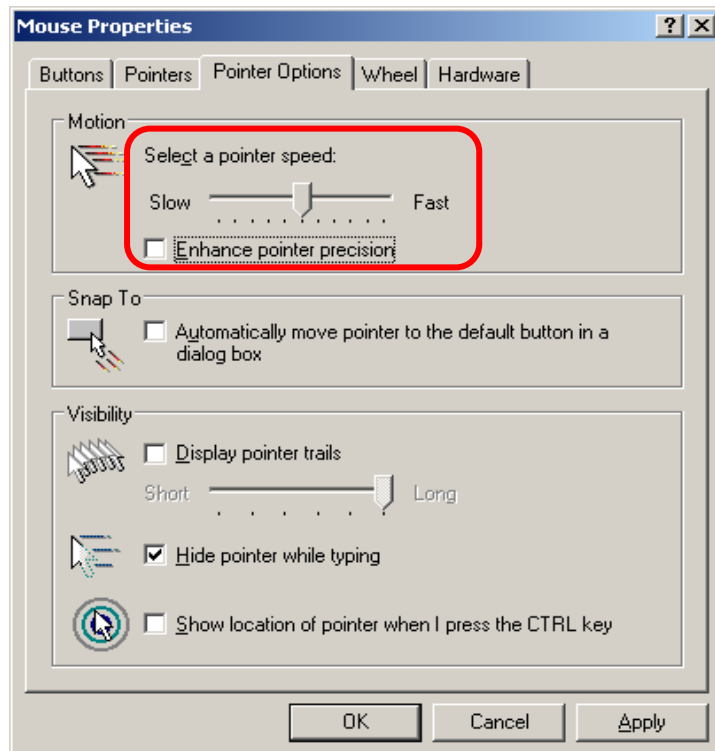
Running the initialize Remote Management Card resets the AC LINK setting (Server-AC LINK) of the BIOS setup to the initial value “Last State.” If you have changed the value, you will need to set it again.

Changing a Mouse Property

Uncheck “Enhance pointer precision” when you use Windows Server 2003 on this server.

Go to [Control Panel] – [Mouse Properties] and select [Pointer Options] tab.

If it is unable to move a mouse cursor on the Remote KVM console, adjust “Select a pointer speed:” to the right on the “Faster” side.



Setting a Management PC

The following provides management PC considerations to connect the server and a management PC.

Setting Your Browser

Configure the following.

- Enable SSL.

Supported browsers

The following browsers are supported.

- Microsoft Internet Explorer 6.0
- Netscape 7.0
- Mozilla 1.6

Java2 Runtime Environment

Java2 Runtime Environment, Standard Edition 1.4.2_16 and later, or Java Runtime Environment (JRE) 5.0 Update 15 and later are required.

Follow the steps below if you use EXPRESSBUILDER for installation:

- When the OS of the management PC is Windows:
 - (1) Activate Windows on the PC on which you want to install Java2 Runtime Environment and set the “EXPRESSBUILDER” DVD.
 - (2) By the auto startup function, the master control menu of EXPRESSBUILDER appears. Click “Software Setup” and then “NEC DianaScope,” and then run the installer of JRE, which you find in the NEC DianaScope install menu.

- When the OS of the management PC is Linux:

The JRE installer (Linux) is stored in the following directory of the EXPRESSBUILDER DVD:

`/dianascope/jre_x`

For installing JRE, log on as root user or obtain the root authority by the su command.

- (1) Copy the JRE installer to any directory. Below is an example of copying the installer from the EXPRESSBUILDER to `/user/local/bin`:

```
cp /mnt/cdrom/dianascope/jre_x/j2re-1_4_2_09-linux-i586.rpm.bin/usr/
local/bin
```

- (2) Go to the directory where you copied the JRE installer. Below is an example that the installer was copied to `/user/local/bin`:

```
cd /user/local/bin
```

- (3) Extract the JRE installer.

```
./j2re-1_4_2_09-linux-i586.rpm.bin
```

- (4) Install JRE. JRE will be installed in the directory of each JRE version under `/usr/java`.

```
rpm -ivh ./j2re-1_4_2_09-linux-i586.rpm
```

- (5) Add an environment variable “JAVA_HOME.” Enter the directory name that you installed JRE.

For bash:

```
export JAVA_HOME=/usr/java/j2re1.4.2_09
```

For tcsh:

```
setenv JAVA_HOME=/usr/java/j2re1.4.2_09
```

- (6) Set the path to JRE.

For bash:

```
export PATH=$JAVA_HOME/bin:$PATH
```

For tcsh:

```
setenv PATH $JAVA_HOME/bin:$PATH
```

IMPORTANT:

For the Mozilla browser, create a symbolic link to the Java Plug-in in the Mozilla plugins directory.

- * If you want to install the latest Java Runtime, download it from the following site. If you use NEC DianaScope on the same management PC, use Java2 Runtime Environment, which you can find in the “EXPRESSBUILDER” DVD.

<http://java.sun.com/j2se/>

If you access the logon page without installing Java2 Runtime Environment, the following message may appear. Check the message and perform installation.



Using Remote Management

Overview

You can control power of this server and use the remote KVM console from a web browser by using web server functions of BMC.

IMPORTANT:

Remote KVM console is available only on the LAN port of the primary CPU/IO module (the operating side's CPU/IO module). This is not available on the LAN port of the secondary CPU/IO module (the waiting side's CPU/IO module).

This function is achieved by Java Applet.

How to get connected

From a Web browser on the management PC, access the following URL.

URL: http://BMC_HostPort/index.htm

TIPS:

“BMC_HostPort” is a BMC IP address or host name followed by a colon and http port number. If the http port number is 80 (the default value), you can omit the port number.

When connecting to network which supports DHCP protocol:

The default host name of BMC is ARMC characters followed by the MAC address if you use DHCP functions and automatically register it with your DNS server.

IP Address	: 192.168.1.1
User Name	: administrator
Password	: (None)
Host Name	: ARMCXXXXXXXXXXXX

Default host

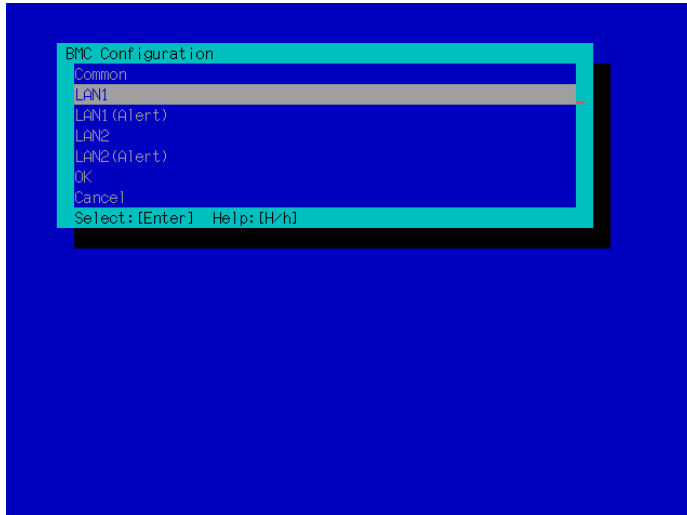
When connecting to network which does not support DHCP protocol:

- (1) The default IP address of the LAN of the managed server is “192.168.1.1” for both CPU/IP module #0 and #1. If you want to access the network that does not support DHCP protocol, access the network that the default IP address can use, and then set the IP address according to your network environment from the managing PC (see “BMC Configuration”).

- (2) If you cannot use the default IP “192.168.1.1,” start up the “EXPRESSBUILDER” DVD on the server and select [Tool menu] → [English] → [System Management] → [Set System Management Parameters] → [Configuration]. Select [New] to register new settings, or [Change] to change the settings. Then, set IP addresses of the managed LAN ports on the [BMC Configuration] menu.

LAN1: CPU/IO Module#0 management LAN port

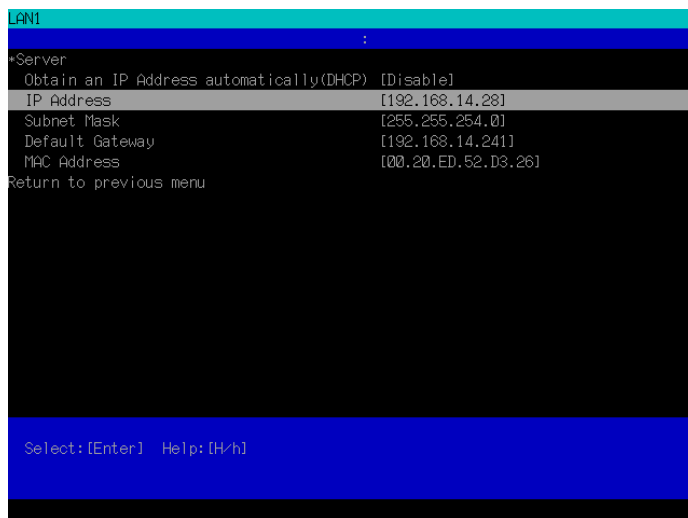
LAN2: CPU/IO Module#1 management LAN port



The following is a configuration screen for LAN1 (CPU/IO module #0). Specify an IP address to use. Make settings for LAN2 (CPU/IO module #1) in the same manner.

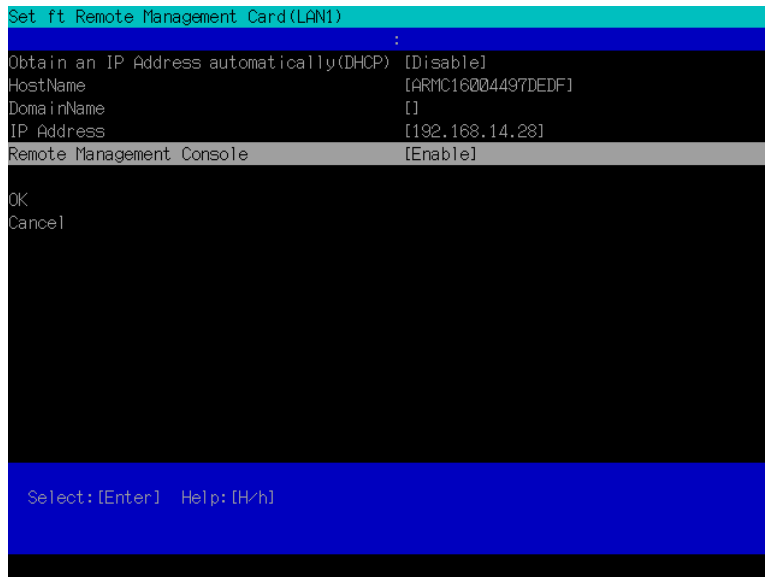
For the settings to take effect, you need to execute [OK] on the previous menu, “BMC Configuration” window.

Specify different IP addresses to LAN1 (CPU/IO module #0) and LAN2 (CPU/IO module #1).

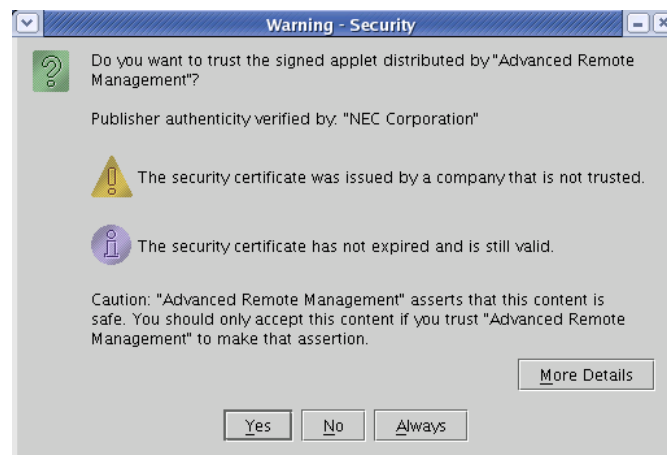


TIPS:

To disable the remote management console function, make the following settings from the EXPRESSBUILDER DVD. Load the EXPRESSBUILDER DVD on the server, and from the main menu, select [Tool menu] - [English] - [System Management] - [Set FT Remote Management Card (LAN1/LAN2)]. Select [Disable] on [Remote Management Console] and register the setting. “Obtain an IP address automatically (DHCP)” “HostName”, “DomainName” and “IP Address” are display only. The image below shows the setting screen for LAN1 (CPU/IO module #0).



If you use remote management for the first time, the “Warning - Security” dialogue box as shown below may be displayed. Check the message, and then click [Yes], or [Always]. Then you will see the logon page. If you are not sure, click [No].

**TIPS:**

If you use SSL for access, the “Warning - Security” dialogue box(es) for server certification may be displayed for SSL in addition to the dialogue box shown above.

Login and logout

Login

When the login page appears, enter the user name and password, and then click [Login].

When you login for the first time, use the following default user name and password.

Default user name: administrator

Default password: None (enter no data)

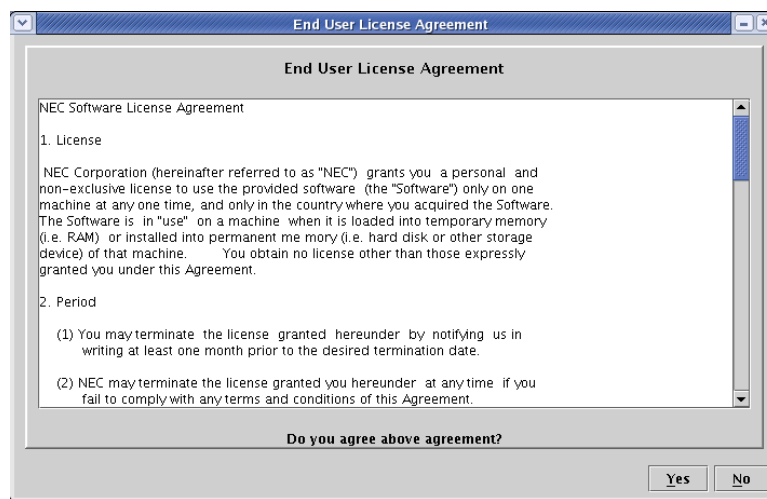
IMPORTANT:

By default, no password is set. Set your password immediately after logging on.

For security, it is recommended to change the default user name as well.

For information on settings and modification, see “BMC Configuration” described later.

When the password is authenticated, the following end user license agreement is displayed.



Read the agreement carefully.

If you can agree, click [Yes], and you can start using remote management functions.

If you cannot agree, click [No]. You cannot use remote management functions.

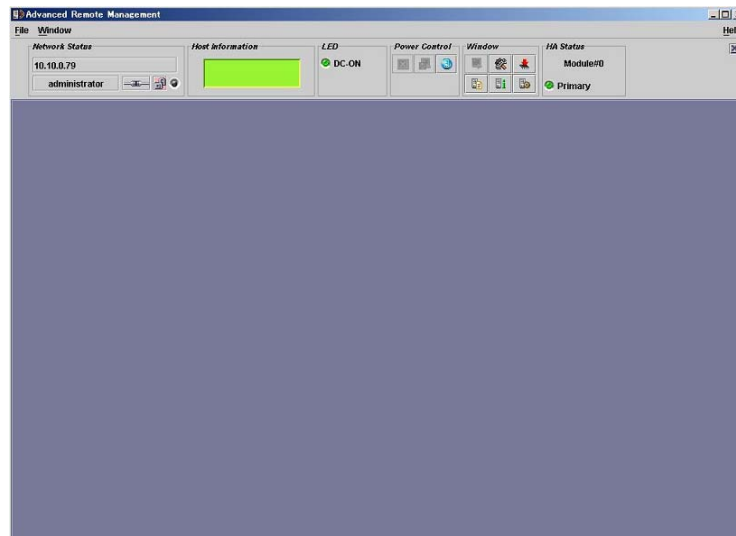
TIPS:

If you click [Yes], you do not see this message again because the data will be stored on the management PC.

Logout

Click the File menu and select Exit to logout. When you log out, the main window closes and you will return to the login page on the browser.

Main Window



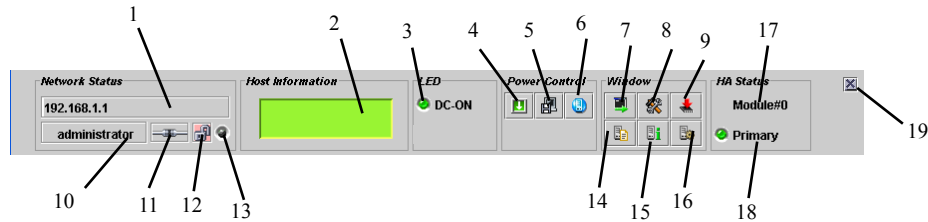
- (1) Click this to show the File menu.
Click “Exit” to quit this applet.
- (2) Click this to show the Window menu.
From the Window menu, you can open windows including the KVM console window.
- (3) Main frame
A window is shown here.
- (4) Click this to show the Help menu.
Click “Help” to see the version information of this applet.

Control panel

The control panel allows you to see the server status and to control the power supply.

The control panel also allows you to activate windows.

Control panel functions



- (1) Displays the BMC host name or IP address
- (2) Displays the LCD of the server.
- (3) The power lamp of the server telling you of the power status
- (4) The same as pressing the POWER switch of the server. Note that the forced power off , pressing the power button for 4 seconds and more, is not supported.
- (5) Performs memory dump on the server (the same as pressing the DUMP switch of the server).
- (6) Makes the Unit ID lamp of the server blink
- (7) Starts up the remote KVM console.
- (8) Starts up the BMC configuration.
- (9) Stats up the firmware update.
- (10) A user name is displayed here.
- (11) Displays the connectivity with BMC.
- (12) Displays communication security status
- (13) Displays network access status
- (14) Opens the window showing system event logs (SEL).
- (15) Opens the window showing the sensor device information (SDR).
- (16) Opens the window showing the information on parts to be replaced for maintenance (FRU).
- (17) Displays the slot position information (module #0 or module #1)
- (18) Displays the slot status (primary or secondary).
- (19) Hides the control panel

Remote KVM Console

Remote KVM console functions of the BMC allow you to transfer a local console to the browser on the management PC over a network.

You can make full access to the server from the management PC using video, keyboard and mouse.

CHECK:

- The remote KVM console supports the following five resolutions:
 - 1024 x 768
 - 800 x 600
 - 640 x 480
 - 720 x 400
 - 720 x 350
 - Set the resolution of the device to one of these values. If any value other than these values, nothing will be shown on the remote KVM console.
 - The mouse cannot be used on the remote KVM console on the operation window of EXPRESSBUILDER.
-

TIPS:

KVM is an acronym for keyboard, video and mouse.


The remote KVM control is different from those using a serial console remotely in that it allows you using graphics directly and remotely.

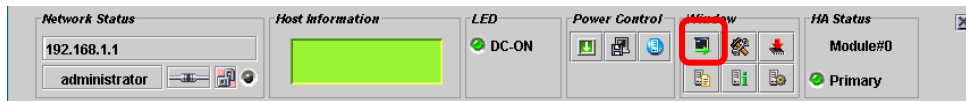
CHECK:

You cannot use the remote KVM remote control for connection via proxy.

When you use the remote KVM console logon with the settings where no proxy is used.

Starting up the remote KVM console window

Click the startup icon [] on the remote KVM console on the control panel to display the KVM console window.



IMPORTANT:

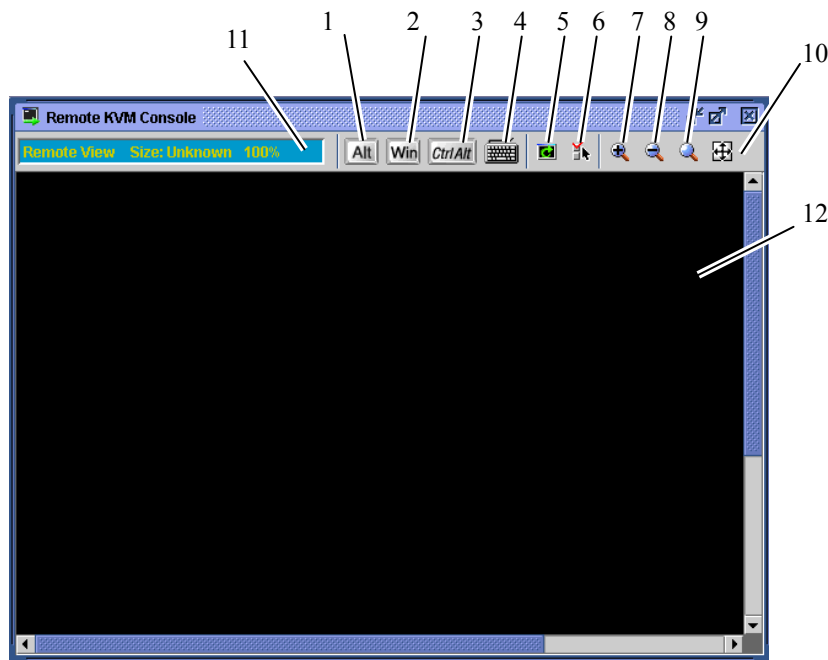
NEVER open the remote KVM console when you log on to the BMC from a local console.

If you do so, data entry from the keyboard or mouse becomes disabled.

CHECK:

You cannot use the KVM console on the secondary side. Use it on the primary side.

Items on the remote KVM console window



- (1), (2) and (3) are special icons. Use them when you want to operate special keys.
- (4) Virtual keyboard icon: use this icon when you want to enter a special key other than those mentioned above.
- (5) Screen refresh icon: use this icon to refresh the window.
- (6) KVM properties icon.
- (7) Enlarge icon: use this icon to enlarge the view.
- (8) Shrink icon: use this icon to reduce the view.
- (9) Equal size icon: use this icon to display images in the same magnification.
- (10) Window size icon: use this icon to adjust the window size to the screen size.
- (11) KVM indicator showing information including resolution.

(12) Remote KVM console screen, on which the server screen is shown.

IMPORTANT:

When you operate **Shift + Caps Lock** or **Num Lock** on the remote KVM console window, such action may not be reflected in the **Shift + Caps Lock** or **Num Lock** status of the management PC LED. Likewise, on the server, the Caps Lock or Num Lock status may become different from LED status after the remote KVM console is used. If this happens, press the key(s) on the device in issue so that LED status and actual operation match.

Operating special keys

Operation of special keys from the keyboard of the management PC is not reflected in the server. Click the following special key icons for operation on the host server.



(raised)



(pressed): the status change every time you click the icon.



(raised)



(pressed): the status change every time you click the icon.


IMPORTANT:

For example, if you want to enter “**Ctrl + Alt + Del**,” click the [Ctrl] and [Alt] icons and then press the **Del** key on the keyboard. By doing so “**Ctrl + Alt + Del**” is sent to the server. After the operation, click the [Ctrl] and [Alt] icons to cancel the special key operation.



(Windows key icon)

Virtual keyboard


When you click the virtual keyboard icon [], the virtual keyboard appears.





You can select either 104 or 109 keyboard from the tab.


By clicking buttons corresponding to each key, you can make entry to the host server.

Zoom-in and zoom-out of the view


Click the [] icon to zoom in the view.

Click the [] icon to zoom out the view.


Click the [] icon to display the screen in the same size as the device.

Click the window resize icon [] to adjust the remote KVM console window size to the remote screen size.

Refreshing the screen

Click the screen refresh icon [] to refresh the remote KVM console screen. If the screen is distorted, refresh the screen.

Modifying properties

When you click the KVM properties icon [], the KVM properties window appears, in which you can specify an interval between screen refreshes.

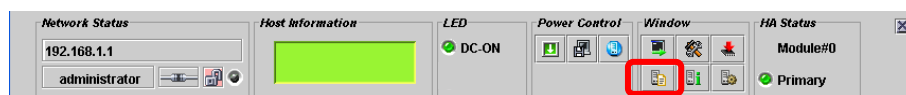
IMPORTANT:


A shorter interval will reduce garbage remaining on the screen. However, note that a shorter interval can slow down the terminal response speed or impact network traffic.

IPMI information


System event logs (SEL), sensor data record (SDR), or field replacement unit (FRU) can be displayed. Such information is referred to as the IPMI information. The information is used to examine errors and events on the server and identify which part should be replaced.

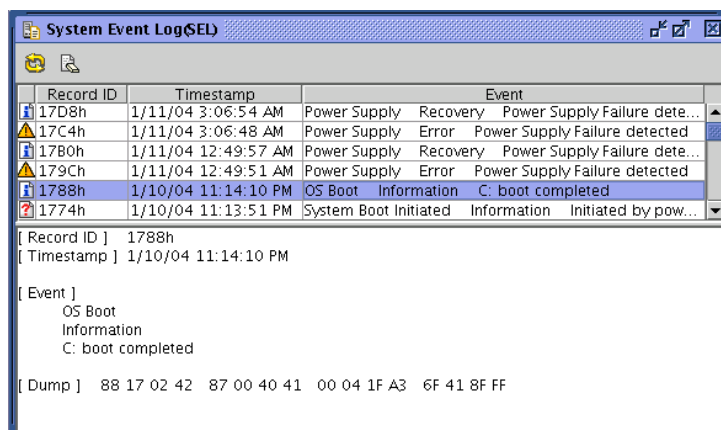
System Event Log (SEL)




When you click the icon to start up system event logs [] on the control panel, SEL information is collected from the BMC and shown on the system event log (SEL) window as shown below.

The upper pane shows a list of system event logs while the lower pane shows details of the entry selected in the list.

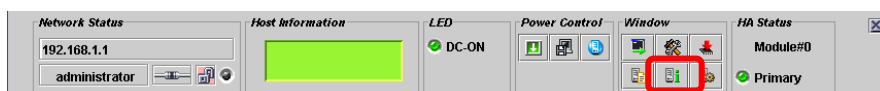
By clicking the reloading icon [], you can reload the SEL information from the BMC and display the latest information.




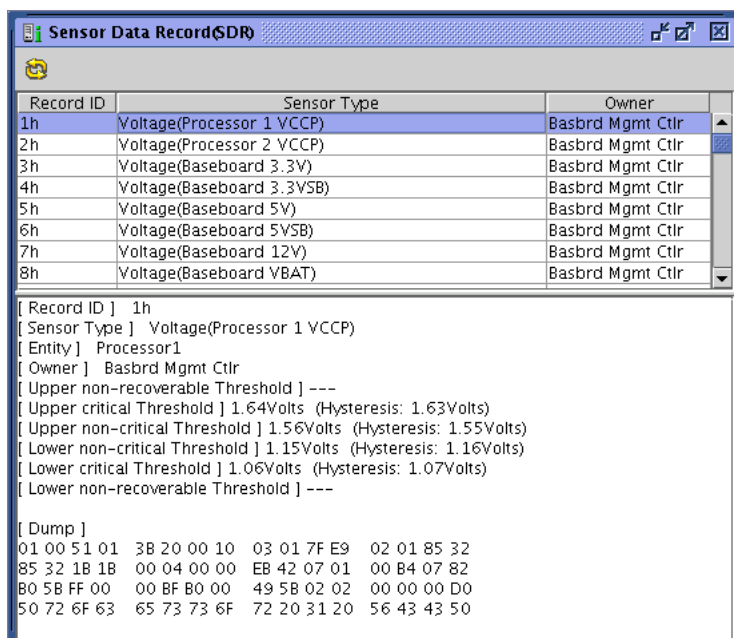
Clearing the SEL information

By clicking the SEL clear icon [], you can clear the SEL information on the BMC. As a message for confirmation appears, click [Yes] if it is OK to clear the information. If you click [No], the SEL information will not be cleared.

Sensor Data Record (SDR)



When you click the icon to start up sensor device information (SDR) [] on the control panel, the SDR information is collected from the BMC and shown on the sensor device information (SDR) window as shown below.



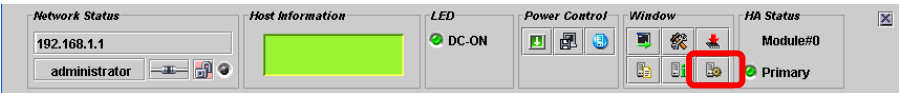
The upper pane shows a list while the lower pane shows details of the entry selected in the list.


TIPS:

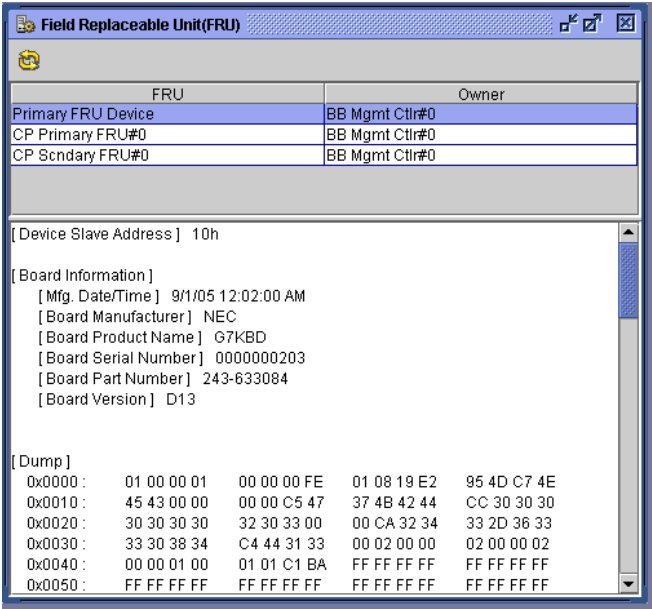
SDR information is definition data on device sensors.

The BMC monitors sensors according to this information.

Field Replaceable Unit (FRU)



When you click the icon to start up information on parts to be replaced for maintenance (FRU) [] on the control panel, FRU information is collected from the BMC and shown on the window for parts to be replaced for maintenance (FRU) as shown below.

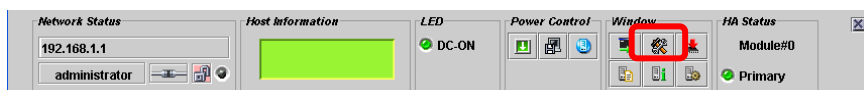



The upper pane shows a list while the lower pane shows details of the entry selected in the list.

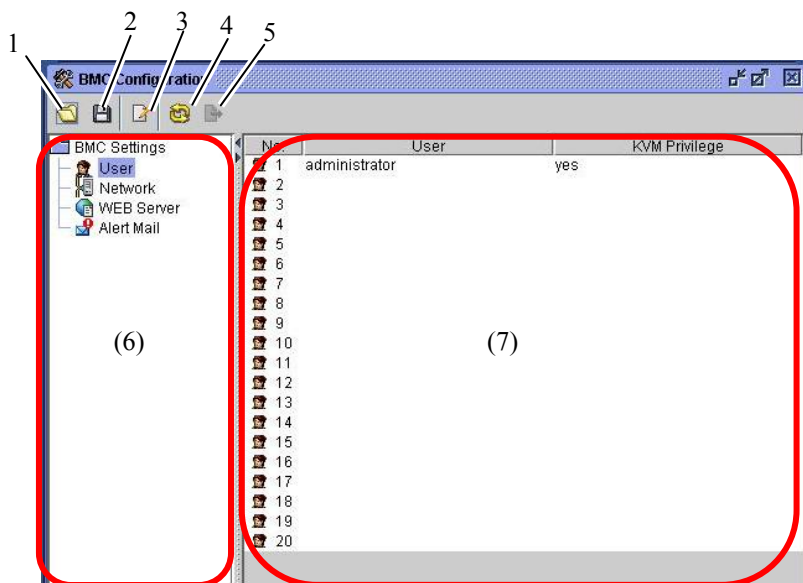
BMC Configuration

You can configure the BMC settings.

Starting up the BMC Configuration window



When you click the icon to start up the BMC configuration [] on Control Panel, the BMC configuration window appears as shown below.



- (1) Reads the BMC configuration file
- (2) Saves the BMC configuration file
- (3) Edits the BMC configuration
- (4) Reloads the BMC configuration
- (5) Sets the data loaded from the file to the BMC in a batch
- (6) Lets you select what to be configured
- (7) Shows the overall information on the current values

TIPS:

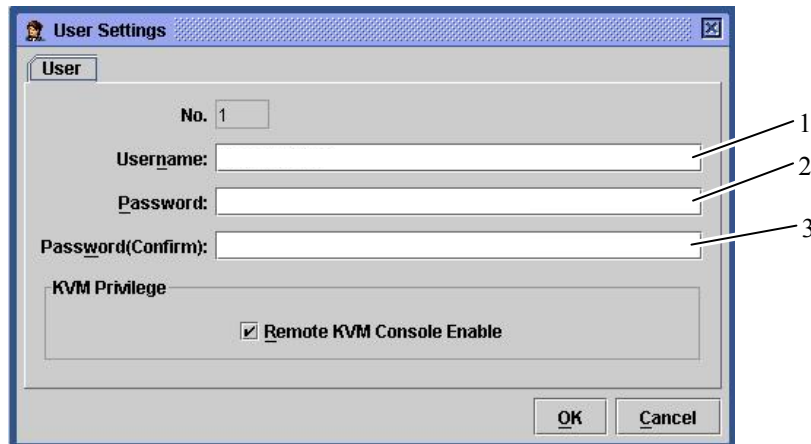
When you load configuration from the file, choose to make settings of the BMC in a batch.

User Settings

Here you can make user account settings.

When you click [User] on the left pane of the BMC configuration window, total of 20 accounts appear in the right pane.

When you select the account you want to modify or add and click the icon for editing [📄], the following window for editing a user account appears.



The image shows a 'User Settings' dialog box with a blue title bar and a close button. It contains a 'User' tab, a 'No.' field with the value '1', and three text input fields labeled 'Username:', 'Password:', and 'Password(Confirm):'. To the right of these fields are three numbered arrows: '1' points to the 'Username' field, '2' points to the 'Password' field, and '3' points to the 'Password(Confirm)' field. Below these fields is a 'KVM Privilege' section with a checked checkbox labeled 'Remote KVM Console Enable'. At the bottom are 'OK' and 'Cancel' buttons.

- (1) Enter the user name.
- (2) Enter the password.
- (3) You can specify whether or not to enable the remote KVM console. Select the check box if you want to enable it.

When you click [OK], all the information you have edited will be written into the BMC.

When you click [Cancel], the window closes without saving what you have edited.

Network Settings

Here you can make network settings of BMC such as IP address configuration.

IMPORTANT:

- The following ports are used for the remote management functions. If your network environment has any firewall, you also need to have configuration for the firewall.

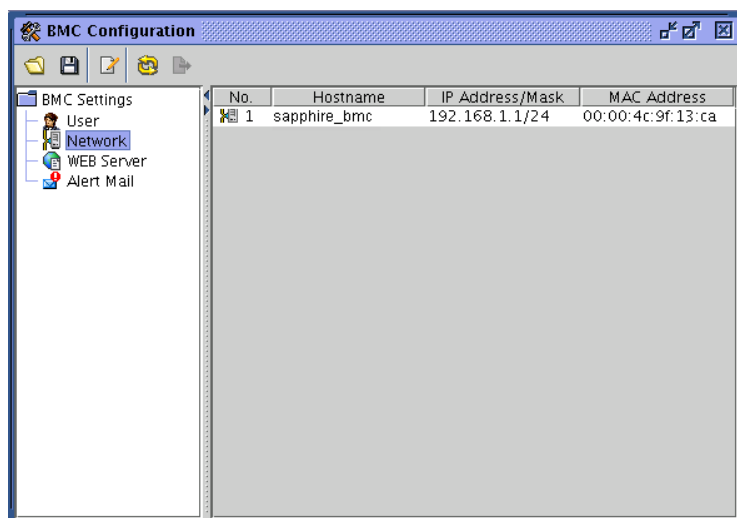
Module name	Port number	Protocol	Direction	Module name	Port number
Remote KVM client	Not determined	UDP	← →	BMC	623
Mail server	25(*1)	TCP	← →	BMC	Not determined
WEB client	Not determined	TCP	← →	BMC	80(*2)
WEB client (SSL)	Not determined	TCP	← →	BMC	443(*3)


*1: Can be modified by selecting [BMC Settings] - [Alert Mail] - [E-Mail Alert Settings] - [SMTP] - [SMTP Port Number].

*2: Can be modified by selecting [BMC Settings] - [WEB Server] - [WEB Server Settings] - [HTTP Port Number].

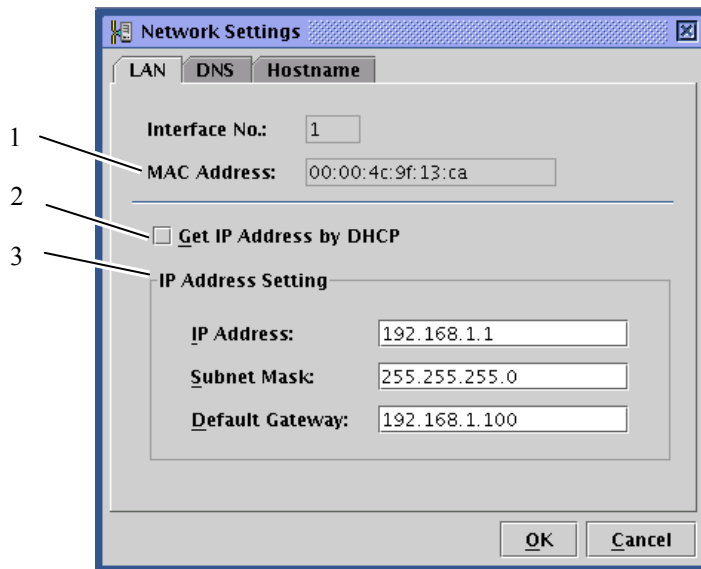
*3: Can be modified by selecting [BMC Settings] - [WEB Server] - [WEB Server Settings] - [SSL Port Number].

When you click [Network] on the left pane of the BMC configuration window, the right pane shows the overall information of the network settings as shown below.



When you click the icon for editing [], the following window for editing appears. The window for network settings has three tabs.

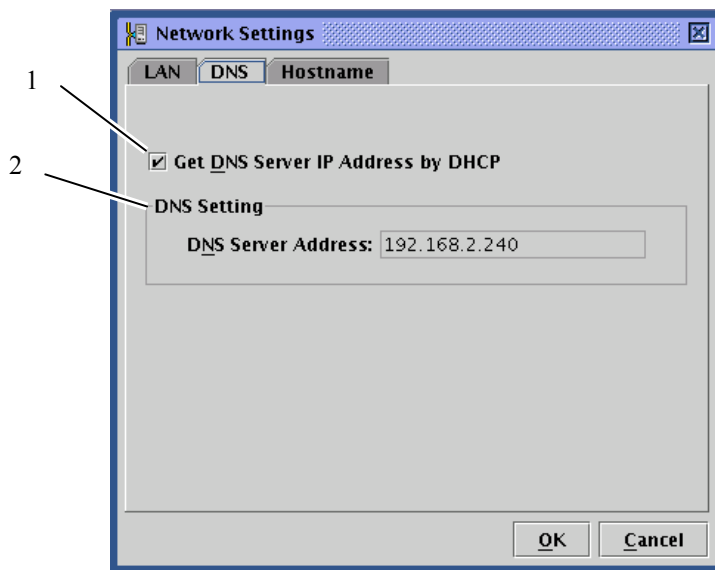
LAN



- (1) The MAC address of the BMC
- (2) Allows you to choose whether or not to acquire an IP address automatically by DHCP.
- (3) Allows you make the IP address settings if the address is not acquired automatically by DHCP. If the address is acquired automatically by DHCP, the data acquired is shown here.

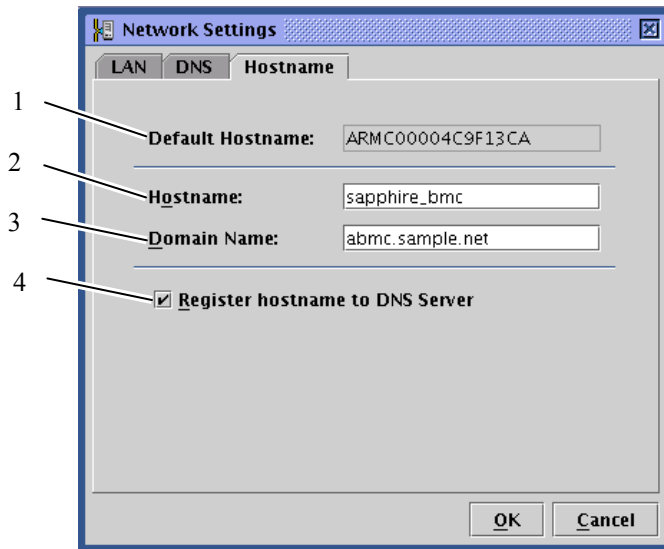
IMPORTANT:

- Specify different IP addresses to CPU/IO module #0 and CPU/IO module #1.
- If you change the IP address, the current connection will be disconnected when the BMC settings are completed by clicking OK. Close the window once, and then log on again by entering the newly set IP address (or host name) in the browser.
- The logon page remaining on the browser is the page you accessed by using the old address. You cannot use it to log on.
- When you configure “default gateway,” the gateway, the server, the management PC should be in a state where communication over network is available.
- If you make the settings in a state where communication is not available, you need to switch on/off the AC of the server in a state where the gateway, the server and the management PC can be communicated over the network.
- After you changed the DHCP setting, you should turn off the AC power of the system and turn on it after 5 seconds or more.
After you changed the DHCP setting using EXPRESSBUILDER and NEC DianaScope Agent, you should turn off the AC power of the system and turn on it after 5 seconds or more..

DNS

- (1) Allows you to select whether or not to automatically acquire the IP address of the DNS server by DHCP.
- (2) If you have selected not to automatically acquire the IP address by DHCP, make settings here. If the address is acquired automatically by DHCP, the acquired address appears here.

Host name



- (1) The default host name to be used when no host name is set when DHCP is used
- (2) Set the BMC host name. If this option is not configured, the default host name mentioned in 1) will be used.
- (3) Set the domain name of the network to which the BMC belongs.
- (4) Choose whether or not to register the host name with the DNS server.

TIPS:

It is recommended to set the BMC host name to be easily guessed from the server's host name on the OS.
For example, you may set the BMC host name as "sapphire_bmc" if the server's host name on the OS is "sapphire."

IMPORTANT:

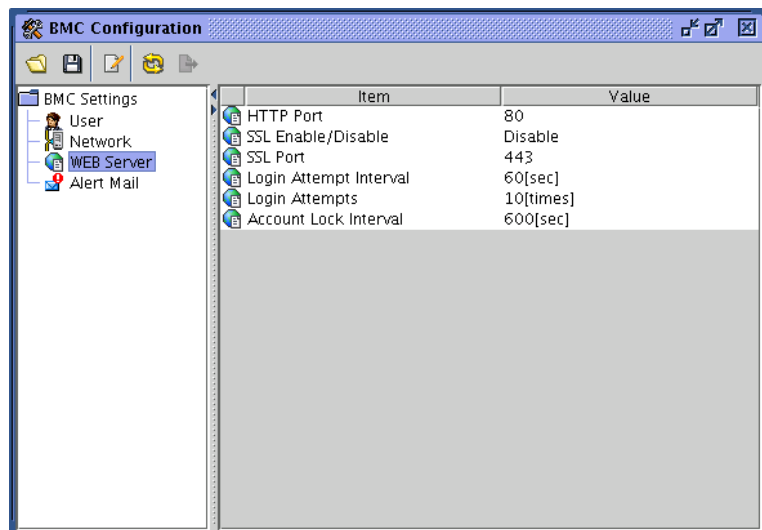
Specify different host names to CPU/IO module #0 and CPU/IO module #1.

When you click [OK], all of what you have set in the three tabs will be written into the BMC.
When you click [Cancel], the editing window closes without saving what you have edited.

WEB server settings


Here you can make web server settings such as HTTP port settings for the BMC.

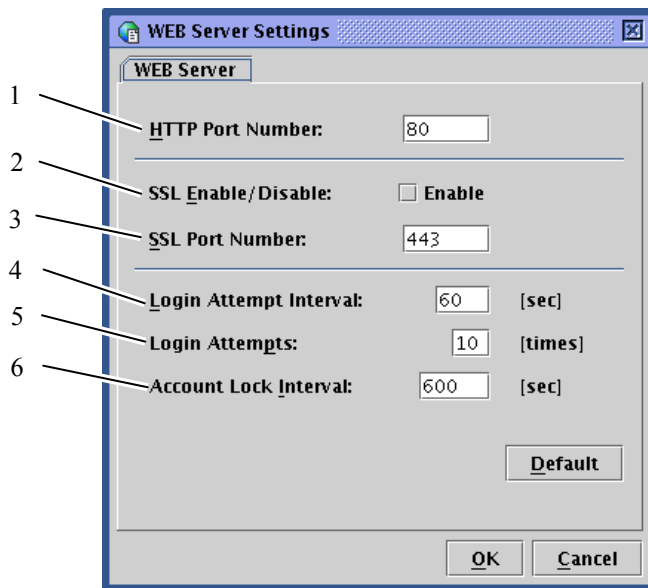
When you click [Web Server] on the left pane of the BMC configuration window, the right pane shows the overall information of the web server settings.



IMPORTANT:

- When you change the HTTP port number, settings of SSL (enable/disable), or SSL port number, the current connection will be temporarily disconnected. Close the window and exit, and then log on again by entering the newly set port number in the browser.
- The logon page remaining on the browser is the page you accessed by using old web server settings. You cannot use it to log on.

When you click the icon for editing [], the window for editing appears as shown below.



- (1) Specify the HTTP port number.
- (2) Specify whether or not to enable SSL communication. If you select the check box for enabling, connection by HTTPS (SSL enabled) is enabled. Clear the check box if you want to disable SSL.

TIPS:

It is recommended to use connection by the encrypted HTTPS protocol unless you have any specific reason such as SSL cannot be used. This option is disabled by default.

- (3) Specify the SSL port number.
- (4) Specify the logon trial period during which you can try logging on again if you have failed to log on.
- (5) Specify the number of logon retries. If the number of retries exceeds the number specified here during the period specified in (4), logon retries will be rejected for the time period specified in (6).
- (6) Specify the time period during which logon is rejected.

TIPS:

Although the three entries mentioned above are effective in blocking automatic and unauthorized logins, they do not completely block such logins.

If you click [Default], the default values for HTTP port number, SSL port number, logon trial period, number of logon retries and the account lock period are displayed. The SSL check box configuration remains the same.

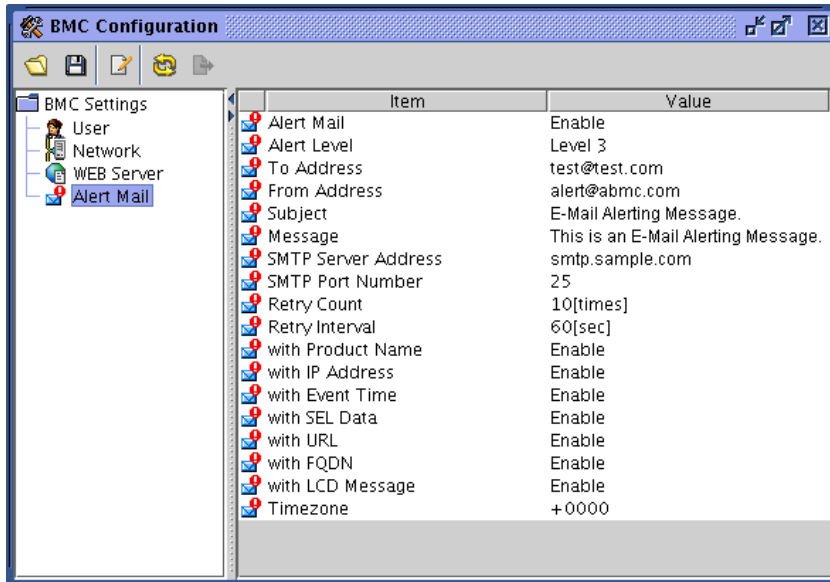
When you click [OK], all of what you have set will be written into the BMC.


When you click [Cancel], the editing window closes without saving what you have edited.

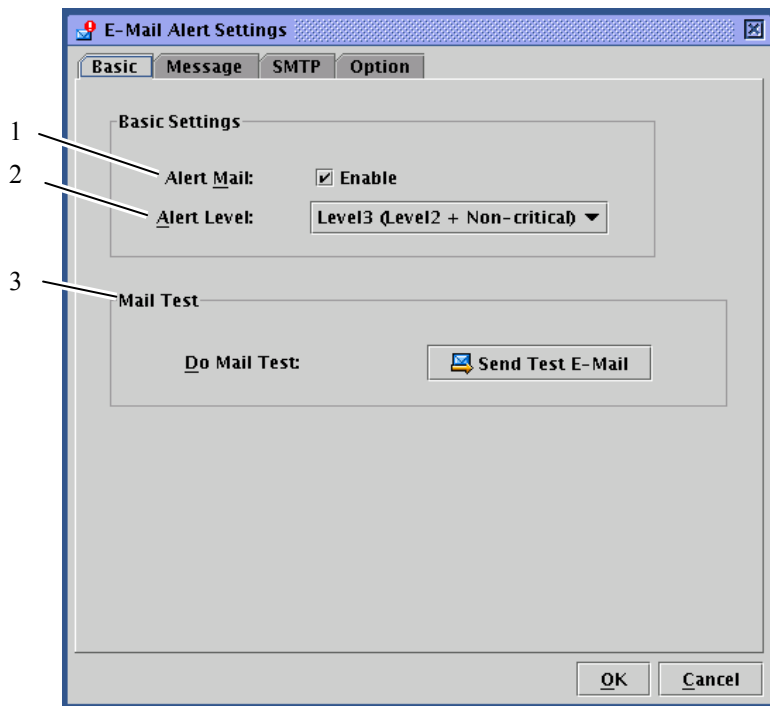
Alert Mail Configuration

This allows you to make alert mail settings for BMC.

When you click [Alert Mail] on the left pane of the BMC configuration window, the right pane shows the summary of the alert mail settings.



When you click the icon for editing [], the window for editing appears as shown in the next page. The window for editing has four tabs: basic, message, SMTP and option. The following describes each tab in detail.

Basic

- (1) Specify whether or not to enable the alert mail functions by the check box. When you select the check box, you can make mail-related settings.
- (2) Select a notice level from six levels. Levels are categorized according to severity of factor events.
- (3) Allows you to send a test mail.

IMPORTANT:

Perform the mail test after you have completely configured “E-Mail Alert Settings” described in the following pages.

Making entries in the editing window does not complete settings. You need to click [OK] after entering all the required information to complete the BMC settings.

TIPS:

The X-Priority: field in the mail header changes according to the severity of factoring event.

Non-recoverable/Critical	X-Priority: 1
Non-critical	X-Priority: 3
OK/Information/Monitoring	X-Priority: 5

Message

E-Mail Alert Settings

Basic **Message** **SMTP** **Option**

Message Settings

To: test@test.com
demo@demo.net

From: alert@abmc.com

Subject: E-Mail Alerting Message.

☒ **Message:**

This is an E-Mail Alerting Message.
For more information, click the URL below.

Get Default Message

OK Cancel

- (1) Specify mail address of receivers to whom alert mail is sent. You can specify up to four addresses.
- (2) Specify the sender's address used in alert mail.
- (3) Enter the subject to be given to alert mail.
- (4) Select whether or not to enable the body messages for all alert mail, which is configured in the next step.
- (5) Enter the body message to be used in all alert mail. If you do not need such a body message, clear the check box of (4). If you click [Get Default Message], the recommended message appears.

TIPS:

The subject and message you configure here will be used in all alert mails.

SMTP

E-Mail Alert Settings

Basic Message **SMTP** Option

SMTP Settings

1 SMTP Server Address: smtp.sample.com

2 SMTP Port Number: 25

3 Retry Count: 3 [times]

4 Retry Interval: 60 [sec]

Default

OK Cancel

- (1) Specify the address of the SMTP server. You can enter the IP address or host name.
- (2) Specify the port number of the SMTP server.
- (3) Specify the number of send retry if sending a mail has failed.
- (4) Specify the time in seconds before the next mail send retry.

If you click [Default], the default values for SMTP port number, number of retries, and retry interval appears. It is recommended to use the default values unless you have specific reasons.

IMPORTANT:

This card does not support SMTP authentication (SMTP-AUTH).

Option

E-Mail Alert Settings

Basic Message SMTP **Option**

Mail Attached Information

☒ Product Name ☒ BMC URL

☒ IP Address ☒ BMC FQDN

☒ Event Time ☒ LCD Message

☒ SEL Dump Data ☒ BMC FW Rev.

Misc Settings

Time Zone: +0000

OK Cancel

- (1) Specify information to add to the body of alert mail.

The information you specify here will be contained in the body of alert mail with the message you specified in the message box in the message tab.

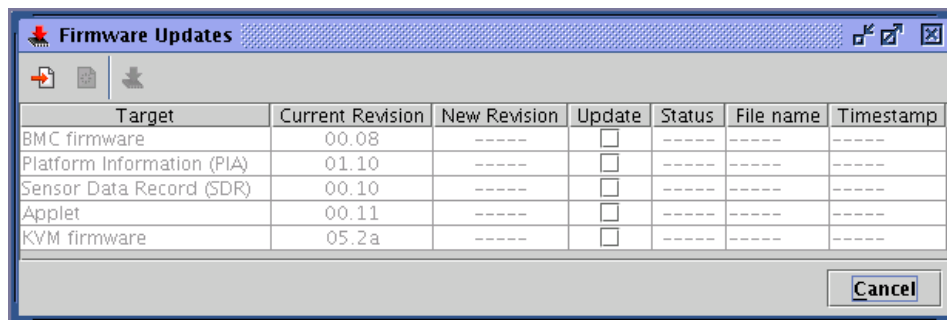
Product Information	Product name, code, number of the server
IP Address	IP address of the BMC
Event Time	Time that the event occurred
SEL Dump Data	Data representing system event logs (SEL) in the hexadecimal format
BMC URL	URL of the ARMC logon page
BMC FQDN	Full domain name of the BMC
LCD Message	LDC message on the server at the time of event occurrence
BMC FW Rev.	Revision information of the BMC firmware/SDR/PIA

- (2) Used in the date field of the mail header of alert mail.

Firmware Update

You can update applets, KVM firmware, BMC firmware, sensor device information (SDR), and platform information (PIA).

Starting up the firmware update window




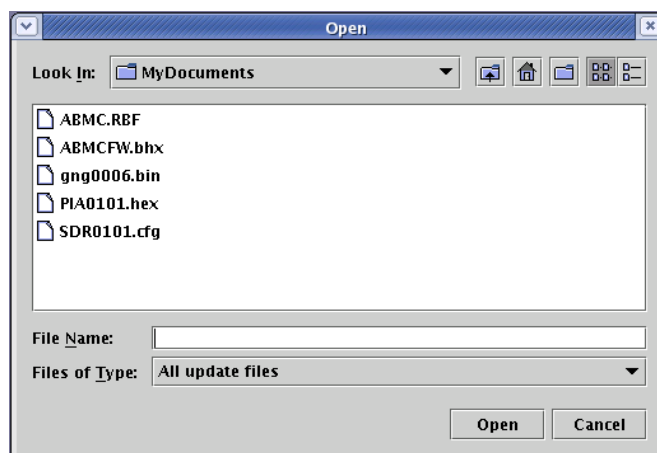
When you click the icon to start up firmware update [] on the control panel, each pieces of revision information is loaded from the BMC to display the following firmware update window.

If you click [Cancel], the firmware update window closes without making any changes.

The following pages provide step-by-step instructions for update.

Loading update data files

When you click the icon for adding update files [], the window to select a file appears.



Specify an update data file.

When you click [Open] after specifying the file, loading of the file begins.

Wait for file loading to complete.

TIPS:

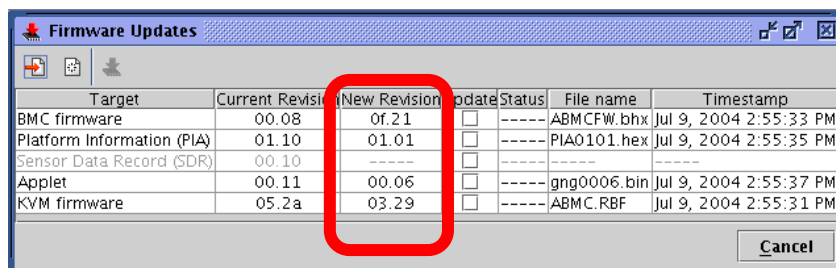
You can update in a batch.

If there are more than one update targets, all the information of the update targets must be loaded. You can select more than one file to be loaded at the same time.

Confirming revision


When loading data files completes, information on current revisions, loaded revisions and file data (file names and time stamps) appears on the window.

Check the information carefully.



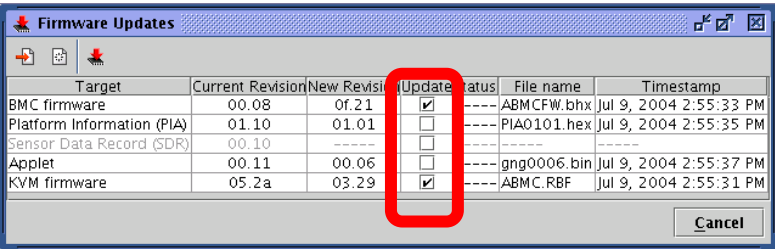
CHECK:

Check each revision carefully because downgrading is possible as well.

If you click the icon for clearing update data [], all loaded data will be discarded. When you click [Cancel], the update window will be closed without saving any loaded data.

Selecting what to be upgraded

Select check boxes of update targets.




CHECK:

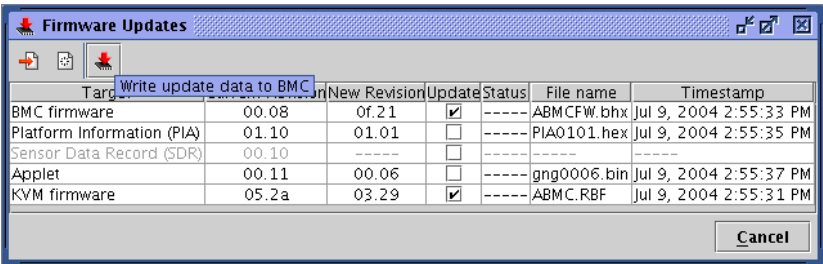
Only those selected here will be written in.
Items with no check box selected will not be written in even if files have been loaded.

IMPORTANT:

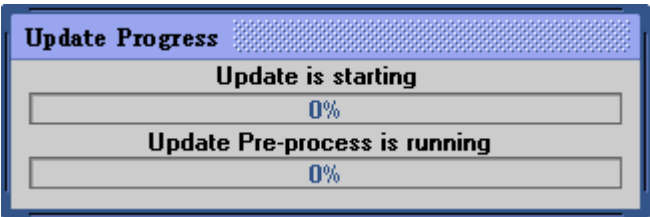
If you update both SDR and PIA, make sure to write in simultaneously. If writing is done twice, the first writing will not take effect.

Writing update data into the BMC

When you click the icon for writing update [], the writing the update data into the BMC begins.



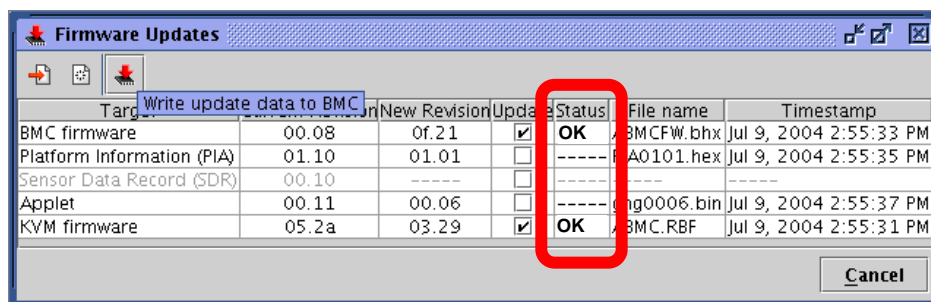
As shown below, the window showing writing process appears for each update target.



If any error is detected during the writing process, an error message is displayed and the process terminates.

End of writing

When writing is completed, the “Status” column displays the result for each target.



CHECK:

- To apply updates for targets other than applet, reboot the server or power off and then on the server.
- When you rebooted or power on the server to apply an update for BMC software, SDR, or PIA, the connection with BMC will be disconnected. Because of this, you need to log in again.
- To apply updates for applets, log out once, close all browsers, and then logon again. You do not need to reboot the server.

Troubleshooting

Error Messages

When using the remote management, an error dialog box may appear on the management PC if some problem occurs. Messages and actions for the errors are described below.

Fatal errors

No.	Error message	Action
1	Fatal error. JavaVM quits.	Try logging in again. If the same message continues to appear, contact your service representative.
2	A fatal software error has occurred.	Try logging in again. If the same message continues to appear, contact your service representative.

Logon error

No.	Error message	Action
1	Authentication error	Check the user name and password, and then enter them again.

Access privilege error

No.	Error message	Action
1	Unauthorized operation. You have no privilege to perform the operation.	Try performing the operation with administrator's privileges. Consult your administrator.

Network errors

No.	Error message	Action
1	The HTTP communication failed.	Check the network environment and try again. Contact your service representative if the error persists. .
2	Could not resolve the IP address.	Check the network environment. You cannot use Remote KVM Console for connections via proxy.
3	Unable to reach the target host.	Check the network environment. You cannot use Remote KVM Console for connections via proxy.
4	The HTTP communication failed.	Check the network environment and try again. Contact your service representative if the error persists. .
5	Failed to download applet.	Check the network environment and try again. Contact your service representative if the error persists.
6	The RMCP+ session is closed.	Check the network environment. If there is no network problem, contact your service representative.
7	Failed to establish the RMCP+ session.	Check the network environment. If there is no network problem, contact your service representative.
8	The RMCP+ transmission failed.	Check the network environment. If there is no network problem, contact your service representative.
9	The specified RMCP+ protocol cannot be used.	Check the network environment. If there is no network problem, contact your service representative.
10	BMC resources to establish a new RMCP+ session are insufficient.	Try again after a connection from other client is finished.

No.	Error message	Action
11	The RMCP+ session time-out occurred.	Check the network environment and server. If you do not find any problem, contact your service representative.

BMC-related error

No.	Error message	Action
1	The IPMI request was aborted.	The network may be busy. Try again. If the error persists, contact your service representative because a failure may have occurred in BMC.
2	Received bad response from BMC.	Check the server. A failure may have occurred in BMC. If you do not find any problem, contact your service representative.
3	BMC does not support IPMI 2.0 functions.	Contact your service representative.
4	Failed to run the IPMI command.	Check the server. A failure may have occurred in BMC. If you do not find any problem, contact your service representative.
5	Failed to send the IPMI message.	Check the network environment. If the network has no problem, contact your service representative.
6	Illegal IPMI message was requested.	Contact your service representative.
7	Specified target is not present.	Check the server. A failure may have occurred in BMC. If you do not find any problem, contact your service representative.

Errors on the Remote KVM Console

No.	Error message	Action
1	Failed to disable Remote KVM Console.	Check the network environment and try again. Contact your service representative if the error persists.
2	Failed to enable Remote KVM Console.	Check the network environment and try again. Contact your service representative if the error persists.
3	KVM packet transmission failed.	Check the network environment and server. If you do not find any problem, contact your service representative.
4	The KVM request was aborted.	This is no problem. Click [OK] and close the message box.
5	UDP packet transmission failed.	Check the network environment and server. If you do not find any problem, contact your service representative.
6	Remote KVM console can not activate because it is disabled	Refer to page 4-58 and enable remote KVM console.
7	Remote KVM Console is used by other client.	Try again after the client using Remote KVM Console finishes using.
8	Failed to shut down Remote KVM Console.	Use Remote KVM Console after waiting 3 or more minutes.
9	Failed to make settings.	Check the network environment and try again. Contact your service representative if the error persists. .
10	The UDP connection is closed.	Check the network environment and server. If you do not find any problem, contact your service representative.

System event log (SEL) display errors

No.	Error message	Action
1	Failed to clear session event logs of BMC.	The network may be busy. Try again. If the error persists, contact your service representative because a failure may have occurred in BMC.
2	Failed to acquire system event logs.	The network may be busy. Try again. If the error persists, contact your service representative because a failure may have occurred in BMC.

Sensor data records (SDR) display error

No.	Error message	Action
1	Failed to acquire sensor data records.	The network may be busy. Try again. If the error persists, contact your service representative because a failure may have occurred in BMC.

Field replaceable (FRU) information display error

No.	Error message	Action
1	Failed to acquire field replaceable units information.	The network may be busy. Try again. If the error persists, contact your service representative because a failure may have occurred in BMC.

BMC configuration errors

No.	Error message	Action
1	Failed to make settings:	Check the network environment and try again. Contact your service representative if the error persists.
2	Failed to acquire BMC Configuration:	Check the network environment and try again. Contact your service representative if the error persists.
3	Used by other software program. Try again after a while.	Try again after a while.
4	Invalid BMC configuration file.	The BMC configuration file may be corrupted. Check the file.
5	The required XML tag is not found.	The BMC configuration file may be corrupted. Check the file.
6	Failed to write the file.	The BMC configuration file is not saved successfully. Change the location to save the file and try again.
7	Invalid user name	You can use only alphanumeric characters, minus sign (–), and underscore (_) for a user name. A user name should be 31 characters or less.
8	The user name is too long	A user name should be 31 characters or less.
9	The password is too long.	Use 16 or less characters.
10	Passwords are not matched.	Enter passwords again.
11	Invalid HTTP port number	You can only use numeric values.
12	Invalid SSL port number	You can only use numeric values.
13	HTTP/SSL should not be the same.	The same port number cannot be specified for HTTP and SSL. Specify different value.
14	Invalid login attempt period	You can only use numeric values.
15	Invalid failed login attempts	You can only use numeric values.
16	Invalid account lock period	You can only use numeric values.
17	Invalid IP address	Use numbers and periods to specify an IP address.
18	Invalid subnet mask	Use numbers and periods to specify a subnet mask.
19	Invalid default gateway	Use numbers and periods to specify a default gateway.
20	Invalid DNS server IP address	Use numbers and periods to specify the IP address of DNS server.
21	Invalid host name	You can use only alphanumeric characters, minus sign (–), and underscore (_) for a host name. A host name should be 64 characters or less.
22	Invalid domain name	You can use only alphanumeric characters, minus sign (–), underscore (_) and period (.) for a domain name. A domain name should be 128 characters or below.
23	The SMTP server address is too long.	Specify the value within 128 characters.

No.	Error message	Action
24	Invalid SMTP port number.	You can only use numeric values.
25	Invalid retry count	You can only use numeric values.
26	Invalid retry interval	You can only use numeric values.
27	"To" is too long.	Specify the value within 128 characters.
28	"From" is too long.	Specify the value within 128 characters.
29	"Subject" is too long.	Specify the value within 256 characters.
30	The message is too long.	The message should be up to 1024 characters.
31	Failed to open the file:	The specified file may not exist. Check the file name.
32	Failed to close the file:	The specified file may be corrupted.
33	Can't open the file:	The specified file may not exist. Check the file name.
34	Timeout has occurred.	Try again. If the error persists, contact your service representative because a failure have occurred in BMC.

Firmware update errors

No.	Error message	Action
1	There are uncompleted update images on BMC as follows:	Reboot the server to complete the update.
2	Failed to acquire status of the update area.	The network may be busy. Try again. If the error persists, contact your service representative because a failure may have occurred in BMC.
3	Update data is too large:	Some update files may be corrupted. Obtain update files again.
4	Failed to prepare update	The network may be busy. Try again. If the error persists, contact your service representative because a failure may have occurred in BMC.
5	Invalid file size:	The update file may be corrupted. Obtain the update file again.
6	Could not find the revision information:	Some update files may be corrupted. Obtain update files again.
7	Failed to create rollback image.	Try again. If the error persists, contact your service representative because a failure may have occurred in BMC.
8	Failed to erase.	Try again. If the error persists, contact your service representative because a failure may have occurred in BMC.
9	Unsupported format version:	Some update files may be corrupted. Obtain update files again.
10	Failed to load the update image file.	Some update files may be corrupted. Obtain update files again.
11	Update has failed.	Try again. If the error persists, contact your service representative because a failure may have occurred in BMC.
12	Could not switch to the update mode.	Try again. If the error persists, contact your service representative because a failure may have occurred in BMC.
13	Could not find the update targets:	Some update files may be corrupted. Obtain update files again.
14	Invalid address:	Some update files may be corrupted. Obtain update files again.
15	Writing has failed.	Try again. If the error persists, contact your service representative because a failure may have occurred in BMC.

No.	Error message	Action
16	Unsupported token is detected:	Some update files may be corrupted. Obtain update files again.
17	Invalid segment information:	Some update files may be corrupted. Obtain update files again.
18	Invalid data length:	Some update files may be corrupted. Obtain update files again.
19	Failed to open the file:	The specified file may not exist. Check the file name.
20	Failed to close the file:	The specified file may be corrupted.
21	Invalid file checksum:	Some update files may be corrupted. Obtain update files again.
22	Failed to parse files.	Some update files may be corrupted. Obtain update files again.
23	Failed to parse files:	Some update files may be corrupted. Obtain update files again.
24	Failed to load files:	Some update files may be corrupted. Obtain update files again.
25	Could not find files:	Some update files may be corrupted. Obtain update files again.
26	Failed to verify	Try again. If the error persists, contact your service representative because a failure may have occurred in BMC.
27	Update will be stopped because interruption has occurred.	Check clients. A software program other than you are using may have interrupted.
28	Online update is now being used.	Try again as necessary after online update performed by other tool is completed.
29	Failed to acquire the current revision.	The network may be busy. Try again. If the error persists, contact your service representative because a failure may have occurred in BMC.
30	Failed to acquire lines:	Some update files may be corrupted. Obtain update files again.
31	Invalid line length:	Some update files may be corrupted. Obtain update files again.
32	Unexpected EOF is detected:	Some update files may be corrupted. Obtain update files again.
33	Unexpected token is detected:	Some update files may be corrupted. Obtain update files again.
34	PIA does not suit this server	It is not Platform Information (PIA) of this server. Obtain update files again.

(This page is intentionally left blank.)

Chapter 5

Installing and Using Utilities

This section describes how to use the EXPRESSBUILDER DVD that comes with your server and to install the utilities stored on the EXPRESSBUILDER. CPU/IO module has a processor function part and IO function part. In utilities in this chapter, the processor function part is referred to as CPU module and IO function part PCI module.

EXPRESSBUILDER

The EXPRESSBUILDER, integrated setup software, can automatically detect the hardware connected to a Fault Tolerant Server series machine to advance the processing. The hardware subject to setup with the EXPRESSBUILDER should have the same configuration as that for operation.

Start Menu

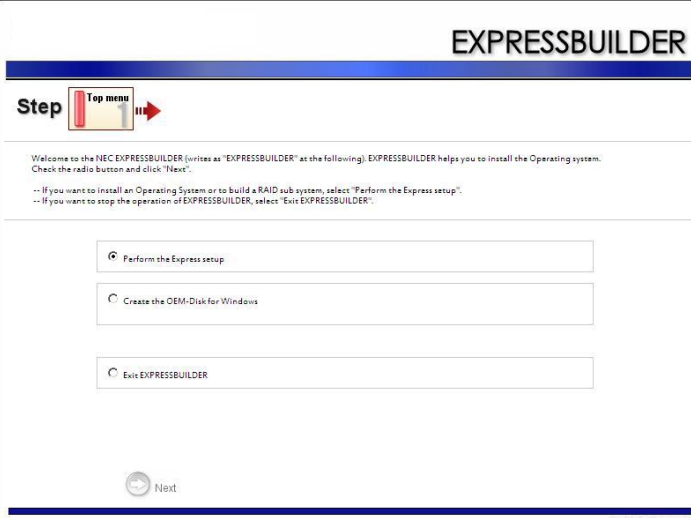
When you insert the EXPRESSBUILDER disk into the optical disk drive and reboot the system, the following menu appears.

BOOT Selection	
OS installation***default***.....	①
Tool menu.....	②

1. OS installation

If you select this item, the Top menu appears.

See “EXPRESSBUILDER Top Menu” for details.



The screenshot shows the EXPRESSBUILDER interface. At the top, the title "EXPRESSBUILDER" is displayed. Below it, a "Step" indicator shows "Top menu" with a red arrow pointing right. The main content area contains a welcome message: "Welcome to the NEC EXPRESSBUILDER (writes as 'EXPRESSBUILDER' as the following). EXPRESSBUILDER helps you to install the Operating system. Check the radio button and click 'Next'." followed by instructions: "-- If you want to install an Operating System or to build a RAID sub system, select 'Perform the Express setup'; -- If you want to stop the operation of EXPRESSBUILDER, select 'Exit EXPRESSBUILDER'". There are three radio button options: "Perform the Express setup" (selected), "Create the OEM-Disk for Windows", and "Exit EXPRESSBUILDER". At the bottom left, there is a "Next" button with a right arrow. The bottom right corner shows the version "Version 5.XX.XXX.XX".

You can start up the OS install function, such as “ExpressSetup” from this menu. See User’s Guide (setup) for details.

2. Tool menu

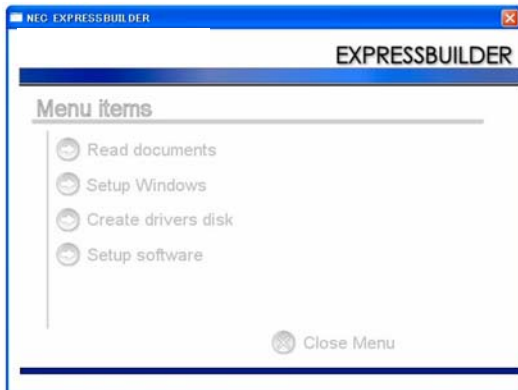
If you select this item after choosing the display language, the Tool menu appears.



You can use the below functions for maintenance.

- Maintenance Utility
Starts up the Offline Maintenance Utility.
- BIOS/FW Updating
Updates the system BIOS.
- ROM-DOS Startup FD
Creates Startup FD is used for starting the ROM-DOS system.
- Test and Diagnostics
Starts up the system test and diagnostics.
- System Management
Starts up the system management function.

Autorun Menu



The Master Control Menu automatically appears when the “EXPRESSBUILDER” DVD is loaded on a computer running Windows (Windows 95 or later or Windows NT 4.0 or later).

TIPS:

Depending on the condition of the system, the menu may not be automatically started. In such a case, execute the file below on the DVD from Windows Explorer or by other means:

`\MC\1ST.exe`

From the Master Control Menu, you can install various software which runs on Windows or view online documents.

TIPS:

Some online documents are provided in the PDF format. Acrobat Reader of Adobe Systems Incorporated is required for viewing such files. If it is not installed, click [Setup] - [Acrobat Reader] and install Acrobat Reader.

To use the Master Control Menu, click items displayed on the window or use the shortcut menu which is displayed by right-clicking.

IMPORTANT:

Before ejecting the DVD, close all online documents and terminate tools started from the Master Control Menu and Menu.

PARAMETER FILE CREATOR

“Parameter File Creator” is a tool to create [Parameter file] that is used for configuring the server with the Express Setup (see Chapter 4 of the User’s Guide (setup) for details).

If you use the Parameter file created by the Express Setup and Parameter File Creator to operate the setup, you can setup from the installation of OS to several utilities automatically except for a few key input to verify the specification. Also, you can install the system with the same specification as before when re-installing the system. We recommend you to create [Parameter file] to setup the servers from EXPRESSBUILDER.

When using a floppy disk, a USB floppy disk drive is required.

IMPORTANT:

You cannot create [Parameter file] for Microsoft Windows Server 2003 x64 Editions..

NOTE:

You can install Windows Server 2003 without [Parameter File]. Also, you can modify/newly create [Parameter File] during the setup with EXPRESSBUILDER.

Parameter File Creator

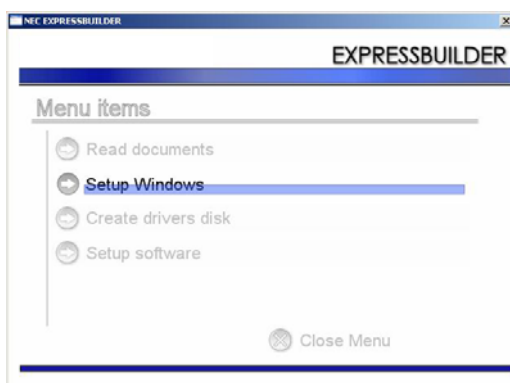
This section describes about specifying setup information that is necessary for OS installation and creating [Parameter file].

Follow the procedure below.

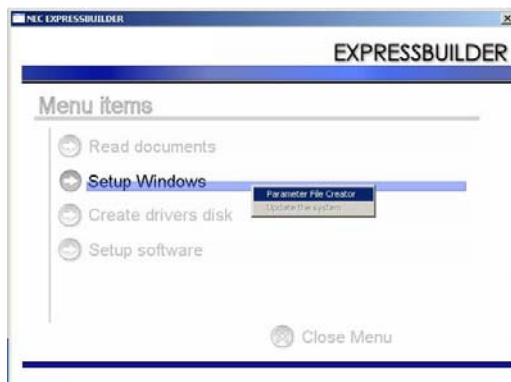
NOTE:

Do not remove EXPRESSBUILDER DVD from drive during a parameter file creation.

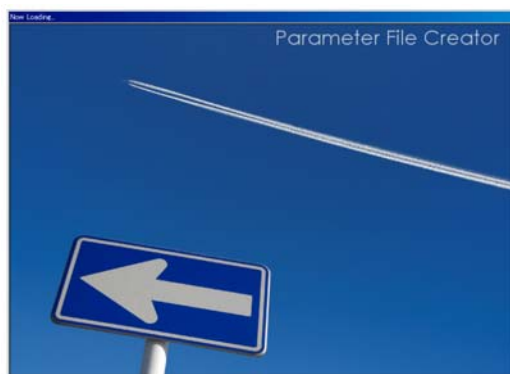
1. Start the OS.
2. Insert the EXPRESSBUILDER DVD into the optical disk drive.
3. Right-click on the screen or left-click [Setup Windows]. The menu will appear.



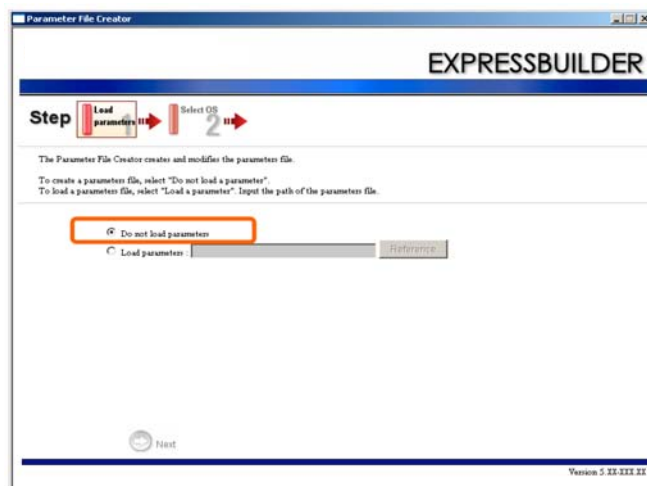
4. Click [Parameter File Creator].



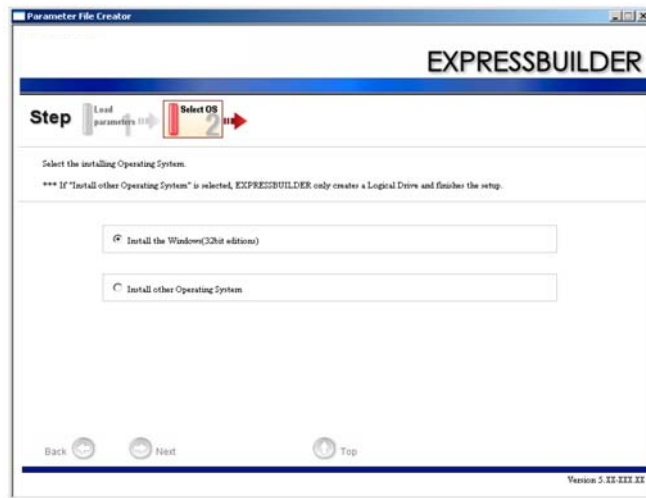
Parameter File Creator will appear.



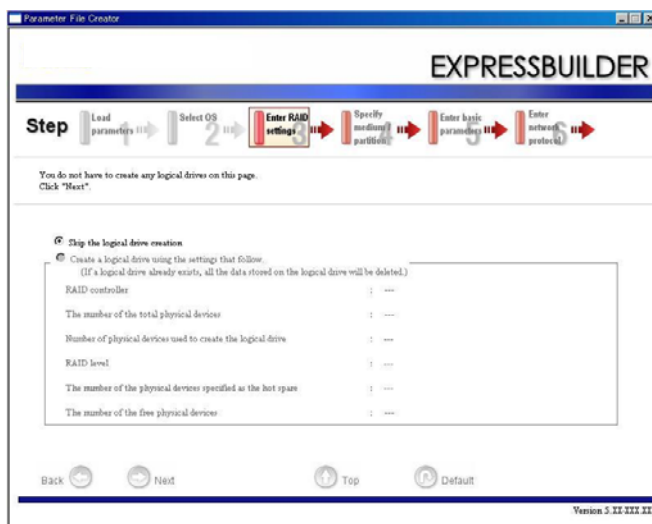
5. [Load Parameters] step is displayed.
Select [Do not load parameters] from the menu, click [Next].



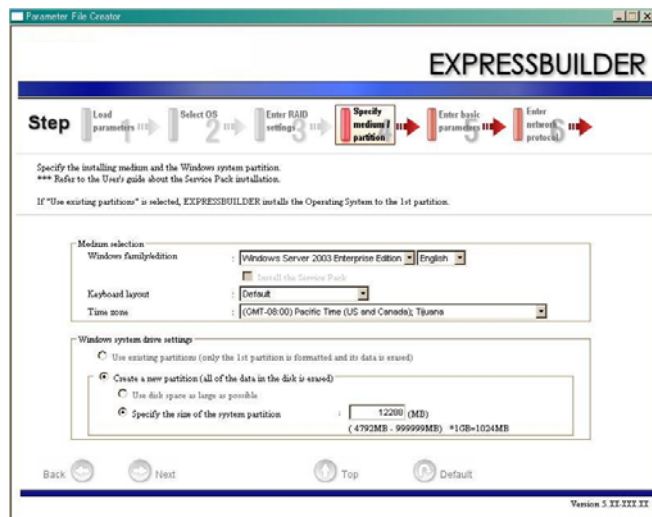
6. Select the installing Operating System.
Select [Install the Windows (32bit editions)] from the menu, click [Next].



7. Enter the setting of a logical drive.
[Enter RAID setting] steps are displayed. Retain the default value, and click [Next].



8. Specify the installing medium and the Windows system partition. [Specify medium/Partition] steps are displayed. Confirm the parameters, modify if necessary, and then click [Next].



NOTE:

About partition size

- Specify the partition size larger than the required minimum size for OS installation.
- Do not specify a larger partition size than the capacity of connected hard disk drive.

If you select “Create a new partition” at “Windows system drive settings,” the contents of the hard disk will be all deleted.

If “Use existing partitions” is selected, EXPRESSBUILDER install the Operating System to the 1st partition (1st partition is deleted). The data in the other partition is kept if the system has two or more partitions. (See the figure below).

First Partition Deleted	Second Partition Retained	Third Partition Retained
-------------------------------	---------------------------------	--------------------------------

You can not re-install the system with the existing partition that is upgraded to Dynamic Disk remained.
Do not select “Use existing partitions” at “Windows system drive settings.”

9. Enter the user information and client license mode.

[Enter basic parameters] steps are displayed. Verify the parameters, modify if necessary, and then click [Next].

EXPRESSBUILDER

Step 1 Load parameters 2 Select OS 3 Enter RAID settings 4 Specify existing partitions 5 **Enter basic parameters** 6 Enter network protocols

Enter the basically parameters:
The computer name is less than 15 character. (Do not set the same name as other computer name, domain name or workgroup name)
The user name and the organization's name are less than 30 character

User information

Computer name : (necessary)

User name : (necessary)

Organization's name :

Administrator password :

Confirm password :

Client license

☒ Per server mode

☐ Per user or per device mode

Back Next Top Default

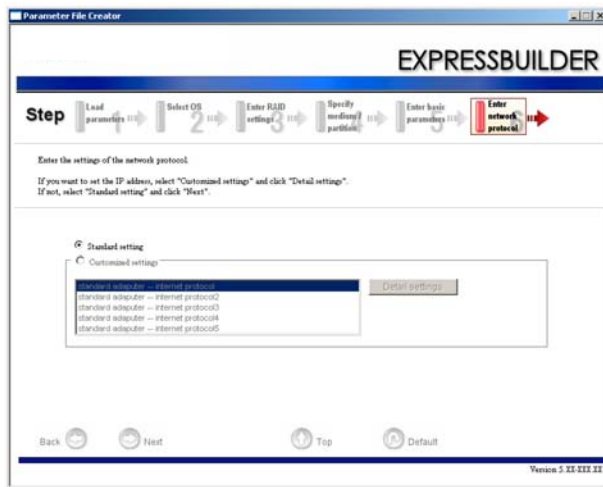
Version 5.11.111.11

NOTE:

You must enter the computer name and the user name.

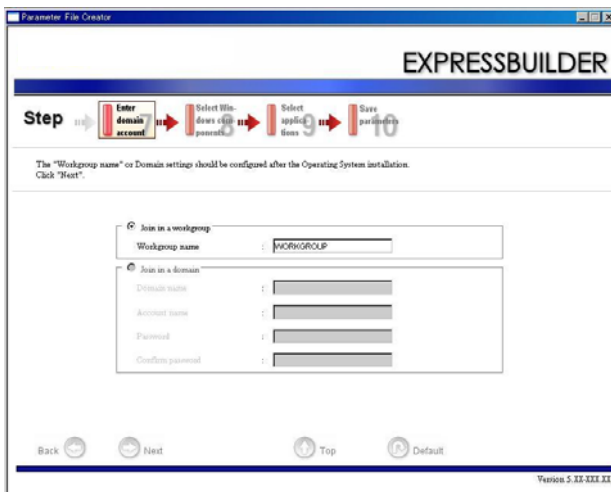
10. Enter the setting of the network protocol.

[Enter network protocol] steps are displayed. Retain the default value, and click [Next].



11. Enter the domain or workgroup name to be used.

[Enter domain account] steps are displayed. Retain the default value, and click [Next].



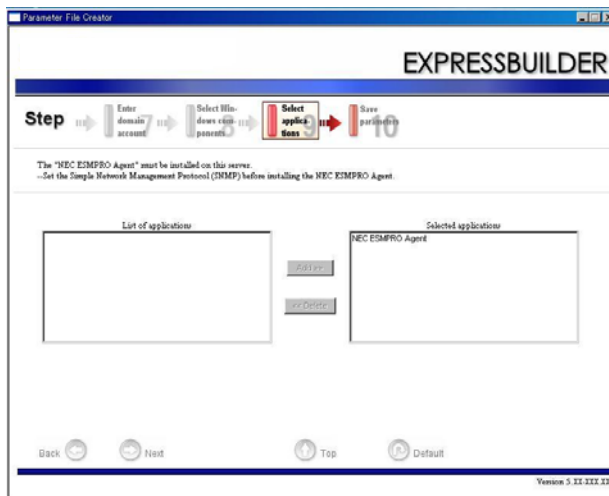
12. Enter the installing components.

[Select Windows components] steps are displayed. Verify the parameters, modify if necessary, and then click [Next].



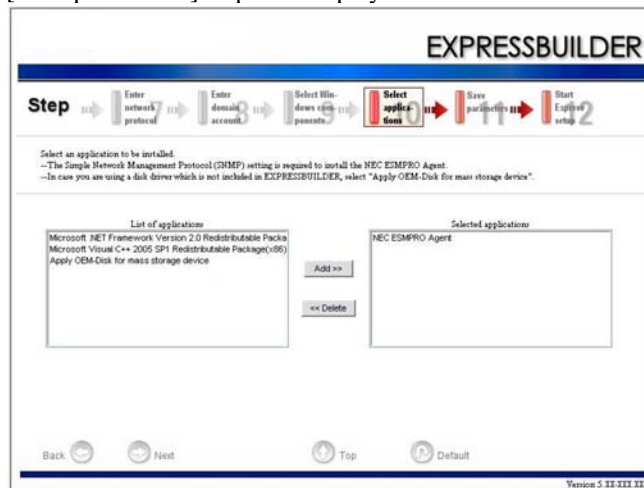
13. Select the installing applications.

[Select applications] steps are displayed. Retain the default value, and click [Next].



14. Save the parameters.

[Save parameters] steps are displayed.



If you want to save the parameters, set the free formatted floppy disk.

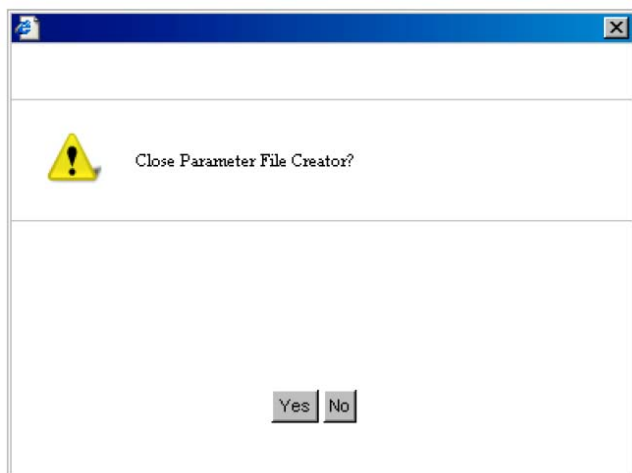
Select [Save parameters], enter the file path of the parameters files into the text box and click [Next].

If not, select [Do not save parameters].

15. Save to a floppy disk.




The floppy disk containing the parameters file has been created.



Click [Yes] to exit Parameter File Creator.

NOTE:

- If you modify existing information file (parameter file), click “Load Parameters” at [Road Parameters] screen. Refer to help to modify information file.
 - If you cancel operation on the way, click  at the upper-right corner of the screen.
-

NEC ESMPRO Agent and Manager

Fault Tolerant Server series system management applications “NEC ESMPRO Manager” and “NEC ESMPRO Agent” are bundled to accessory “EXPRESSBUILDER DVD.”

This section describes the functions and features provided by NEC ESMPRO Manager and NEC ESMPRO Agent and the notes on their operations.

These applications are necessary for continuous operation of Fault Tolerant Server series.

Overview

NEC ESMPRO Manager and NEC ESMPRO Agent are the server management software provided for the stable operation of a server system and effective system operations. They can manage the configuration information and operating status of server resources to prevent server faults from occurring. If a server fault occurs, they detect the fault to notify the system Administrator of the occurrence. This enables the system Administrator to take appropriate action against faults.

- Importance of server management
 - “Constantly stable operation” and “less management workload” are keywords in server management.
 - Stable operation of server
 - Shutdown of a server immediately leads the customer to lose business opportunities and profits. This requires servers to always operate in their perfect state. If a fault occurs in a server, it is necessary to detect the occurrence as soon as possible, make clear the cause, and take appropriate action. The shorter the time taken from the occurrence of a fault to the recovery from the fault is, the smaller the loss of profits (and/or costs) is.
 - Load reduction of server management
 - The server management requires many jobs. In particular, if the system becomes large or remote servers are used, required jobs increase further. The reduction of the load of the server management brings the decrease in costs (and thus customer's benefit).
- What are NEC ESMPRO Manager and NEC ESMPRO Agent?

NEC ESMPRO Manager and NEC ESMPRO Agent are server management software used to manage and monitor Fault Tolerant Server series systems on the network. The installation of NEC ESMPRO Manager and NEC ESMPRO Agent enables the server configuration, performance, and fault information to be acquired, managed, and monitored in real time and also the occurrence of a fault to be detected immediately by the alert report function.
- Effects of using NEC ESMPRO Manager and NEC ESMPRO Agent

NEC ESMPRO Manager and NEC ESMPRO Agent have sufficient effects on a variety of needs in versatile and complicated system environments.

 - Detection of server fault
 - NEC ESMPRO Agent collects a variety of fault information on Fault Tolerant Server series systems to identify the states of the systems. If a server detects a fault, the server provides NEC ESMPRO Manager with the proper alert report.
 - Prevention of server fault
 - NEC ESMPRO Agent includes the preventive maintenance function predicting the occurrence of a fault in advance as countermeasures for preventing faults from occurring. It can previously detect the increase in the chassis temperature and the empty capacity in a file system.
 - Management of server operation status
 - NEC ESMPRO Agent can acquire the detailed hardware configuration and performance information on Fault Tolerant Server series systems. The acquired information can be viewed at any point through NEC ESMPRO Manager.
 - Collective management of distributed servers
 - NEC ESMPRO Manager provides the GUI interface that allows servers distributed on the network to be managed efficiently.

Detection of Server Fault

NEC ESMPRO Manager and NEC ESMPRO Agent detect errors causing faults to occur at an early stage and notify Administrators of fault information real-time.

■ Early detection of error

If a fault occurs, NEC ESMPRO Agent detects the fault and reports the occurrence of the fault to NEC ESMPRO Manager (alert report). NEC ESMPRO Manager displays the received alert in the AlertViewer and also changes the status colors of the server and server component in which the fault occurs. This allows you to identify the fault at a glance. Further, checking the content of the fault and the countermeasures, you can take appropriate action for the fault as soon as possible.

■ Types of reported faults

The table below lists the typical faults reported by NEC ESMPRO Agent.

Component	Reported information
CPU	<ul style="list-style-type: none">• CPU load is over the threshold• CPU degrading, etc.
Memory	ECC 1-bit error detection, etc.
Power supply	<ul style="list-style-type: none">• Voltage lowering• Power failure, etc.
Temperature	Temperature increase in chassis, etc.
Fan	Fan failure (decrease in the number of revolutions), etc.
Storage	File system usage rate, etc.
LAN	<ul style="list-style-type: none">• Line fault threshold over• Send retry or send abort threshold over, etc.

Prevention of Server Fault

NEC ESMPRO Agent includes the preventive maintenance function forecasting the occurrence of a fault as countermeasures for preventing faults from occurring.

NEC ESMPRO Manager and NEC ESMPRO Agent can set the threshold for the CPU usage rate and the empty capacity in a file system, etc. in the server. If the value of a source exceeds the threshold, NEC ESMPRO Agent reports the alert to NEC ESMPRO Manager.

The preventive maintenance function can be set for a variety of monitoring items including the CPU usage rate.

Management of Server Operation Status

NEC ESMPRO Agent manages and monitors a variety of components installed in the server. You can view the information managed and monitored by NEC ESMPRO Agent on the DataViewer of NEC ESMPRO Manager.

NEC ESMPRO Agent also manages and monitors components and conditions required to keep the server reliability at a high level such as hard disks, CPU, fans, power supply, and temperature.

Functional availability on the DataViewer:

Function name	Availability	Function outline	
Hardware	Available	This function shows the hardware's physical information.	
	Memory bank	Available	This function shows the memory's physical information.
	Device information	Available	This function shows the device's unique information.
	CPU	Available	This function shows CPU's physical information.
System	Available	This function shows CPU's logical information and monitors CPU utilization. This function shows memory's logical information and monitors the status.	
I/O devices	Available	This function shows information about I/O devices (such as Floppy disk, serial port, parallel port, keyboard, mouse, video).	
System environment	Available	This function monitors tempareture, fan, voltage, power supply and door.	
	Tempareture	Available	This function monitors tempareture inside of chassis.
	Fan	Available	This function monitors fan.
	Voltage	Available	This function monitors voltage inside of chassis.
	Power supply	Unavailable	This function monitors power supply unit.
	Door	Unavailable	This function monitors chassis intrusion(open/close of cover/door of chassis).
Software	Available	This function shows information about service, driver and OS.	
Network	Available	This function shows network (LAN) information and monitors packet.	
Expansion device	Unavailable	This function shows information about expansion bus device.	
BIOS	Available	This function shows BIOS information.	
Local polling	Available	This function monitors values of MIB that agent takes at random.	

Monitoring (Management) of Fault Tolerant Server series

Fault Tolerant Server series is a fault tolerant system. It can continue the operation even if a major component fails. Fault Tolerant Server series improves the system availability with the hardware, NEC ESMPRO, and system software functions.

If a major component fails, the NEC ESMPRO fault report function can notify the system Administrator of the occurrence of the fault. In addition, the DataViewer of NEC ESMPRO Manager can monitor the system status and also identify the failed component.

NEC ESMPRO provides several maintenance functions such as the update of F/W and BIOS in the Fault Tolerant Server series in the online state (in which the system continues the operation but the components used to update F/W or BIOS is suspended) and the suspension of a specific component.

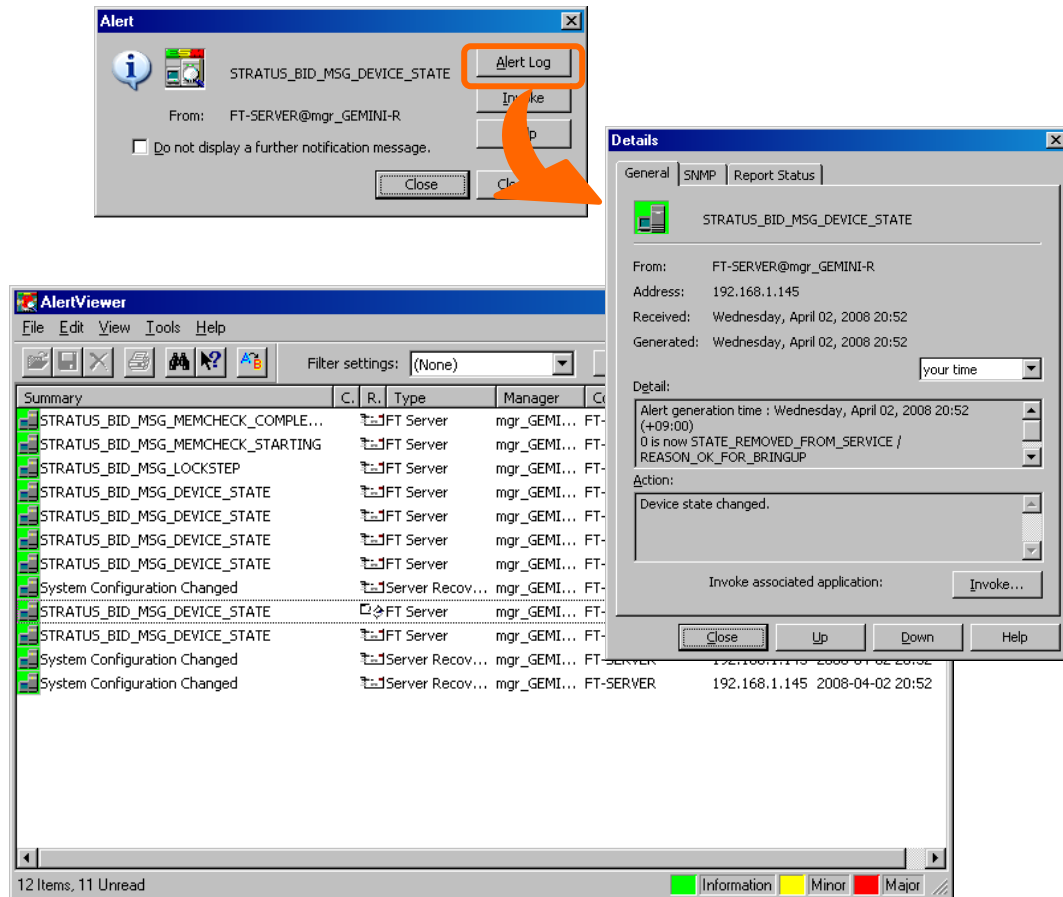
The table below lists the Fault Tolerant Server series management tasks using NEC ESMPRO and system functions.

Fault Tolerant Server series management task	NEC ESMPRO function or tool (on managed Fault Tolerant Server series)*	NEC ESMPRO function or tool (on management manager)
Monitoring of major component states	—	NEC ESMPRO Manager DataViewer
Diagnosis and start/stop of major components and F/W update	NEC ESMPRO Agent ft server utility	NEC ESMPRO Manager DataViewer
Verification of alert or verification of fault occurrence event information	Event Viewer	NEC ESMPRO Manager AlertViewer

* When the administration manager is also the managed Fault Tolerant Server series (or NEC ESMPRO Manager is installed on the managed Fault Tolerant Server series), all functions of the administration manager can be used on the managed Fault Tolerant Server series.

The report of a fault occurrence in the Fault Tolerant Server series (alert) is immediately sent to the NEC ESMPRO Manager. When the NEC ESMPRO Manager receives the alert, a popup message appears.

The alert contains the detailed information of the fault and the proper countermeasures. You can take the appropriate action for the alert.



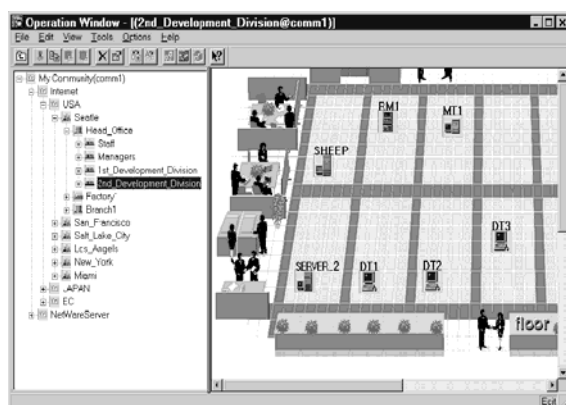
Collective Management of Distributed Servers

The excellent GUI provided by NEC ESMPRO Manager allows servers on a network to be managed collectively. The management screen is designed in the Explorer format to indicate the components in a server hierarchically for effective server management.

NEC ESMPRO Manager manages servers by using the following three types of GUIs.

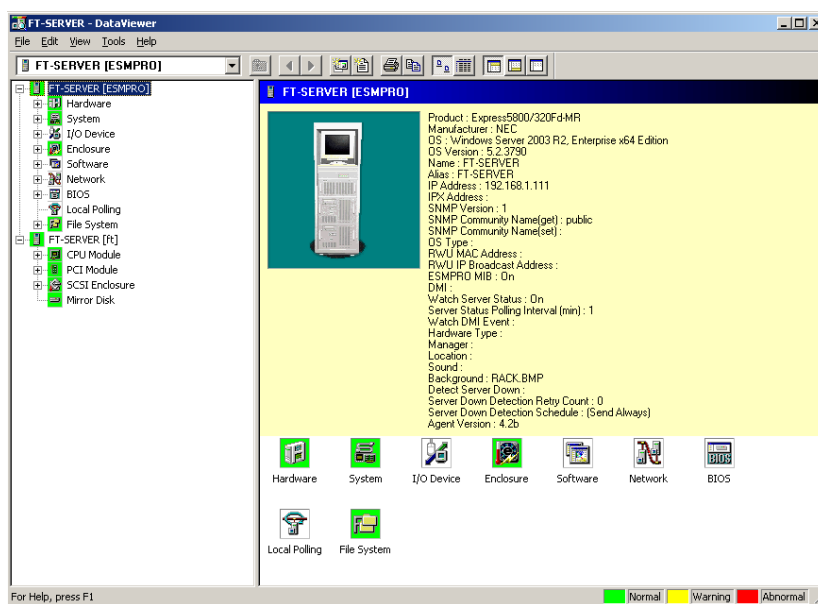
■ Operation Window

The operation window is used to create the map of servers connected to network to manage them. The map can be multi-layered depending on the installation areas, organizations, and objects.



■ DataViewer

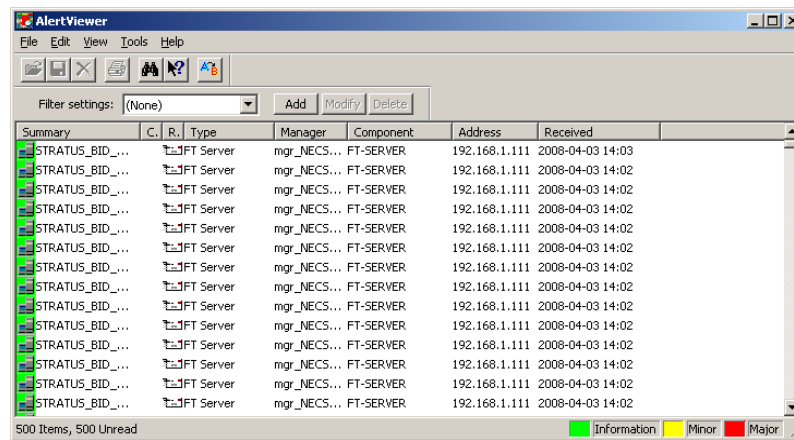
The DataViewer indicates the server source configuration information in the Explorer format. In addition, it changes the status color of the failed server component. This enables you to identify the failed portion.



- AlertViewer

The AlertViewer manages fault reports sent from servers together. A fault occurred in a server is immediately reported to the AlertViewer.

The Administrator can recognize all faults on the network instantly.



NEC ESMPRO Agent

NEC ESMPRO Agent is a utility which acts as an agent (proxy) between Fault Tolerant Server series and NEC ESMPRO Manager (management PC). For details on the operating environment, the setting required before the setup, and the installation procedure, see the separate volume "User's Guide (Setup)."

Device ID in Alert Report

Some Fault Tolerant Server series reports use unique device IDs which correspond to the devices listed in the table below as the device identification information.

Device name	Device ID
CPU module 0	0
DIMM CH0/CH1 SLOT 0 on CPU module 0	0/0
DIMM CH0/CH1 SLOT 1 on CPU module 0	0/1
DIMM CH0/CH1 SLOT 2 on CPU module 0	0/2
DIMM CH0/CH1 SLOT 3 on CPU module 0	0/3
DIMM CH0/CH1 SLOT 4 on CPU module 0	0/4
DIMM CH0/CH1 SLOT 5 on CPU module 0	0/5
CPU0 on CPU module 0	0/20
CPU1 on CPU module 0	0/23
CPU module 1	1
DIMM CH0/CH1 SLOT 0 on CPU module 1	1/0
DIMM CH0/CH1 SLOT 1 on CPU module 1	1/1
DIMM CH0/CH1 SLOT 2 on CPU module 1	1/2
DIMM CH0/CH1 SLOT 3 on CPU module 1	1/3
DIMM CH0/CH1 SLOT 4 on CPU module 1	1/4
DIMM CH0/CH1 SLOT 5 on CPU module 1	1/5
CPU0 on CPU module 1	1/20
CPU1 on CPU module 1	1/23
PCI module 0	10
PCI slot 1 on PCI module 0	10/6
PCI slot 2 on PCI module 0	10/7
PCI slot 3 on PCI module 0	10/8
PCI module 1	11
PCI slot 1 on PCI module 1	11/6
PCI slot 2 on PCI module 1	11/7
PCI slot 3 on PCI module 1	11/8
SCSI enclosure 0	10/40
SCSI slot 1 on SCSI enclosure 0	10/40/1
SCSI slot 2 on SCSI enclosure 0	10/40/2
SCSI slot 3 on SCSI enclosure 0	10/40/3
SCSI enclosure 1	11/40
SCSI slot 1 on SCSI enclosure 1	11/40/1
SCSI slot 2 on SCSI enclosure 1	11/40/2
SCSI slot 3 on SCSI enclosure 1	11/40/3

Supplement

Note the followings when using NEC ESMPRO Agent.

Application log registered when system starting

- About the event of “Source: Perflib”

When system is starting, Perflib log may be registered to the application log.

The detailed information about an event log is described on Microsoft Product Support Services. Please check the contents.

- [INFO] Events for Performance Monitor Extensions
<http://support.microsoft.com/default.aspx?scid=kb;en-us;226494>
- Application Log Events Generated When You Start Performance Counter Query
<http://support.microsoft.com/default.aspx?scid=kb;en-us;296187>
- Event ID 2003 Warning Message Logged When Loading Performance Counters
<http://support.microsoft.com/default.aspx?scid=kb;en-us;267831>

Visit the Microsoft Help and Support on regular basis where you can find other information than the above at <http://support.microsoft.com/default.aspx?LN=en-us>.

Maintenance-related Functions

When you want to use maintenance-related functions of the Fault Tolerant Server series, contact your maintenance personnel.

CPU Information

If you select [CPU Module] – [CPU] in the [ft] tree of the DataViewer, unknown or incorrect information appears in some information items.

The CPU information can be viewed by selecting [System] – [CPU] in the [ESMPRO] tree.

Status during CPU Module Diagnosis

While diagnosing a stopped CPU module, the CPU is no longer in the duplex mode and the CPU and the memory cannot be used. However, the status of [CPU] and [DIMM] displayed under [CPU module] in the ft tree on a DataViewer becomes “Online,” and the status color becomes green.

Change of Installation States of CPU and PCI Modules

If you dynamically change the configuration of the CPU or PCI module in the relevant system during review of the server information by using the DataViewer, the message prompting you to reconstruct the tree of the DataViewer will appear. If you click the [Yes] button, the tree is reconstructed in the DataViewer to reflect the change of the system configuration on the DataViewer. Clicking the [No] button does not cause the tree to be reconstructed in the DataViewer. If so, the information in the DataViewer may be different from the current system information because the change of the system configuration is not reflected on the DataViewer.

SCSI Slot Information

When the PCI module is detached and you select [SCSI Slot] – [General], the displayed “Hardware LED” information may not be correct.

To check the status of SCSI slots, see the string information in the “Status” column.

Impact When Module Status Changes

PCI modules, SCSI adapters, SCSI buses, and modules under the SCSI enclosure have impact on each other. For example, when the “Status” item of a module changes to “fault,” it may be caused by another module’s error. Therefore, you need to check the status of the other modules based on alert information.

Status Color after Mounting a Hard Disk Drive

When creating a new mirror, the status of the hard disk and its upper component, SCSI enclosure, will continue to change frequently after you mount a hard disk until the mirror is completed. During this process, the status color may turn to abnormal, but when the mirror is created successfully, it will return normal.

Total Status of the PCI Module

When each module’s status is simplex, the total status of the PCI module displayed on the DataViewer is yellow (warning) and the status will be reflected to the server status. The ft control software 3.0 or later does not display the information on Ethernet or SCSI adapter on the tree of the DataViewer. If an error occurs on an Ethernet or SCSI adapter, view the alert reports.

Hard Disk Drives Mirrored by the Rapid Disk Resync (RDR) Function

The DataViewer’s [Mirror Disk] tree of [ft] shows a pair of hard disk drives constructing mirroring as one mirror. Therefore the status of a volume (such as span volume and striping volume) over multiple hard disk drives created by the RDR function may not be displayed correctly. Use the RDR Utility for checking the state of mirrored hard disk drives created by the RDR function.

The Information on the Hard Disk Drive in the Disk Expansion Unit is not Displayed Correctly.

When the Disk Expansion Unit is mounted, the information on the hard disk drive in the Disk Expansion Unit may not be displayed on the [SCSI Enclosure] – [SCSI Slot] information on a DataViewer. In such case, reboot the system.

LAN Monitoring Report

The LAN monitoring function defines the line status depending on the number of transmission packets and the number of packet errors within a certain period. Thus, the LAN monitoring function may report a line fault or high line load only in a temporary high line impedance state. If a normal state recovery is reported immediately, temporal high line impedance may have occurred thus there is not any problem.

LAN Monitoring Threshold

Because the Fault Tolerant Server series detects hardware faults on the network in the driver level, NEC ESMPRO Agent does not monitor line faults. Thus, the value set for “Line fault occurrence rate” of a [LAN] tab of [NEC ESMPRO Agent properties] in the control panel is not used.

Community Authority

Depending on your OS type or its version, settings for community, SNMP service’s security function, are not made, or default settings of authority are different.

To enable the remote shutdown and threshold change functions via NEC ESMPRO Manager, make settings of community and set its authority to “READ CREATE” or “READ WRITE.”

Hardware Monitoring by ESM PRO

In Fault Tolerant Server/-MR, an alert report is not issued if an error on temperature/fan/power supply/voltage is detected in CPU module and PCI module.

Moreover, the trees [Temperature], [Fan], [Voltage], and [Power Supply] are not displayed on [System Environment] of DataViewer of NEC ESM PRO Manager.

System Environment Monitoring

On Fault Tolerant Server/-MR, monitoring of temperature, fan and voltage under [System Environment] of [ESM PRO] tree in the DataViewer is set to enable and cannot be changed to disable by default.

Change of SNMP Community

If the security setting of the SNMP Service of a system, where the NEC ESM PRO Agent is installed, is changed from the default “public” to a community name, change the community settings of the NEC ESM PRO Agent, too.

1. Double-click the [NEC ESM PRO Agent] icon in [Control Panel].
2. Select a desired community name from the [SNMP Community] list box in [SNMP Setting] of the [General] sheet.
The community names to receive SNMP packets from are listed in the [SNMP Community] list box.
3. Click [OK] to terminate the operation.

Printer Information's Available Time:

When you add a new printer, install its driver and make its settings, if you do not make settings for the available time from Add Printer Wizard, the printer's available time (From and To) in [Printers and Faxes] are [00:00], on the other hand, Manager's time are [9:00]. To display them properly, make the settings of printer from [Printers and Faxes]. The procedures are as follows;

1. Start [Printers and Faxes], and open the printer properties you want to make settings for. (Select the [Printers and Faxes], right-click and select [Properties].)
2. Select the [Advanced] tab.
3. Enter values in the available time (From and To), and click [OK] in the [Advanced] and [Properties] dialog boxes.

Now, you can see the correct information from Manager, too.

Disk Maintenance while NEC ESMPRO Agent is Running

The following works to disks (hard disk drive or magneto optical) are not allowed while NEC ESMPRO Agent is running;

To format or delete a partition by Disk Administrator or by other means.

To request programmatically to remove media from removable disks such as MO, Zip and PD.

1. Select the [Start] – [Settings] – [Control Panel]
2. Open the [Service]
3. Select a service named “ESMCommonService,” and click the [Stop].
4. Verify that “ESMCommonService” stopped, and close the [Service].
5. Do the disk-related works.
6. Open the [Service] again, select “ESMCommonService” and click the [Start].
7. Verify that “ESMCommonService” is active and close the [Service] and [Control Panel].

Connection with Hard Disk Drive

The preventive hard disk drive maintenance function may not work properly when a hard disk drive which was used in a system where NEC ESMPRO Agent is installed is connected to other systems. Make sure not to connect such hard disk drives.

Change Settings of File System Monitoring Function

New settings in thresholds of monitoring interval and free space monitoring are not reflected immediately after they are changed. They are reflected at the next monitoring interval of monitoring service.

CPU Load Ratio of SNMP Service (snmp.exe)

While monitoring the server from NEC ESMPRO Manager, the CPU load ratio of SNMP Service on the NEC ESMPRO Agent side may increase at every monitoring interval (default: 1 minute).

NEC ESMPRO Manager and NEC ESMPRO Agent exchange information through SNMP Service. If the server status monitoring by NEC ESMPRO Manager is on (default: ON), NEC ESMPRO Manager regularly issues a request to NEC ESMPRO Agent to get the current status of the server. In response, NEC ESMPRO Agent checks the status of the server. As a result, the CPU load ratio of SNMP Service increases temporarily.

If you have trouble of terminating a movie player application, turn off the server status monitoring by NEC ESMPRO Manager or extend the monitoring interval.

Hang of SNMP Service

SNMP Service has a module called “SNMP Extended Agent.” This module may be registered when you install some software that uses SNMP Service.

If you start SNMP Service, SNMP Extended Agent is also loaded at the initialization. However, if the initialization is not completed within a specified period, SNMP Service will hang.

It may take time to complete the initialization due to temporary high load on the system. In this case, wait for the system load become low enough before restarting SNMP Service.

Pop-up message of esmcmn.exe is displayed when starting the system:

The following pop-up message may be displayed when you restart the system which NEC ESMPRO Agent is installed to and removal drives such as MO and DVD-RAM are mounted on, without closing Windows Explorer, after displaying the contents of media and removing the media by the software eject (by right-clicking the DVD drive on Windows Explorer and selecting [Eject]) The message (the drive name) displayed varies depending on the systems. If the pop-up message “There is no disk in the drive. Please insert a disk into drive A:.” is displayed, click [Cancel] or [Continue] to close the dialog box. If you do not close the dialog box, you cannot start the Workstation service and related services, causing unstable operation of the system. Also, if you restart the system, execute it after terminating the program such as Windows Explorer which displays a media.

Example

**CPU Information**

In [CPU Information] of DataViewer's system tree, the external clock is listed as “Unknown.”

When [ft] Tree Appears on Date Viewer in an Incorrect Manner

If you open a DataViewer immediately after the system starts up, the tree or the state of a DataViewer may not be displayed correctly due to high load of the system. In about 20 minutes after the system startup, when a pop-up message (below) which prompts you to reconstruct a DataViewer appears, click [OK]. The DataViewer will be reconstructed and the tree and the status will be displayed correctly.

DataViewer

The system configuration of the host may have been changed. Do you wish to reconstruct the tree?

Floppy Disk Drive Name

After unplugging and plugging the PCI module of the primary side, the floppy disk drive name of [I/O Device] on DataViewer may be different from the name that is recognized by the OS.

(Example: drive name on DataViewer: “A”
drive name recognized by the OS: “B”)

Check the floppy disk drive name on Explorer.

Floppy Disk Drive Information

If you add or delete floppy disk drive connected with USB while the system is running, the drive information under the [I/O Device] in the DataViewer will be updated at the next system startup.

Information of the keyboard/mouse connected with USB

When the keyboard or mouse is connected with USB, the keyboard or mouse information under the [I/O Device] in the DataViewer is listed as “Unknown.”

Ethernet Adapters You Do Not Use

If an Ethernet adapter is not used (not connected to cable), set it to “Disable” in [Network Connections] from Control Panel. If an Ethernet adapter you are about to disable has dual LAN settings (AFT function), remove the dual LAN settings before disable it.

DataViewer display when only one of the PCI modules (IO modules) is operating

When only one of the PCI modules (IO modules) is operating (non-dual configuration), the SCSI enclosure or mirror disk status cannot be displayed normally.

To check if the dual configuration is changed to the simplex operation mode, check the event log, AlertViewer log, or the status color of PCI module of DataViewer.

Display of Ethernet Board of ftServer Utility

FtServer Utility displays the information of Network Controller.

Fault Tolerant Server/-MR has four in-built Network Ports. Two trees of the Ethernet Board are displayed since a module has two Network Controllers.

NEC ESMPRO Manager

To monitor and manage a computer, on which NEC ESMPRO Agent is installed, with a management PC online, use NEC ESMPRO Manager that is bundled with the product.

For detailed procedures of installation and setting, see online documents or NEC ESMPRO Online Help.

TIPS:

- Online documents provide cautions and information for using NEC ESMPRO Manager. See *NEC ESMPRO Manager User's Guide* in the EXPRESSBUILDER DVD.
- The sample screen shown in this subsection may differ from that of your server software; however, it offers the same function.

Monitoring by Use of DataViewer

To monitor the state of the Fault Tolerant Server series on a management computer with installation of NEC ESMPRO Manager, the DataViewer is used. If you click each of the modules and items to be checked sequentially on the tree view in the Windows Explorer format, the DataViewer indicates their states on the right side of the screen.

You can manage the status on a Web browser using Web component functions of NEC ESMPRO Manager. For details, see Help on Web Component.

This section describes the tree structure and displayed screens in the DataViewer.

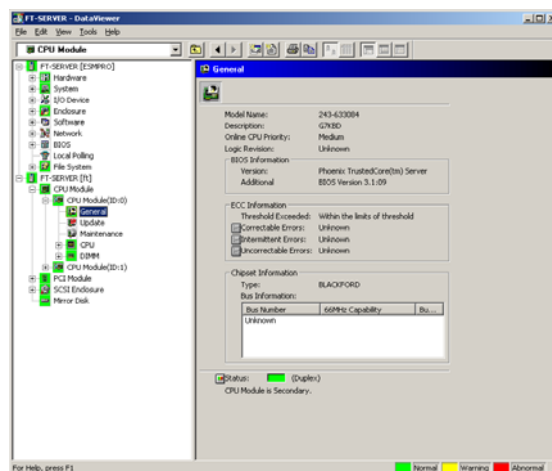
To make the DataViewer indicate the state of each module and those of the components on it, select the server to be monitored from NEC ESMPRO Manager to start the DataViewer (in the following description, the start procedure of the DataViewer is omitted).

Monitoring CPU Module

To monitor the CPU modules and the components on the CPU module, see the [CPU Module] tree. To see the information on the [CPU Module] tree, select the target CPU module from [CPU Module] in the [ft] tree.

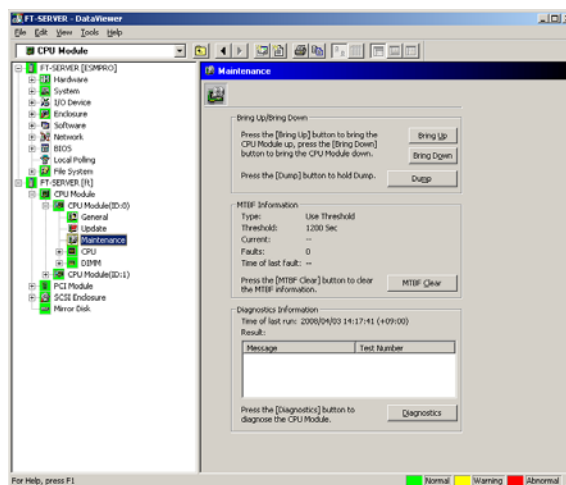
You can see the following information on the modules and the components on the CPU modules in the [CPU Module] tree.

- General
Allows the configuration and other information on the CPU modules to be viewed.



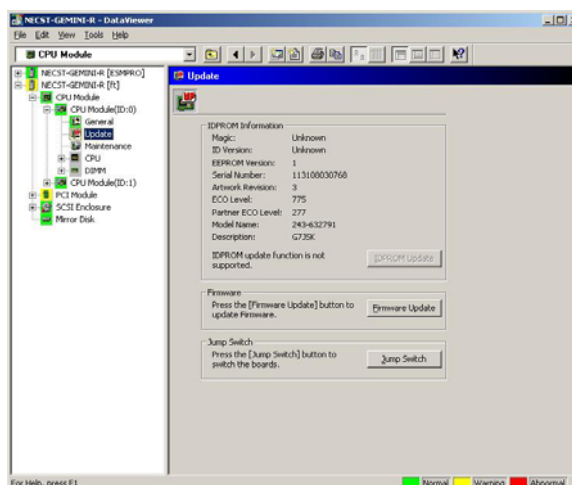
■ Maintenance

Allows the start/stop, MTBF information clear, dump acquisition, and diagnosis of the CPU modules to be provided. See “Maintenance of Fault Tolerant Server series” described later for the start/stop and MTBF information clear of the CPU modules.



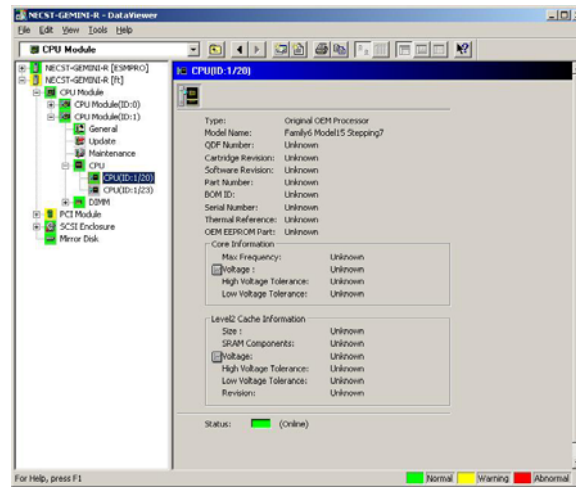
■ Update

Allows the device identification information of the CPU modules to be viewed and BIOS of the CPU modules to be updated. See “Maintenance of Fault Tolerant Server series” described later for the update of BIOS of the CPU modules. The detailed device identification information can be checked by selecting [ESMPRO] tree→[Hardware] tree→[Field Replaceable Unit] tree.



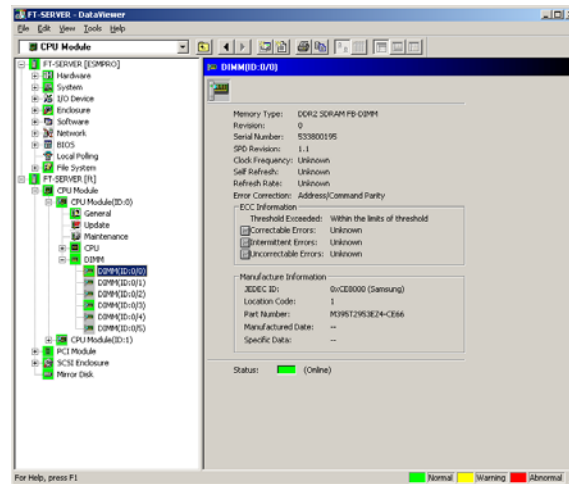
■ CPU

Allows the information of the CPU on the CPU modules to be viewed.



■ DIMM

Allows the information of DIMM on the CPU modules to be viewed.



Monitoring PCI Module

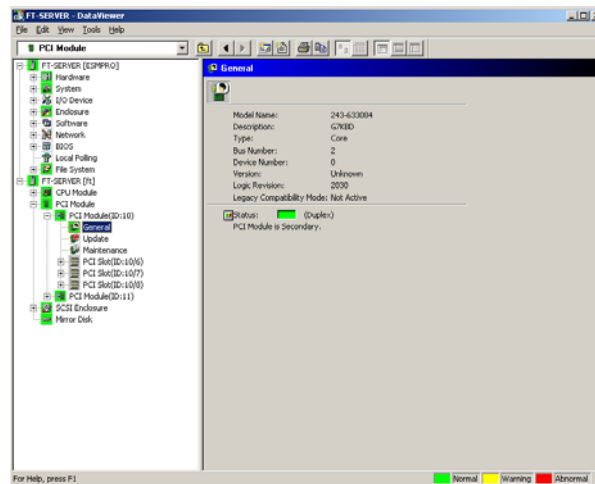
To monitor the PCI modules and the components on the PCI modules, refer to the [PCI Module] tree. To see the information on the [PCI Module] tree, select the target PCI module from [PCI Module] in the [ft] tree.

You can see the following information on the PCI modules and the components on the PCI modules of the [PCI Module] tree.

(This section describes the general information screens of the PCI modules. The components on the PCI modules are described later.)

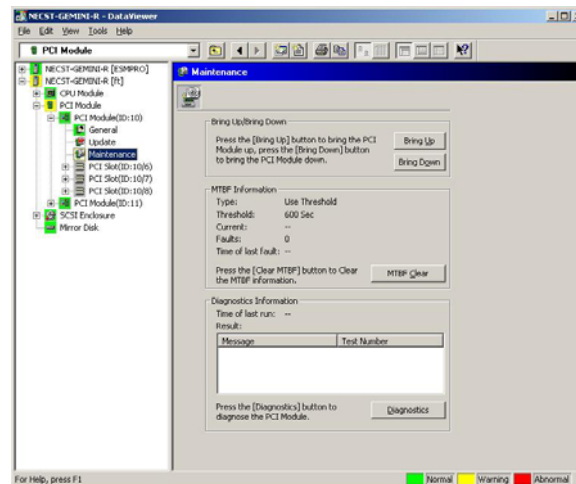
■ General

Allows the configuration and other information of the PCI modules to be viewed.



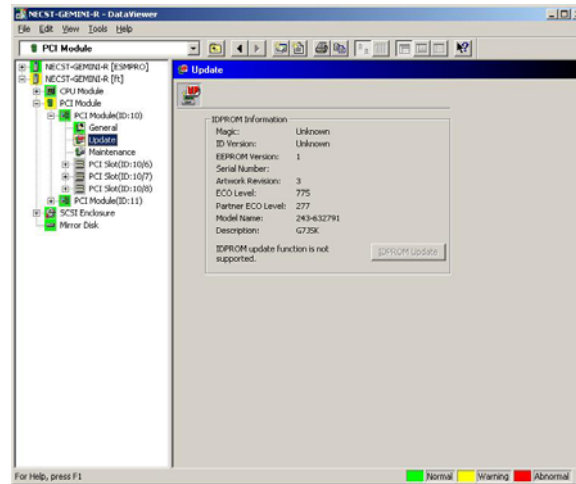
■ Maintenance

Allows the start/stop, MTBF information clear, and diagnosis of the PCI modules to be provided. See “Maintenance of Fault Tolerant Server series” described later for the start/stop and MTBF information clear of the CPU modules.



■ Update

Allows the device identification information of the PCI modules to be viewed. The detailed device identification information can be checked by selecting [ESMPRO] tree→[Hardware] tree→[Field Replaceable Unit] tree.



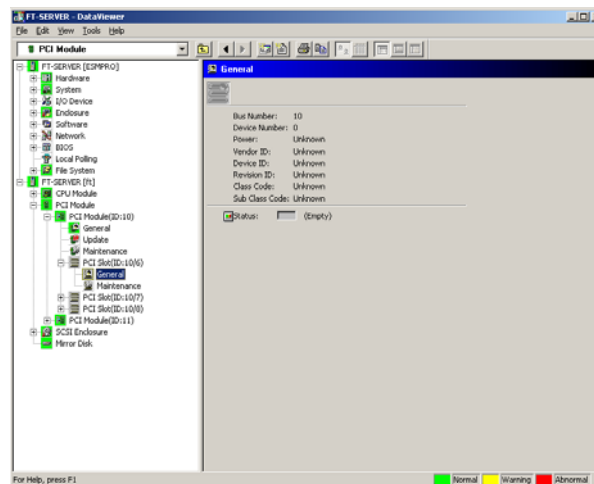
Monitoring PCI Slots and Devices on PCI Module

To monitor the PCI slots and devices on the PCI modules, see the [PCI slot] tree. To see the information on the [PCI slot] tree, select [PCI Module]→[PCI module (containing PCI slot to be seen)]→[PCI slot] of the [ft] tree.

You can see the following information on the PCI slot and the devices on the PCI slot in the [PCI slot] tree.

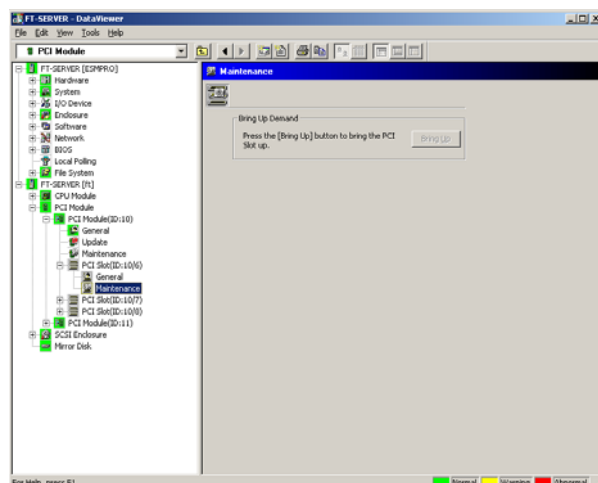
■ General

Allows the PCI slot configuration information to be viewed.



■ Maintenance

Allows a device on the PCI slot to be started. This function is not supported in the current version.



■ PCI Device – General

Allows the information of devices on the PCI slot to be viewed.
This function is not supported in the current version.

■ PCI Device – Detail

Allows the detailed information of a device on the PCI slot to be viewed.
This function is not supported in the current version.

■ PCI Bridge – General

Allows the information of bridges on the PCI bus to be viewed.
This function is not supported in the current version.

■ PCI Bridge – Bus

Allows the bus information of a bridge on the PCI bus to be viewed.
This function is not supported in the current version.

■ PCI Bridge – Detail

Allows the detailed information of a bridge on the PCI bus to be viewed.
This function is not supported in the current version.

Monitoring SCSI adapter on PCI module

To monitor the SCSI adapters on the PCI modules, see the [SCSI adapter] tree. To see the information on the [SCSI adapter] tree, select [PCI Module]→[PCI module (connected to SCSI adapter to be seen)]→[SCSI adapter] of the [ft] tree.

You can see the following information on the SCSI adapters in the [SCSI adapter] tree. This function is not supported in the current version.

- General
Allows the SCSI configuration information to be viewed. This function is not supported in the current version.
- Maintenance
Allows the MTBF information of SCSI adapters to be viewed and cleared. This function is not supported in the current version.
- Update
Allows the firmware of SCSI adapters to be updated. This function is not supported in the current version.
- SCSI bus
Allows the information on the SCSI bus connected to SCSI adapters and devices to be viewed. This function is not supported in the current version.

Monitoring Ethernet adapter on PCI module

To monitor the Ethernet adapters on the PCI modules, see the [Ethernet adapter] tree. To see the information on the [Ethernet adapter] tree, select [PCI Module]→[PCI module (connected to the Ethernet adapter to be seen)]→[Ethernet adapter] of the [ft] tree. You can see the following information on the Ethernet adapters in the [Ethernet adapter] tree.

IMPORTANT:

Disable the unused Ethernet adapter (that is not connected to cables) by using [Network Connection] in Control Panel. However, if the Ethernet adapter to be disabled is set to dual LAN configuration (AFT feature), disable it after removing dual LAN configuration. If it is not disabled and the cable is not connected to it, ESMPRO/ServerAgent determines that the port is faulty (does not have any media), and the status color of [ft] - [PCI module] - [Ethernet Board] of the DataViewer turns red (abnormal). The server status color of the integrated viewer also turns red (abnormal).

- General
This function is not supported in the current version.
- Detail
This function is not supported in the current version.
- Maintenance
This function is not supported in the current version.

Monitoring SCSI Enclosure

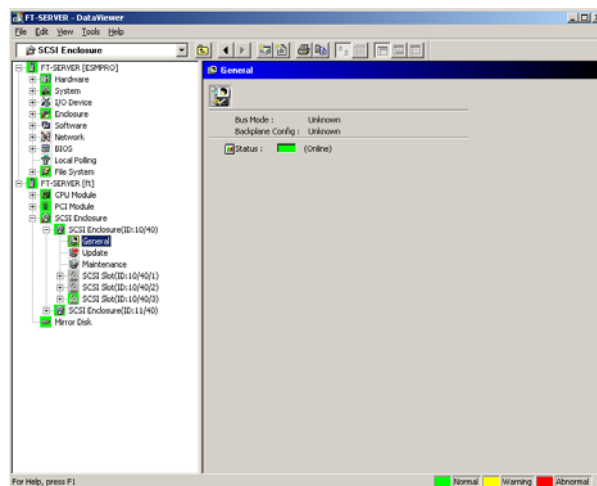
To monitor the SCSI enclosure, see the [SCSI enclosure] tree. To see the information on the [SCSI enclosure] tree, select [SCSI enclosure] of the [ft] tree.

You can see the following information of the SCSI enclosure from the [SCSI enclosure] tree.

- General

Allows the configuration and other information of the SCSI enclosure to be viewed.

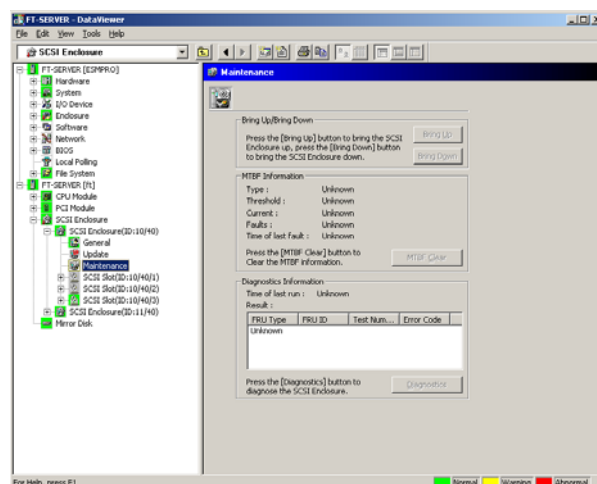
IMPORTANT: You need to be aware that PCI modules, SCSI adapters, SCSI buses, and modules under the SCSI enclosure have impact on each other. For details, see “Impact When Module Status Changes” described above.



- Maintenance

Allows the MTBF information of the SCSI enclosure to be viewed or cleared.

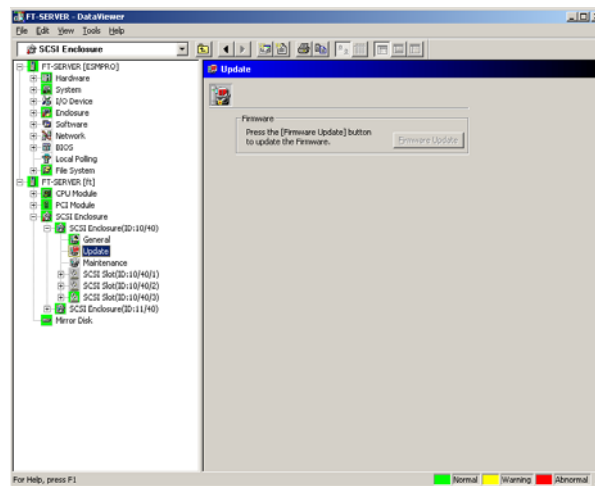
This function is not supported in the current version.



■ Update

Allows the firmware of the SCSI enclosure to be updated.

However, this function is not supported in the current version.



■ Electronics – General

This function is not supported in the current version.

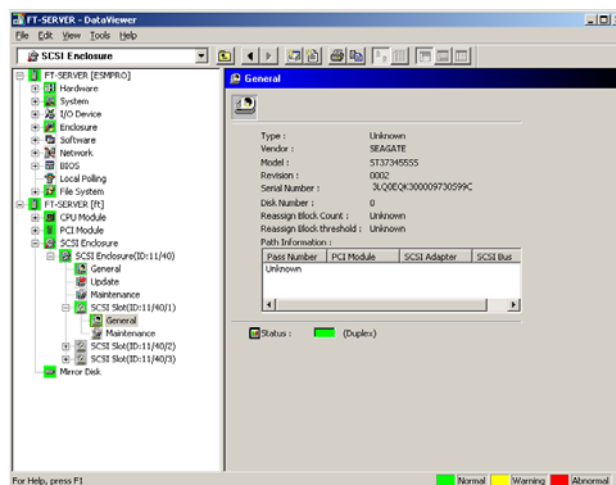
■ Electronics – Maintenance

This function is not supported in the current version.

■ SCSI Slot – General

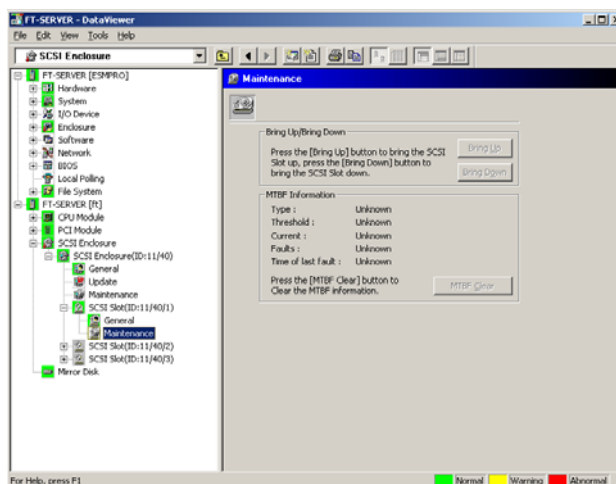
Allows the configuration and other information of the SCSI slot to be viewed.

IMPORTANT: You need to be aware of the status of hard disk during the mirror creation. For details, see “Status Color Changes after Hard Disk Drive is Mounted” described earlier in this chapter.



■ SCSI Slot – Maintenance

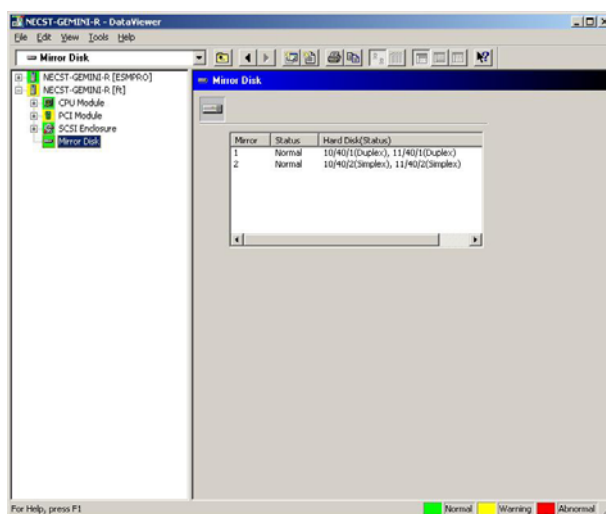
Allows the MTBF information of the SCSI slot to be viewed or cleared.
This function is not supported in the current version.



Monitoring Mirror Disk

To monitor the mirror disk components, see the [Mirror Disk] tree. To view information on [Mirror Disk] tree, select [Mirror Disk] under [ft] tree.

You can see the redundancy status of the mirrors and the device IDs of the SCSI slots into which these hard disk components are connected.



[Mirror Disk]

Monitoring Hard Disk Drive (HDD)

To monitor the hard disks and detect disk failures at an early stage, use the NEC ESMPRO Manager and Agent. You can see configurations and information of hard disk in the DataViewer.

Monitoring HDD Operations

This section describes how to maintain hard disk drives.

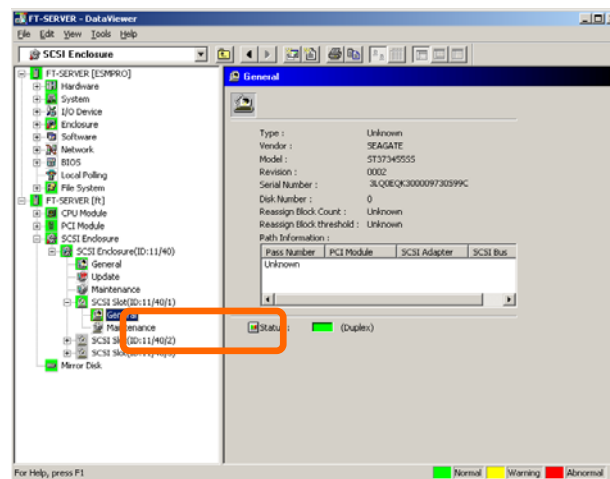
1. Verification of HDD failure

If NEC ESMPRO Agent detects some problem with a HDD, it will report an alert of the problem to NEC ESMPRO Manager. Please check the AlertViewer in the manager regularly.

Ex. If a HDD in SCSI Slot (10/40/1) is broken, agent reports the following alert.

Device 10/40/1 is now BROKEN.

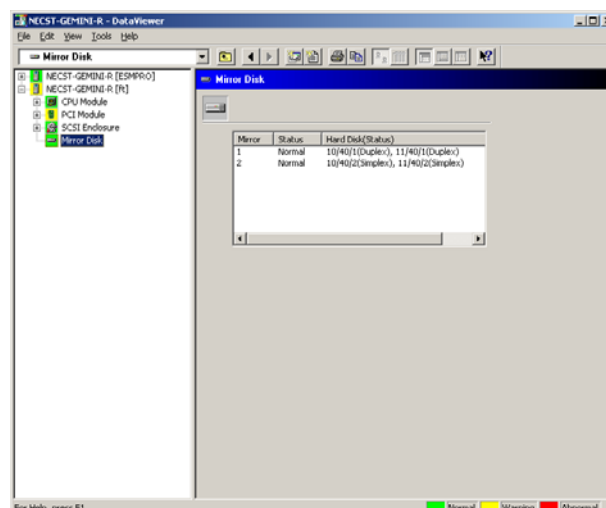
And manager displays the problem information of the hard disk in the [SCSI enclosure] → [SCSI Slot] → [General] of the DataViewer.



[SCSI Slot] → [General]

2. Verification of mirror status

To check the redundancy status of the failed mirror disk, open [Mirror Disk] screen under [ft]. On this screen, you can check the redundancy status of the mirror and the status of the mirrored hard disks.



[Mirror Disk]

IMPORTANT: The mirroring redundancy status will change depending on the status of the two hard disks that make up a mirror as follows:

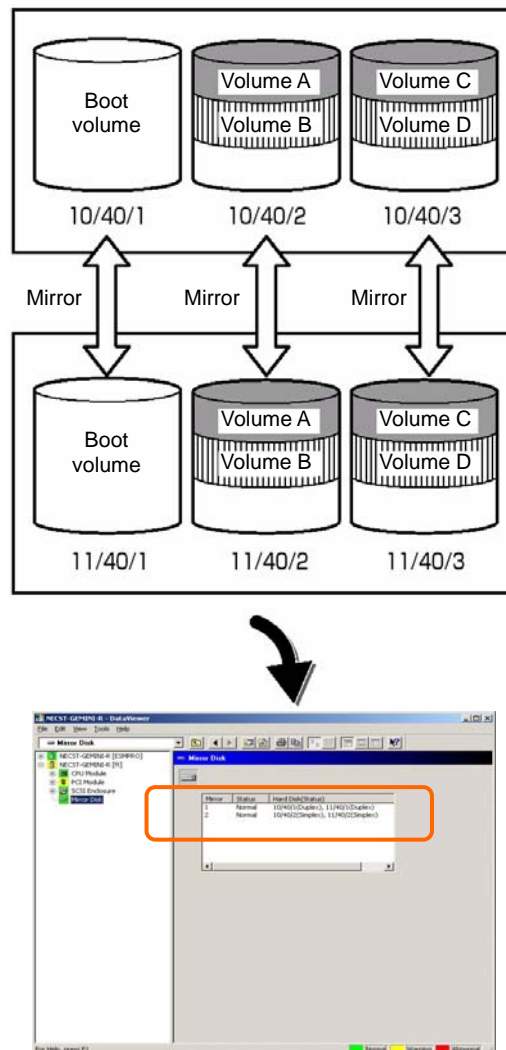
Status of hard disk drive 1	Status of hard disk drive 2	Status of mirror volume
Duplex	Duplex	Normal
	Simplex	—
	Others	Warning
Simplex	Duplex	—
	Simplex	Normal
	Others	Warning
Others	Duplex	Warning
	Simplex	Warning
	Others	—

“—”: No status is shown.

TIPS: Unless the hard disks make up a mirror, the Mirror Disk screen does not show any information.

IMPORTANT: The Mirror Disk screen shows a pair of hard disks constructing mirroring as a mirror. Note that when multiple volumes are created in these hard disks, the information on the volumes will not be displayed.

If multiple volumes are created within a single disk:



The screen shows information on a pair of hard disks that make up a mirror. It does not show information based on volumes (ex. Volume A, Volume B).

3. Recovery from a hard disk failure

If a hard disk breaks, the broken disk must be replaced immediately. This section describes alert reports and status shown by the DataViewer while disks are replaced to restore mirroring.

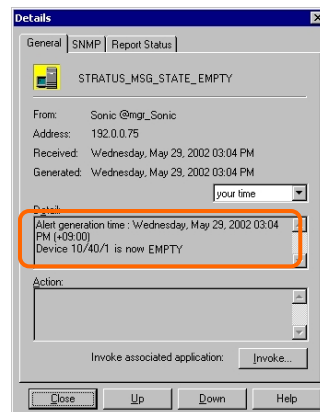
(1) Detecting problem of a hard disk

See [1. Verify of hard disk failure] above.

(2) Removing the hard disk

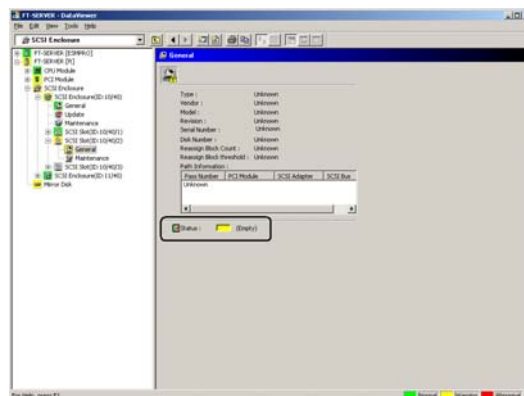
Disconnect the hard disk with the problem. At this time, NEC ESMPro Agent reports the following alert to manager. And icons related to the hard disk with problem change the state of warning in the DataViewer.

Since the hard disk has been removed, the status of the SCSI slot will be “EMPTY.”



TIPS: You can identify the new hard disk by DevicePathID (ex. 10/40/1).

When one hard disk with problem was disconnected, SCSI slot changes the status to “Warning.”

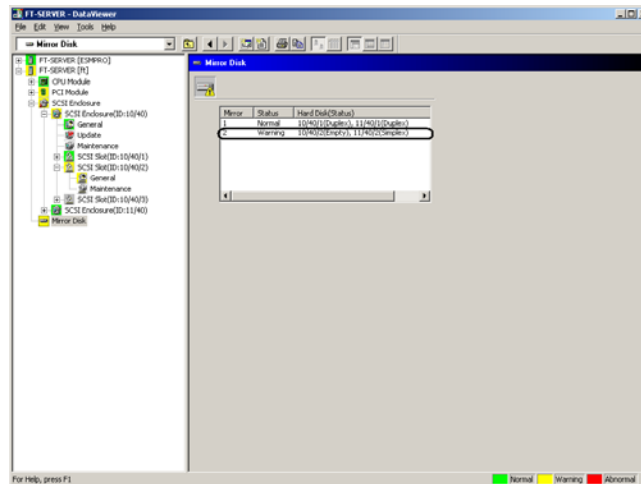


[SCSI Slot] → [General]

IMPORTANT: The status color of the SCSI slot differs depending on the connection of mirrored hard disks:

- If one of the mirrored disks was removed: Warning
- If both of the mirrored disks were removed: Gray

Also, at this time, the redundant status of mirrored disks is changed to “Warning.”

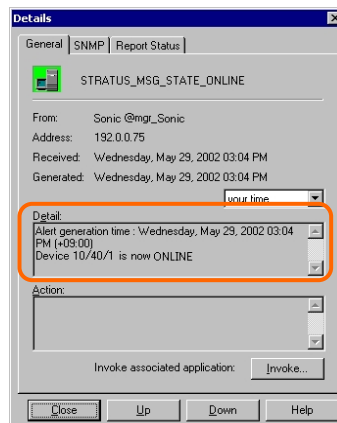


[Mirror Disk]

(3) Connect a new hard disk

Next, connect a new hard disk to the same SCSI Slot. At this time, NEC ESMPro Agent reports the following alert to manager. And icons related to the hard disk are changed to the state of normal in the DataViewer.

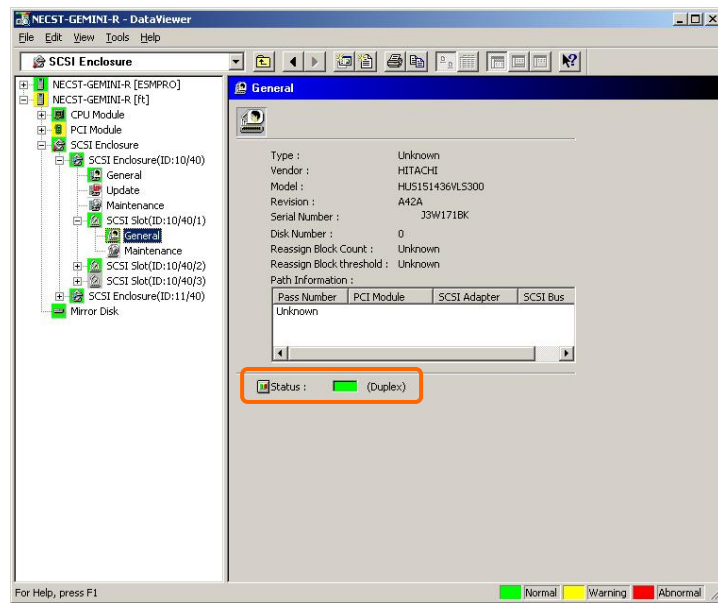
When the hard disk is connected, SCSI Slot changes the status to “ONLINE.”



[Alert report]

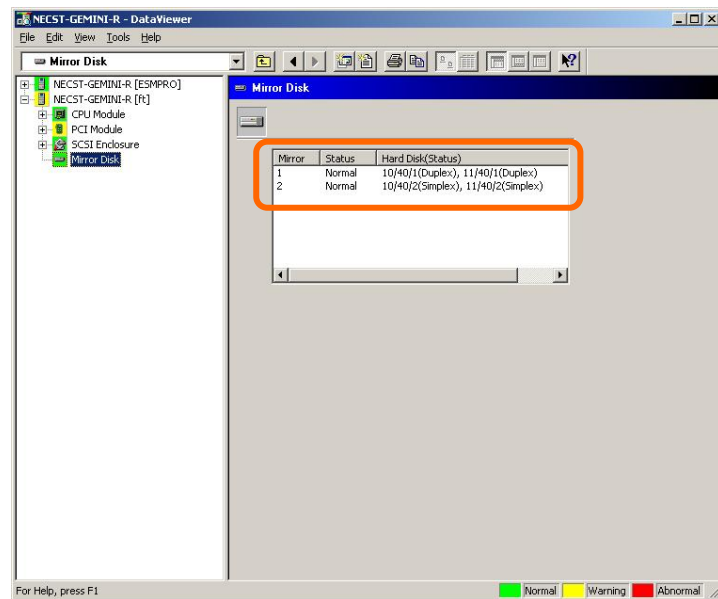
TIPS: You can identify the new hard disk by DevicePathID (ex. 10/40/1).

When the hard disk is connected, SCSI Slot changes the status to “Normal.”



[SCSI Slot] → [General]

Also, at this time, the state of the mirrored disks changes to “Normal.”



[Mirror Disk]

Maintenance of Fault Tolerant Server series

Fault Tolerant Server series maintenance can be done in two ways; one is to use NEC ESMPRO Manager for remote maintenance and the other is to use the NEC ESMPRO Agent ft server utility on the Fault Tolerant Server series for local maintenance.

TIPS: To start the NEC ESMPRO Agent ft server utility installed in the Fault Tolerant Server series, select the items as follows:

Start Menu→[Programs]→[NEC ESMPRO Agent]→[ft server utility]

The maintenance functions that can be executed from NEC ESMPRO include three types, those common to all components, those specific to particular components, and general system settings.

The maintenance functions common to all components are operated in the same way basically (the operation procedure and typical examples of screen images are described below).

The table below lists the availability of maintenance functions common to all components.

Component	Start		Stop		MTBF clear		Diagnosis		F/W update	
	R	L	R	L	R	L	R	L	R	L
CPU module	√	√	√	√	√	√	√	√	√	√
PCI module	√	√	√	√	√	√	√	√	—	—
PCI slot	—	—	—	—	—	—	—	—	—	—
Ethernet adapter	—	—	—	—	√	√	—	—	—	—
SCSI adapter	—	—	—	—	—	—	—	—	—	—
SCSI enclosure	—	—	—	—	—	—	—	—	—	—
SCSI electronics	—	—	—	—	—	—	—	—	—	—
SCSI slot	—	—	—	—	—	—	—	—	—	—

R: Remote. Executable from remote management PC by using NEC ESMPRO Manager

L: Local. Executable on local server by using ft server utility

√: Supported

—: Not supported

Note: The MTBF clear of SCSI adapter and Ethernet cannot be performed to built-in devices.

The table below shows the component-specific maintenance functions executable from NEC ESMPRO.

Component	Dump harvest		Dump harvest during system operation		Board switch	
	R	L	R	L	R	L
CPU module	–	√	√	√	√	√

R: Remote. Executable from remote management PC by using NEC ESMPRO Manager

L: Local. Executable on local server by using ft server utility

√: Supported

–: Not supported

Component	Bus reset		Change of primary SCSI bus	
	R	L	R	L
SCSI bus	–	√	–	–

R: Remote. Executable from remote management PC by using NEC ESMPRO Manager

L: Local. Executable on local server by using ft server utility

√: Supported

–: Not supported

The table below shows the support of the whole system setup functions.

Component	Quick dump		Auto firmware update		Auto module start	
	R	L	R	L	R	L
Whole system	–	√	–	√	–	√

R: Remote. Executable from remote management PC by using NEC ESMPRO Manager

L: Local. Executable on local server by using ft server utility

√: Supported

–: Not supported

The table below shows the support of the preventive disk maintenance (S.M.A.R.T.) setup function.

Component	Preventive disk maintenance (S.M.A.R.T.) setup	
	R	L
SCSI disk	–	–

R: Remote. Executable from remote management PC by using NEC ESMPRO Manager

L: Local. Executable on local server by using ft server utility

√: Supported

–: Not supported

Start and Stop of Components

To start or stop a component with NEC ESMPRO Manager, use the [Maintenance] tree of the component in the [ft] tree of the DataViewer. Open the tree of the component to be started or stopped and select the [Maintenance] tree.

To start or stop a component with the ft server utility, use the utility screen of the component.

The table below shows the common cases in which a component is to be started or stopped.

Component	Start		Stop	
	Remote	Local	Remote	Local
CPU Module	When the cause of down is reviewed and the system is restarted in module down state. Executable in any of the following module states (this can be viewed on manager screen): <ul style="list-style-type: none"> Removed Broken Shot Firmware Update Complete Diagnostics Passed 	When the cause of down is reviewed and the system is restarted in module down state. Executable in the following module state: <ul style="list-style-type: none"> When the status LED 1 is amber and the status LED 2 is off Only the status LED illuminates amber when the module is in one of the following states: <ul style="list-style-type: none"> Removed Broken Shot Firmware Update Complete Diagnostics Passed 	When system is stopped forcibly due to replacement or malfunction of module. Executable in the following module state (this can be viewed on manager screen): <ul style="list-style-type: none"> Duplex 	When system is stopped forcibly due to replacement or malfunction of module. Executable in the following module state: <ul style="list-style-type: none"> Only the green LED is on and in redundant configuration state The both green LEDs are on when the module is in the following state: <ul style="list-style-type: none"> Duplex
PCI Module	Same as above	Same as above	Same as above	Same as above
SCSI Slot	—	—	—	—

Remote: Executable from remote management PC by using NEC ESMPRO Manager

Local: Executable on local server by using ft server utility

—: Not supported

IMPORTANT: PCI modules, SCSI adapters, SCSI buses, and modules under the SCSI enclosure have impact on each other. You need to be aware of this, for example, when you replace a PCI module. For details, see “Impact When Module Status Changes” described earlier in this chapter.

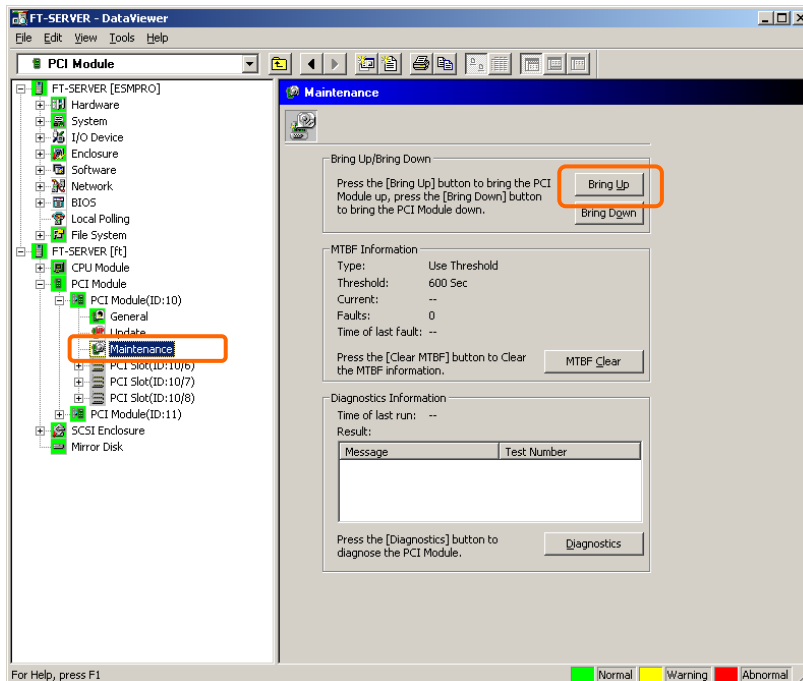
Procedure in NEC ESMPRO Manager

Start

1. Select the target component in the [ft] tree.
2. Check the current state with the “Status” display on the target component screen.
3. Click the [Bring Up] button in the [Maintenance] screen for the target component.

A certain time is required for the start.

The start result can be verified by “State” on the target component screen. The result of the start operation is reported by the Fault Tolerant Server series as an alert.



Stop

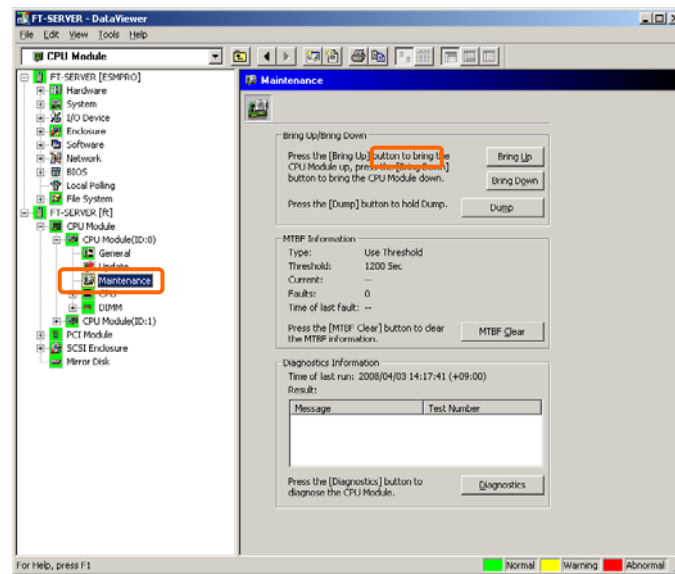
Perform the procedure below before replacing a component.

1. Select the target component in the [ft] tree.
2. Check the current state with the “State” display on the target component screen.
3. Click the [Bring Down] button in the [Maintenance] screen for the target component.

A certain time is required for the stop.

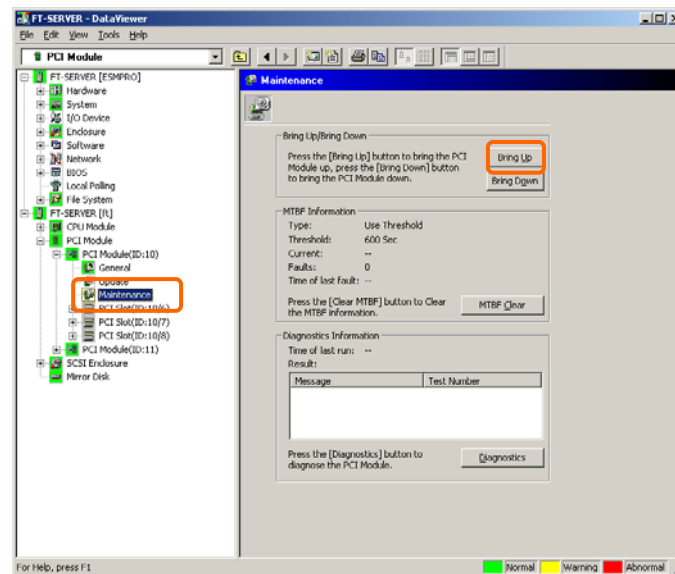
The stop result can be verified by “State” on the target component screen. The result of the stop operation is reported by the Fault Tolerant Server series as an alert.

Sample screen of NEC ESMPRO Manager 1



[Maintenance] screen of PCI module
[CPU Module] - [CPU Module] - [Maintenance]

Sample screen of NEC ESMPRO Manager 2



[Maintenance] screen of PCI module
[PCI Module] - [Maintenance]

Procedure in the ft server utility

Start

1. Select the target component by using the ft server utility.
2. Check the current state of the target component with the LEDs.
3. Click the [Up] button of the target component.

A certain time is required for the start.

The start result can be verified by the LEDs on the target component. The result of the start operation is registered in the event log.

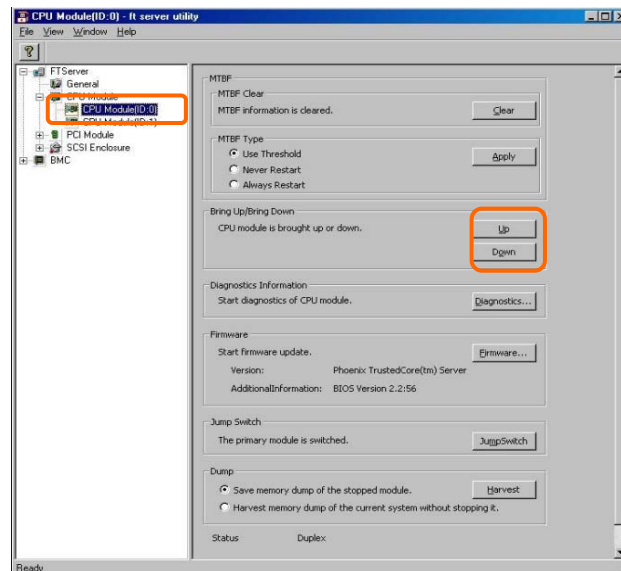
Stop

1. Stop before replacing components.
2. Select the target component by using the ft server utility.
3. Check the current state of the target component with the LEDs.
4. Click the [Down] button of the target component.

A certain time is required for the start.

The start result can be verified by the LEDs on the target component. The result of the start operation is registered in the event log.

Sample screen of ft server utility



Check and Clear of MTBF Information

The MTBF information of a component can be viewed or cleared (initialized).

Fault Tolerant Server series manages the MTBF (mean time between failure) of each component. If a fault occurs in a component, the Fault Tolerant Server series calculates the MTBF of the component again. If the calculated value is lower than the pre-defined threshold, the Fault Tolerant Server series disables the component to be used.

Contact your maintenance personnel if such a symptom as above occurs.

IMPORTANT: A disabled component with the MTBF lower than the threshold can be forcibly enabled by clearing the MTBF. However, contact your maintenance personnel for the forced use of such a component.

To clear the MTBF information of a component with NEC ESMPRO Manager, use the [Maintenance] tree of the component of the [ft] tree of the DataViewer. Open the tree of the component whose MTBF information is to be cleared and select the [Maintenance] tree.

To clear the MTBF information of a component with the ft server utility, use the utility screen of the component. The table below shows the potential cases in which the MTBF information of a component is to be cleared. Contact your maintenance personnel for clearing MTBF information.

Component	MTBF clear	
	Remote	Local
CPU Module	To start the module forcibly after replacing a module or if MTBF became lower than the threshold due to malfunction and disabled the module. Executable in the following module state (this can be viewed on manager screen): <ul style="list-style-type: none"> Broken MTBF is lower than the threshold.	To start the module forcibly after replacing a module or if MTBF became lower than the threshold due to malfunction and disabled the module. Executable in the following module state: <ul style="list-style-type: none"> The amber LED is on. The event indicating that MTBF is lower than the threshold is registered in the event log.
PCI Module	Same as above	Same as above
Ethernet Adapter	To start the module/component forcibly after replacing a module or if MTBF became lower than the threshold due to malfunction and disabled the module/component. Executable in the following module state (this can be viewed on manager screen): Broken MTBF is lower than the threshold.	To start the module/component forcibly after replacing a module or if MTBF became lower than the threshold due to malfunction and disabled the module/component. Executable in the following module state (this can be viewed on manager screen): <ul style="list-style-type: none"> The amber LED is on. The event indicating that MTBF is lower than the threshold is registered in the event log.
SCSI Adapter	—	—

IMPORTANT: You can also clear MTBF information for the PCI module, Ethernet Adapter and SCSI Adapter by unplugging and plugging the live wire of the PCI module.

Component	MTBF clear	
	Remote	Local
SCSI Enclosure	—	—
SCSI Electronics	—	—
SCSI Slot	—	—

Remote: Executable from remote management PC by using NEC ESMPRO Manager

Local: Executable on local server by using ft server utility

—: Not support

Procedure in NEC ESMPRO Manager

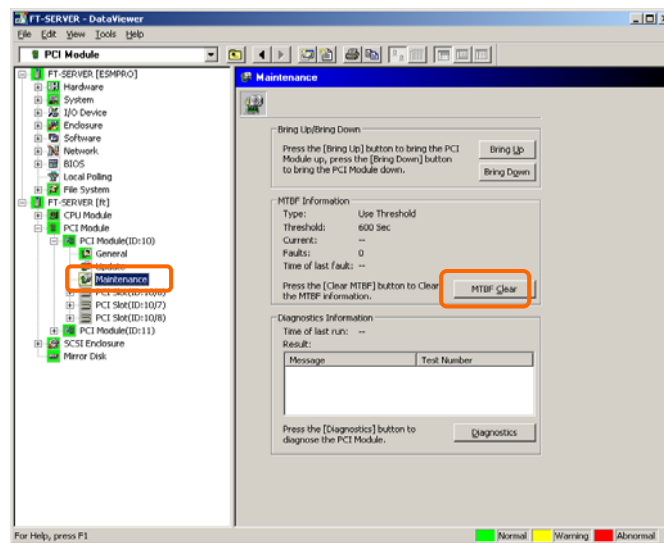
Perform the procedure below before replacement of a component.

1. Select the target component in the [ft] tree.
2. Check the current state with the “State” display on the target component screen.
3. Click the [MTBF Clear] button in the [Maintenance] screen for the target component.

The MTBF clearing result can be verified by “State” on the target component screen. The result of the MTBF clearing operation is reported by the Fault Tolerant Server series as an alert.

4. Start the component.

Sample screen of NEC ESMPRO Manager



[Maintenance] screen of SCSI enclosure
[PCI module] – [Maintenance]

Procedure in the ft server utility

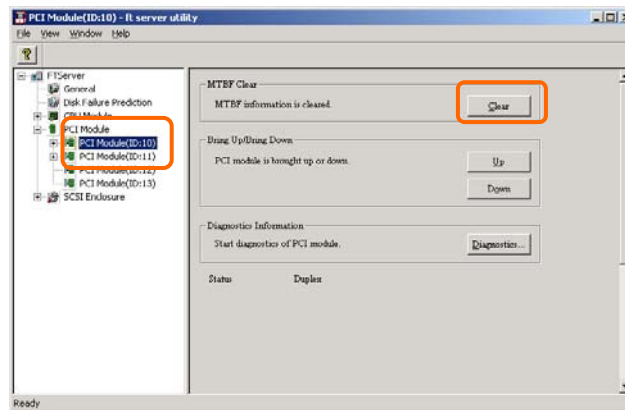
Perform the procedure below before replacement of a component.

1. Select the target component by using the ft server utility.
2. Check the current state of the target component with the LEDs and event log.
3. Click the [Clear] button in [MTBF Clear] of the target component.

The MTBF clearing result can be verified by the LEDs on the target component. The result of the MTBF clearing operation is registered in the event log.

4. Start the component.

Sample screen of ft server utility



[PCI Module]

Diagnostics

The Fault Tolerant Server series provides the self-check diagnosis function for some components. If a fault occurs in a component, the Fault Tolerant Server series can diagnose the component to detect the fault.

To diagnose a component with the NEC ESMPRO Manager, use the [Maintenance] tree of the component in the DataViewer. Open the tree of the component to be diagnosed and select the [Maintenance] tree.

To diagnose of a component with the ft server utility, use the utility screen of the component.

The table below shows the potential cases in which a component is to be diagnosed.

Component	Diagnosis	
	Remote	Local
CPU Module	<p>When a phenomenon causing the module to be down occurs or a phenomenon supposed to be a malfunction occurs.</p> <p>Executable in any of the following module states (this can be viewed on manager screen):</p> <ul style="list-style-type: none"> • Removed • Broken • Shot • Firmware Update Complete <p>To diagnose the module under operation, bring down the module before the diagnosis.</p>	<p>When a phenomenon causing the module to be down occurs or a phenomenon supposed to be a malfunction occurs.</p> <p>Executable in any of the following module states:</p> <ul style="list-style-type: none"> • When the status LED 1 is red and the status LED 2 is off <p>Only the status LED 1 illuminates amber when the module is in one the following states:</p> <ul style="list-style-type: none"> • Removed • Broken • Shot • Firmware Update Complete (no fault found by diagnosis) <p>To diagnose the module under operation, bring down the module before the diagnosis.</p>
PCI Module	Same as above	Same as above

Remote: Executable from remote management PC by using NEC ESMPRO Manager

Local: Executable on local server by using ft server utility

–: Not support

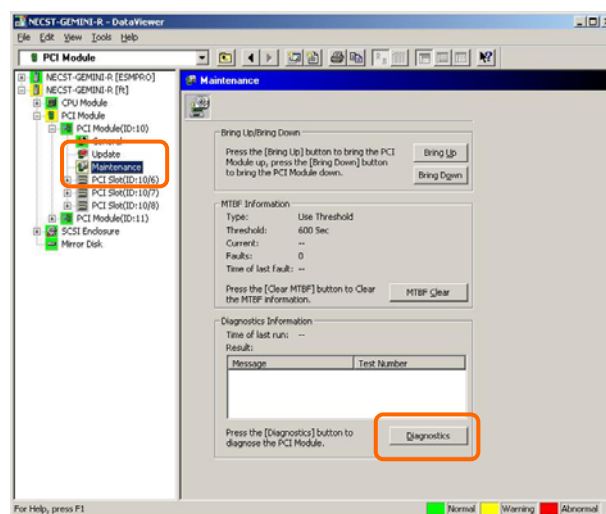
Procedure in NEC ESMPRO Manager

1. Select the target component in the [ft] tree.
2. Check the current state with the “State” display on the target component screen. If the component is operating, stop the component.
3. Click the [Diagnostics] button in the [Maintenance] screen for the target component.

The diagnosis result can be verified by “Result” of the diagnosis on the target component screen. The result of the diagnosis is reported by the Fault Tolerant Server series as an alert.

The result of diagnosis executed last is displayed in the [Diagnosis Information] column. In addition, if a fault is detected by the result of the diagnosis, the state of the [General] tree of the component is changed.

Sample screen of NEC ESMPRO Manager



[Maintenance] screen of PCI module
[PCI Module] – [Maintenance]

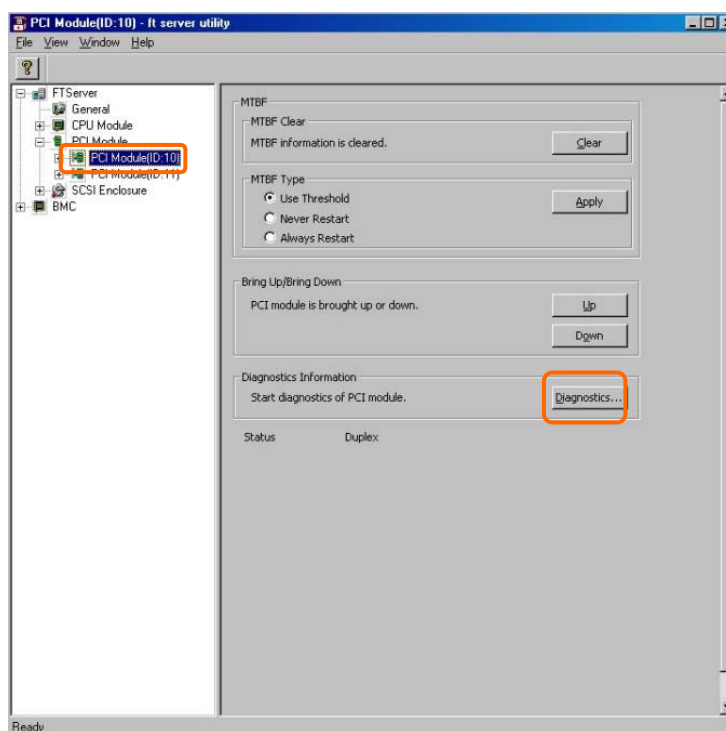
Procedure in the ft server utility

1. Select the target component by using the ft server utility.
2. Check the current state of the target component with the LEDs. If the component is operating, stop the component.
3. Click the [Diagnostics] button in the [Diagnosis Information] on the target component.

The diagnosis result can be verified by the LEDs on the target component. The result of the diagnosis is registered in the event log.

4. Start the component.

Sample screen of ft server utility



[PCI Module]

Firmware Update

Fault Tolerant Server series can update firmware (including BIOS) if some hardware components operate in the online state (in which the system continues the operation but the component trying to update firmware or BIOS is stopped).

To update firmware with NEC ESMPRO Manager, use the [Update] tree of the component in the DataViewer. Open the tree of the component for which firmware is updated and select the [Update] tree.

To update the firmware of a component with the ft server utility, use the utility screen of the component.

To update the firmware of a component, the firmware image file of the firmware for update must previously be stored in the managed server. On the firmware update screen, specify the path to the firmware image file for update.

The table below shows the potential cases in which the firmware of a component is to be updated.

Component	Firmware update	
	Remote	Local
CPU Module	<p>When BIOS must be updated to new one. Executable in any of the following module states (this can be viewed on manager screen):</p> <ul style="list-style-type: none"> • Removed • Broken or forced stop • No fault found by diagnosis <p>To update the module under operation, bring down the module before the update.</p>	<p>When BIOS must be updated to new one. Executable in the following module state:</p> <ul style="list-style-type: none"> • When the status LED 1 is amber and the status LED 2 is off <p>Only the status LED 1 illuminates amber when the module is in one of the following states:</p> <ul style="list-style-type: none"> • Removed • Broken or forced stop • No fault found by diagnosis (Firmware Update Complete) <p>To update the module under operation, bring down the module before the update.</p>

Remote: Executable from remote management PC by using NEC ESMPRO Manager

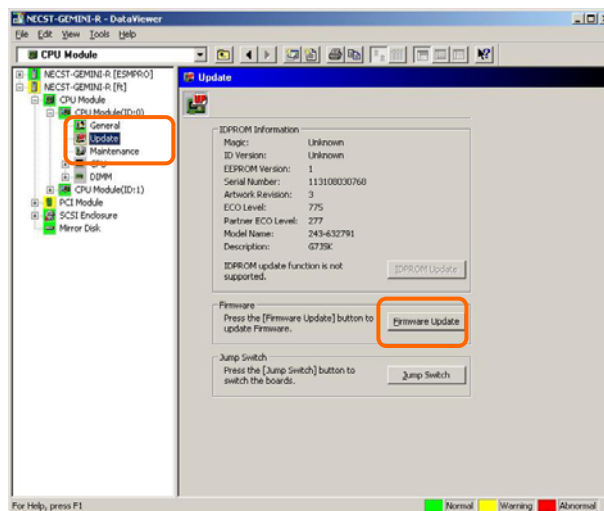
Local: Executable on local server by using ft server utility

—: Not support

Procedure in NEC ESMPRO Manager

1. Save the image data of the update firmware in an arbitrary directory of the Fault Tolerant Server series.
Save the image data in any way. Write down the path to the directory in which the image data is saved.
2. Select the target component in the [ft] tree.
3. Check the current state with the “State” display on the target component screen. If the component is operating, stop the component.
4. Click the [Firmware Update] button in the [Update] screen for the target component.

Sample screen of NEC ESMPRO Manager

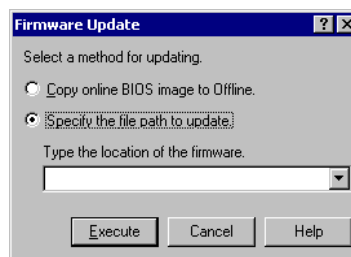


[Update] screen of CPU module
[CPU Module] – [Update]

5. Select [Specify the file path to update], enter the directory in which the updated firmware specified in the input box in step 1 is saved, and click the [Execute] button.

Perform the firmware update.

The update result can be verified by the state on the target component screen (indication of “Firmware update completed”). The result of the update processing is reported by the Fault Tolerant Server series as an alert.

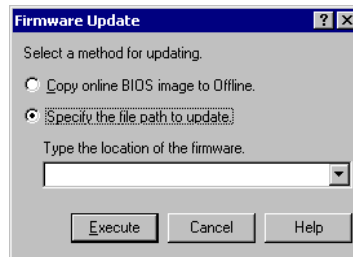


6. After the BIOS for a single CPU module is completed, click the [Jump Switch] button. The module completely updated is started and the active module is stopped.

7. Start the other module stopped.

Starting the module causes the firmware to be updated automatically. However, if the [Enable automatic firmware update] property is invalid, update the module in the procedure as follows:

- (1) Check the current state with the “State” display on the target component screen. If the component is operating, stop the component.
- (2) Click the [Firmware Update] button in the [Update] screen for the target component.
- (3) Select the update method in the [Firmware Update] dialog box and click the [Execute] button.
- (4) Start the module.



Even if you do not have the image data of firmware for update, the firmware can be copied from the other module.

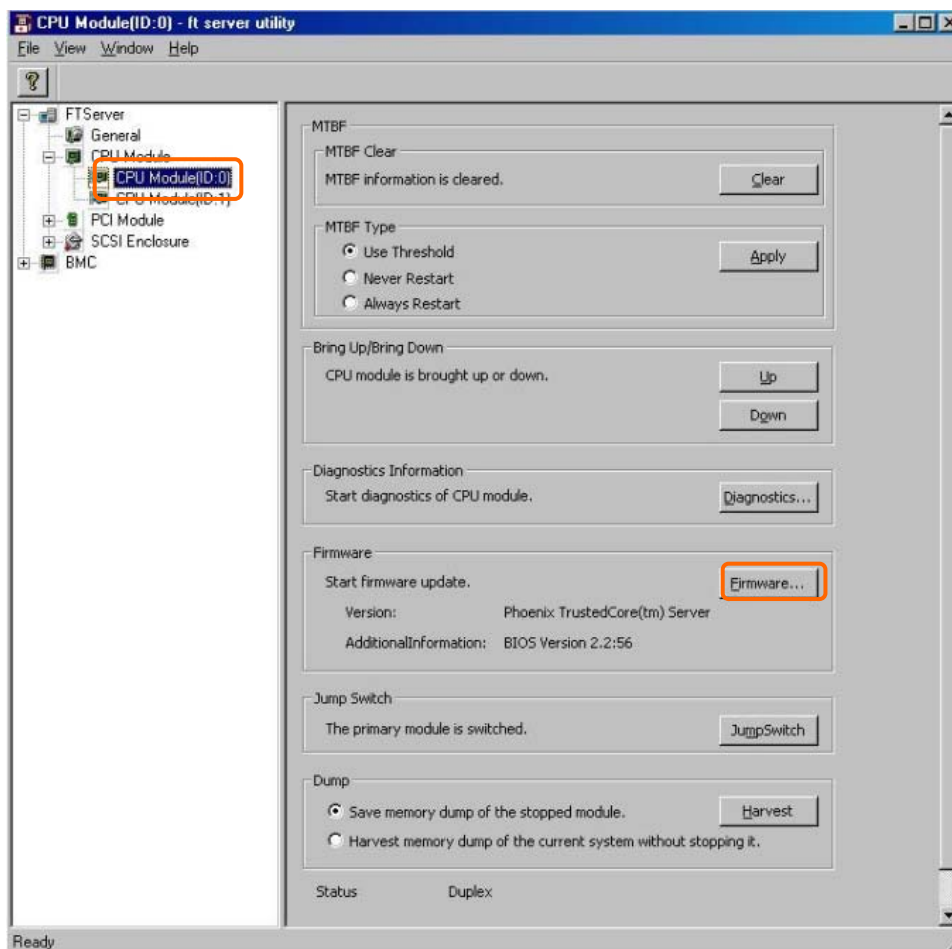
By starting the module, the firmware will be updated automatically. However, when the [Enable automatic firmware update] property is disabled, follow the steps below to update the firmware:

- 1.** Start the system using the module of the firmware copy source.
See the current status by the “Status” indication on the target component screen of the copy destination and verify that it is stopped.
- 2.** On the [Update] screen of the target component, click [Firmware update].
- 3.** When a firmware updating dialog appears, check [Copy online BIOS image to Offline] and execute it.
Firmware is updated by copying the firmware on the online side to the offline side.
- 4.** Start the stopped module.

Procedure in ft server utility

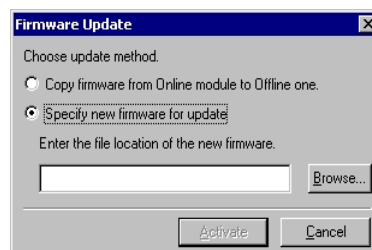
1. Save the image data of the update firmware in a desired directory of the Fault Tolerant Server series.
Save the image data in some manner. Write down the path to the directory in which the image data is saved.
2. Select the target component with the ft server utility.
3. Check the current state of the target component with the LEDs. If the component is operating, stop the component.
4. Click the [Firmware...] button for the target component.

Sample screen of ft server utility



[CPU Module]

5. Select [Specify new firmware for update], enter the directory in which the updated firmware specified in the input box in step 1 is saved, and click the [Activate] button. Perform the firmware update.

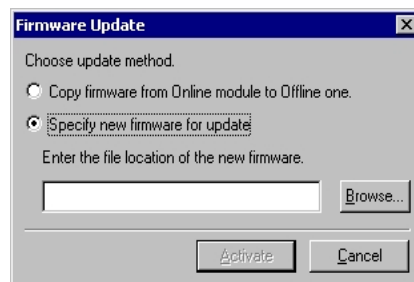


6. Check the update result with the event log.
7. After the BIOS for a single CPU module is completed, click the [Jump Switch] button.
The module completely updated is started and the module under operation is stopped.

8. Start the other inactive module.

Starting the module causes the firmware to be updated automatically. However, if the [Enable automatic firmware update] property is disabled, update the module in the procedure as follows:

- (1) Check the current state with the “State” display on the target component screen. If the component is operating, stop the component.
- (2) Click the [Firmware...] button for the target component.
- (3) Select the update method in the [Firmware Update] dialog box and click the [Activate] button.
- (4) Start the module.



Even if you do not have the image data of firmware for update, the firmware can be copied from the other module.

By starting the module, the firmware will be updated automatically. However, when the [Enable automatic firmware update] property is disabled, follow the steps below to update the firmware:

1. Start the system using the module of the firmware copy source.
See the current status by the “Status” indication on the target component screen of the copy destination and verify that it is stopped.
2. Click the [Firmware...] button for the target component.
3. When a firmware updating dialog appears, check [Copy firmware from Online module to Offline one] and execute it.
Firmware is updated by copying the firmware on the online side to the offline side.
4. Start the stopped module.

Dump Collection

To collect the dump file with NEC ESMPRO Manager, use [CPU Module] → [Maintenance] tree in the DataViewer.

To collect the dump with the ft server utility, use the utility screen of the component.

IMPORTANT: Acquire the dump only for the examination of a fault.

The dump can be collected in two ways. In each way, the dump file is collected with the same path and file name “%SystemDrive%\NECDump\MEMORY.DMP” as the dump file of the OS standard.

■ Collecting dump of inactive module

The dump is acquired from the inactive CPU module (due to the occurrence of a fault or forced stop).

■ Collecting dump under system operation

Either of the CPU modules is entered into the offline state and the dump is collected during system operation. After the acquisition, the CPU module is returned to the online state again. This can be done only in the duplex system.

The table below shows the potential cases in which the dump is acquired.

Component	Saving dump of stopped module		Saving dump of component under system operation	
	Remote	Local	Remote	Local
CPU Module	–	When a fault or malfunction occurs in the system. Save the dump if requested by maintenance personnel. Executable in the following module state: <ul style="list-style-type: none"> • The amber LED is on However, this function operates only in a fault state. An execution error occurs in any other cases. The amber LED is on when the module is in one of the following states: <ul style="list-style-type: none"> • Removed • Broken • Shot • Firmware Completion of update • No fault found by diagnosis 	When a fault or malfunction occurs in the system. Save the dump if requested by maintenance personnel. Executable in the following module state (this can be viewed on manager screen): <ul style="list-style-type: none"> • Duplex 	When a fault or malfunction occurs in the system. Save the dump if requested by maintenance personnel. Executable in the following module state: <ul style="list-style-type: none"> • When only the green LED is on and the module is in redundant configuration state Only the green LED is on when the module is in the following state: <ul style="list-style-type: none"> • Duplex

Remote: Executable from remote management PC by using NEC ESMPRO Manager

Local: Executable on local server by using ft server utility

–: Not support

Procedure in NEC ESMPRO Manager

The [Dump] button of NEC ESMPRO Manager performs the function of “saving dump during system operation.”

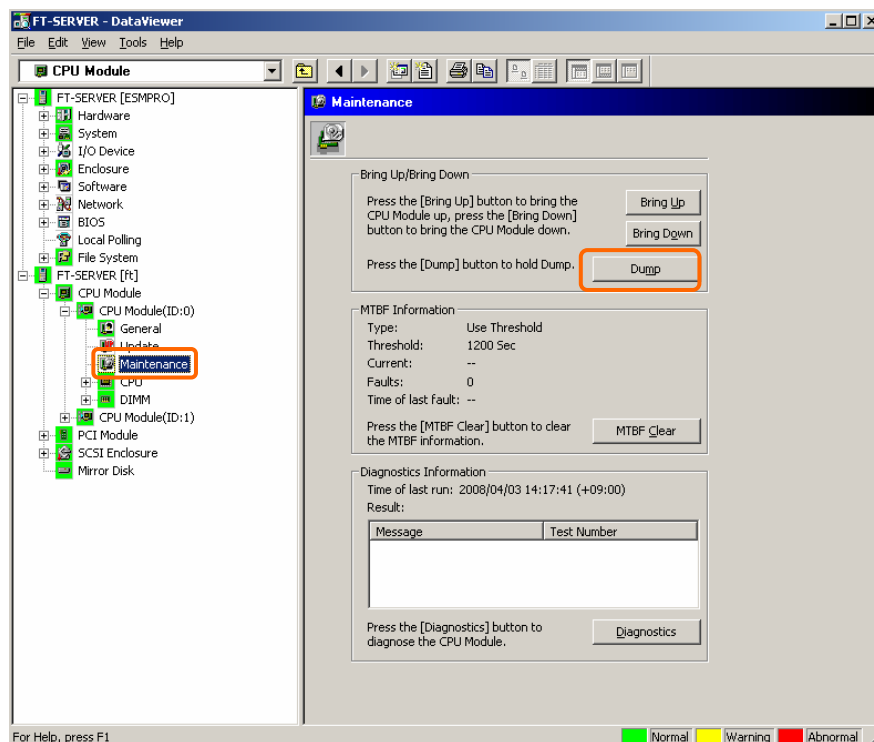
1. Select [CPU Module] in the [ft] tree.
2. Check the current state with the “State” display on the target component screen.
3. Click the [Dump] button in the [Maintenance] screen for the target component.

A certain time is required for the dump saving.

The dump is stored as %SystemDrive%\NECDump\MEMORY.DMP on the managed server.

The result of the dump saving is reported by the Fault Tolerant Server series as an alert.

Sample screen of NEC ESMPRO Manager



[Maintenance] screen of CPU module
[CPU Module] – [Maintenance]

Procedure in ft server utility

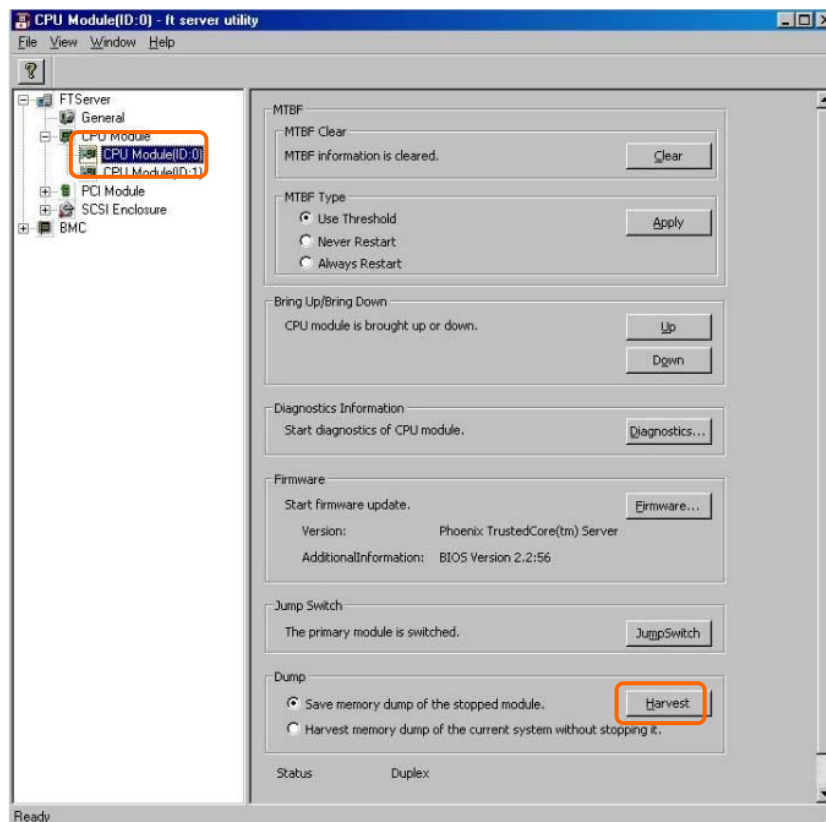
1. Select the target CPU module by using the ft server utility.
2. Check the current state of the target CPU module with the LEDs.
3. Select the dump acquisition method with [Dump] of the target CPU module and click the [Harvest] button.

A certain time is required for the dump acquisition.

The dump is stored as %SystemDrive%\NECDump\MEMORY.DMP on the server.

The result of the dump acquisition can be verified in the event log.

Sample screen of ft server utility



[CPU Module]

Setup of System Operation

The following properties can be set as the operation setup of the whole system.

■ Quick dump

If this property is enabled (by checking “Enable” on the setup screen), the dump is acquired in parallel with the system startup if a fault occurs in the system. If this property is disabled, the dump is acquired by the dump function normally provided by OS.

The initial setup value is “Enable.”

■ Auto firmware update

If a new CPU module containing BIOS different from that of the existing CPU module in version with this property being enabled (by checking “Enable” on the setup screen), the BIOS of the new CPU module is updated to the BIOS of the existing CPU module to match with each other. If this property is disabled, the BIOS of the new CPU module is not update automatically.

The initial setup value is “Enable.”

■ Auto module start

If this property is enabled (by checking “Enable” on the setup screen), the CPU or PCI module newly inserted is automatically started to be operable. If this property is disabled, the module is not started automatically.

The initial setup value is “Enable.”

IMPORTANT:

In the Fault Tolerant Server series with ft control software over 3.0, it is always necessary to set “Enable.” Do not set “Disable.”

The system operation can be set on [ft] tree→[General] screen of the ft server utility.

The table below shows the potential cases in which the system operation setup is changed. Contact your maintenance personnel for the change of the system operation setup. Setting change will take effect after system reboot. However, the utility does not indicate that reboot is required.

Component	Quick dump		Auto firmware update		Auto module start	
	Remote	Local	Remote	Local	Remote	Local
Whole system	–	Executable if the system is operating. When dump is acquired by using the dump function normally installed in OS at occurrence of system fault.	–	Executable if the system is operating. When firmware is updated manually at insertion of new CPU module	–	Executable if the system is operating. When firmware is updated manually at insertion of new CPU/PCI module

Remote: Executable from remote management PC by using NEC ESMPRO Manager

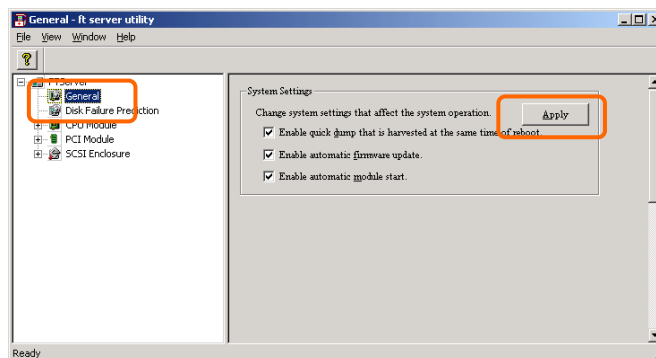
Local: Executable on local server by using ft server utility

–: Not supported

Configure the system settings using the ft server utility in the following procedure. The system cannot be configured using the NEC ESMPRO Manager.

1. Select [General] in the [ft] tree.
2. Check the property of carrying out the modification with [System Settings] (or cancel the check).
3. Click the [Apply] button.

Sample screen of ft server utility



Refresh of View based on State Change Alert Setting

A new function is supported so that NEC ESMPRO Manager window will be updated on a system state change basis (in other words, whenever necessary). This function is OFF by default. See the [Setting] below about how to turn it ON.

NEC ESMPRO Manager window is updated by one minute-interval polling by default. Therefore, there is some time-lag for NEC ESMPRO Manager to recognize changes in NEC Agent. By using this function, the time-lag can be reduced. However, it may consume a little bit more network band width since each state change will be notified to NEC ESMPRO Manager as some kind of alert.

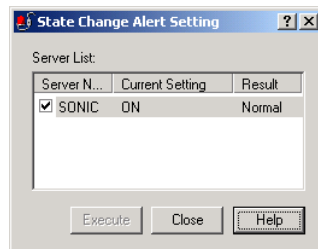
[Setting]

1. Select [Program] - [NEC ESMPRO Manager] from the Start menu and click [Manager Settings].



[Manager Settings] dialog box

2. Check [Enable the State Change Alert Setting].
3. Click the [Agent Setting...] button.



[State Change Alert Setting] dialog box

4. Check the name of servers sending the state change alert to the Manager when the Agent recognizes changes in the state.

Click the [Execute] button for the setting change to take effect.

BMC Firmware Update

The firmware of the BMC on the PCI module can be updated.

The BMC firmware can be updated by using the ft server utility.

To update the BMC firmware, the firmware image file must previously be updated on the managed server. On the BMC firmware update screen, specify the path of the image file of the firmware to be updated.

IMPORTANT: Contact your maintenance engineer for the update of the BMC firmware.

Component	BMC firmware update	
	Remote	Local
BMC	—	When update to new firmware is required.

Remote: Executable from remote management PC by using NEC ESMPRO Manager

Local: Executable on local server by using ft server utility

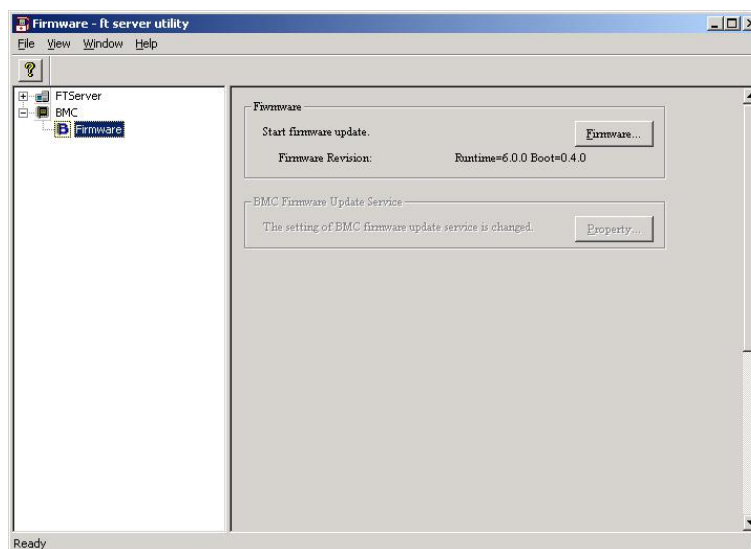
—: Not supported

Procedure of Update from ft server utility

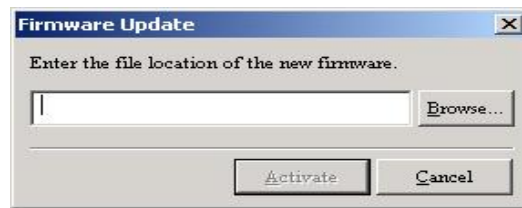
Update the firmware in the following procedure.

1. Click [Firmware] - [Firmware...].

[Firmware Update] dialog box appears.



2. Enter the location to store the new firmware, and click [Activate].
[Verification] dialog box appears.



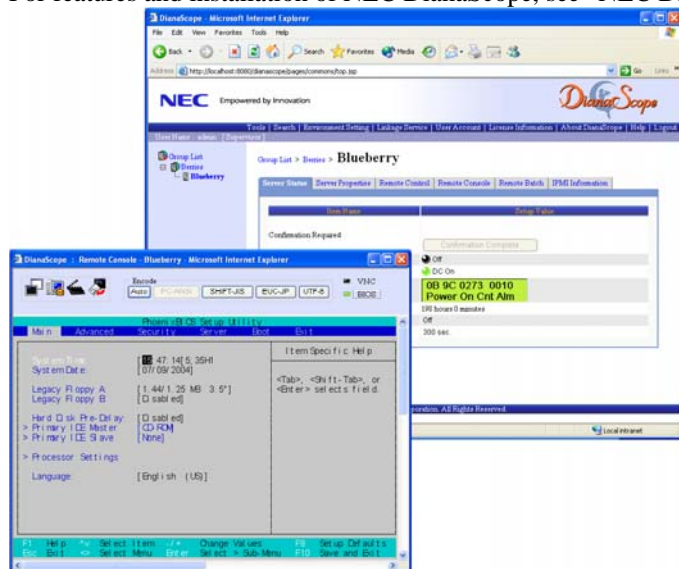
3. Click [OK].
Execute the firmware update.



NEC DianaScope

NEC DianaScope is software for remote management of Fault Tolerant Server series.

For features and installation of NEC DianaScope, see “NEC DianaScope Online Document” in “EXPRESSBUILDER.”



TIPS:

To use NEC DianaScope with Fault Tolerant Server series, appropriate server license is required.

- UL1198- 001E DianaScope Additional Server License (1)
License for managing one server.
- UL1198- 011E DianaScope Additional Server License (10)
License for managing ten servers.

ft remote management card comes with one license of NEC DianaScope.

Notes

The online document provides general descriptions of overall servers to be remotely managed by NEC DianaScope, but this section indicates notes that require special attention for remotely managing this server using NEC DianaScope.

- Fault Tolerant Server series can be managed remotely only when ft remote management card is installed.
- When remotely managing this server from NEC DianaScope, only LAN connection is available. Direct connection and connection via modem are not supported.
- NEC DianaScope cannot power off, power cycle or reset the server. Fault Tolerant Server series does not support such functions.

Active Upgrade

This section describes Active Upgrade process.

Introduction

Active Upgrade process allows you to upgrade system and application software while the important applications on a Fault Tolerant Server series system are online and available to users.

This section describes the overview of Active Upgrade process, the procedure and prerequisites necessary for preparing the system for the upgrade process, and configuring and performing the upgrade process with Active Upgrade Console. It also describes the troubleshooting when a problem occurs in Active Upgrade process.

TIPS:

The information described in this section is also included in the [Active Upgrade Help] file. You can find it in the [ftSys] folder from [Start] menu on the Active Upgrade Console and your system (after installing Active Upgrade software).

CAUTION:

The ft remote management card (F-RMC), is required to use Active Upgrade.

Overview

Active Upgrade™ technology allows you to upgrade system and application software on a Fault Tolerant Server series system with minimal downtime.

Instead of taking your system offline to run upgrade procedures, you can use Active Upgrade technology to split the system into two independently running systems, one “side” of which you upgrade while the other “side” continues to run your applications without interruption.

To learn more about Active Upgrade technology, see the following topics:

- “Features” on this page.
- “Active Upgrade Process” on page 5-70

Features

Active Upgrade technology enables the following:

- Install software updates with minimal disruption to your critical applications.

The applications required for the server operation continue to run on one side of the system while you install software on, and even restart, the other side. There is only a brief disruption when you are finished installing updates, as your critical applications are restarted on the upgraded software.

- Test the latest software updates in your environment **before** making the updates permanent.

After your critical applications are restarted on the upgraded software, you can verify the success of your software updates in a production environment, with real users and system load. If you want to keep the changes, there is no additional downtime. Otherwise, as quickly as your system can restart, you can abort the upgrade to go back to the original version of your software.

- Abort the upgrade process at any point up until you commit the changes.

If, for any reason, you are not satisfied with an upgrade, you can abort the upgrade session to return the system to its original state. Nothing is permanent until you choose to commit the changes. (Also, there might be no disruption to your critical applications if you abandon the upgrade early in the upgrade process, before testing the software in your production environment).

TIPS:

Active Upgrade Process, page 5-70

Software Upgrade Support, page 5-77

Prerequisites, page 5-78

Active Upgrade Process

The Active Upgrade process involves the following basic steps:

1. You prepare your system to ensure it meets the prerequisites of the Active Upgrade process.
2. You use the Active Upgrade Console to select the disks that will be affected by the software upgrade and to provide information about any applications or services that require special handling during the upgrade process.
3. You run a readiness check in the Active Upgrade Console to verify that your system meets the prerequisites for the Active Upgrade process.
4. You start the upgrade process by initiating *split mode*, which divides the fault-tolerant, duplexed system (Figure 1) into two independent, simplexed systems (Figure 2) — a *Production Side*, which continues to run your applications, and an *Upgrade Side*, on which you can run software installation packages.

Figure 1 Duplexed System

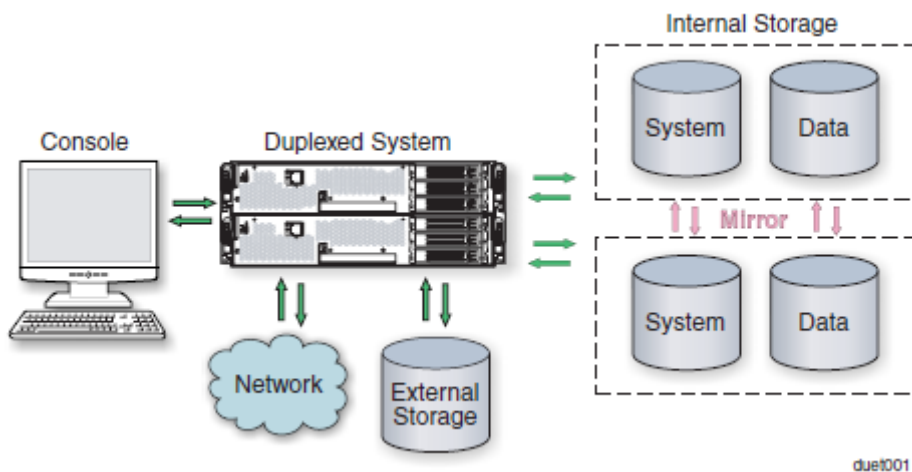
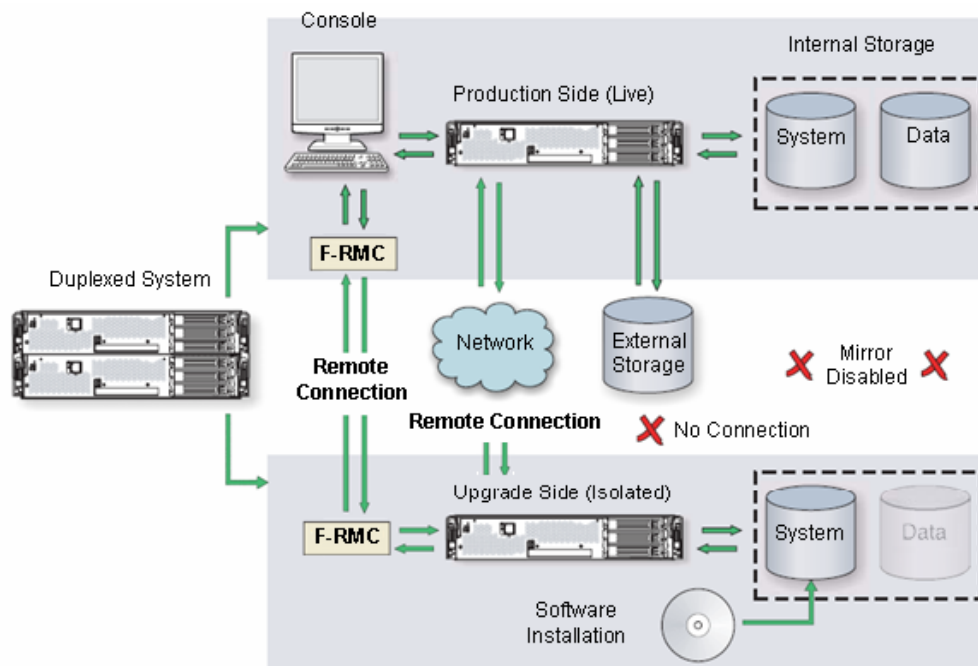


Figure 2. Splitting the System



When you split the system, the Active Upgrade Console disables any Rapid Disk ReSync (RDR) mirroring between the internal disks in each CPU/IO module enclosure and isolates the Upgrade Side from system resources such as the network, any user-specified application data disks, and any external PCI resources (such as external storage). It also disables user-specified applications and services on the Upgrade Side so they cannot restart if you restart the Upgrade Side.

Meanwhile, the Production Side retains access to system resources and continues to run your applications uninterrupted.

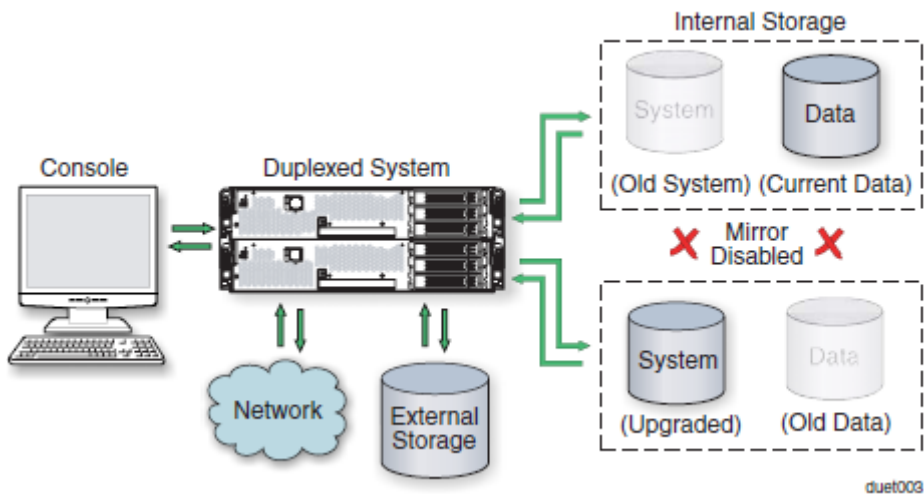
- After the system successfully enters split mode, you establish a remote connection to the Upgrade Side of the system through the private network that exists between ft remote management cards and between Ethernet PCI adapters in each CPU/IO module enclosure. Using this remote connection, you can perform any of the following upgrade tasks **on the Upgrade Side**:

- Run software installation utilities and updaters (see “Software Upgrade Support” on page 5-77 for restrictions).
- Restart the operating system, if necessary.
- Perform limited testing of the installed updates (the Upgrade Side has no access to the network, external storage, or application data disks during this stage).

You can also completely abort the upgrade from the Active Upgrade Console, if necessary.

- When you are finished installing software on the Upgrade Side, you disconnect the remote connection to the Upgrade Side and initiate the *merge* process.

When you merge the system, the Active Upgrade Console stops your applications on the Production Side and unmounts any application data disks to ensure that pending disk updates are flushed to disk. It then merges system resources so that the network, external storage, and application data disks become available to the whole system again. With the exception of the internal disks, all critical system resources return to duplex mode.

Figure 3. Merged System

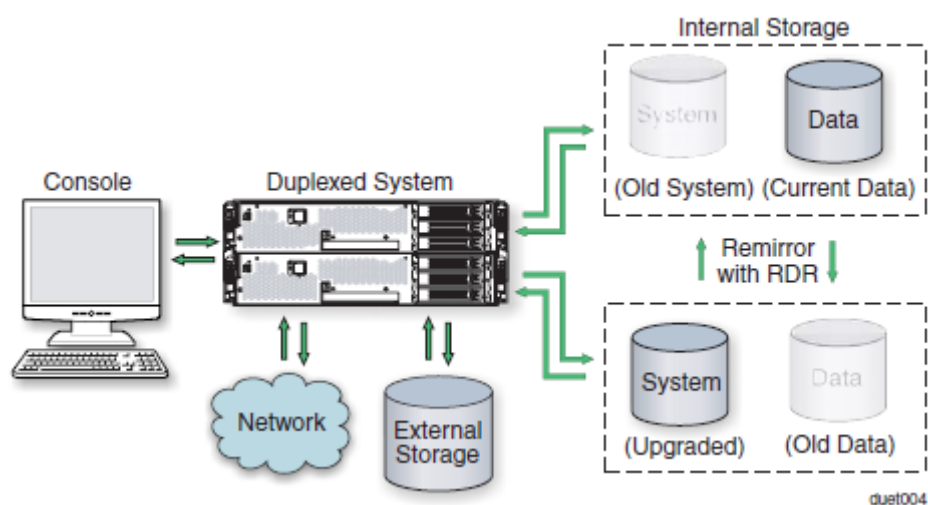
Finally, the system restarts your applications, including the Active Upgrade Console, from the Upgrade Side system disk. Depending on the complexity of your applications and the upgrade you performed, your applications may be backed up and running in under a minute.

7. After the system is successfully merged, you can test your applications and verify the success of your upgrade(s) with full access to the system's resources. If you discover a problem, you can still abort the upgrade process and restore the system to its previous state, because the original copy of your system disk (on the Production Side) has not been overwritten yet.
8. When you are certain that the upgrade(s) were successful, you can *commit* the changes to make them permanent.

When you commit the changes, the Active Upgrade Console resynchronizes the RDR disks in your system by **overwriting** the original Production Side system disk and stale Upgrade Side data disks with their partner disks, which are up-to-date.

NOTE:

Because the original version of your system disk is erased during the commit process, you **cannot** abort an upgrade session after initiating the commit process.

Figure 4. Committing the Upgrade

When the RDR disk resynchronization is finished, all critical system resources are running in duplex mode, and the Active Upgrade process is complete. You do not need to restart the system, and, because your application is already running on the upgraded software, there is no additional downtime.

TIPS:

Aborting the Active Upgrade Process, page 5-74

Active Upgrade State Model, page 5-75

Software Upgrade Support, page 5-77

Prerequisites, page 5-78

Aborting the Active Upgrade Process

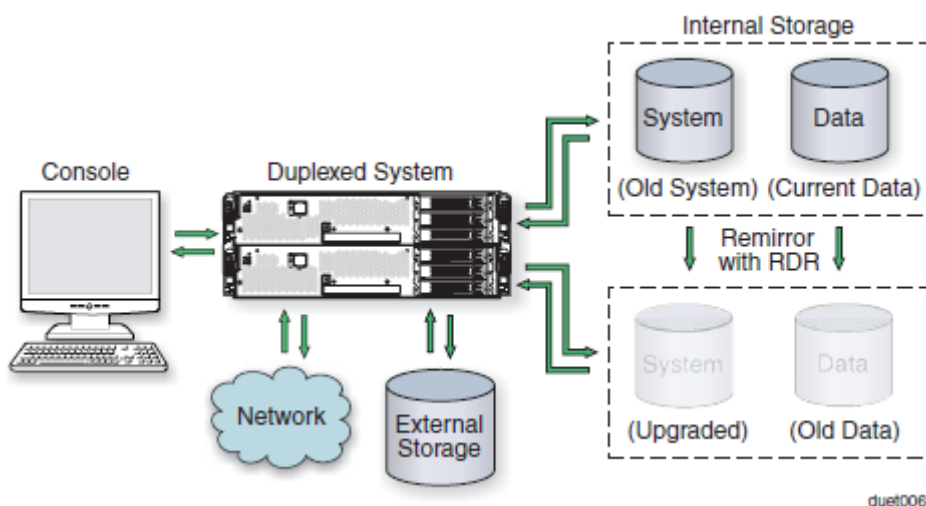
Aborting the Active Upgrade process stops the current upgrade session and returns your system to its original state. If necessary, you can abort the Active Upgrade process at any point up until you commit the upgrade.

If you abort the upgrade session while the system is in split mode, no downtime is incurred. Your applications continue to run on the Production Side while the Active Upgrade Console restores the system to duplex mode.

If you abort the upgrade session while the system is in merge mode, a short period of downtime is incurred while the Active Upgrade Console initiates a system restart. The Active Upgrade Console shuts down the Upgrade Side and restarts the system from the Production Side, which automatically restarts your applications from the Production Side. The period of downtime is only as long as it takes your system and applications to restart.

In either case, the abort process uses RDR resynchronization to restore the internal disks to their original state by **overwriting** the unwanted Upgrade Side system disk and stale Upgrade Side data disks with their original partner disks.

Figure 5. Aborting the Upgrade



After you abort the Active Upgrade process, you can start another Active Upgrade session as soon as the RDR disk resynchronization is complete.

TIPS:

Active Upgrade State Model, page 5-75

Active Upgrade Process, page 5-70

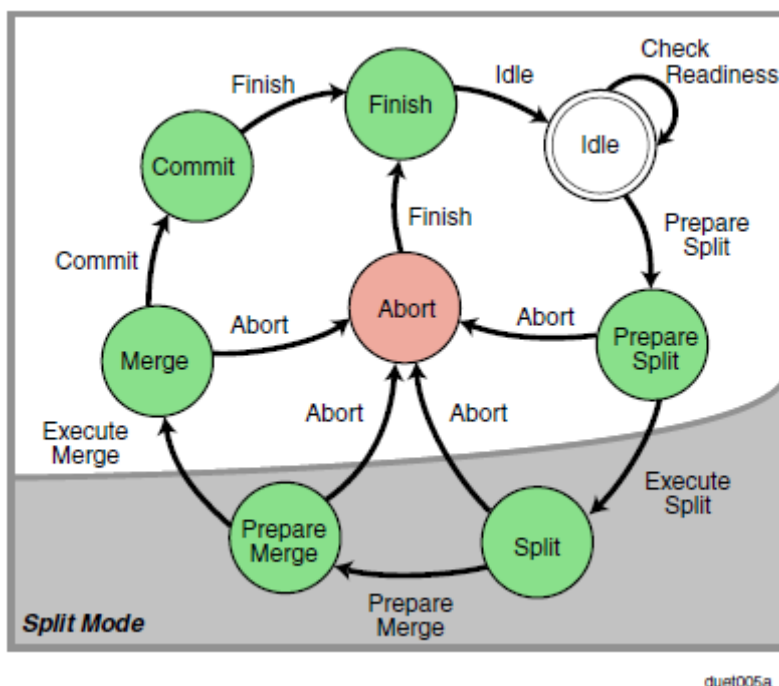
Software Upgrade Support, on page 5-77

Prerequisites, page 5-78

Active Upgrade State Model

The state model in Figure 6 shows all of the possible Active Upgrade states, and the order in which they occur during the Active Upgrade process.

Figure 6. Active Upgrade State Model



The state model helps to demonstrate the sequence of events in the Active Upgrade process, as follows:

1. All upgrade sessions start in the Idle state, where you can run the readiness check as many times as necessary to verify that your system meets the prerequisites of the Active Upgrade process.
2. When you start an upgrade session, the Active Upgrade Console switches to the PrepareSplit state, during which it runs a final readiness check and additional background tasks. If the system is ready, the console immediately switches to the Split state and proceeds to divide the system into two independently running systems.

IMPORTANT:

After the upgrade session leaves the Idle state, you must complete the full upgrade process in sequence, or, if necessary, abort the process altogether. You cannot go back to a previous state or skip states, and you cannot proceed to the next state if the upgrade is in a Broken or Busy operational state.

3. When you are done installing software on the Upgrade Side and you start the merge process, the Active Upgrade Console switches to the PrepareMerge state, during which it runs additional readiness tests and background tasks. If the system is ready, the console immediately switches to the Merge state and restarts your applications on the Upgrade Side.
4. When you are satisfied that everything is working correctly and you start the commit process, the Active Upgrade Console switches to the Commit state, during which it starts the resynchronization of your RDR disks. You can subsequently start the finish process, during which the Active Upgrade Console switches to the Finish state, cleans up system resources, and then returns the system to the Idle state. The upgrade session is complete.

If necessary, you can abort the Active Upgrade process from the PrepareSplit, Split, PrepareMerge, and Merge states. When you abort the upgrade session, the Active Upgrade Console switches to the Abort state, during which it restores your system to its original configuration and starts the resynchronization of your RDR disks. You can subsequently initiate the finish process, as you would after committing an upgrade.

Alternatively, you can retry any of the Active Upgrade states to recover the system from a transient failure and move on to the next states without aborting the entire Active Upgrade process.

All of these Active Upgrade states are reported in the activity log and status bar of the Active Upgrade Console during the upgrade process. See “Understanding the Active Upgrade Console Interface” on page 5-88 for more information.

TIPS:

Active Upgrade Process, page 5-70

Software Upgrade Support, page 5-77

Prerequisites, page 5-78

Preparing for the Active Upgrade Process

Preparing for the Active Upgrade process involves the following tasks:

- Learning about the types of upgrades that the Active Upgrade process supports.
- Learning about the prerequisites for your Fault Tolerant Server series system.
- Learning how the Active Upgrade Console can control your critical applications.
- Performing pre-upgrade tasks on your ftServer system, such as:
 - Configuring the Remote KVM console.
 - Configuring the Remote Desktop Connection.
 - Installing the Active Upgrade Console.
 - Configuring Windows Firewall for the Active Upgrade process.
 - Gathering information about your system.
 - Copying any software installation packages to the system **before** the upgrade starts.
- Starting the Active Upgrade Console.
- Understanding the Active Upgrade Console.

Software Upgrade Support

Active Upgrade technology supports the installation or upgrade of application software that meets the following criteria:

- The application's executable files, configuration files, and temporary files (for example, cache files) reside on internal system disks that are mirrored with RDR.
- The application's persistent data files reside on separate data disks, either internal or external. (Data volumes that reside on the same physical disk as a system volume are not supported.)
- The application's installation or upgrade utility does not involve changes to files or databases on the data disks while the system is in split mode. (For example, the utility cannot create new databases or convert existing data records to be compatible with the new version of the application).
The Upgrade Side has no access to the data disks while the system is split.

Active Upgrade technology does not support the following types of upgrades:

- Any upgrade that requires network connectivity during the upgrade process. For example, you cannot use an installer program that downloads its installation files from the Internet as the upgrade progresses. If possible, you must download the complete installer to the system prior to initiating split mode.
- BIOS, BMC firmware updates that can be performed while the system is duplexed and online.

For more information on BIOS and BMC firmware update, see "Firmware Update" on page 5-54.

TIPS:

Overview, page 5-69

Prerequisites, page 5-78

Recommendations, page 5-79

Managing Critical Applications During the Upgrade Process, page 5-80

Pre-Upgrade Tasks, page 5-81

Prerequisites

Active Upgrade technology is supported **only on Fault Tolerant Server series system** that:

- Are running in duplex mode prior to starting the upgrade process.

The CPU/IO modules must be duplexed, and all critical resources in the enclosures must be duplexed.

A critical resource is a device (like a CPU, hard disk, or host bus adapter) that is necessary to maintain fault tolerance. Non-fault-tolerant resources (like tape drives) connected to the system will not affect the Active Upgrade process.

- Contain duplexed Ethernet PCI adapters.

All **embedded** Ethernet PCI adapters must be teamed with the Intel PROSet utility, and each Ethernet team must contain at least one Ethernet PCI adapter from each CPU/IO module . Furthermore, at least one team of embedded Ethernet PCI adapters must have an active network link in each CPU/IO module.

All ports on any dual-port adapter must be either teamed or not teamed. You cannot have only one port on an adapter teamed.

You do not need to team non-embedded Ethernet PCI adapters, but it is recommended. The readiness check in Active Upgrade Console will display a warning for each unteamed Ethernet PCI adapter, but the warnings will not prevent you from proceeding with the Active Upgrade process.

IMPORTANT:

If you need to modify Ethernet teams that are actively providing network connectivity, this could impact network connectivity and should be scheduled to minimize impact to your critical applications.

See “DUAL LAN CONFIGURATION” in Chapter 3, “Windows Setup and Operation” for more information about configuring Ethernet PCI adapters and Ethernet teams.

- Has one new IP address for Active Upgrade ready.

You need to prepare one IP address to communicate between the Production Side/the Upgrade Side using PCI adapter during the Split. The IP address is allocated to the Upgrade Side system with the Split status.

- Do not use the devices connected with USB except the keyboard and mouse.

In Active Upgrade, if you are using the devices connected with USB other than the keyboard and mouse, be sure to remove them physically before performing Active Upgrade.

- Contain the ft remote management card.

The ft remote management card provides the connection between the Production Side and Upgrade Side during the Active Upgrade process. Both ft remote management cards must be configured properly and connected to the same subnetwork, preferably on a dedicated maintenance network.

- Can tolerate running in simplex mode for a brief period during the upgrade.

Because each side of the system runs in simplex mode during the upgrade, an interruption on the side that is actively running your critical applications can result in downtime.

IMPORTANT:

You cannot restart the operating system on the Production Side during an upgrade (though you can restart the Upgrade Side as many times as necessary.) Also, it is unsafe to pull an enclosure from a split-mode, simplexed system because doing so terminates all processes running on that enclosure.

- Can tolerate a potential decrease in performance during the upgrade.

For example, if your system contains teamed network adapters that are configured for load balancing or link aggregation, there might be a decrease in network performance when the system is split because the network adapters on the Upgrade Side lose access to the network.

- Have been updated with the latest firmware to support Active Upgrades, including required BMC updates.

Furthermore, the Active Upgrade process has the following storage requirements:

- All internal hard disks must be configured with Rapid Disk Resync (RDR) and must be duplexed (synchronized) before the Active Upgrade process starts.
- The operating system boot volume and all active Windows operating system components must be located on internal RDR disks. This includes any volumes that contain paging (virtual memory) files for the operating system.
- Any disk that contains software you want to upgrade **cannot** contain persistent data files for your business-critical applications (those applications that will continue to run during the Active Upgrade process). You must store your data files on separate data disks, either internal or external. (Data volumes that reside on the same physical disk as a system or paging volume are also not supported.)
- External storage devices are always considered data disks. You cannot upgrade software on external storage devices, as these devices not available to the Upgrade Side of the system while the system is in split mode.

TIPS:

Overview, page 5-69

Software Upgrade Support, page 5-77

Recommendations, page 5-79

Managing Critical Applications During the Upgrade Process, page 5-80

Pre-Upgrade Tasks, page 5-81

Recommendations

When preparing your system for the Active Upgrade process, also consider the following recommendations:

- Use static IP addresses for embedded Ethernet teams.
- If your system is protected by Windows Firewall, enable the exception for Active Upgrade Console as shown in “Configuring Windows Firewall for the Active Upgrade Process” on page 5-84.

If Windows Firewall is running, and the exception for Active Upgrade Console is not enabled, communication between the Production Side and Upgrade Side might fail during the Active Upgrade process.

- Use caution when applying hotfixes from any source. Applying updates indiscriminately may introduce serious problems to your Fault Tolerant Server series system.

TIPS:

Overview, page 5-69

Software Upgrade Support, page 5-77

Prerequisites, page 5-78

Managing Critical Applications During the Upgrade Process, page 5-80

Pre-Upgrade Tasks, page 5-81

Managing Critical Applications During the Upgrade Process

The Active Upgrade Console enables to specify how business-critical applications are started and stopped during the Active Upgrade process.

If your Fault Tolerant Server series system runs business-critical applications, such as Microsoft Exchange Server or SQL Server, these applications can run on only one side of the system—the Production Side—when you split the system. They must be stopped on the other side—the Upgrade Side—to prevent resource conflicts and to allow you to proceed with upgrade tasks. Furthermore, when you merge the system, the same applications must be stopped on the Production Side and restarted on the Upgrade Side, so you can test the applications with the newly-upgraded system disk, and possibly commit the upgrade.

In general, critical applications are launched and exited automatically by the operating system. For example, your application might be configured to launch as a service in the Services Control Manager, or as a startup item in the system registry. But these resources control your applications only when the operating system itself is launched or exited. In most cases, to minimize downtime, the Active Upgrade Console executes upgrade operations, like split and merge, **without** restarting the operating system. Therefore, if you want to launch and exit your applications at the appropriate times during the upgrade process, you must configure the Active Upgrade Console itself to control the applications

Active Upgrade Console provides two methods for controlling your critical applications during the upgrade process. The method you use for each application depends on the type of application you want to control:

- Application services

If your application runs as a standard service that already accounts for interdependencies (with other services) and requires no special handling, you can specify it on the **Application Services** page of the Active Upgrade Console during the configuration process. On the **Application Services** page, you can select each service you want to manage from the list of services on your system, and, when you start the upgrade process, the Active Upgrade Console will automatically start and stop these services at the appropriate times. See “Selecting Application Services to Control” on page 5-101 for more information.

- Custom actions

If you have a custom application or integrated applications from several different software vendors, and you have special executables that start and stop these applications, you can specify the executables on the **Custom Actions** page of the Active Upgrade Console during the configuration process. Using the controls on the **Custom Actions** page, you can specify when your executables will run during the upgrade process, and, if you have several executables, you can specify the order in which they will run. See “Configuring Custom Actions” on page 5-103 for more information.

TIPS:

Software Upgrade Support, page 5-77

Selecting Application Services to Control, page 5-101

Configuring Custom Actions on page 5-103

Pre-Upgrade Tasks

To prepare for upgrading the system, do the following:

1. Ensure that your Fault Tolerant Server series system meets the requirements and recommendations discussed in “Software Upgrade Support” on page 5-77, “Prerequisites” on page 5-78, and “Recommendations” on page 5-79.
2. If necessary, plan for the brief downtime associated with restarting your critical applications while merging the system.
3. Run backups of the system.
4. Verify the integrity of all RDR disks, as follows:
 - a. In RDR Utility, click **Logical Disk Information**.
 - b. Right-click an RDR virtual disk.
 - c. Select **Verify RDR Virtual Disk**.
 - d. Repeat for each RDR disk.
5. Upgrade the BMC firmware, if necessary, to support Active Upgrade technology.
6. Configure Remote Desktop Connection if necessary as described in “Configuring Remote Desktop Connection” on page 5-98.
7. Verify the prerequisites to use Remote KVM Console and configure if required.
8. Prepare the IP address to allocate to the Upgrade Side’s system.
9. Install the Active Upgrade Console as described in “Installing the Active Upgrade Software” on page 5-83.
10. If applicable, enable the exception for Active Upgrade Console in Windows Firewall properties, as shown in “Configuring Windows Firewall for the Active Upgrade Process” on page 5-84.
11. Gather information about your system using the worksheet in “Gathering Information” on page 5-85.
12. If necessary, copy any required software installation packages to the system, as described in “Copying Software Installation Packages to the System” on page 5-.

When you are finished preparing for the upgrade, start the Active Upgrade Console. Follow the on-screen instructions (and this document) to configure the process, and, when applicable, run the Readiness Check to verify if your system is ready to upgrade.

TIPS:

Installing the Active Upgrade Software, page 5-83
Software Upgrade Support, page 5-77
Prerequisites, page 5-78
Recommendations, page 5-79

Configuring Remote Desktop Connection

In the setup window of Remote Desktop Connection, enable the remote connection. For more information, see the Windows online Help.

If the remote connection is not enabled, the Production Side with Remote Desktop Connection cannot access the Upgrade Side in split mode.

Configuring Remote KVM Console

Configure Remote KVM Console function.

Refer to [Remote Management Function] in [Chapter 4. System Configuration].

IMPORTANT:

On Active Upgrade, Remote KVM Console function is used in order to display the console of the Upgrade side on the Production Side during Split status.

You need to execute [Server Initial Configuration] and [Managing PC Configuration] in [Chapter 4. System Configuration]-[Remote Management Function] for this server.

Preparing an IP address to assign to the Upgrade Side

Prepare one IP address that meets the conditions below for Active Upgrade. You need this IP address to connect to the Upgrade side with Ethernet PCI Adapter while split.

- A network address that is the same as the one assigned to the Ethernet team
- An unassigned, unused IP address

For how to configure IP address, see “Setting the IP address for the Upgrade Side System.”

Installing the Active Upgrade Software

IMPORTANT:

Your login account must be in the Administrator group to install the Active Upgrade Console.

To install the Active Upgrade Console, do the following:

1. Insert the ftServer Active Upgrade Software CD-ROM into one of the CD/DVD drives. If the installation process does not start automatically, do the following:
 - a. Open My Computer.
 - b. Right-click on the appropriate CD/DVD icon, and click Explore in the shortcut menu.
 - c. In the CD/DVD file listing, double-click **install.exe** to start the installation utility.

The Active Upgrade Software Setup Wizard is displayed.

2. Click **Next** to view the end-user license agreement.
3. If you agree to the terms of the license, click the radio button for **I accept the terms in License Agreement** and click **Next**.
4. Click **Install** to install the files.
5. Click **Finish** to close the wizard.

The setup process installs the Active Upgrade Console and associated files in C:\Program Files\ftsys\ActiveUpgrade. It also creates Start menu items under **ftsys** and a shortcut on your desktop for the Active Upgrade Console.

TIPS:

Pre-Upgrade Tasks, page 5-81

Configuring the Active Upgrade Process, page 5-93

Configuring Windows Firewall for the Active Upgrade Process

The Active Upgrade Console requires network access to:

- Communicate with system components and underlying services in the fit control Software.
- Allow communication between the Production Side and the Upgrade Side while the system is split, so you can perform upgrade tasks.

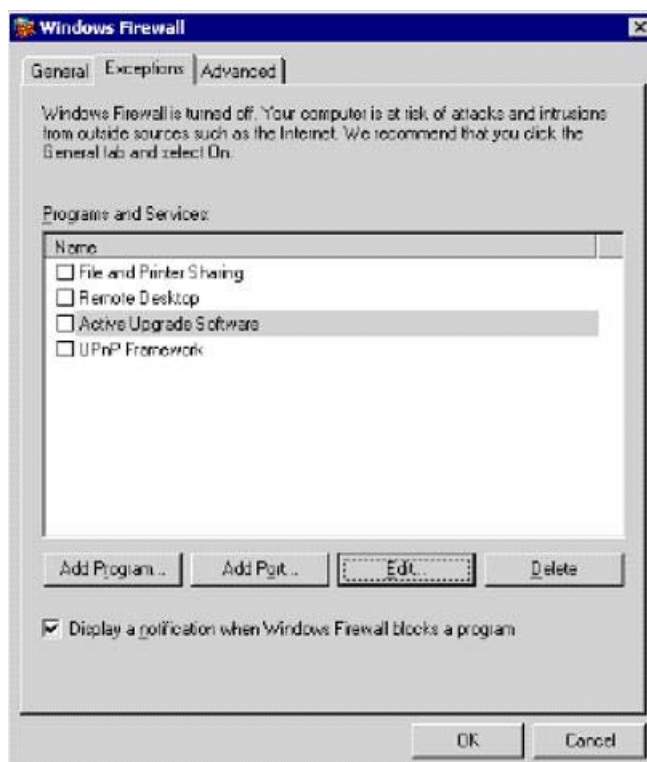
If you have enabled Windows Firewall to protect your system, it might prevent you from using some of the features of Active Upgrade Console; therefore, you should enable the exception for the Active Upgrade Console in your Windows Firewall settings.

Install the Active Upgrade software **before** configuring Windows Firewall. The installation process adds an entry for the Active Upgrade Console to the list of Windows Firewall exceptions. This entry is disabled by default.

To configure Windows Firewall

1. Open the **Windows Firewall** control panel.
2. Click the **Exceptions** tab to display the list of exceptions (see below figure, “Windows Firewall Exceptions”).
3. Click the check box next to **Active Upgrade Software** to activate it.
4. Click **OK** to enable this exception and close the control panel.

Windows Firewall Exceptions



TIPS:

Pre-Upgrade Tasks on page 5-81

Configuring the Active Upgrade Process on page 5-93

Gathering Information

Before you start configuring the Active Upgrade process on your system, considering the following questions:

- Did you decide the IP address for the Active Upgrade?
This IP address should be the same network address that is allocated to Ethernet team and should be a new one.
- After you complete this upgrade, will you ever want to run the same type of upgrade again? If so, plan to create a configuration file with the details of your upgrade, so you can use it again at a later date.
- Did your support provider give you a configuration file that you could use as a template for your specific system and the type of upgrade you are performing? Or, do you have settings from other existing configuration files that you want to incorporate into your current configuration? (If applicable, you might be able to use more than one configuration file at a time by nesting them).
- Which disks in your system contain the software you want to upgrade? Which disks cannot or should not be upgraded given the prerequisites of the Active Upgrade process? You will need to select these disks before splitting the system.
- Which software installation utilities are you going to run during the Active Upgrade process? (If you are copying these to the system from a network resource, you need to do so before initiating split mode.) Do any of these installer programs require access to the network or data disks during the upgrade? (If so, you cannot use them with Active Upgrade technology.)
- How do you start and stop critical applications on the system you want to upgrade? Are the applications configured as services in the Services snap-in to Microsoft Management Console? Or do you need to run custom actions (executables such as .bat, .vbs, .exe) to start your applications, possibly in a particular order? You need to identify these services and custom actions during configuration to allow the Active Upgrade Console to start and stop your applications at the appropriate times during the upgrade process. See “Managing Critical Applications During the Upgrade Process” on page 5-80 for more information.
- Do you want to preserve Event Viewer log entries that are generated on the Production Side while the system is running in split mode? These log entries are typically lost during the commit process, when the system resynchronizes your RDR disks. If you want to save the files, you can configure the Active Upgrade Console to copy them to a backup directory before it commits the upgrade. You can save the standard log files as well as any custom log files you have opened in the Event Viewer.

When you finish answering these questions, you can use the worksheet on the next page to record your configuration information.

Active Upgrade Process Worksheet

Item	Value
IP address for Active Upgrade	<div></div> <div></div> <div></div>
Configuration files to use	<div></div> <div></div> <div></div>
Disks to upgrade	<div></div> <div></div> <div></div>
Disks that cannot be upgraded	<div></div> <div></div> <div></div>
Software installation utilities to run	<div></div> <div></div> <div></div>
Application services to start/stop	<div></div> <div></div> <div></div>
Custom actions to run	<div></div> <div></div> <div></div>
Log files to back up	<div></div> <div></div> <div></div>

TIPS:

Pre-Upgrade Tasks, page 5-81
Software Upgrade Support, page 5-77
Prerequisites, page 5-78
Recommendations, page 5-79
Managing Critical Applications During the Upgrade Process, page 5-80
Configuring the Active Upgrade Process, page 5-93

Copying Software Installation Packages to the System

When the system runs in split mode, the Upgrade Side has no access to the network, external storage, or application data disks; therefore, if you need to download or copy any High Priority updates (hotfixes), installation packages, or disk images (for example, .msi files) to the system, put them on one of the disks you want to upgrade **before** you split the system. You might want to do so even before you run the Active Upgrade Console.

Make note of the location of the installation packages so you can find them later.

IMPORTANT:

If your installation packages are on CD-ROM, no action is necessary. You can access the DVD-ROM drive on the upgrade side while the system is in split mode.

TIPS:

Pre-Upgrade Tasks, page 5-81
Configuring the Active Upgrade Process, page 5-93

Understanding the Active Upgrade Console Interface

The Active Upgrade Console window (see the figure below) is divided into four major parts: a title bar, a navigation bar, a main window, and a status bar.

Active Upgrade Console




- 1 Title bar
- 2 Navigation bar
- 3 Main window

TIPS:

Starting and Exiting the Active Upgrade Console, page 5-
Pre-Upgrade Tasks, page 5-81
Configuring the Active Upgrade Process, page 5-93

Title Bar

The title bar displays the name of the current page of the Active Upgrade Console.

The title bar also contains a Help button (), which you can click to display the Help topic associated with the current page of the Active Upgrade Console.

(You can also access the Help from the Production Side or Upgrade Side by clicking **Start**, **All Programs**, **ftSys**, and **Active Upgrade Help** to open the Help viewer.)

TIPS:

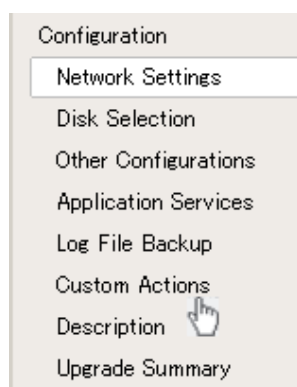
Starting and Exiting the Active Upgrade Console, page 5-
Understanding the Active Upgrade Console Interface, page 5-88
Pre-Upgrade Tasks, page 5-81
Configuring the Active Upgrade Process, page 5- 93

Navigation Bar

The navigation bar displays your current location in the Active Upgrade Console.

If you are creating or editing a configuration file, the navigation bar also allows you to skip between configuration pages by clicking any item under the **Configuration** heading (see the figure below), or by clicking **Active Upgrade** to start a readiness check.

Navigation Bar: Opening a Configuration Page



After you initiate an upgrade (by clicking **Split** on the **Active Upgrade** page), the navigation bar reverts to a static mode, in which it only indicates where you are in the upgrade process and does not allow you to skip between pages. You must follow the upgrade steps (split, merge, commit, and finish) in order to complete the upgrade process, or you can abort the process altogether.

The navigation bar contains the following entries:

- **Configuration** — Allows you to create or select a configuration file to modify, or to start the upgrade process with no configuration file.
- **Network Settings**— Allows you to verify the system network configuration and to configure IP address of the Upgrade Side. When you execute Active Upgrade for the first time, be sure to configure IP address of the Upgrade Side.
- **Disk Selection** — Allows you to select the disks that contain the software you want to upgrade.
- **Other Configurations** — Allows you to select other configuration files that will be incorporated into the current configuration.
- **Application Services** — Allows you to select the application services that need to be stopped and restarted during the upgrade process.
- **Log File Backup** — Allows you to select the Event Log (.evt) files from the Production Side that the Active Upgrade Console will preserve upon merging the system. (Otherwise, any event messages generated on the Production Side while the system is in split mode are lost when you commit the upgrade).
- **Custom Actions** — Allows you to specify executables that the Active Upgrade Console can use to stop and start your applications (or to perform special tasks) during the upgrade process.
- **Description** — Allows you to specify a title and comments for the current configuration file.
- **Upgrade Summary** — Displays a summary of the current upgrade configuration, and allows you to save the current configuration file.
- **Active Upgrade** — Allows you to perform a readiness test and, if applicable, to split the system for an upgrade.
- **Split System** — Indicates that the system is entering split mode, and allows you to merge system resources (or abort the upgrade) after you finish running installation packages.
- **Merge System** — Indicates that the system is entering merge mode, and allows you to commit (or abort) the upgrade after you have tested your changes.
- **Commit Upgrade** — Indicates that the system is committing the upgrade, and allows you to finish the process by cleaning up ft series system resources.
- **Abort Upgrade** — Indicates that the upgrade process has been aborted, and allows you to finish the process by cleaning up ft series system resources. (You can abort the upgrade process at any point prior to committing the upgrade.)
- **Finish** — Indicates that the upgrade process is complete and allows you to save a copy of the activity log to a file, start another upgrade, or exit the Active Upgrade Console.
- **Link:**
 - **Remote Desktop**

Allows you to establish a Remote Desktop Connection session to the Upgrade Side while the system is split to perform upgrade tasks.

TIPS:

Starting and Exiting the Active Upgrade Console, page 5-106

Understanding the Active Upgrade Console Interface, page 5-88

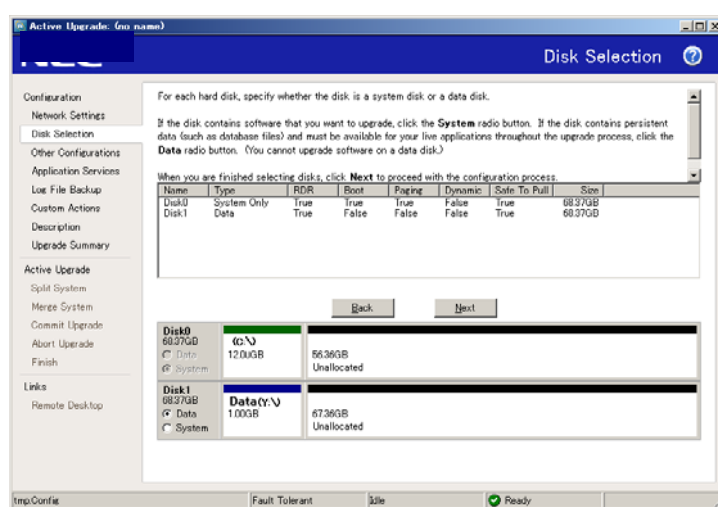
Pre-Upgrade Tasks, page 5-81

Configuring the Active Upgrade Process, page 5-93

Main Window

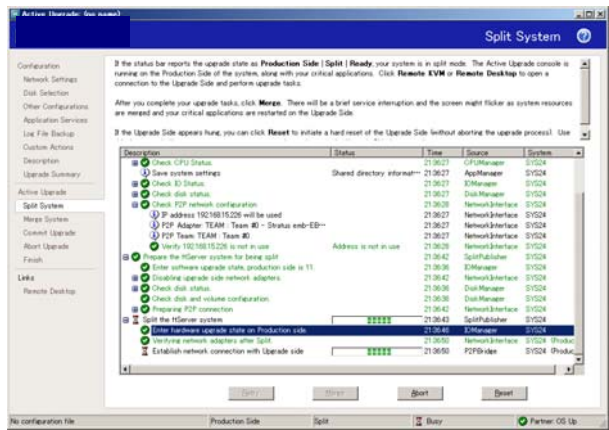
The main window contains controls associated with the configuration and execution of the Active Upgrade process.

During the configuration phase, main window allows you to specify settings for your system (see the figure below), which you can save to a configuration file.

Main Window: Configuring the Active Upgrade Process

When you perform a readiness test and begin the upgrade process, the configuration settings in the main window are replaced with an activity log (see the figure below) that allows you to track the progress and success of the Active Upgrade process.

Main Window: Activity Log



For more information on viewing and interpreting items in the activity log, see “Viewing Active Upgrade Process Status” on page 5-135.

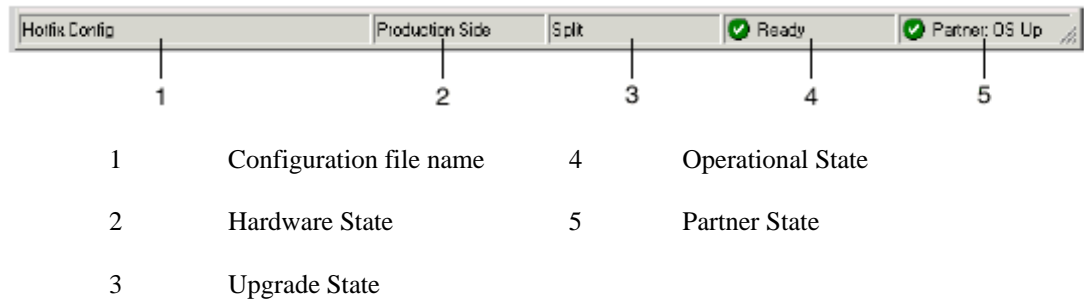
TIPS:

- Starting and Exiting the Active Upgrade Console, page 5-106
- Understanding the Active Upgrade Console Interface, page 5-88
- Pre-Upgrade Tasks, page 5-81
- Configuring the Active Upgrade Process, page 5-93

Status Bar

The status bar (shown below), which is located at the bottom of the Active Upgrade Console window, reports a quick summary of the status of the upgrade.

Status Bar



For more information about interpreting items in the status bar, see “Viewing Active Upgrade Process Status” on page 5-135.

TIPS:

- Starting and Exiting the Active Upgrade Console, page 5-106
- Understanding the Active Upgrade Console Interface, page 5-88
- Pre-Upgrade Tasks, page 5-81
- Configuring the Active Upgrade Process, page 5-93

Configuring the Active Upgrade Process

Configuring the Active Upgrade process involves the following tasks:

- Creating and managing configuration files
- Configuring the IP address for the Upgrade Side
- Selecting disks to upgrade
- Selecting other configuration files to include
- Selecting application services to control
- Selecting Event Viewer log files to back up
- Configuring custom actions
- Providing a description for a configuration file
- Displaying the upgrade summary

Creating and Managing Configuration Files

Configuration files allow you to save upgrade configurations that you can use immediately or in the future.

If you frequently perform upgrades your system, you can create a configuration file to preserve your settings so you can perform similar upgrades as often as necessary. If applicable, you can create multiple configuration files, each with different system settings to prepare the system for a particular type of system or application software upgrade.

In addition, you can *call* one or more existing configuration files from the configuration file you are currently editing, so that the settings from the called files will also apply to the file you are editing. This is called *nesting*.

The default location for Active Upgrade configuration files is \Program Files\ftsys\ActiveUpgrade\User Configurations, but you can save a configuration file in any directory. If you specify a different directory when saving or opening files, the Active Upgrade Console uses the same user-specified directory (on a per-user basis) the next time you open the file browser.

IMPORTANT:

You can save a configuration file to any disk – system or data, internal or external. The Active Upgrade Console automatically copies configuration files to a staging area before beginning the upgrade to ensure that they are available throughout the upgrade process.

See TIPS for more information about working with configuration files.

TIPS:

Creating a Configuration File, page 5-94
Loading a Configuration File, page 5-95
Editing an Existing Configuration File, page 5-96
Performing an Upgrade with No Configuration File, page 5-96
Saving a Configuration File, page 5-97
Selecting Other Configurations to Include, page 5-99
Providing a Description for a Configuration File, page 5-109

Creating a Configuration File

Creating a configuration file allows you to generate a configuration file that you can save and use immediately or at a later time.

To create a configuration file

1. On the **Configuration** page, click **Create Configuration File**.
2. In the **Create Configuration File** dialog box, specify a file name for the new file. (When you save the file, a **.config** extension is automatically appended to the file name.)
3. Next to **Save in**, select the directory in which to save the configuration file.
You can specify any directory on the system. The default location is \Program Files\ftsys\ActiveUpgrade\User Configurations; however, if you choose a new configuration directory, the Active Upgrade Console will use the new directory the next time you create or open a file.
4. Click **Save** to start editing the configuration.

After you create a configuration file, the configuration process opens on the **Disk Selection** page.

TIPS:

Creating and Managing Configuration Files, page 5-93
Saving a Configuration File, page 5-97
Providing a Description for a Configuration File, page 5-109

Loading a Configuration File

Loading a configuration file allows you to open an existing configuration file for use. After you load a configuration file, you can view the **Upgrade Summary**, and, if applicable, proceed with the upgrade as configured, but you cannot modify the configuration.

IMPORTANT:

To modify a configuration file, use the **Edit Configuration File** option.

To load a configuration file

1. On the **Configuration** page, click **Load Configuration File**.
2. Do one of the following to select the configuration file:
 - In the **Locate Configuration File** dialog box, type the full path name and file name for the configuration file next to **Configuration File**. (You must include the **.Config** file extension.)
 - Click **Browse** to locate the file using a file browser. (The browser displays only files with the **.Config** extension.) Click the file in the file browser, then click **Open** to select the file.
3. In the **Locate Configuration File** dialog box, click **Load** to open the configuration file.

(You can also drag a configuration file onto the **Configuration** page of the Active Upgrade Console window to load it.)

When you load a configuration file, the file opens on the **Upgrade Summary** page.

TIPS:

Creating and Managing Configuration Files, page 5-93
Displaying the Upgrade Summary, page 5-110
Performing the Upgrade, page 5-111

Editing an Existing Configuration File

Editing a configuration file allows you to open and edit a configuration file that you have previously saved. After you edit the configuration file, you can view the **Upgrade Summary**, and, if applicable, proceed with the upgrade as configured.

To edit a configuration file

1. On the **Configuration** page, click **Edit Configuration File**.
2. Do one of the following to open the file:
 - In the **Locate Configuration File** dialog box, type the full path name and file name for the configuration file next to **Configuration File**.
 - Click **Browse** to locate the file using a file browser. (The browser displays only files with the **.Config** extension.) Click the file in the file browser, then click **Open** to select the file.
3. In the **Locate Configuration File** dialog box, click **Load** to open the configuration file.

When you edit a configuration file, the file opens on the **Disk Selection** page.

TIPS:

Creating and Managing Configuration Files, page 5-93

Saving a Configuration File, page 5-97

Selecting the Disk to Upgrade, page 5-118

Displaying the Upgrade Summary, page 5-110

Performing an Upgrade with No Configuration File

If the upgrade you want to perform does not require any special settings, you can proceed without a configuration file.

IMPORTANT:

When you execute the Active Upgrade for the first time, you need to use the configuration file to update. You can upgrade without the configuration file only when you have executed the Active Upgrade with the configuration file before.

For example, if you have only one system disk, and you just want to split the system briefly to test how a hotfix would affect the operating system without committing the changes, you might not need a configuration file.

To proceed without a configuration file, click **No Configuration File** on the **Configuration** page. The Active Upgrade Console immediately displays the **Active Upgrade** page and runs a readiness check. If your system meets the prerequisites for the Active Upgrade process, you can split the system at this time.

TIPS:

Creating and Managing Configuration Files, page 5-93

Performing the Upgrade, page 5-111

Saving a Configuration File

The Active Upgrade Console automatically prompts you to save your configuration file if you leave the Configuration section of the application, or exit the application. (To save the configuration file, click **Yes**, otherwise click **No** or **Cancel**.)

You can also optionally click **Save** or **Save As** on the **Upgrade Summary** page, as described in the following procedure.

To save the current configuration file

1. Click **Upgrade Summary** in the navigation bar.
2. On the **Upgrade Summary** page, do one of the following:
 - Click **Save** to save the configuration file with the name and path name you previously specified. Your file is saved.
 - Click **Save As** to save the configuration file with a new file name or path name. Continue to step 3.
3. In the Save Configuration File dialog box, specify a name for the new file. (When you save the file, a .Config extension is automatically appended to the file name.)
4. Next to Save in, select the directory in which to save the configuration file.
5. Click Save to save the file. Your file is saved.

TIPS:

Creating and Managing Configuration Files, page 5-93

Displaying the Upgrade Summary, page 5-110

System IP Configuration on the Upgrade Side

Use [Network Settings] screen to allocate the IP address for the Upgrade Side's system with Split status. Verify the configuration by checking the Ethernet team configuration, status and the allocated IP address that appear on [Network Settings] screen. In [Upgrade-side IP address] field, allocate the IP address to the Upgrade Side.

IMPORTANT:

- Team adapter name or network adapter name may not be displayed appropriately in [Name] row or [Network Settings] screen. This has no effect on the Active Upgrade's operation.
 - Available IP address for the Upgrade side system is as follows:
 - IP address that belongs to the same network address as the one allocated to the Ethernet team.
 - An unused IP address.
-

Selecting Disks to Upgrade

Use the **Disk Selection** page to select the disks that contain the software you want to upgrade with the Active Upgrade process. By marking these disks in your upgrade configuration, you ensure that they will be available to the Upgrade Side of the system when the system is in split mode.

When you open the **Disk Selection** page, the Active Upgrade Console scans for and displays the disks in your system. **Only internal disks mirrored with RDR are displayed, as these are the only disks that can be configured.**

You can mark each disk as a *system disk* or a *data disk*:

System Disk

A disk that contains the system or application software you want to upgrade. Only disks marked as **System** will be available to the Upgrade Side while the system is split.

The Active Upgrade Console automatically marks some disks as system disks. These *mandatory system disks* contain either boot files or paging files (virtual memory files) that are currently in use by the running operating system. You cannot change a mandatory system disk to a data disk.

IMPORTANT:

You cannot use a system disk for storing persistent data (for example, database files) related to your critical applications. Any new data written to the original system disk by the Production Side while the system is in split mode is overwritten when you commit the upgrade. (See the "Overview" for information about the steps of the Active Upgrade process.)

Data Disk

A disk that contains persistent data for your critical applications. Any disk marked as **Data** will be available **only** to the Production Side while the system is split. You **cannot** upgrade software on a data disk.

IMPORTANT:

All external storage devices are automatically considered data disks.

(See the prerequisites for the Active Upgrade process for additional restrictions.)

Volumes on the **Disk Selection** page are color-coded as described in the below table.

Hard Disk Color Coding

Color	Description
Black	Unassigned disk space
Blue	Data disk
Light Green	System disk
Dark Green	Mandatory system disk
Red	Disk is currently simplexed because it is being resynchronized with RDR

For more information about any volume, move your cursor over the volume to display ToolTip help.

To select system and data disks

- For any disk you want to mark as a system disk, click the **System** radio button.
(This automatically marks any volume that the disk contains as a system volume.)
- For any disk you want to mark as a data disk, click the **Data** radio button.

IMPORTANT:

Volumes can span multiple physical disks, and physical disks can contain multiple volumes. If a volume spans two or more disks, and you mark one of the disks that contains that volume as a system disk, any disk that contains a part of that volume automatically becomes a system disk.

When you are finished selecting disks, you can click **Next** to proceed with the next configuration step.

TIPS:

Prerequisites, page 5-78

Displaying the Upgrade Summary, page 5-110

Selecting Other Configurations to Include

Use the **Other Configurations** page to optionally call one or more existing configuration files into the configuration file you are currently editing, so that the settings from the called files will also apply to the file you are editing. This is known as nesting files, or creating nest files.

The configuration files that you call into the current configuration file are *child configurations*, and the file from which you call the child configurations is the *parent configuration*.

Potential uses for the nest files include:

- Your support provider creates a configuration file that you can call into an existing configuration file for your system.
- You create separate configuration files, each for upgrading a different application, which you can enable or disable as necessary in your parent configuration.
- You create a configuration file for an application that runs on several of your systems and call that file into a parent configuration file that is specific to each system.

The following restrictions apply to the nest files:

- Child configuration files must be located in the same directory as the call target files. When you select configuration files in the Active Upgrade Console, only the files in the current working directory are displayed.
- If a call-target configuration files have more than one child configuration files, they also become a part of your configuration.
- If a setting in a child configuration conflicts with a setting in the parent configuration, the Active Upgrade Console uses the setting in the parent configuration; the parent configuration always ignores disk selections from child configurations.
- If you call a configuration created on a different system, configuration items (such as application services and custom actions) must be present and applicable on the current system; otherwise, the parent configuration will fail the readiness check.

To call a child configuration file into the current file

1. On the **Other Configurations** page, select the check box next to the configuration file(s) you want to call into the current file.
2. In the file window, verify that you have selected the correct configuration files. Also, if any of the files contain additional child configurations, ensure that you are including only the configurations that apply to the current parent file.
3. When you are finished editing the current configuration, save the configuration file.

To remove a child configuration file from the current configuration, clear the check box next to that configuration file. (If you need to remove a child configuration from another configuration file, you must edit that configuration file separately.)

When you have finished specifying child configuration files, you can click **Next** to proceed with the next configuration step.

TIPS:

Creating and Managing Configuration Files, page 5-93

Saving a Configuration File, page 5-97

Displaying the Upgrade Summary, page 5-110

Selecting Application Services to Control

Use the **Application Services** page to select the critical application services you want the Active Upgrade Console to automatically stop and restart during the upgrade process.

If you select a service on the **Application Services** page, the Active Upgrade Console controls the service as follows:

- When the system is split, the console stops the service on the Upgrade Side, saves its current **StartupType**, and changes the **Startup Type** to **Disabled**. This helps to prevent application errors associated with the Upgrade Side losing access to data disks and the network while the system is split.
- When the system is merged, the console stops the service on the Production Side, restores the previous Startup Type for the service on the Upgrade Side, and starts the service on the Upgrade Side. This ensures continuous availability of the service, enables comprehensive testing on the Upgrade Side, and prevents any conflicts associated with two instances of a service running at the same time.

When an upgrade is aborted, and if the system is in merge mode, the console shuts down the Upgrade Side to stop the service automatically. The console automatically restarts the Production Side based on its default **Startup Type**. This restores the system to its previous, fault-tolerant state.

IMPORTANT:

1. Standard operating system services do not require control during the Active Upgrade process. Select only services that are related to your critical applications (such as Exchange, SQL and IIS).
 2. The Active Upgrade Console never changes the default Startup Type for a service on the Production Side. Maintaining the default Startup Type on the Production Side ensures that a service will always be able to restart on the Production Side if the upgrade process is aborted or failed.
-

Selection of Application Services

Check Box State	Description
Cleared	Not selected.
Checked	Selected in the current configuration file.
Checked (Gray)	Selected in a child configuration file. If applicable, you can click the check box to explicitly select the service in the current configuration file, but you cannot deselect it without editing the child configuration.

To select a service for the Active Upgrade Console to control

1. On the **Application Services** page, find a service you want to stop and start.
2. Click the check box to the left of the service name.
3. Repeat these steps for each service you want to stop and restart.

To deselect a service, clear the check box to the left of the service name.

(By default, the services on the **Application Services** page are listed alphabetically. If you prefer to sort them by other criteria, click on one of the column headings. For example, if you want to group services by those you have selected and not selected, click the heading above the check boxes.)

When you have finished selecting services to control, or if you have no services to control, you can click **Next** to proceed with the next configuration step.

TIPS:

Configuring Custom Actions, page 5-103
Managing Critical Applications During the Upgrade Process, page 5-80
Displaying the Upgrade Summary, page 5-110

Selecting Event Viewer Log Files to Back Up

Use the **Log File Backup** page to optionally preserve Windows Event Viewer log files from the Production Side of your system during the Active Upgrade process.

When you commit an upgrade, the system reestablishes the RDR mirrors of any system disks by overwriting the Production Side disks (which contain the old version of your software) with the newer Upgrade Side disks (which contain your newly-upgraded software). Because the event log files on the Production Side are lost during this process, you might want to preserve them for future reference. These log files will contain the only record of log messages your live applications generated while the system was split.

The **Log File Backup** page allows you to select from all event logs available in the Windows Event Viewer, including user-created logs.

IMPORTANT:

For information about creating a Custom Action that preserves other files from the Production Side system disk, see “Configuring Custom Actions” on page 5-103.

Saving Event Viewer log files

1. Specify a directory in which to save the files by doing one of the following:
 - In the Staging Directory dialog box, type the full path name of the directory.
 - Click Browse to locate a folder using the Browse for Folder dialog box. Click a folder and click OK to select it.

IMPORTANT:

1. You must save the files to a disk that is available to the Production Side while the system is split — either a data disk or an external disk. Do **not** save the files to a system disk or network disk.
 2. There is no default directory. You must specify a directory, otherwise, the Active Upgrade Console displays a warning message.
-
2. For each log you want to save, click the log name to highlight it, then click the check box to the left of the log name to preserve the file.

When you have finished selecting Event Viewer log files to preserve, you can click **Next** to proceed with the next configuration step.

TIPS:

Configuring Custom Actions, page 5-103
Displaying the Upgrade Summary, page 5-110

Configuring Custom Actions

Use the **Custom Actions** page to customize the way that the Active Upgrade process will run in your environment. You can create custom actions to perform the following types of tasks:

- **Specify how a critical application is stopped and started during the Active Upgrade process.**

For example if you use special executables to start and stop your applications, you can use the controls on Custom Actions page to specify when these executables will run during the upgrade process; if you have several executables, you can specify the order to run.

- **Check if a certain condition exists before starting the upgrade process.**

For example, you can write a program to verify that a critical backup has completed on the following; if the critical backup has completed; if the system load on the system is acceptable, or if it is a certain time of a day before starting the upgrade process.

- **Backup files during the upgrade process.**

Any files that are modified on the Production Side system disks while the system is in split mode are lost during the commit process, when the RDR mirrors are resynchronized. If applicable, you can write a program to save copies of important files before you commit an upgrade. For example, you can save a copy of an application-specific log file that does not appear in the system Event Viewer. (For information about saving Event Viewer logs, see “Selecting Event Viewer Log Files to Back Up” on page 5-102.)

By default, the **Custom Actions** page supports executables that are batch files (.bat) or application files (.exe). If you want to use a Visual Basic script (.vbs), see “Programming Notes for Custom Actions” on page 5-105 for special instructions.

IMPORTANT:

1. Custom actions run consecutively when called. If one action fails to terminate, it might prevent the next action from executing, and, ultimately, prevent the upgrade process from continuing. When you specify an executable for a custom action, verify that it runs successfully outside of the Active Upgrade process, and ensure that it completes in a timely manner.
 2. Executables for custom actions must be located on a system disk. If an executable is located on an external or network disk, the Upgrade Side will lose access to the executable while the system is in split mode.
 3. For information about writing your own programs for custom actions, see “Programming Notes for Custom Actions” on page 5-105.
-

To configure a custom action

1. On the Custom Actions page, do one of the following:

- Next to **File**, type the full path name and file name of the executable you want to run. The file must already exist on the system.

Example: C:\bin\mybatchfile.bat

- Click **Browse** to locate the executable using a file browser. Click the file name in the file browser, and click Open to select the file.

2. Next to **Arguments**, type any arguments that you need to run with your executable.

No arguments are required; however, see “Programming Notes for Custom Actions” on page 5-105 for information about passing optional Active Upgrade environment variables to your executable.

3. In the drop-down list for **Control type**, select the option that best describes when the Active Upgrade Console will execute your custom action, as discussed in the below table.

Control Types for Custom Actions

Control Type	Purpose
Start Application	Executes the custom action whenever the Active Upgrade Console needs to start applications. For example, the console needs to restart applications on the Upgrade Side when you merge the system.
Stop Application	Executes the custom action whenever the Active Upgrade Console needs to stop applications. For example, the console needs to stop applications on the Upgrade Side when you split the system. It also stops applications on the Production Side when you merge the system.
Readiness Check	Executes the custom action once during the readiness check, before you initiate the Active Upgrade process. This control type allows you to build your own verifications into the readiness check.
Advanced	<p>Executes the custom action during every step of the Active Upgrade process, including interim steps such as PrepareSplit and PrepareMerge, which occur prior to the Split and Merge operations.</p> <p>This control type allows you to have more precise control over a custom action. Your executable will run each time the Active Upgrade process switches states, but you can write a program with conditional statements based on Active Upgrade environment variables to specify exactly when and where particular tasks should be executed. For example, you can write a conditional statement that will trigger only on the Upgrade Side if the system is in merge mode.</p> <p>If you have more than one custom action, the Advanced control type also allows you to control the order in which the custom actions are executed (step 4).</p>
Backup	Executes the custom action when the system is merged, allowing you to back up files that were modified on the Production Side system disk while the system was in split mode (before these files are lost during the commit process).

4. If you selected the **Advanced** control type, optionally select an item from the **Timing** drop-down list which best describes the order in which you want this custom action to run with your other custom actions. The below table, “Timing for the Advanced Control Type”, describes the timing options. If the timing does not matter, keep the **Default** setting.

IMPORTANT:

The **Timing** will not affect the order in which custom actions run with other Active Upgrade tasks. Use this option only if you want to ensure that one custom action runs before or after another custom action.

Timing for the Advanced Control Type

Timing	Purpose
Default	Executes the custom action in the default, consecutive order.
Before	Executes the custom action early in the list of custom actions, before items marked as Default or After.
After	Executes the custom action late in the list of custom actions, after items marked as Before or Default.

Your custom actions will run consecutively according to their timing options. Subsequent custom actions will not start until the current custom action terminates.

5. Click **Add** to accept the custom action. (If the **Add** button is inactive, ensure that you typed the **File** path name and executable name correctly. The executable file must exist to be added.)

You can view the custom actions you have created at the bottom of the **Custom Actions** page. If you want to remove a custom action from the list, select it and click **Remove**.

When you have finished specifying custom actions to run, or if you have no custom actions to specify, you can click **Next** to proceed with the next configuration step.

TIPS:

Programming Notes for Custom Actions, page 5-105
 Selecting Application Services to Control, page 5-101
 Managing Critical Applications During the Upgrade Process, page 5-80
 Displaying the Upgrade Summary, page 5-110

Programming Notes for Custom Actions

The following topics describe some of the features available for programming and monitoring custom actions:

- “Starting and stopping applications” on this page
- “Using Active Upgrade Environment Variables” on page 5-106 “Generating Exit Values” on page 5-107
- “Viewing Standard Output and Error Stream” on page 5-107
- “Executing Visual Basic Scripts” on page 5-108

Starting and stopping applications

If you write a program to control a critical application during the upgrade process, ensure that your program not only stops and starts the application at the appropriate times, but also **disables** and **enables** the default startup mechanism for the application (for example, the default **Startup Type** setting in the Services Control Manager or a startup item in the system registry). If you do not disable the default startup type for an application, it might interfere with or override your custom action.

See “Selecting Application Services to Control” on page 5-101 for information about how the Active Upgrade Console changes the **Startup Type** for application services.

TIPS:

Programming Notes for Custom Actions, page 5-105

Configuring Custom Actions, page 5-103

Using Active Upgrade Environment Variables

You can optionally use the environment variables specified in the below table in any executable that you write for a custom action. These environment variables are useful if you want to write a conditional statement in your executable that, for example, runs only on a particular side of the system or only during a particular stage of the Active Upgrade process.

Environment Variables for Custom Actions

Environment Variable	Description
ACTIVE_UPGRADE_SIDE	Describes the side of the system on which the program is running. Values: Production, Upgrade
ACTIVE_UPGRADE_STATE	Describes the current upgrade state. Values: Idle, PrepareSplit, Split, PrepareMerge, Merge, Commit, Abort
ACTIVE_UPGRADE_REQUEST	Describes the next upgrade task that the Active Upgrade Console will execute. Values: Idle, CheckReadiness, PrepareSplit, ExecuteSplit, PrepareMerge, ExecuteMerge, Commit, Abort, Start, Stop, Backup
ACTIVE_UPGRADE_HW_SPLIT	Describes whether or not the ft series system is running in split mode. Values: Yes, No

If you want these environment variables to be available to your executables, you must pass the variables to each executable in which you will use them.

For example, to pass only the ACTIVE_UPGRADE_SIDE variable to an executable, append the following string to the **Arguments** for the custom action on the **Custom Actions** page:

```
%ACTIVE_UPGRADE_SIDE%
```

To pass multiple variables, add a space between each variable, as follows:

```
%ACTIVE_UPGRADE_SIDE% %ACTIVE_UPGRADE_REQUEST%
```

TIPS:

Active Upgrade State Model, page 5-75
Programming Notes for Custom Actions, page 5-105
Configuring Custom Actions, page 5-103

Generating Exit Values

An exit value of 0 indicates that the executable exited normally.

Any other exit value indicates that there was an error, which will prevent the Active Upgrade process from continuing with the current upgrade request. If this happens, you must correct the problem and click **Retry** in the Active Upgrade Console to retry the current upgrade request (which also runs the custom action again). The Active Upgrade process will not continue until the executable for your custom action runs successfully.

TIPS:

Programming Notes for Custom Actions, page 5-105
Configuring Custom Actions, page 5-103

Viewing Standard Output and Error Stream

After your program executes, you can view standard output and error output from the program in the Active Upgrade Console, as follows:

1. In the activity log, expand an **Execute custom actions** node.

(There can be more than one **Execute custom actions** node, depending on the types of custom actions you have created. Find the node for the upgrade stage in which your custom action was set to run.)
2. Double-click a specific custom action to display more information about it.
3. In the detail window, view the output for your program under Status. If necessary, scroll down in the **Status** box to see the full output. Or move your cursor over the **Status** box to view the output as ToolTip help.

If you save the activity log to a file, you can also view the output in that file. See “Saving the Activity Log to a File” on page 5-141 for more information.

TIPS:

Programming Notes for Custom Actions, page 5-105
Configuring Custom Actions, page 5-103

Executing Visual Basic Scripts

By default, the **File** field on the **Custom Actions** page accepts only batch files (.bat) and application files (.exe). If you want to use a Visual Basic script (.vbs) on the **Custom Actions** page, you need to specify the command-line based script host (cscript.exe) in which the executable will run.

When performing the procedure in “Configuring Custom Actions” on page 5-103, do the following:

Next to **File**, type:

%SystemRoot%\system32\cscript.exe

(%SystemRoot% is an environment variable that automatically inserts your system root directory, typically C:\WINDOWS.)

Next to **Arguments**, type the full path name and file name of the executable. For instance:

C:\bin\myvbscript.vbs

If applicable, you can type additional arguments that are specific to your script file or options that are specific to the cscript session.

For example, you might want to specify the //T option for the cscript session to control the maximum amount of time your executable is allowed to run:

C:\bin\myvbscript.vbs //T:30

The preceding example would terminate the executable and cscript session after 30 seconds. Setting this type of time limit is a useful way of ensuring that your executable will not delay the upgrade process.

For more information about the cscript command, open a **Command Prompt** session and enter **cscript /?**

TIPS:

Programming Notes for Custom Actions, page 5-105

Configuring Custom Actions, page 5-103

Providing a Description for a Configuration File

Use the **Description** page to specify a title and comments for your configuration file.

These items appear on the **Other Configurations** page, the **Upgrade Summary** page, and in the **Locate Configuration File** dialog box when you are selecting a configuration file to load or edit.

Type a brief summary next to **Title**, and type additional details next to **Comments**.

For **Comments**, you might want to include information such as:

- Purpose of the configuration file (type of upgrade)
- System(s) to which the file applies
- Special setting required before using the file for an upgrade
- Your name and contact information (or the contact information on your support provider)
- Date you created or updated the file

When you have finished providing a description for the configuration file, you can click **Next** to proceed with the next configuration step.

TIPS:

Creating and Managing Configuration Files, page 5-93

Saving a Configuration File, page 5-97

Displaying the Upgrade Summary, page 5-110

Displaying the Upgrade Summary

When you finish creating a new configuration file, or when you load or edit an existing configuration file, you can display a summary of the upgrade configuration that the file contains.

To display the upgrade summary, click **Upgrade Summary** in the navigation bar of the Active Upgrade Console. The summary window displays information including:

- Configuration file name, title and description
- The IP address to add to the upgrading system
- Disks you selected for the upgrade
- Other configuration files called by the current file
- Application services to launch and exit
- Custom actions to run
- Event Viewer log files to back up

If applicable, you can also save the current configuration file from the **Upgrade Summary** page.

When you are finished viewing the Upgrade Summary, and, if necessary, saving the configuration file, you can click **Next** to proceed with the Active Upgrade process.

If you have changed your configuration file since you last saved it, the Active Upgrade Console displays a message indicating that you should save the file. To save the file, click **Yes**, otherwise click **No** or **Cancel**.

In the next step, the Active Upgrade Console runs a readiness check to verify that your system meets the prerequisites for an online upgrade. If necessary, you can abort the process before you split the system (or at any point up until you commit the upgrade).

TIPS:

Saving a Configuration File, page 5-97

Performing a Readiness Check, page 5-111

Aborting the Upgrade, page 5-133

Performing the Upgrade

Performing the Active Upgrade process can involve the following tasks:

- Performing a readiness check
- Splitting the system
- Merging the system
- Committing the upgrade
- Aborting the upgrade (if necessary)
- Finishing the upgrade
- Viewing the Active Upgrade process status

Performing a Readiness Check

Before you can initiate split mode on a system, the system must pass a readiness check. The readiness check verifies that your system meets the prerequisites for the Active Upgrade process. For example, the readiness check ensures that:






- The system is currently running in the duplex mode.
- The disks you selected as the system disks are present and are mirrored with RDR.
- The embedded Ethernet PCI adapters in your system are configured to Ethernet teams, and each team contains at least one adapter from each physical enclosure.
- The IP address configured to the system of the Upgrade Side must be an unused one, and this IP address is the same network address as the one Ethernet team.
- The application services you specified for control are currently running, and can be exited when necessary.
- The executables for any custom action are present on the system and are ready to run.

To perform a readiness test, choose to do **one** of the following:

- Click Next on the Upgrade Summary page (if you are using a configuration file).
- Click Active Upgrade on the navigation bar (the readiness test starts automatically if you have recently opened or changed your configuration).
- Click Retry on the Active Upgrade page.
- Click No Configuration File on the Configuration page.

The activity log reports the overall results of the readiness check as well as the results for each individual test. The below list describes the general meaning of the activity log entries.

Activity Log Entries

Icon	Text Color	Severity	Description
	Green	Success	Task completed without error
	Black	Pending	Task is in progress
	Black	Information	Task information, no action necessary
	Black	Warning	A problem that should be addressed, but will not block an upgrade
	Red	Error	A problem that must be corrected before continuing with upgrade

The status bar at the bottom of the window will indicate one of the following states for the current operation:

-  Busy

A readiness check is in progress. Allow time for the task to complete.

-  Ready

The system meets the prerequisites for the Active Upgrade process. You can proceed with the upgrade process by splitting the system.

-  Broken

One or more components in the system does not meet the prerequisites for the Active Upgrade process. You must resolve the problem before you can continue with the upgrade.

(For more information about interpreting Active Upgrade status, see “Viewing Active Upgrade Process Status” on page 5-135.)

If the check is successful, you can click **Split** to proceed with splitting the system. See “Splitting the System.”

If one of the readiness tests fails, you must resolve the problem, then click **Retry** to run the readiness test again. When the problem is resolved, you can click **Split** to proceed with splitting the system.

TIPS:

Prerequisites, page 5-78

Splitting the System, page 5-136

Viewing Active Upgrade Process Status, page 5-135

Saving the Activity Log to a File, page 5-141

Aborting the Upgrade, page 5-133

Troubleshooting, page 5-141

Splitting the System

Splitting a Fault Tolerant Server series system divides it into two independently-functioning systems: the Production Side, which continues to run your applications, and the Upgrade Side, which you can safely upgrade.

Splitting the system:

- Disables RDR mirroring between the internal disks in each CPU/IO module enclosure
- Detach the Upgrade Side from system resources such as the network, any user-specific application data disks, and any external PCI resources (such as an external storage).
- Disables any user-specified applications and services on the Upgrade Side so they cannot restart if you restart the operating system on the Upgrade Side.
- Queues any ActiveService Network alerts generated on the Upgrade Side until the system is merged.

You can split a system only if it meets the prerequisites for the Active Upgrade process and has passed the readiness check.

IMPORTANT:

1. When in split mode, the Upgrade Side has no access to the network; the Upgrade Side can only access to the Production Side. If you need a network resource to obtain any software installation packages you intend to run, transfer the software to the system **before** you initiate split mode. Furthermore, put the software on one of the system disks, as these are the only disks you can access on the Upgrade Side while the system is in split mode.
 2. Split the system only when you are sitting at the console for your Fault Tolerant Server series system. The Active Upgrade Console is not supported over remote connections.
-

CAUTION:

Do not perform any hardware maintenance, including the removal of either CPU/IO module, after you have initiated the Active Upgrade process (by clicking Split).

To split the system

1. Ensure that you have addressed any critical errors or warnings that were indicated by the readiness check.
2. Exit any non-essential applications.
3. Click **Split** on the **Active Upgrade** page.

When the system successfully enters split mode:

- Active Upgrade Console continues to run on the Production Side of the system.
- The Active Upgrade Console switches to the Split System page.
- The upgrade state, reported in the status bar, is **Production Side\Split\Ready**, indicating that the system is currently split and ready to be merged after your software installation.

IMPORTANT:

Do not select [Abort] to interrupt the Active Upgrade process. The interruption could fail and the duplex may not complete. If the interruption failed, restart the OS to finish the interruption normally according to the following procedures; it enables to duplex the system.

- (1) Select the Upgrade Side's PCI module on the ft Server Utility.
 - (2) Verify if [Status] of the Upgrade Side's PCI module is [Terminate].
 - (3) Select [Boot] to start the Upgrade Side's PCI module.
 - (4) Select [Retry] on the Active Upgrade console to finish the interruption process.
-

Splitting the system should take only a few minutes. The process will time out if it takes longer than 5 minutes.

IMPORTANT:

1. Throughout the upgrade process, icons will appear and disappear in the system tray as PCI devices, such as Ethernet PCI adapters, are reconfigured or disabled for the current upgrade operation. This is normal. Do not attempt to enable or reconfigure any of these PCI devices while the upgrade session is in progress.
 2. If your system is running EMC® PowerPath® software for an external storage system, you might experience a brief delay (10-15 seconds) when the system splits, as PowerPath reroutes storage operations through the Production Side.
 3. If the Firewall setting is not appropriate, the split process could fail. If this occurs, select [Abort] to terminate Active Update. After the Active Upgrade is finished, automatic duplex processing is executed. When this duplex processing is completed, execute the Active Upgrade again.
-

If the split process fails the first time, you can click **Retry** to try again. If the problem persists, you can click **Abort** to abort the upgrade process, or see “Troubleshooting” for information about resolving the problem.

When the system is split, you can:

- Manage upgrade tasks on the Upgrade Side.
- Manage your applications on the Production Side.
- Verify the Upgrade Side before merging the system.

To perform upgrade tasks, you must establish a remote connection to the Upgrade Side, as explained in “Managing Upgrade Tasks on the Upgrade Side” on page 5-116.

TIPS:

After you establish a connection to the Upgrade Side, you can optionally check the status of your application services on the Upgrade Side, to verify that they have been stopped by the Active Upgrade Console. Refer to “Verifying the Status of Application Services” on page 5-141.

TIPS:

Managing Upgrade Tasks on the Upgrade Side, page 5-116
Managing Your Applications on the Productions Side, this page
Verifying the Upgrade Side Before Merging the System, page 5-127
Merging the System, page 5-128
Viewing Active Upgrade Process Status, page 5-135
Aborting the Upgrade, page 5-133
Troubleshooting, page 5-141

Managing Upgrade Tasks on the Upgrade Side

While the system is in split mode, you can perform any of the following upgrade tasks **on the Upgrade Side**:

- Run software installers and updaters (see “Running Software Installers” on page 5-121, and “Software Upgrade Support” on page 5-77 for restrictions).
- Restart the operating system, if necessary (see “Restarting the Upgrade Side” on page 5-124).
- Perform limited testing of the installed updates (see “Verifying the Upgrade Side Before Merging the System” on page 5-127)

If necessary, you can also completely abort the upgrade process from the Active Upgrade Console on the Production Side.

Because the Active Upgrade Console itself runs on the Production Side of the system, you need to establish a remote connection to the desktop on the Upgrade Side before you can complete any of these upgrade tasks, as explained in “Connecting to the Desktop on the Upgrade Side” on page 5-117.

TIPS:

Connecting to the Desktop on the Upgrade Side, page 5-117
Running Software Installers, page 5-121
Restarting the Upgrade Side, page 5-124
Viewing Active Upgrade Process Status, page 5-135
Merging the System, page 5-128
Aborting the Upgrade, page 5-133
Troubleshooting, page 5-141

Connecting to the Desktop on the Upgrade Side

While the system is in split mode, the Active Upgrade Console runs on the Production Side of the system. To perform upgrade tasks, you must establish a remote connection to the Upgrade Side.

You can access the Upgrade Side using one of two methods:

- Remote KVM

Allows you to transfer the Upgrade Side’s console to the Production Side’s browser with BMC remote KVM console. Allows you the complete access from the Production Side to the Upgrade Side using the video, keyboard and mouse.

- Remote Desktop

Allows you to control the keyboard, video and mouse of the Upgrade Side through the Windows Remote Desktop component. You might prefer this option if you are more familiar with it, or if it runs faster in your environment.

To use either connection method, click on the associated link in TIPS below.

TIPS:

Connecting to the Upgrade Side with Remote KVM on page 5-118
Connecting to the Upgrade Side with Remote Desktop on page 5-120

IMPORTANT:

- Before connecting to the Upgrade Side from the Production Side by using Remote Desktop or Remote KVM, you need to complete the Split operation appropriately and check no error is output on the activity log. If Remote Desktop or Remote KVM is used during the Split operation, the connection may fail. If this occurs, retry the connection after the Split.
 - Active Upgrade Console that appears on the Upgrade Side is just for monitoring the status such as [Remote Activity Log] under [Active Upgrade Operation Check] – [Activity Log] in many cases. However, the Active Upgrade Console looks like the console of the Production Side in some cases. In such a case, you need to care following issues.
 - Never select any buttons (such as [Abort] or [Merge]) or any links (such as [Remote Desktop]) on the Active Upgrade Console of the Upgrade Side when in split mode. If you inappropriately select any of them, you may face an error or will not be able to refer to the data drive after the merge is completed. When this kind of trouble occurs, you need to take following procedures.
 - When operation is unavailable because of the error, execute the same operation again from the Active Upgrade Console of the Production Side.
 - When the data drive cannot be referred to the merge status, select [Retry] button and execute merge operation again. If you can't refer data drive after retrying the merge, select [Abort] button to exit the Active Upgrade, then again execute the Active Upgrade.
-

Connecting to the Upgrade Side with Remote KVM allows you to control the keyboard, video, and mouse of the Upgrade Side using the BMC remote console feature.

To initiate a Remote KVM session with the Upgrade Side

IMPORTANT:

When you use Remote KVM session, you need to prepare the setting of the Remote KVM before starting the Active Upgrade. Refer to [Chapter 4 System Configuration] – [Remote Management Function] for the Remote KVM settings.

1. Access the following URL with the web browser on the Production Side:

http://BMC_HostPort/index.htm

TIPS:

“BMC_Host Port” consists of the IP address allocated to the LAN port of the Upgrade Side module that include “:” (colon) and the http port number on the back of the IP. When the http number is 80 (default), you can omit the port number.

2. If the browser displays a warning indicating that the Web site is being blocked, click **Add** to display the Trusted Sites dialog box. Click **Add** to add the site to your Trusted Sites zone, then click **Close** to dismiss the dialog box.
3. If the browser displays additional warning messages about running Web-based content, click **Close** or **OK** to dismiss these messages.

After you initiate the remote session, see TIPS for more information about what you can do on the Upgrade Side and how you can merge the system after you have finished performing upgrade tasks.

To terminate a Remote KVM session with the Upgrade Side

1. Verify that the install processing is completed as well as the install program is all finished.
2. Select [X] on the upper right-hand side of the Remote KVM consol to close the window.
3. Select File menu on the upper left-hand side, choose **Finish** to log out from the main window.
4. Close the browser window with login page.

TIPS:

Terminating the Remote KVM is not mandatory. You can merge the system while maintaining the Remote KVM connection.

TIPS:

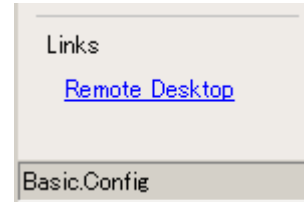
Connecting to the Upgrade Side with Remote Desktop, page 5-120
Running Software Installers, page 5-121
Restarting the Upgrade Side, page 5-124
Viewing Active Upgrade Process Status, page 5-135
Merging the System, page 5-128
Aborting the Upgrade, page 5-133
Troubleshooting, page 5-141

Connecting to the Upgrade Side with Remote Desktop

Remote Desktop allows you to control the keyboard, video and mouse of the Upgrade Side through the Windows Remote Desktop component.

To establish a Remote Desktop Connection to the Upgrade Side

1. Click **Remote Desktop** in the navigation bar of the Active Upgrade Console on the Production Side. The system opens a Remote Desktop Connection window.
2. When the window displays the login screen for the remote system, enter your administrative username and password and click **OK**. The Upgrade Side desktop is displayed.



For more information on what you can do, such as on the Upgrade Side after establishing the remote connection, and how to merge the system after completing the upgrade process, each connection, see TIPS below

TIPS:

If you want to refer to the Active Upgrade Help file while you are using the Upgrade Side desktop, click **Start** on the Upgrade Side desktop, then click **All Programs**, **ftSys**, and **Active Upgrade Help** to open the Help viewer.

If you maximize the Remote Desktop connection window, its title bar (which displays the IP address of the Upgrade Side as well as minimize, maximize and exit buttons), might disappear from view (autohide). Only the Upgrade Side desktop will be displayed, as if it is your local desktop. If you want to redisplay the title bar to access its controls, push the mouse pointer to the top of the screen.

TIPS:

The Remote Desktop title bar is a helpful reminder that you are using the Upgrade Side desktop. If you have maximized the window for Remote Desktop and you want the title bar to be displayed for the duration of your connection, click the pin button (pushpin) on the left side of the title bar. (The pin button is displayed only when the window is maximized.)

For more information about managing a Remote Desktop session, see the Windows online Help.

To terminate a Remote Desktop Connection to the Upgrade Side

1. Verify that any installer processes are complete, and that you have exited any installer programs.
2. Click [Shut Down] in the Start menu of your remote session.
3. In the Shut Down Windows dialog box, click [Disconnect].

TIPS:

If you are about to merge the system, you can remain logged on to maintain the current desktop session. After the merge, you will be using the Upgrade Side desktop.

Running Software Installers

The following topics describe how to run software installers on the Upgrade Side while the system is split:

- “Windows Automatic Updates” on page 5-146
- “Other Installation Packages” on page 5-123

(To review the types of upgrades that Active Upgrade technology supports, see “Software Upgrade Support” on page 5-77.)

TIPS:

Software Upgrade Support, page 5-77

Managing Upgrade Tasks on the Upgrade Side, page 5-116

Viewing Active Upgrade Process Status, page 5-135

Merging the System, page 5-128

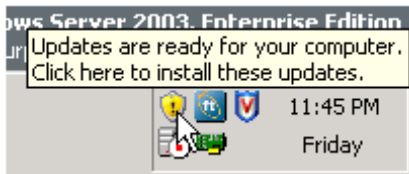
Aborting the Upgrade, page 5-133

Troubleshooting, page 5-141

Windows Automatic Updates

If you are using Windows Automatic Updates, and you previously downloaded all of the required software updates, the Automatic Updates icon should be present in the system tray, and it should report that updates are ready for your computer (see the figure below). If so, you are ready to apply the updates.

Automatic Updates Icon in System Tray



IMPORTANT:

Before installing any software, **ensure that you are working on the Upgrade Side desktop** (through a remote connection). Do not install software on the Production Side.

To apply the downloaded updates

1. Click on the Automatic Updates icon in the Upgrade Side system tray to display the **Automatic Updates** dialog box.
2. Select the radio button for **Custom Install** and click **Next**.

The next page displays a list of the updates you downloaded and allows you to select which ones will be installed at this time.

3. Select only the updates that you previously checked for compatibility with your Fault Tolerant Server series system, then click **Install**.

During the installation process, the Automatic Updates dialog box minimizes to the system tray. When the installation is complete, you can display the dialog box again. It should report that all updates were successfully installed.

Some updates might require you to restart the operating system on the Upgrade Side. You can click **Restart Now** to allow Automatic Updates to restart the Upgrade Side automatically, or you can manually restart later. You can restart the Upgrade Side as many times as necessary to complete the installation.

See “Restarting the Upgrade Side” on page 5-124 for information about reconnecting to the Upgrade Side after you restart it.

TIPS:

Software Upgrade Support, page 5-77
Managing Upgrade Tasks on the Upgrade Side, page 5-116
Viewing Active Upgrade Process Status, page 5-135
Merging the System, page 5-128
Aborting the Upgrade, page 5-133
Troubleshooting, page 5-141

Other Installation Packages

If you previously downloaded individual software installers to a system disk, open the Upgrade Side folder that contains those installer files. Run each installer one at a time.

TIPS:

Before installing any software, **ensure that you are working on the Upgrade Side desktop** (through a remote connection). Do not install software on the Production Side.

Some installers might require you to restart the operating system on the Upgrade Side. You can allow these installers to restart the Upgrade Side automatically, or you can manually restart later. You can restart the Upgrade Side as many times as necessary to complete the installation; however, you might want to avoid restarting until you have run additional installers to reduce the total number of times you need to restart.

See “Restarting the Upgrade Side” on page 5-124 for information about reconnecting to the Upgrade Side after you restart it.

TIPS:

Software Upgrade Support, page 5-77

Managing Upgrade Tasks on the Upgrade Side, page 5-116

Viewing Active Upgrade Process Status, page 5-135

Merging the System, page 5-128

Aborting the Upgrade, page 5-133

Troubleshooting, page 5-141

Restarting the Upgrade Side

When the system is running in split mode, if necessary, you can restart the operating system on the Upgrade Side at any time. You can either allow a software installer to restart the system automatically or you can perform the following procedure to restart the system manually.

IMPORTANT:

Before you restart the system, ensure that you are working on the Upgrade Side desktop (through a remote connection). Do not restart the Production Side.

To manually restart the Upgrade Side



1. On the Upgrade Side, click **Shut Down** in the Start menu.
2. In the **Shut Down Windows** dialog box, select **Restart** from the drop-down menu and click **OK**.

If you are using **Remote KVM**, the AVR session will remain connected while the Upgrade Side is restarting; however, you must log on again when the Upgrade Side is finished restarting. (To send the Ctrl-Alt-Del key sequence necessary for login, use a virtual keyboard.)



If you are using **Remote Desktop Connection**, the connection to the Upgrade Side is terminated, and the Production Side desktop is displayed. While the Upgrade Side is restarting, you can view its status in the activity log and the status bar of the Active Upgrade Console. When the console displays the message **Partner: OS Up**, you can click **Remote Desktop** to log on to the Upgrade Side again.

IMPORTANT:

When you restart the Upgrade Side, the following activity log may be displayed on the Active Upgrade Console:

-  Partner (Upgrade) state is now Hung:
-  Unexpected state transition in Split state.

There may be an output of these activity logs even when the Upgrade Side's restart completed normally. If the following activity logs are displayed after about five minutes, select [Retry] to retry the split process so that you can continue the Active Upgrade.

-  Partner (Upgrade) state is now Running OS.
-  Reestablished network connection with Upgrade side.

If there is no output of those activity logs, select [Abort] to interrupt the Active Upgrade.

TIPS:

Though the Active Upgrade Console reports that the Upgrade Side operating system is up, it might take another minute or two for all services to finish loading and for login to be possible.

TIPS:

Running Software Installers, page 5-121
Viewing Active Upgrade Process Status, page 5-135
Merging the System, page 5-128
Aborting the Upgrade, page 5-133
Troubleshooting, page 5-141

Resetting the Upgrade Side Hardware

If the Upgrade Side system hangs up while the system is operating with the Split mode, you can reset the Upgrade Side hardware by clicking [Reset] button.

By resetting the Upgrade Side hardware, the system recovers.

IMPORTANT:

1. Do not reset the Upgrade Side hardware on the following cases:
 - When the Upgrade Side does not reboot properly.
 - When the remote connection from Production Side to the Upgrade Side does not set up properly.
 - When the Upgrade Side hangs up.
 2. If you reset the hardware while the Upgrade Side is working properly, the Upgrade side may not launch properly. If this occurs after resetting the hardware, press [Abort] button to interrupt the Active Upgrade, then retry the Active Activate from the start.
 3. Do not reset the hardware while split. If the hardware is reset while split, the spilt may fail. If this occurs, select [Abort] button to interrupt the Active Upgrade, then retry the Active Upgrade.
-

Managing Your Applications on the Production Side

While the system is split, you can continue to access and use your applications on the Production Side; however, **you must avoid doing any of the following on the Production Side** desktop:

- Installing or upgrading software.
- Creating or modifying any files on the system disk, including the system registry.
- Restarting the operating system.

IMPORTANT:

- Any changes you make to files on the Production Side system disks will be lost during the commit process, because the system overwrites these system disks (which contain the old version of your software) with the newer Upgrade Side disks to complete the upgrade. If you need to preserve files from the original system disks, you can save them to a data disk.
 - Be careful when switching between the Production Side desktop and the remote connection to the Upgrade Side desktop. When you resume software installation or restart the system, always ensure that you are on the Upgrade Side.
-

TIPS:

Managing Upgrade Tasks on the Upgrade Side, page 5-116

Viewing Active Upgrade Process Status, page 5-135

Merging the System, page 5-128

Aborting the Upgrade, page 5-133

Troubleshooting, page 5-141

Verifying the Upgrade Side Before Merging the System

After you have upgraded or installed software on the Upgrade Side, you can perform limited testing on the Upgrade Side system disks, as long as your activities do not require access to the following resources, which are currently unavailable:

- Network
- External storage
- Application data disks

For example, you might want to perform the following tasks before you merge the system:

Verify the presence and version number of each software package (see “Verifying the Status of Installed Software” on page 5-143).

If possible, verify that you can start the applications you installed or upgraded.

If possible, configure the settings for any applications you installed or upgraded.

If you are satisfied that everything is working correctly, you can merge the system to stop your applications on the Production Side and restart them on the Upgrade Side for final verification.

If there are any problems, you can abort the upgrade to return the system to its original state. Aborting the upgrade while the system is in split mode will not incur downtime, because your critical applications are still running on the Production Side.

TIPS:

Managing Upgrade Tasks on the Upgrade Side, page 5-116

Viewing Active Upgrade Process Status, page 5-135

Merging the System, page 5-128

Aborting the Upgrade, page 5-133

Troubleshooting, page 5-141

Merging the System

After finishing to perform the upgrade tasks on the Upgrade Side of the system, you can merge the system to verify your changes before you permanently commit them.

Merging the system:

- Stops your applications and services on the Production Side.
- Merges system resources so that the network, external storage, and application data disks become available to the Upgrade Side.
- Restarts your applications (including the Active Upgrade Console) from the Upgrade Side.

IMPORTANT:

If you execute the Active Upgrade under Backup Exec environment, merge after the split process is completed, and restart the OS on the Upgrade Side.

If you do not restart the OS on the Upgrade Side, merge process may fail. If it failed, press [Abort] to finish the Active Upgrade. After the Active Upgrade, the duplex process will be done automatically; after the duplex process is done, retry the Active Upgrade.

To merge the system

1. Verify that all upgrade processes are complete, and that you have exited any installer programs.
2. Optionally, terminate any Remote KVM or Remote Desktop sessions.

IMPORTANT:

If you terminate the Remote Desktop, “Disconnect” instead of “Logoff.” You can remain logged on to the Upgrade Side if you want to maintain the current desktop session. After the merge, you will be using the Upgrade Side desktop.

3. Verify that the upgrade state, as reported in the status bar, is **Production Side\Split\Ready**.

If the status is **Busy**, you must wait for the current task to complete. If it is **Broken**, you might need to abort the upgrade.

4. Click **Merge**.

IMPORTANT:

- Your screen might flicker and you might briefly lose control of your keyboard and mouse as the system is merged.

- Do not select [Abort] button to interrupt the Active Upgrade during the merge. The disk may not be recognized from the OS. When the disk isn't recognized from the OS, go to [Disc Management] then execute [Disk Rescan].

If the disk status becomes [missing] or [offline], right click the disk and select [Disk Reactivation] to verify the disk status becomes [online].

- If you exit the remote desktop connection to the Upgrade Side, or if you exit the remote KVM connection to the Upgrade Side, the following error message appears on the Active Upgrade Console of the Production Side while operating the merge.

- A user must be logged into the upgrade-side console for this operation to complete

- When this error message appears, complete the merge by following the below procedure:

1. Click the Remote Desktop link and login to the Upgrade Side.
 2. Select [Retry] button on the Active Upgrade Console of the Production Side and retry the merge operation.
-

Depending on the complexity of your applications and the upgrade you performed, your applications should be backed up and running in under a minute.

After the merge process completes, the upgrade state is **Fault Tolerant\Merge\Ready**, indicating that the system is currently merged and the upgrade is ready to be committed. You can test your applications to verify that the upgrade was successful.

If the merge process fails the first time, you can click **Retry** to try again. If the problem persists, you can click **Abort** to abort the upgrade process, or see “Troubleshooting” for information about resolving the problem.

IMPORTANT:

If you selected [Abort] to interrupt the Active Upgrade after the merge process is done, OS will be restarted.

After the OS restart is completed, the interruption will be executed. The interruption may fail, however. If it failed, retry the merge process by selecting [Retry].

TIPS:

Verifying the Upgrade Side Before Committing the Upgrade, page 5-130

Committing the Upgrade, page 5-132

Viewing Active Upgrade Process Status, page 5-135

Aborting the Upgrade, page 5-133

Troubleshooting, page 5-141

Verifying the Upgrade Side Before Committing the Upgrade

After you have merged the system, your critical applications (including the Active Upgrade Console) are running from the software on the Upgrade Side system disks. At this point, you can test the software you installed and verify the general health of the system with full access to the system’s resources, including:

- Network resources
- External storage
- Application data disks

For example, you might want to perform the following tasks before you commit the upgrade:

- Verify that all of your critical applications have restarted on the Production Side (see “Verifying the Status of Application Services” on page 5-141).
- Verify that you have access to your network, external storage, and application data disks.
- Verify that client systems can reach all of the services that you Fault Tolerant Server series system provides.
- Verify that the presence and the version number of each software package (see “Verifying the Status of Installed Software” on page 5-143).
- Verify that you can launch and run any applications that you have installed or upgraded.
- Verify the configurations for your applications and the operating system, which could have been altered by software installation.

If you are satisfied that everything is working correctly, you can commit the upgrade to make the changes permanent.

If there are any problems, you can abort the upgrade to return the system to its original state. However, **aborting the upgrade while the system is in merge mode will incur downtime**, because the Active Upgrade Console must stop your critical applications on the Upgrade Side before it can restart them on the Production Side.

TIPS:

Committing the Upgrade, page 5-132

Viewing Active Upgrade Process Status, page 5-135

Aborting the Upgrade, page 5-133

Troubleshooting, page 5-141

Committing the Upgrade

When you are finished testing your applications on the merged system, and you are satisfied that everything is working correctly, you can commit the upgrade to make it permanent.

Committing the upgrade

- Rebuild the mirror of any internal RDR system disk by overwriting the original partner disk with its newer, upgraded partner disk.
- Rebuild the mirror of any internal RDR data disk by overwriting the stale partner disk with its newer, activated disk. The stale disk refer to the one that your applications have been writing data throughout the upgrade process.
- Does not restart your applications, as they are already running on the upgraded system. There is no additional downtime.

CAUTION:

You cannot abort the upgrade process after you commit an upgrade because the original state of the system is lost (overwritten) as a result of completing the upgrade process. Ensure that your system is working as expected before clicking **Commit**.

How to commit the upgrade

1. Close all non-essential applications.
2. Verify that the upgrade state, as reported in the status bar, is **Fault Tolerant\Merge\Ready**.
3. Click **Commit**.

IMPORTANT:

Your screen might flicker and you might briefly lose control of your keyboard and mouse as the system commits the upgrade.

The commit process should take only a few minutes. After it completes, the upgrade state is **Fault Tolerant\Commit\Ready**. You can click **Finish** to clean up ft series resources, as described in “Finishing the Upgrade” on page 5-134.

If the commit process fails the first time, you can click **Retry** to try again. If the problem persists, see “Troubleshooting” for information about resolving the problem.

TIPS:

Finishing the Upgrade, page 5-134
Viewing Active Upgrade Process Status, page 5-135
Verifying If RDR Disks Are Resynchronizing, page 5-144
Troubleshooting, page 5-141

Aborting the Upgrade

If necessary, you can abort the Active Upgrade process and restore the system to its original state at any point of the upgrade process **prior to committing the upgrade**.

CAUTION:

You cannot abort the upgrade process after you commit an upgrade because the original state of the system is lost (overwritten) as a result of completing the upgrade process.

When you abort an upgrade, the Active Upgrade Console:

- Cancels the current Active Upgrade operation.
- If applicable (and if your system is in the merge state), initiates a system restart. It shuts down the Upgrade Side and restarts the system from the Production Side, which automatically restarts your applications from your original Production side system disks.
- If applicable, reestablishes the mirror of any internal RDR system disk by overwriting the upgraded partner disk with the original partner disk.
- If applicable, reestablishes the mirror of any internal RDR data disk by overwriting the stale partner disk with its newer, live partner disk (the disk to which your applications have been writing data throughout the upgrade process).
- If applicable, bring the Upgrade Side online to enable fault-tolerant, duplex mode.

To abort an upgrade, click the **Abort** button on the **Active Upgrade** page, the **Split System** page, or the **Merge System** page.

IMPORTANT:

Your screen might flicker and you might briefly lose control of your keyboard and mouse as the system recovers its original state.

The abort process should take only a few minutes. When the process completes, the upgrade state is **Fault Tolerant\Abort\Ready**. You can click **Finish** to clean up ftServer resources, as described in “Finishing the Upgrade” on page 5-134.

If the abort process fails the first time, you can click **Retry** to try again. If the problem persists, see “Troubleshooting” for information about resolving the problem.

TIPS:

Finishing the Upgrade, page 5-134

Viewing Active Upgrade Process Status, page 5-135

Verifying If RDR Disks Are Resynchronizing, page 5-144

Troubleshooting, page 5-141

Finishing the Upgrade

To complete the Active Upgrade process and clean up fitServer system resources after committing or aborting an upgrade, click **Finish** on the **Commit Upgrade** page or **Abort Upgrade** page.

The finish process should take only a few minutes. When the process completes, the upgrade state is **Fault Tolerant\Idle\Ready**.

If the finish process fails the first time, you can click **Retry** to try again. If the problem persists, see “Troubleshooting” for information about resolving the problem.

On the **Finish** page, upon successful completion of the Active Upgrade process, you can:

- Click **Exit** to close the Active Upgrade Console.
- Click **Save Log** to save the activity log to a file.
- Click **Active Upgrade** in the navigation bar to initiate another readiness test and upgrade with the same configuration.
- Click **Configuration** in the navigation bar to create, edit, or load another configuration file.

IMPORTANT:

Though the Active Upgrade process is complete, your RDR disks continue to resynchronize in the background. If you intend to initiate another upgrade process, you must wait for the resynchronization to complete before you do so. See “Verifying If RDR Disks Are Resynchronizing” on page 5-144 for more information.

TIPS:

Viewing Active Upgrade Process Status, page 5-135

Verifying If RDR Disks Are Resynchronizing, page 5-144

Troubleshooting, page 5-141

Viewing Active Upgrade Process Status

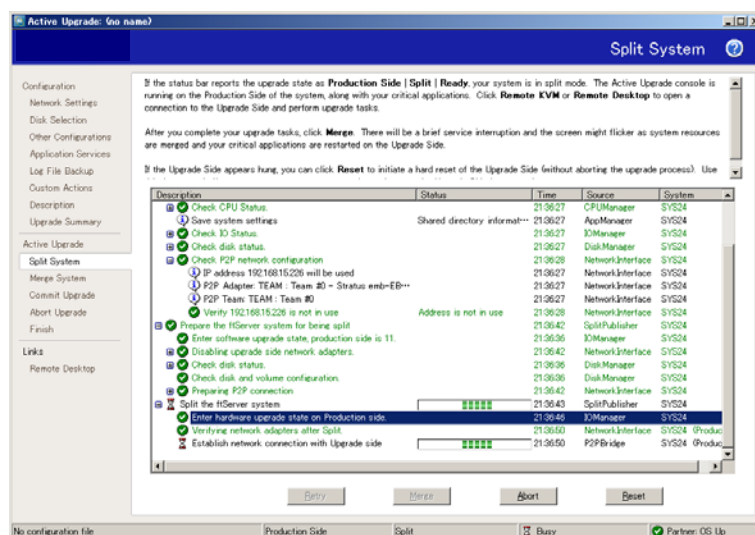
You can view the status of the Active Upgrade process at any point during the upgrade. The Active Upgrade Console indicates status in two ways:


- “Activity Log” on page 5-135
- “Status Bar” on page 5-138

Activity Log

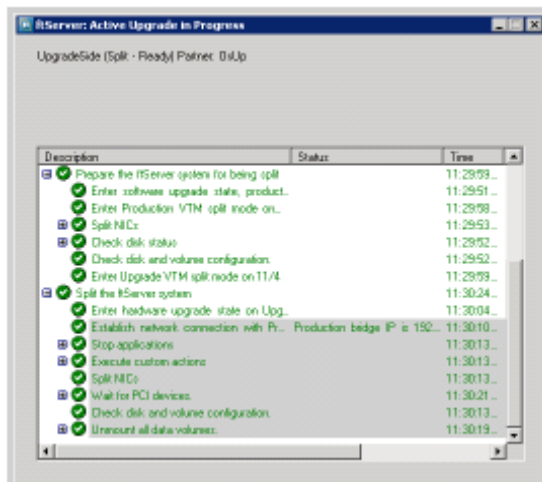
The activity log shown below, which reports details about each upgrade operation, is displayed in the main window of the Active Upgrade Console after you have initiated a readiness test or upgrade session.

Activity Log (in Active Upgrade Console)



If you want to check the status of the upgrade process when you are logged on to the Upgrade Side of the system (while in split mode), you can also double-click the Active Upgrade icon () in the system tray to open the remote activity log shown below.

Remote Activity Log



IMPORTANT:

You can only view status in this window. To control the remaining steps of the Active Upgrade process, you must minimize or close the connection to the Upgrade Side and use the Active Upgrade Console on the Production Side.

Table below describes the general meaning of activity log entries that appear in the local and remote activity logs.

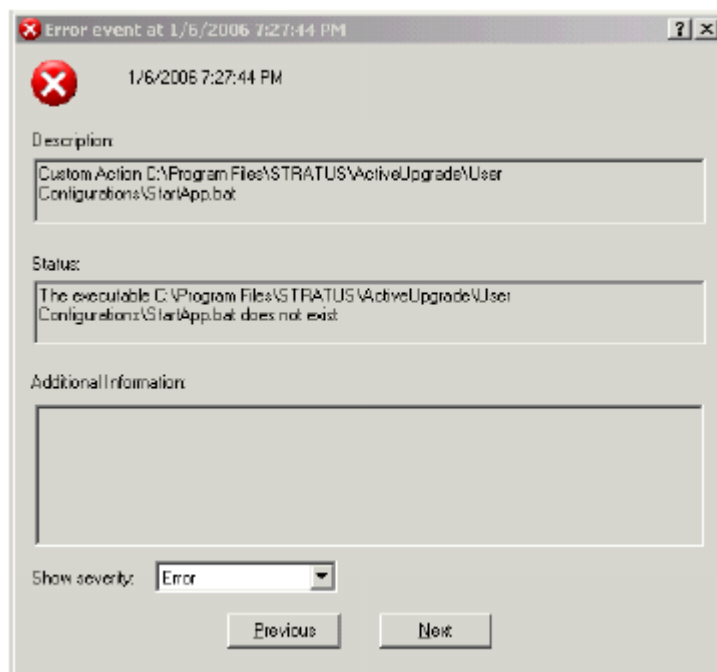
Activity Log Entries

Icon	Text Color	Severity	Description
	Green	Success	Task completed without error
	Black	Pending	Task is in progress
	Black	Information	Task information, no action necessary
	Black	Warning	A problem that should be addressed, but will not block an upgrade
	Red	Error	A problem that must be corrected before continuing with upgrade

Some upgrade items are collapsed into a single line. To display all of the associated items, click on the expand (+) button to the left of the item. To collapse them again, click on the collapse (-) button to the left of the item.

Double-click on any item in the activity log to open a detail window with more information about that item.

Activity Log Detail



In the detail window, you can click the **Previous** and **Next** buttons to review other items of the same severity. For example, if you are viewing an error, you can click **Next** to see the next error item. To change the severity level of the items you want to review, select an option from the **Show severity** pulldown menu. (A severity type will be unavailable if there are currently no items of that severity in the activity log).

If necessary, you save the items from the activity log in the Active Upgrade Console to a file. See “Saving the Activity Log to a File” on page 5-141 for more information.

TIPS:

Status Bar, page 5-138

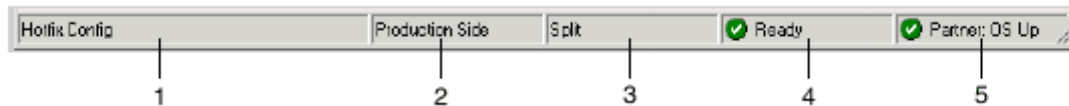
Saving the Activity Log to a File, page 5-141

Troubleshooting, page 5-141

Status Bar

The status bar (below figure), which is located at the bottom of the Active Upgrade Console window, reports a quick summary of the status of the upgrade.

Status Bar



- 1 Configuration file name
- 2 Hardware State (Table 1)
- 3 Upgrade State (Table 2)
- 4 Operational State (Table 3)
- 5 Partner State (Table 4)

The Hardware State reports whether or not your critical applications are running in lockstep. The below table describes the possible hardware states.

Status: Hardware State

Hardware State	Description
Fault-tolerant	The system is duplexed.
Production Side	The system is currently running in split mode, and your applications are running from the Production Side (the original copy of your software). The Upgrade Side is available for installation tasks.

The Upgrade State reports the stage of the upgrade your system is entering or has entered. The below table describes the possible upgrade states.

Status: Upgrade State

Upgrade State	Description
Idle	The current upgrade session is idle. The Active Upgrade process has just finished, or it has not been initiated yet.
Prepare Split	The Active Upgrade Console is preparing to split the system by running a final readiness check and additional background tasks.
Split	If the operational state is Ready , the system is running in split mode. Otherwise, the Active Upgrade Console is in the process of initiating split mode.
Prepare Merge	The Active Upgrade Console is preparing to merge the system by running additional readiness tests and background tasks.
Merge	If the operational state is Ready , the system is merged. Otherwise, the Active Upgrade Console is in the process of merging the system.
Commit	The Active Upgrade Console is in the process of committing your changes (making them permanent).

Upgrade State	Description
Abort	The upgrade process has been aborted, and the Active Upgrade Console is in the process of restoring the system to its previous state.

The Operational State reports the status of the last operation that was requested. Table describes the possible operational states.

Table 3 Status: Operational State

Operational State	Description
Ready	The previous operation has been completed successfully. The Active Upgrade process is ready to enter the next upgrade state.
Busy	The current operation is still in progress. Allow time for the operation to complete.
Broken	The Active Upgrade Console could not complete the current operation. Check the activity log for errors. You must correct the errors and click Retry to complete the operation, or click Abort to abort the current upgrade session.

The Partner State reports the status of the partner system. For example, while the system is in split mode, the Active Upgrade Console is running on the Production Side, and this field reports the health of the Upgrade Side of the system. Table 4 describes the possible partner states.

Table 4 Status: Partner State

Partner State	Description
DC On	The partner system operating system is shut down, but the system still has standby (housekeeping) power.
DC Off	The partner system operating system is shut down and standby power is off.
BIOS POST	The partner system is performing a BIOS Power On Self Test (POST).
Hung: BIOS POST	The partner system hung in the BIOS POST.
OS Booting	The partner operating system is booting.
Hung: OS Booting	The partner system hung in the boot process.
OS Up	The partner operating system is up. (However, the system might not be available for use until other system resources finish loading.)
Hung: OS Up	The partner operating system is hung.
OS Rebooting	The partner operating system is rebooting.
Hung: OS Rebooting	The partner system hung while rebooting.
OS Shutting Down	The partner operating system is shutting down.
Hung: OS	The partner system hung while it was shutting down.

Partner State	Description
OS Crashed	The partner operating system crashed.
OS Shut Down	The partner operating system finished shutting down, but the system is still powered on.

TIPS:

Activity Log, page 5-135

Saving the Activity Log to a File, page 5-141

Troubleshooting, page 5-141

Troubleshooting

If necessary, you can collect information about the Active Upgrade process and resolve problems by:

- Saving the activity log to a file.
- Viewing the status of your application services
- Viewing the status of your installed software.
- Verifying if RDR disks are resynching.
- Learning about general problems and solutions.
- Getting help and support.

Saving the Activity Log to a File

If necessary, you can save the contents of the activity log to a file for later viewing.

To save the activity log to a file

1. Right-click on the activity log, and select **Save to File** in the shortcut menu.
2. Next to **Save in**, select a folder in which to save the file.
3. Next to **File name**, type a name for the file. (Activity log files are saved in XML format, which you can view in Internet Explorer. The .xml extension is added automatically.)
4. Click **Save**.

NOTE:

If you have just completed an upgrade session, you can also save the activity log by clicking **Save Log** on the **Finish** page.

TIPS:

Viewing Active Upgrade Process Status, page 5-135
Troubleshooting, page 5-141

Verifying the Status of Application Services

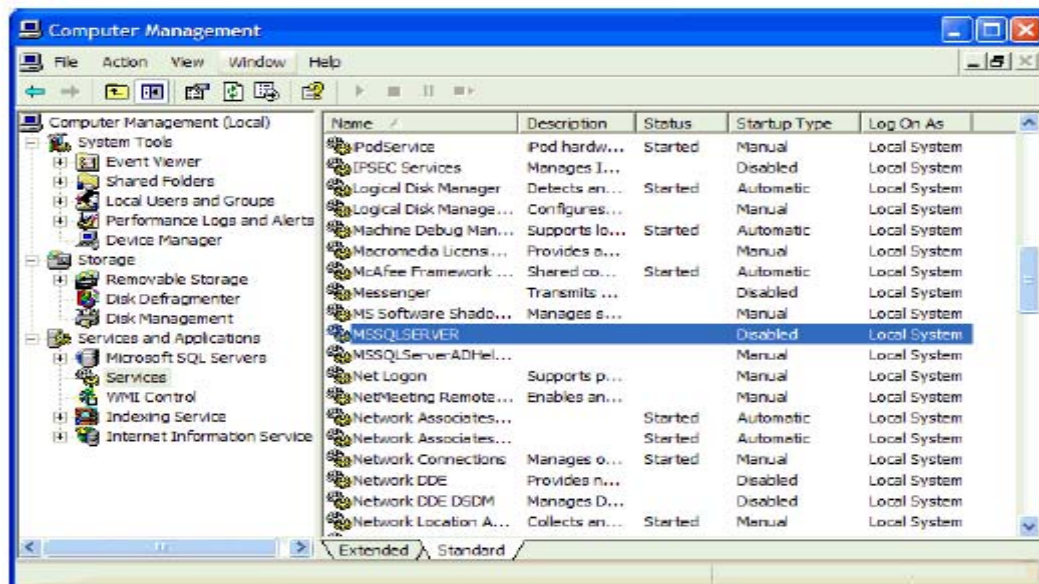
At various stages of the Active Upgrade process, you can optionally verify the status of services you specified for control on the **Application Services** page of the Active Upgrade Console.

To verify the status of a service

1. Right-click **My Computer** on your desktop (or in the **Start** menu).
2. Select **Manage** from the shortcut menu. **Computer Management** is displayed.
3. If necessary, click **Services and Applications** to expand it.
4. Click **Services** to display the below-shown Service Control Manager in the right pane of the window.
5. Search for a service in the list and view its current **Status** and **Startup Type** in the fields next to the service name.

For example, while the system is in split mode, any service you selected for control by the Active Upgrade Console should be stopped (blank **Status** field) and its Startup Type should be **Disabled** on the Upgrade Side of the system, as shown with the MSSQLSERVER service in.

Service Control Manager



TIPS:

Managing Critical Applications During the Upgrade Process, page 5-80

Selecting Application Services to Control, page 5-101

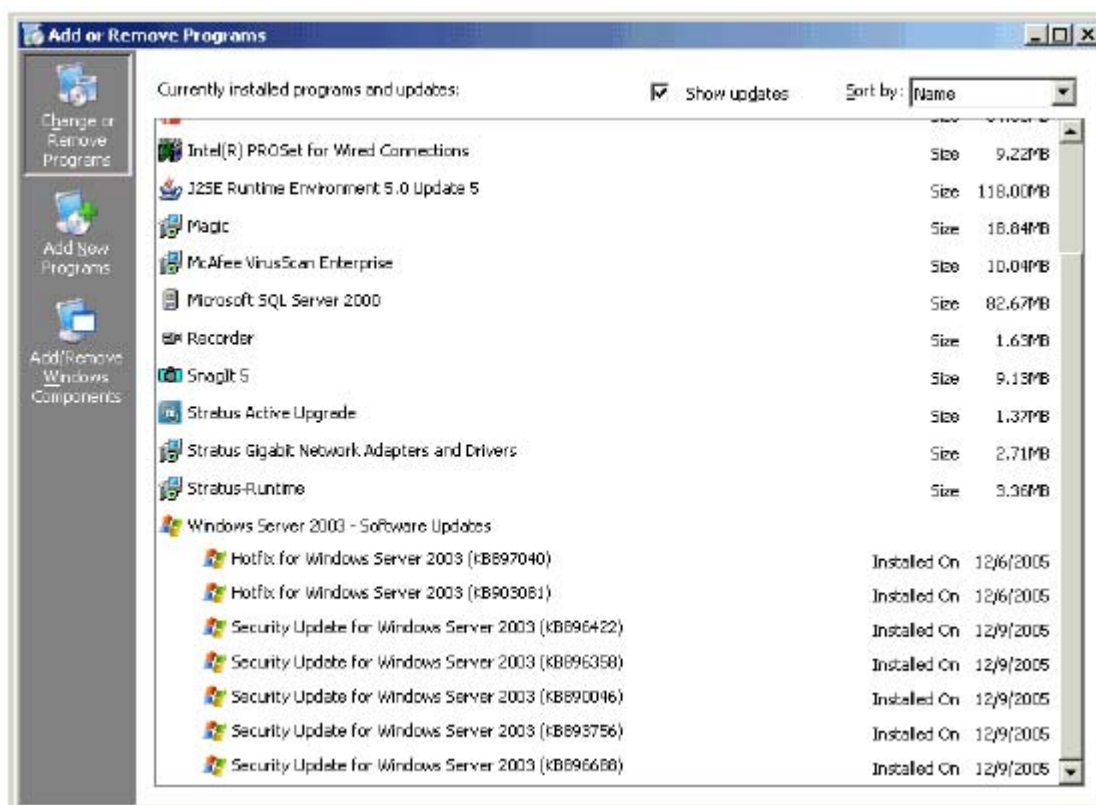
Viewing Active Upgrade Process Status, page 5-135

Troubleshooting, page 5-141

Verifying the Status of Installed Software

While you are running in split or merge mode, or after you have finished the Active Upgrade process, you might want to verify the status of the software packages that you installed.

If necessary, you can view a list of most of the programs present on your system in the **Add or Remove Programs** control panel shown below.

Add or Remove Programs Control Panel

If you installed any Windows updates, select the **Show updates** check box in the control panel to display the updates in the list of programs.

NOTE:

If your system is in split or merge mode, remember to view the **Add or Remove Programs** control panel **on the Upgrade Side**. The same control panel on the Production Side will not list the new software you installed on the Upgrade Side.

TIPS:

Running Software Installers, page 5-121

Viewing Active Upgrade Process Status, page 5-135

Troubleshooting, page 5-141

Verifying If RDR Disks Are Resynchronizing

When you complete or abort the Active Upgrade process, the system reestablishes the mirrors between the RDR partner disks in each CPU- I/O enclosure. If you intend to initiate another upgrade process, you must wait for the resynchronization to complete before you do so.

You can tell if a disk is resynching by viewing the LEDs on the front panel of the disk. For information about interpreting the LEDs, see “Disk Operations Using the RDR (Rapid Disk Resync) Function” in Chapter 3, “Windows Setup and Operation.”

You can also view the status of your disks using one of the following methods:

- Run a readiness check. On the Active Upgrade page, click **Retry**. If the disks are still resynching, the upgrade state will be reported as **Fault Tolerant\Idle\Broken** and the activity log will display errors indicating that the disks are not ready.
- Verify the disks on the Disk Selection page. Any volume that is in red is simplexed (and thus, probably still resynching). When a disk volume is only green, it is duplexed and you can start another upgrade. For more about the disk status on the **Disk Selection** page, see “Selecting Disks to Upgrade” on 5-98.

To view the status of an RDR virtual disk in RDR Utility

1. On RDR Utility, click **Logical Disk Information**.
2. Click one of the **RDR Virtual Disk** items (RDR Virtual Disk x).
3. Check the value of the **Status** property, which displays **Resync nn%** (where *nn* is the percentage completed) while the disk is resynchronizing. When the resync process is finished, the value is **None**.

Ensure that the value of the **Status** property for all RDR Virtual Disks is **None** before you retry the Active Upgrade process.

TIPS:

Selecting Disks to Upgrade, page 5-98

Performing a Readiness Check, page 5-111

Viewing Active Upgrade Process Status, page 5-135

Troubleshooting, page 5-141

General Problems and Solutions

The table below describes some common problems that could prevent your system from passing the readiness check.

IMPORTANT:

Never perform hardware maintenance, such as removing and replacing system components, while the Active Upgrade process is running. If you experience a problem that prevents the Active Upgrade process from completing successfully, you should always be able to abort the upgrade session to restore your system to its original state.

Troubleshooting: Readiness Check

Error	Action
IO board <i>nn</i> is unsafe to pull	Verify that all critical system resources (including disks, Ethernet PCI adapters, and VTMs) are configured correctly and duplexed. See “Prerequisites” on page 5-78 for more information.
RDR disk is not duplexed	If you recently ran an upgrade session, wait for the RDR resynchronization process to complete before running another upgrade session. See “Verifying If RDR Disks Are Resynchronizing” on page 5-144 for more information.
Embedded NIC not teamed	Use the PROset utility to configure your Ethernet PCI adapters into teams. All embedded Ethernet PCI adapters must be teamed. See “Prerequisites” on page 5-78 and “Recommendations” on page 5-79 for more information about configuring Ethernet PCI adapters.
No IP address on Upgrade ready team	Use the Network Connections control panel to assign an IP address (preferably a static IP address) to the Ethernet team. See “Prerequisites” on page 5-78 and “Recommendations” on page 5-79 for more information about configuring Ethernet PCI adapters.
Team does not have link on both sides	Ensure that an embedded Ethernet team has at least one adapter in each CPU- I O enclosure with an active network link. Verify that the network cables are plugged in on both sides, and that the Ethernet team has a valid IP address. See “Prerequisites” on page 5-78 and “Recommendations” on page 5-79 for more information about configuring Ethernet PCI adapters.
Active Upgrade may fail. Check DHCP server.	The Active Upgrade Console cannot obtain IP addresses from your DHCP server. If possible, assign static IP addresses to your Ethernet teams and VTMs to avoid problems during the Active Upgrade process.

The following tables describes some common problems with custom actions.

Troubleshooting: Custom Actions

Error	Action
The executable <i>filename</i> does not exist.	Ensure that the executable file associated with your custom action is located in the directory you specified during the configuration process. Also, ensure that the custom action is located on a system disk, otherwise the Upgrade Side will lose access to the executable while the system is in split mode.
Custom action failed with exit value <i>n</i>	<p>Check the output for the custom action for errors. See “Viewing Standard Output and Error Stream” on page 5-107 for more information.</p> <p>You must correct the problem and click Retry in the Active Upgrade Console to retry the current upgrade request (which also runs the custom action again). The Active Upgrade process will not continue until the executable for your custom action runs successfully.</p> <p>If possible, test and debug the executable outside of the Active Upgrade process. Ensure that it terminates with exit value 0 and that it completes in a timely manner.</p>

Troubleshooting: Miscellaneous Problems

Problem	Action
Active Upgrade Console fails to start	Wait a minute, and try to start Active Upgrade Console again. If the problem persists, it might mean that the Active Upgrade Console cannot communicate with related services on your local system. If your system is running a network firewall solution, check the firewall logs for blocked communications and explicitly add these items to your trusted zone. For information about configuring Windows Firewall, see “Configuring Windows Firewall for the Active Upgrade Process” on page 5-84.
Remote KVM browser window appears, but does not open connection	Ensure that Java™ 2 Runtime Environment (JRE) is installed and running. Also ensure that you have added the VTM console Web address to your Trusted Sites list, and that you have allowed blocked Web-based content. See “Connecting to the Upgrade Side with Remote KVM” on page 5-118 for more information.
Failed to disable PCI device: QLogic Fibre Channel Adapter	If you have installed QLogic SANsurfer Fibre Channel HBA Software to upgrade the BIOS in your host bus adapter, you should uninstall this utility when you are done upgrading the BIOS. If the utility remains on your system, it may retain access to storage system resources and prevent certain storage operations. In this case, the Active Upgrade Console cannot split system resources because it cannot disable the HBA on the Upgrade Side. To resolve the problem, you must abort the upgrade, uninstall SANsurfer, restart the system (or stop the SANsurfer service), and restart the upgrade process.
The underlying connection was closed: Unable to connect to the remote server	If your system is running a network firewall solution, check the firewall logs for blocked communications and explicitly add these items to your trusted zone. For information about configuring Windows Firewall, see “Configuring Windows Firewall for the Active Upgrade Process” on page 5-84.
A connection attempt failed because the connected party did not properly respond...	
Unable to see the disc that should exist in [Disk Managing] in [Computer Management].	Go to [Disk Management] and execute [Disk Rescan]. When the disk status appears [Missing] or [Offline], right click the disk and select [Disk Reactivation] to verify the disk status becomes [Online].

TIPS:

Viewing Active Upgrade Process Status, page 5-135

Troubleshooting, page 5-141

This page is intentionally left blank.

Chapter 6

Maintenance

This chapter describes the daily maintenance of Fault Tolerant Server series and precautions when relocating or storing the server.

Checking Alert

Always check whether any alert is reported to NEC ESMPro Manager on the management PC. Check whether any alert is reported on the Operation Window, Data Viewer, or Alert Viewer of NEC ESMPro Manager.

[illegible]

Summary	C.	R.	Type	Manager	Component	Address	Received
Mail Store...			T:Security	mrg_199427	199427	140.0.0.27	02/14/2006
Mail Store...			T:Security	mrg_199427	199427	140.0.0.27	02/14/2006
Mail Store...			T:Security	mrg_199427	199427	140.0.0.27	02/14/2006
PowerLine Rec...			D:PowerS	mrg_199427	199427	140.0.0.27	02/09/2006
Power Supply Error			D:PowerS	mrg_199427	199427	140.0.0.27	02/09/2006
Power Supply Error			D:PowerS	mrg_199427	199427	140.0.0.27	02/09/2006

The screenshot shows the TOPYAK 2.0 software interface. The main window is titled "TOPYAK 2.0 (UNITED MARS)". On the left, there is a tree view showing the configuration structure. The central area displays a photograph of the TOPYAK 2.0 device. On the right, there is a detailed configuration table for the selected device.

Field	Value
Name	Example1
Model	Example1
Manufacturer	Example1
Version	1.0.0.0
IP Address	192.168.1.1
Port	502
Modbus	Enabled
BACnet	Enabled
LonWorks	Enabled
Protocol	Modbus
Device Type	Device
Device ID	1
Device Name	Example1
Device Address	1
Device Description	Example1
Device Manufacturer	Example1
Device Model	Example1
Device Version	1.0.0.0
Device IP Address	192.168.1.1
Device Port	502
Device Protocol	Modbus
Device Device Type	Device
Device Device ID	1
Device Device Name	Example1
Device Device Address	1
Device Device Description	Example1
Device Device Manufacturer	Example1
Device Device Model	Example1
Device Device Version	1.0.0.0
Device Device IP Address	192.168.1.1
Device Device Port	502
Device Device Protocol	Modbus

Data Viewer

Checking STATUS LEDs

Check the LED indication on the front of the Fault Tolerant Server series, on hard disks installed in 3.5-inch hard disk drive bay, or on LCD display when the server is powered on or powered off by the shut down operation. The functions and indications of LEDs are described in Chapter 2. If any indication that shows an error, contact your sales agent.



Making Backup Copies

We recommend you make backup copies of your valuable data stored in hard disks of the server on a regular basis. For backup storage devices suitable for the server and backup tools, consult with your sales agent.

When you have changed the hardware configuration or BIOS configuration, select "System Information Management" and then "Save" of the Off-line Maintenance Utility to make a backup copy of the system information.

Cleaning

Clean the server on a regular basis to keep the server in a good shape.

 WARNING	
	<p>Observe the following instructions to use the server safely. There are risks of death or serious personal injury. See "PRECAUTIONS FOR SAFETY" in Chapter 1.</p> <ul style="list-style-type: none"> • Do not disassemble, repair, or alter the server. • Do not look into the DVD-ROM drive. • Disconnect the power plug before cleaning the server.

Cleaning the Fault Tolerant Server series

For daily cleaning, wipe the external surfaces of the server with a dry soft cloth. Follow the procedure below if stains remain on the surfaces:

IMPORTANT:

- To avoid altering the material and color of the server, do not use volatile solvents such as thinner or benzene to clean the server.
 - The power receptacle, the cables, the connectors on the rear panel of server, and the inside of the server must be kept dry. Do not moisten them with water.
-

1. Make sure that the server is powered off.
2. Unplug the power cord of the server from a power outlet.
3. Wipe off dust from the power cord plug with a dry cloth.
4. Soak a soft cloth in neutral detergent that is diluted with cold or warm water, and squeeze it firmly.
5. Rub off stains on the server with the cloth prepared in Step 4.
6. Soak a soft cloth in water, squeeze it firmly and wipe the server with it once again.
7. Wipe the server with a dry cloth.
8. Wipe off dust from the fan exhaust opening on the rear of the server with a dry cloth.

Cleaning the Keyboard and Mouse

IMPORTANT:

A keyboard and a mouse use USB interface. Therefore it is not necessary to power off the server when connecting or disconnecting them.

Disconnect the keyboard from the server while the devices in the system (the server and the peripheral devices) remain turned on. Wipe the keyboard surface with a dry cloth. Then connect the keyboard to the server.

The mouse operation depends on the degree of smoothness of the internal ball rotation. To keep the mouse ball clean, use the mouse in a place with little dust. Follow the steps below to clean the mouse regularly:

1. Disconnect the mouse from the USB port of the keyboard while the server remains powered on.
2. Turn the mouse upside down, and rotate the mouse ball cover counterclockwise to remove it. Take out the ball from the mouse.
3. Wipe the mouse ball with a dry soft cloth.

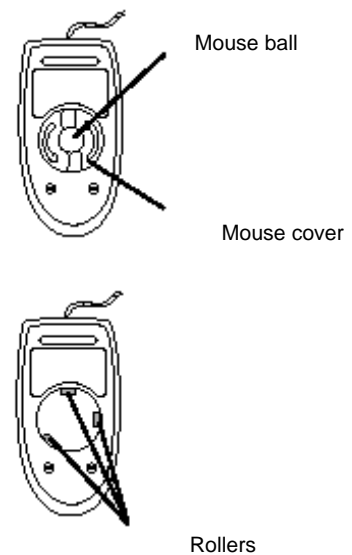
If stains remain, use a soft cloth to wipe them off. Soak the soft cloth in neutral detergent that is diluted with water or warm water, and squeeze it firmly.

4. Wipe three small rollers inside the mouse with cotton swab.
Use the cotton swab soaked with alcohol if stains remain.

5. Put the mouse ball back into the mouse.

If the mouse or rollers are wet in steps 3 and 4, put it back after fully dried.

6. Place the mouse ball cover, and rotate it clockwise until it is locked.
7. Connect the mouse to the server .



Cleaning the Floppy Disk Drive

A read/write error may occur due to stains on the read/write head of the floppy disk drive.

Use the cleaner dedicated for floppy disk drive to clean the read/write head. It is recommended to clean the head on regular basis.

Cleaning DVD/CD-ROM

A dusty DVD/CD-ROM or dust-accumulated tray causes the device to fail to read data correctly.

Follow the procedure below to clean the tray and DVD/CD-ROM regularly:

1. Make sure that the server is powered on.
2. Press the Eject button on the front of the DVD-ROM drive.
The tray comes out.
3. Hold the DVD/CD-ROM lightly and take it out from the tray.

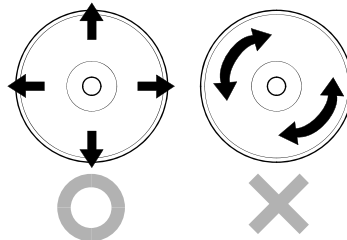
IMPORTANT: Do not touch the signal side of the DVD/CD-ROM with your hand.

4. Wipe the tray with a dry soft cloth.

IMPORTANT: Do not wipe the lens of the DVD-ROM drive. Doing so may damage the lens and may cause a malfunction of the drive.

5. Gently push on the tray front to close the tray.
6. Wipe the signal side of the CD/DVD-ROM with a dry soft cloth.

IMPORTANT: Wipe DVD/CD-ROMs from the center to the outside. Use only CD-ROM cleaner if necessary. Cleaning a DVD/CD-ROM with record spray/cleaner, benzene, or thinner causes damage to the DVD/CD-ROM contents. At worst, inserting the DVD/CD-ROM into the server may cause failure.



Cleaning Tape Drive

Dirt on the tape head may be a cause of unsuccessful backup and damage to tape cartridge. Clean the tape head regularly using a cleaning tape. For procedure and interval of cleaning as well as lifetime of a tape cartridge to use, see instructions included with the tape drive.

SYSTEM DIAGNOSTICS

The System Diagnostics runs several tests on the server.

Select [Tool menu] - [Test and Diagnostics] in the **EXPRESSBUILDER** to diagnose the system.

Test Items

The following items are tested in system diagnostics.

- Memory
- CPU cache memory
- Hard disk drive used as a system

IMPORTANT: When executing the system diagnostics, make sure to remove the LAN cable. Executing the system diagnostics with the LAN cable connected, the network may be influenced.

TIPS: On checking the hard disk drive, no data is written into the disk.

Startup and Exit of System Diagnostics

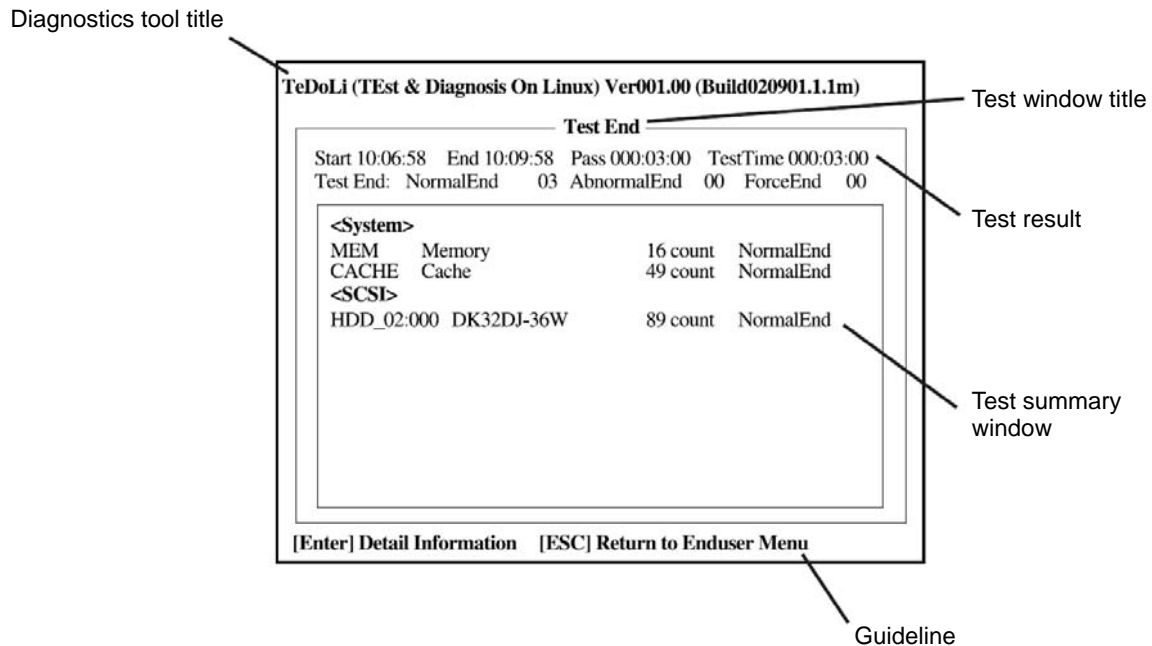
Follow the steps below to start the system diagnostics. (If the server is running, shut it down, and execute Step 1 through Step 12.)

1. Shutdown the OS, and power off the server. Then, unplug the power cord.
2. Disconnect all the LAN cables from the server.
3. Plug the power cord and power on the server.
4. Use the **EXPRESSBUILDER** DVD to start the system.
5. Select [Tool menu].

6. Select [Test and diagnostics].

Select [End-User Mode] and the system diagnostics starts. The diagnostics will be completed in approximately three minutes.

When the diagnostics is completed, the screen of the display changes as shown below:



Diagnostics tool title

Shows the name and version of the diagnostic tool.

Test window title

Shows the progress of the diagnostics. “Test End” is displayed when the diagnostics completes.

Test result

Shows the start, end, and elapsed time and completion status of the diagnostics.

Guideline

Shows the details of the keys to operate window.

Test summary window

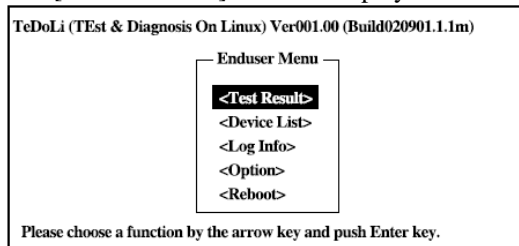
Shows the results of each test that executed the diagnostics. Move the cursor and press the **Enter** key on the cursor line to display the details of the test.

When an error is detected by the system diagnostics, the relevant test result in the test summary window is highlighted in red, and “Abnormal End” is displayed in the result on the right side.

Move the cursor to the test that detected the error, and press the **Enter** key. Record the error message that has been output to the Detail Information screen and contact your sales agent.

7. Follow the guideline shown at the bottom of the screen, and press the **Esc** key.

The [Enduser Menu] below is displayed.



<Test Result>

Shows the diagnostics completion screen of the above diagnostics.

<Device List>

Shows a list of connected devices.

<Log Info>

Shows the log information of the diagnostics. It can be saved on a floppy disk. To save it on a floppy disk, insert a formatted floppy disk to the floppy disk drive, and select <Save(F)>.

<Option>

Optional features can be used from this menu.

<Reboot>

Reboots the system.

8. Select <Reboot> in the [Enduser Menu] above.
The server restarts and the system is started from the **EXPRESSBUILDER**.
9. Exit the **EXPRESSBUILDER**, and remove the DVD from the DVD-ROM drive.
10. Power off the server and unplug the power cord from the receptacle.
11. Reconnect all the LAN cables that have been disconnected in Step 2 to the server.
12. Plug the power cord.

This completes the system diagnostics.

OFF-LINE MAINTENANCE UTILITY

The Maintenance Tools is a tool of this product for preventive maintenance, as well as for trouble analysis and its settings. Follow the below procedure to start the Maintenance Tool.

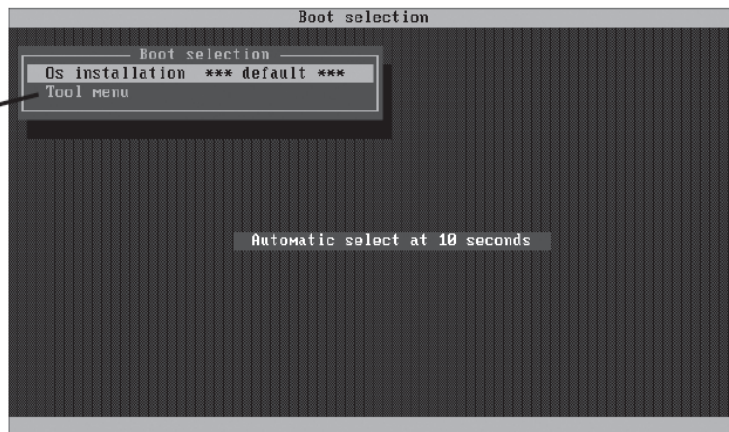
Starting the Off-line Maintenance Utility

The Off-line Maintenance Utility may be started in the following ways.

Fault Tolerant Server series does not support the feature to start the Off-line Maintenance Utility from the maintenance partition.]

1. Boot peripheral devices at first, then power on the Express server.
2. Load the [EXPRESSBUILDER] DVD into the optical disc drive of the Express server.
3. After loading the DVD, reset (by pressing <Ctl> + <Alt> + <Delete> keys) or power off and on to reboot the Express server.
Following menu appears on the DVD.

Tool Menu:
Select this to launch the Off-line
Maintenance Utility.



IMPORTANT:

Default selection is [OS installation] on the menu. When there is no operation for ten seconds after the Boot Selection menu appears, [OS installation] starts automatically.

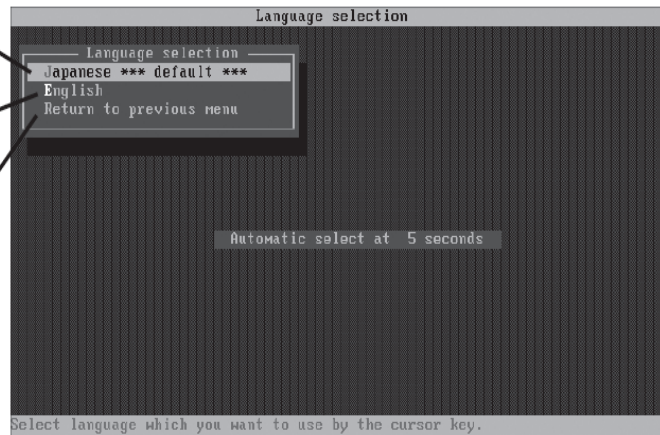
4. Select [Tool Menu].

Following Language selection menu appears.

Japanese:
Menu is displayed in Japanese
from now

English:
Menu is displayed in English
from now

Return to previous menu:
Boot Selection menu is
displayed



IMPORTANT:

Default menu selection is [Japanese]. When there is no key operation for five second after Language menu appears, [Japanese] starts automatically.

5. Select [English]

When [English] is selected, following tool menu appears.



6. Select one of the tool and start.

Function of Maintenance Tools

The following functions are available in the Maintenance Tools.

Maintenance Utility

The Off-line Maintenance Utility is started in “Maintenance Utility.” The Off-line Maintenance Utility is an OS-independent maintenance program. When you are unable to start the OS-dependent NEC ESMPRO to troubleshoot a problem, the Off-line Maintenance Utility can be used.

IMPORTANT:

- The Off-line Maintenance Utility is intended for use of your service representative. The **EXPRESSBUILDER** DVD contains a file that describes the operation of the utility, but do not attempt to use the utility by yourself. Contact your service representative and follow their instructions.
 - See the on-line help for details for the Off-line Maintenance Utility. For further information, ask your service representative.
-

The Off-line Maintenance Utility provides the following features.

- IPMI Information Viewer

Provides the functions to view the system event log (SEL), sensor data record (SDR), and field replaceable unit (FRU) and to make a backup copy of them.

Using this feature, you can find system errors and events to determine a maintenance part.
- BIOS Setup Viewer

Provides the functions to export the current configuration data defined with the SETUP utility to a text file.
- System Information Viewer

Provides the functions to view and information on the processor (CPU) and on the BIOS. You can export the information to a text file.
- System Information Management

Provides the function to make a back-up copy of your data.

Without the backup data, the system-specific information and/or configuration may not be restored.

Only the authorized service maintenance staff is allowed to restore the backup data.
- System Management

The parameters of BMC (Baseboard management Controller) are set for remote control and alert.
- BIOS/FW Updating

This menu allows you to update the software module such as BIOS and firmware of the server by using the update disk (3.5-inch floppy disk) that is distributed from your customer service representative.

After rebooting the system, an update program is started automatically from floppy disk, and the various BIOS and firmware programs are updated.

IMPORTANT:

Do not turn off the server while the update program is running. If the update processing is discontinued, the system becomes unable to start.

- ROM-DOS startup FD

Create a support disk for starting the ROM-DOS system.

- Test and diagnostics

Execute various tests on the server system to check if the server functions are normal and if the connection between the server and additional board is normal.

After the Test and diagnostics is executed, a system check program assigned to each model starts.



- System Management

The parameters of BMC (Baseboard Management Controller) are set for remote control and alert.

This menu's function is the same as the "System Management" of the "Maintenance Utility."

RELOCATING/STORING THE FAULT TOLERANT SERVER SERIES

Follow the procedure below to relocate or store the server.

 CAUTION	
	<p>Observe the following instructions to use the server safely. There are risks of fire, personal injury, or property damage. See “PRECAUTIONS FOR SAFETY” in Chapter 1 for details.</p> <ul style="list-style-type: none">• Never attempt to lift the server only by yourself.• Do not install the server in any place other than specified.• Do not connect/disconnect any interface cable with the power cord of the server plugged to a power source.

IMPORTANT:

- If the server needs to be relocated/stored due to a change in the floor layout to a great extent, contact the sales agent.
 - Make sure to make a backup copy of your valuable data in the hard disk, if any.
 - When moving the server with hard disks, make sure not to give a shock to the hard disks.
 - When storing the server, keep it under storing environment conditions (temperature: -10 to 55°C, humidity: 20 to 80%, non-condensing).
-

1. Take a floppy disk and a DVD out of the server, if any.
2. Power off the server.
3. Unplug the power cord of the server from a power outlet.
4. Remove all the cables from the server.
5. Remove all the mounted CPU/IO modules.
6. Remove the 4U chassis and the rails from the rack cabinet.
7. Carry 4U chassis and CPU/IO modules separately.
8. Protect the server with the shock-absorbing materials, and pack it securely.

IMPORTANT:

Check and adjust the system clock before operating the server again after relocating or storing it.

If the server and the built-in optional devices are moved from a cold place to a warm place in a short time, condensation will occur and cause malfunctions and breakdown when these are used in such state. When you start operating these equipments again after the transportation or the storage, make sure to wait for a sufficient period of time to use them in the operating environment.

If the system clock goes out of alignment remarkably as time goes by, though the system clock adjustment is performed, contact your sales agent.

TO THE ACCIDENT OF PCI MODULE

You may encounter the following error during the mirroring procedure in a case such as after module is added; however, hard error does not occur.

Check whether the following error log is added.

If the error log is added, perform the following procedure.

If it is not hard error, you can recover. If this procedure is failed, contact your Administrator or a member of the Administrators group.

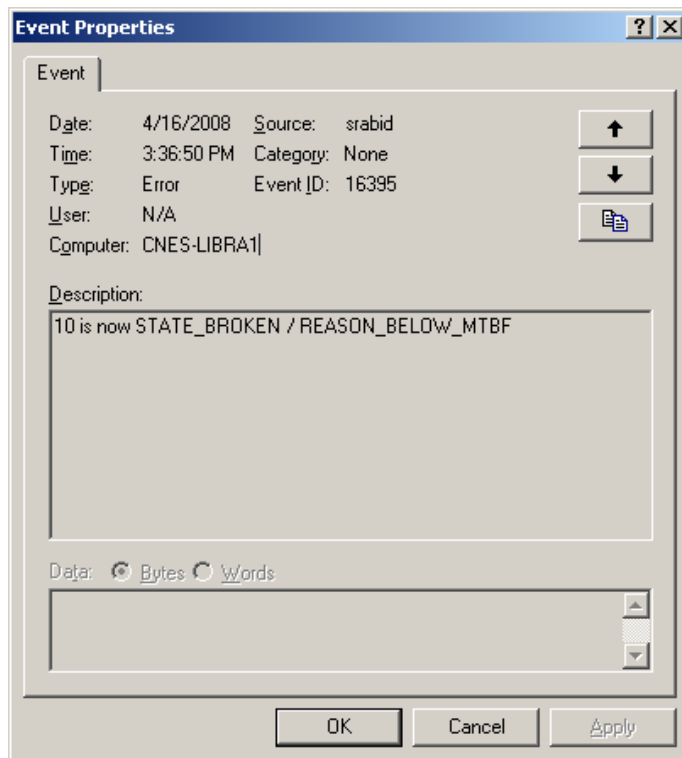
Procedure to Confirm

Check the following message from the event log.

Note: Sample of PCI module 1 (ID: 10).

Source : srabid

Event ID : 16395



Procedure to Recover

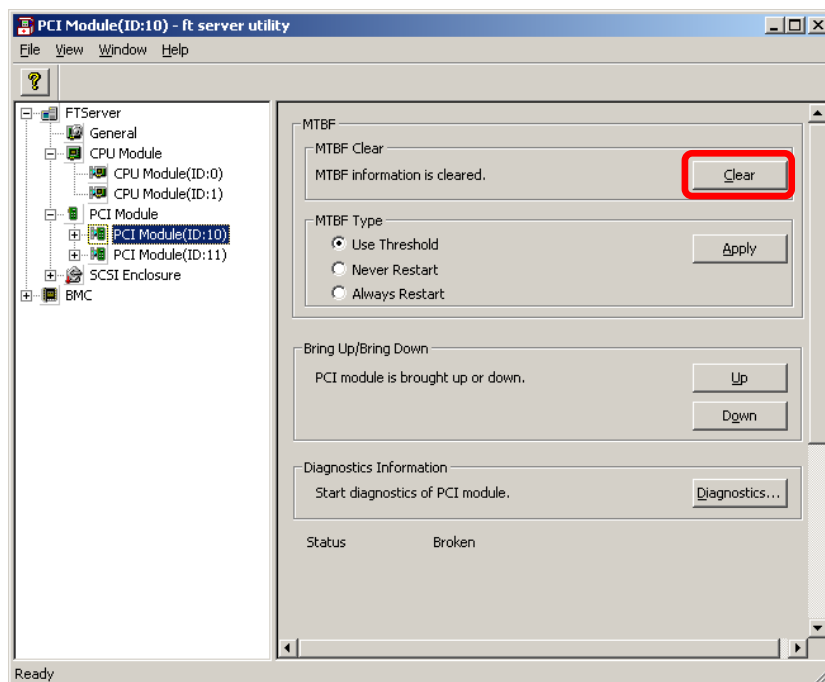
If access of system is high, cancel the procedure or reduce the access.

(1) Clear MTBF by PCI module and stop/start of PCI module by ft server utility.

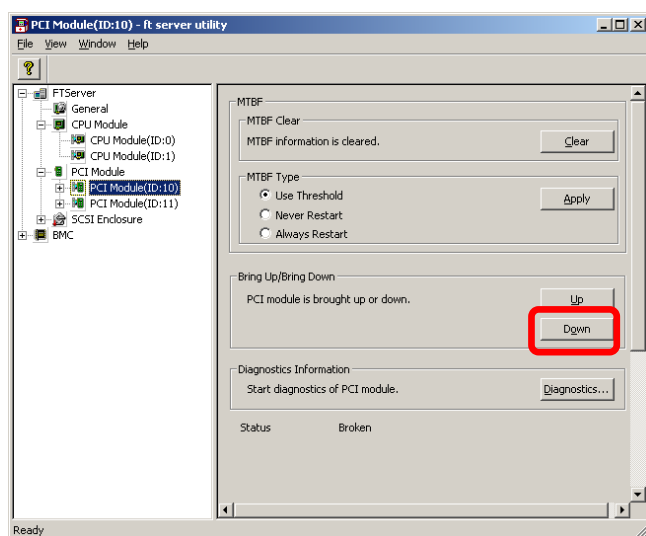
Procedure

1. Cancel the procedure or wait for finish of the procedure.
2. Clear of MTBF by PCI module 1 (ID:10).
3. Stop the PCI module 1.
4. Start the PCI module 1.

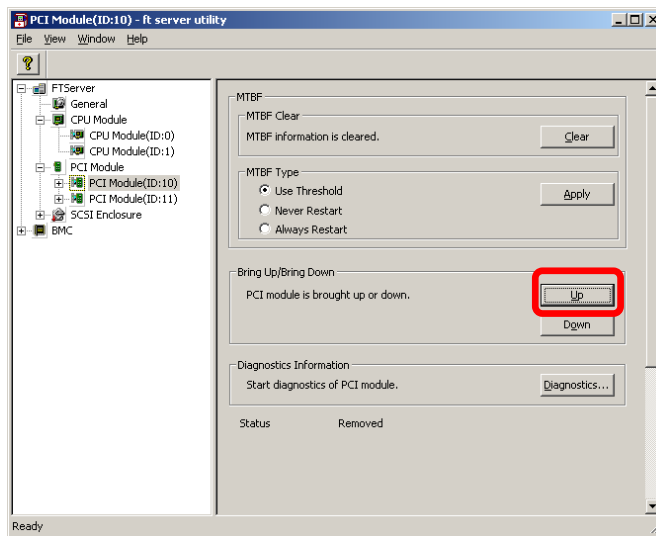
(2) Clear MTBF by the PCI module 1.



(3) Stop of PCI module 1.

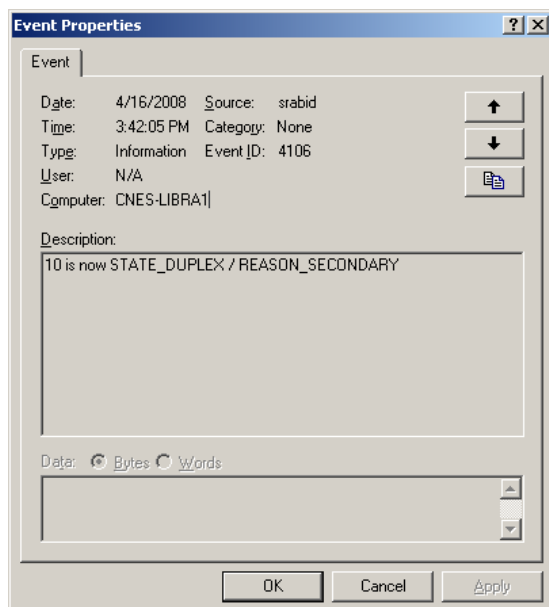
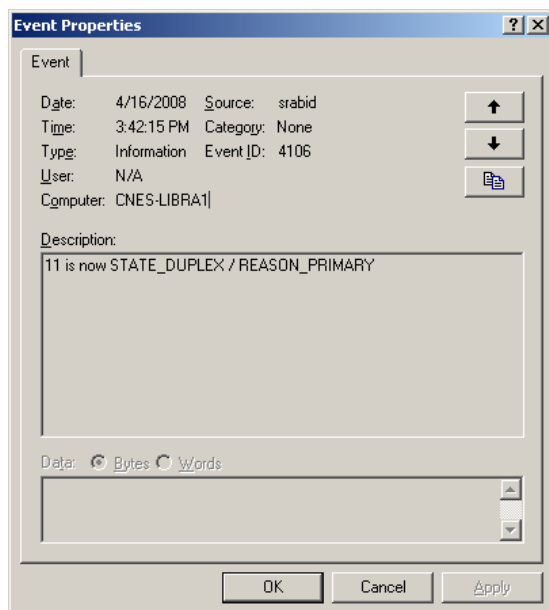


(4) Start of PCI module 1.



Procedure to Check

Check whether the following error is added on system event log.
If following events are added, the procedure is performed correctly.



(This page is intentionally left blank.)

Chapter 7

Troubleshooting

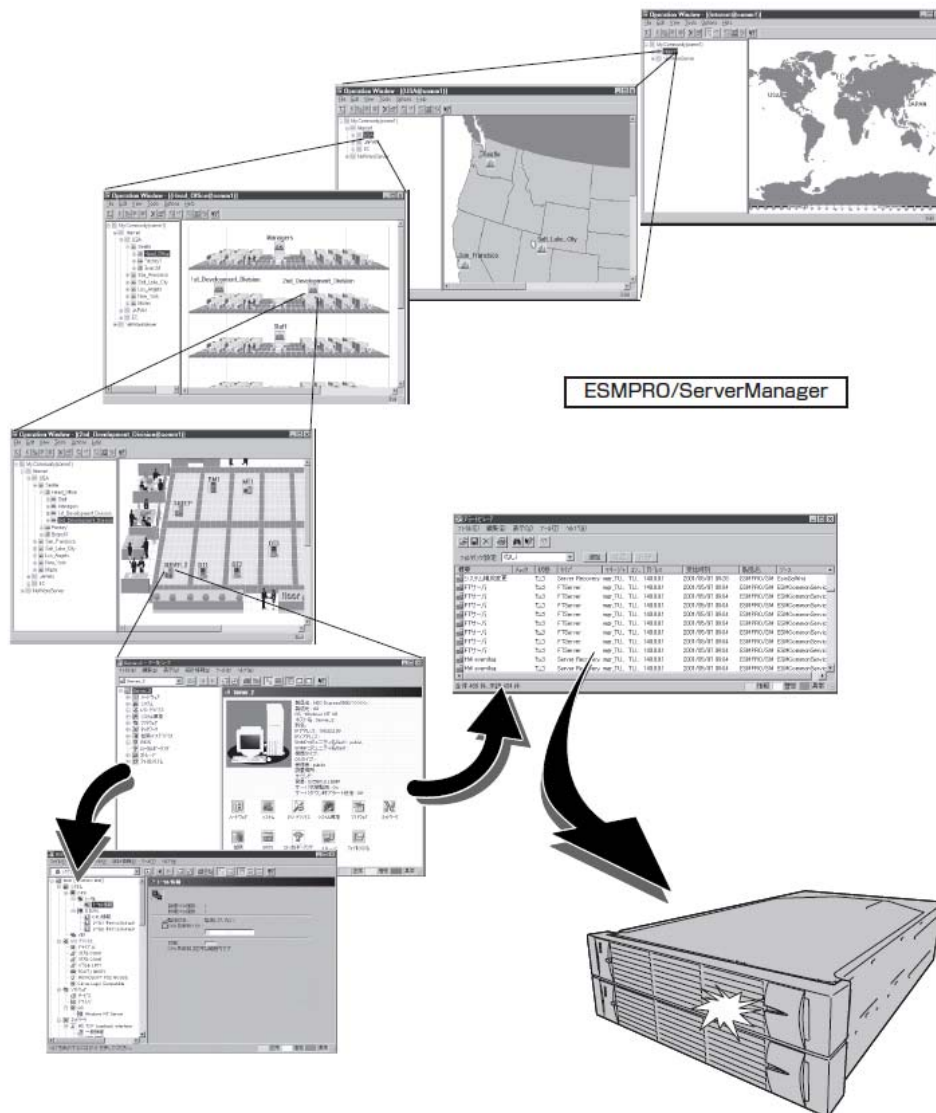
This section covers some of the issues that can occur with this server, and provides the trouble shooting steps you can refer to.

TO LOCATE THE ERRORS

Use NEC ESMPRO to monitor the occurrence of fault during the system operation.

Especially take note on whether any alert is reported to NEC ESMPRO Manager on the management PC. Check whether any alert is reported on the Operation Window, Data Viewer, or Alert Viewer of NEC ESMPRO Manager.

[Example]



ERROR MESSAGES

If the Fault Tolerant Server series enters the abnormal state, the error is posted by various means. This section explains the types of error messages.

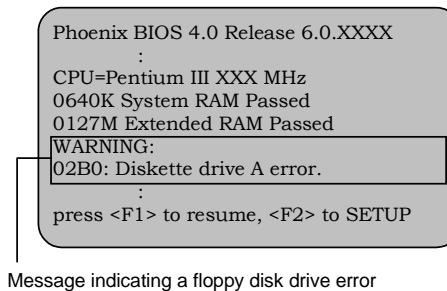
Error Messages by LED Indication

The LEDs on the front and rear panels of the Fault Tolerant Server series and near the handles of hard disks inform the user of the various server statuses by the colors and the patterns of going on, going off, and flashing. If trouble seems to have occurred, check the LED indication. For the LED indication and meanings, see page 2-17 “LEDs.”

This User’s Guide describes actions to be taken for watch error message. However, if replacement of modules is necessary, contact your sales agent.

POST Error Messages

Powering on the server automatically starts the self-diagnostic program, POST (Power On Self-Test). When POST detects any error, it displays an error message and its measure on the display unit. Follow the table below to troubleshoot such errors.



Message indicating a floppy disk drive error

TIPS:

For error messages on optional PCI boards, refer to the manual provided with those options.

On-screen error message	Cause	Action
0200 Failure Fixed Disk	<ul style="list-style-type: none"> HDD is faulty CPU/IO module is faulty. 	<ul style="list-style-type: none"> Replace the HDD. Replace the CPU/IO module.
0210 Stuck Key	Keyboard connection error	<ul style="list-style-type: none"> Disconnect the keyboard and connect it back again. Replace the keyboard.
0211 Keyboard error	Keyboard is faulty.	<ul style="list-style-type: none"> Disconnect the keyboard and connect it back again. Replace the keyboard. If restarting does not help, replace the CPU/IO module.
0212 Keyboard Controller Failed	Keyboard controller is faulty.	If restarting the server does not help, replace the CPU/IO module.
0213 Keyboard locked - Unlock key switch	Keyboard is locked.	Unlock the key switch.
0230 System RAM Failed at offset	DIMM is faulty.	<ul style="list-style-type: none"> Replace DIMM. Replace the CPU/IO module.
0231 Shadow RAM Failed at offset	Shadow RAM is faulty.	<ul style="list-style-type: none"> Replace DIMM. Replace the CPU/IO module.
0232 Extended RAM Failed at address line	Extended RAM is faulty.	<ul style="list-style-type: none"> Replace DIMM. Replace CPU/IO module.
0233 Memory type mixing detected	Memory of the different types is installed.	Memory of the different types is installed. Replace DIMM with appropriate one.
0250 System battery is dead -Replace and run SETUP	System battery is dead.	<ul style="list-style-type: none"> Replace system battery. Replace CPU/IO module.
0251 System CMOS checksum bad-Default configuration used	System CMOS configuration is changed.	<ul style="list-style-type: none"> Reconfigure the system CMOS by using BIOS setup. Clear system CMOS using hardware jumper.
0252 Password checksum bad -Password cleared	Password is cleared.	<ul style="list-style-type: none"> Reconfigure by using BIOS setup. Clear system CMOS using hardware jumper.
0260 System Timer error	System Timer is faulty.	Reconfigure by using BIOS setup. If the error cannot be solved after this, replace the CPU/IO module.
0270 Real time clock error	RTC is faulty.	
0271 Check date and time setting	Date and time are incorrectly set.	

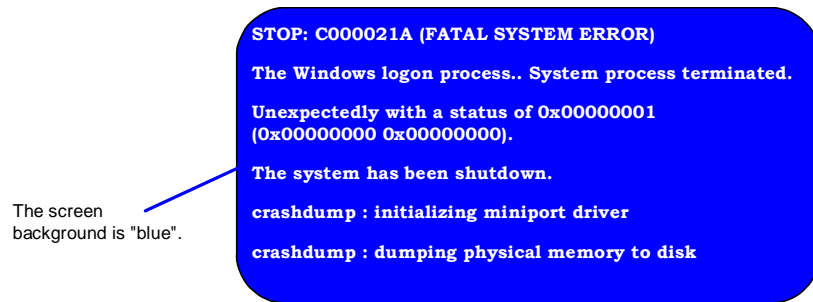
On-screen error message	Cause	Action
02D0 System cache error - Cache disabled	CPU cache is faulty.	If replacing the CPU does not help, replace the CPU/IO module.
02D1 System Memory exceeds the CPU's caching limit	CPU cache is faulty.	
0613 COM A configuration change	COM A configuration is faulty.	If restarting does not help after resetting the setting to default by using BIOS setup, replace the CPU/IO module.
0614 COM A config, error - device disable	Device constructing COM A is faulty.	
0615 COM B configuration change	COM B configuration is faulty.	
0616 COM B config, error - device disable	Device constructing COM A is faulty.	
0B28 Unsupported Processor detected on Processor 1	Unsupported CPU is mounted.	Check the supported CPU and replace it. If this does not help, replace the CPU/IO module.
0B29 Unsupported Processor detected on Processor 2	Unsupported CPU is mounted.	
0B80 BMC Memory Test Failed	RMC device is faulty.	Replace the CPU/IO module.
0B81 BMC Firmware Code Area CRC check failed		
0B82 BMC core Hardware failure		
0B83 BMC IBF or OBF check failed	RMC device is faulty.	Replace the CPU/IO module.
0B8B BMC progress check timeout	BMC check is suspended.	Replace the CPU/IO module.
0B8C BMC command access failed	BMC command access failed.	Replace the CPU/IO module.
0B90 BMC Platform Information Area corrupted	BMC device is faulty.	Replace the CPU/IO module.
0B91 BMC update firmware corrupted		
0B92 Internal Use Area of BMC FRU corrupted	Data within SROM is faulty.	Replace the system backboard.
0B93 BMC SDR Repository empty	SDR data is faulty.	If updating SDR does not help, replace the CPU/IO module.
0B94 IPMB signal lines do not respond	SMC is faulty.	Replace the CPU/IO module or a system backboard after determining where IPMB error has occurred based on OS information.
0B95 BMC FRU device failure	NVRAM within BMC is faulty.	Replace ft Remote Management Card. In the case ft Remote Management Card is not mounted, or in the case the failure still remains after replacing the card, replace CPU/IO module.
0B96 BMC SDR Repository failure	SDR repository within BMC is faulty.	
0B97 BMC SEL device failure	SEL repository within BMC is faulty.	
0B98 BMC RAM test error	BMC RAM is faulty.	If updating FPGA does not solve the problem, replace the ft Remote Management Card. In the case the ft Remote Management Card is not mounted, or in the case the failure still remains after replacing the card, replace CPU/IO module.
0B99 BMC Fatal hardware error	BMC FPGA is faulty.	
0B9A BMC not responding	BMC device is faulty.	Replace ft Remote Management Card. In the case ft Remote Management Card is not mounted, or in the case the failure still remains after replacing the card, replace CPU/IO module.

On-screen error message	Cause	Action
0B9B Private I2C bus not responding	I2C bus is faulty.	If turning AC power off and on does not help, replace the CPU/IO module or the system backboard.
0B9C BMC internal exception	BMC device is faulty.	Replace ft Remote Management Card. In the case ft Remote Management Card is not mounted, or in the case the failure still remains after replacing the card, replace CPU/IO module
0B9D BMC A/D timeout error		
0B9E SDR repository corrupt	SDR data is faulty.	If updating SDR does not solve the problem, replace ft Remote Management Card. In the case ft Remote Management Card is not mounted, or in the case the failure still remains after replacing the card, replace CPU/IO module.
0B9F SEL corrupt	SEL repository within BMC is faulty.	Replace ft Remote Management Card. In the case ft Remote Management Card is not mounted, or in the case the failure still remains after replacing the card, replace CPU/IO module.
0BA0 SDR/PIA mismatched. SDR, PIA must be updated.	SDR and PIA data do not match.	If updating SDR/PIA does not solve the issue, replace ft Remote Management Card. In the case ft Remote Management Card is not mounted, or in the case the failure still remains after replacing the card, replace CPU/IO module.
0BB0 SMBIOS - SROM data read error	<ul style="list-style-type: none">• I2C bus is faulty.• SROM is faulty.• BMC is faulty.	If turning AC power off and on does not help, replace the system backboard.
0BB1 SMBIOS - SROM data checksum bad	Data within SROM is faulty.	
0BC0 POST detected startup failure of 1st Processor	CPU is faulty.	Replace the CPU.
0BC1 POST detected startup failure of 2nd Processor		
8100 Memory Error detected in DIMM group #1	DIMM is faulty.	Replace the DIMM Slot0 (2 DIMMs).
8101 Memory Error detected in DIMM group #2	DIMM is faulty.	Replace the DIMM Slot1 (2 DIMMs).
8102 Memory Error detected in DIMM group #3	DIMM is faulty.	Replace the DIMM Slot3 (2 DIMMs).
8120 Unsupported DIMM detected in DIMM group #1	Unsupported DIMM is mounted.	Check supported DIMMs and replace them. If replacing the DIMMs does not help, replace the CPU/IO module.
8121 Unsupported DIMM detected in DIMM group #2		
8122 Unsupported DIMM detected in DIMM group #3		
8130 Mismatch DIMM detected in DIMM group#1	DIMM group do not match.	
8131 Mismatch DIMM detected in DIMM group#2		
8132 Mismatch DIMM detected in DIMM group#3		

On-screen error message	Cause	Action
8150 NVRAM Cleared By Jumper	CMOS clear jumper is mounted.	Turn off the DC power and change back the jumper setting.
8151 Password Cleared By Jumper	Password clear jumper is mounted.	
8160 Mismatch Processor Speed detected on Processor 1	CPU frequency does not match.	Check supported CPUs and replace them. If replacing the CPU does not help, replace CPU/IO module.
8161 Mismatch Processor Speed detected on Processor 2		
9064 Mixed CPU Steppings detected	Different CPU steppings are found.	Check supported CPUs and replace them. If replacing the CPU does not help, replace CPU/IO module.
9002 Memory not installed.	DIMM is not implemented. DIMM is faulty.	Mount or replace the DIMM.
9003 Memory implementation error detected	Error is detected on memory implementation.	Check supported DIMMs and replace the DIMM. If replacing the DIMM does not help, replace the CPU/IO module.
9006 HW Memory Test failed.	Memory is faulty.	Replace the DIMM. If replacing it does not help, replace the CPU/IO module.
9000	A serious error occurred during a POST.	There are some error messages in addition to this error code. Check the other error message.
9090-9097	A memory error has occurred, or memory is faulty.	(a) Verify that the memory is mounted properly. (b) Replace the memory. If this does not help, replace the module.

Windows Server 2003, Enterprise Edition Error Messages

If a fatal error (e.g., a STOP or system error) occurs after Windows Server 2003, Enterprise Edition starts, the screen of the display unit turns blue and displays detailed error messages.



Take notes of the messages displayed on the screen, and call your sales agent.

If a fatal error occurs, the server automatically executes memory dump processing and saves the memory dump data in an arbitrary directory (see the end of this chapter). The maintenance personnel of your sales agent may ask you to provide this data. Thus, copy the file into a medium (e.g., DAT) to be ready to pass it to the maintenance personnel.

IMPORTANT:

A message may appear indicating that virtual memory is insufficient when you restart the system after a STOP or system error has occurred. Ignore the message and start the system.

If an error such as a stop error of the OS occurs, the normal dump function may run instead of the quick dump function depending on the system status. However, the memory dump file can be used for failure analysis equivalent to that of the quick dump function.

TIPS:

Before copying the file into a medium, start the Event Viewer to confirm that the Save Dump event log is included in the system event logs and the memory dump has been saved.

The following message may be displayed during usage.

"Your system is low on virtual memory. To ensure that Windows runs properly, increase the size of your virtual memory paging file. For more information, see Help."

When this message is displayed, extend a physical memory following the procedure below.

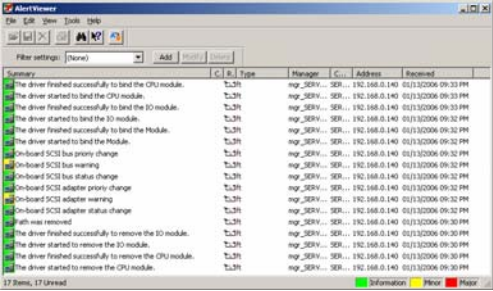
1. Add a physical memory
2. Change the configuration of the paging file (Change more than $\text{< physical memory capacity } \times 1.5 \text{ >}$)

The system also displays a warning message if an internal device or peripheral equipment (e.g., disk, network, or printer) encounters an error. Take notes of the message, and call your sales agent.

Server Management Application Error Message

If the server management tool such as NEC ESMPRO Agent or NEC ESMPRO Manager has been installed in the Fault Tolerant Server series or management PC, you can obtain the error information from the display unit of the server or management PC.

See Chapter 5 or online documentation for details of such application programs.



The screenshot shows the AlertViewer application window with a list of system events. The events are categorized by type (Information, Minor, Major) and include details such as the manager, address, and received time.

Summary	C	S	Type	Manager	C	Address	Received
The driver finished successfully to bind the CPU module.	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
The driver started to bind the CPU module.	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
The driver finished successfully to bind the IO module.	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
The driver started to bind the IO module.	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
The driver finished successfully to bind the Module.	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
The driver started to bind the Module.	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
On-board SCSI bus priority change	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
On-board SCSI bus warning	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
On-board SCSI bus status change	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
On-board SCSI adapter priority change	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
On-board SCSI adapter warning	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
On-board SCSI adapter status change	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
High was removed	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
The driver finished successfully to remove the IO module.	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
The driver started to remove the IO module.	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
The driver finished successfully to remove the CPU module.	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM
The driver started to remove the CPU module.	T	31		mgr SERV...	SER...	192.168.0.140	01/13/2006 09:33 PM

17 Items, 17 Unread

Information Minor Major

TROUBLESHOOTING

When the server fails to operate as expected, see the following to find out your problem and follow the given instruction before asking for repair.

If the server still fails to operate successfully after solving your problem, take a note on the on-screen message and contact your sales agent.

Problems with Fault Tolerant Server series

Fail to power on the server:

- ☐ Is the server properly supplied with power?
 - Check if the power cord is connected to a power outlet (or UPS) that meets the power specifications for the server.
 - Check if the two pieces of the provided power cord are connected to the main unit properly.
 - Make sure to use the power cord provided with the server. Check the power cord for broken shield or bent plugs.
 - Make sure the power breaker for the connected power outlet is on.
 - If the power cord is plugged to a UPS, make sure the UPS is powered and it supplies power. See the manual that comes with the UPS for details.

Power supply to the server may be linked with the connected UPS using the BIOS setup utility of the server.

<Menu to check: [Server] - [AC-LINK] - [Power On]>
 - Make sure the POWER switch on the power unit is on.
- ☐ Did you press the POWER switch?
 - Press the POWER switch on the front of the Fault Tolerant Server series to turn on the power (the POWER LED lights).
- ☐ Did you install the CPU/IO module properly?
 - Check if the CPU/IO module is properly installed in the server. Secure the CPU/IO module with screw located on the module removable handle.

The screen turns blue during OS boot:

- Wait for the period of time you set at BIOS [Boot Monitoring]; after the boot module is automatically swapped, the server will be rebooted and the OS will start up.

POST fails to complete:

- ☐ Is the DIMM installed?
 - At least one DIMM is required for operation.
- ☐ Is the memory size large?
 - The memory check may take a time if the memory size is large. Wait for a while.
- ☐ Did you perform any keyboard or mouse operation immediately after you started the server?
 - If you perform any keyboard or mouse operation immediately after start-up, POST may accidentally detect a keyboard controller error and stops proceeding. In such a case, restart the server once again. Do not perform any keyboard or mouse operation until the BIOS start-up message appears when you restart the server.
- ☐ Does the server have appropriate memory boards or PCI card?
 - Operation of the server with unauthorized devices is not guaranteed.

Server reboots while running the Adaptec SAS/SATA Configuration utility:

- ☐ Have you modified the Setup settings?
 - From [Server] - [Monitoring Configuration] - [Option ROM Scan Monitoring] of Setup, select "Disabled." If [Option ROM Scan Monitoring] is enabled, the system may reboot while using the *SCSISelect* utility. Change back the setting after you finish using the utility.

Fail to access to external devices:

- ☐ Are cables properly connected?
 - Make sure that the interface cables and power cord are properly connected. Also make sure that the cables are connected in the correct order.
- ☐ Is that device compliant with Fault Tolerant Server series?
 - Operation of the server with unauthorized devices is not guaranteed.
- ☐ Is the power-on order correct?
 - When the server has any external devices connected, power on the external devices first, then the server.
- ☐ Did you install drivers for connected optional devices?
 - Some optional devices require specific device drivers. Refer to the manual that comes with the device to install its driver.
- ☐ Is SCSI controller (including options) configuration correct?
 - If the sever has an optional SCSI controller board and SCSI devices are hooked up to the server, make correct settings by the SCSI controller board's SCSI BIOS utility. For details, see manuals included with the SCSI controller board.

CPUs not in Duplex mode:

- Check if the memory configuration is correct.
- Check if third-party CPUs or memory (DIMM) are used.

Disks not in Duplex mode:

- Unless you perform mirroring (including reconfiguration after failed disks are replaced) in correct order, the mirror may not be (re)configured. Check if the steps were correct.

The keyboard or mouse fails to operate:

- ☐ Is the cable properly connected?
 - Make sure that the cable is connected to the correct connector on the rear of the server.
- ☐ Are the keyboard and mouse are compliant with Fault Tolerant Server series?
 - Operation of the server with unauthorized devices is not guaranteed.
- ☐ Does the server have drivers installed?
 - Refer to the manual that comes with your OS to check that the keyboard and mouse drivers are installed. (These drivers are installed along with the OS.) Some OS allow you to change the keyboard and mouse settings. Refer to manual that comes with your OS to check that the keyboard and mouse settings are correct.

Screen freezes, keyboard and mouse don't work:

- If the amount of memory is large, it takes time to copy the memory in dual mode and the system stops working temporarily during the copying, but it is not system trouble.

Message "New Hardware Found" appears:

- Such a message may appear at the system startup or when a CPU/IO module is replaced and incorporated into the system. This is due to the server's operating specifications and does not pose any problem.

Fail to access (read or write) to the floppy disk:

- ☐ Does the floppy disk drive contain a floppy disk?
 - Insert a floppy disk into the floppy disk drive until it clicks.
- ☐ Is the floppy disk write-protected?
 - Place the write-protect switch on the floppy disk to the "Write-enabled" position.
- ☐ Is the floppy disk formatted?
 - Use a formatted floppy disk or format the floppy disk in the floppy disk drive. Refer to the manual that comes with the OS for formatting a floppy disk.

Fail to access to the CD/DVD-ROM:

- ☐ Is the CD/DVD-ROM properly set in the CD/DVD-ROM drive tray?
 - The tray is provided with a holder to secure the CD/DVD-ROM. Make sure that the CD/DVD-ROM is placed properly in the holder.
- ☐ Is the CD/DVD-ROM applicable to the server?
 - The CD/DVD-ROM for Macintosh is not available for use.

Fail to access the hard disk:

- ☐ Is the hard disk applicable to the server?
 - Operation of any device that is not authorized by the manufacturer is not guaranteed.
- ☐ Is the hard disk properly installed?
 - Make sure to lock the hard disk with the lever on its handle. The hard disk is not connected to the internal connector when it is not completely installed (see Chapter 8). When the hard disk is properly installed, the drive power LED for the hard disk is lit while the server is powered.

Fail to start the OS:

- ☐ Is a floppy disk in the floppy disk drive?
 - Take out the floppy disk and restart the server.
- ☐ Is the EXPRESSBUILDER DVD (or the other bootable DVD/CD-ROM) in the DVD-ROM drive?
 - Take out the CD-ROM and restart the server.
- ☐ Is the OS damaged?
 - Use the recovery process of the OS to attempt to recover the damaged OS.

OS behavior is unstable:

- ☐ Have you updated your system?
 - For update procedure, see the separate volume "User's Guide (Setup)."

The system does not operate according to the configured settings of "Automatic Restart" at the occurrence of error.

- The system may or may not restart automatically even if the "Automatic Restart" settings are made at occurrence of an error is set. If the system does not restart automatically, restart it in manual mode.

The power cannot be turned off while the blue screen of Windows Server 2003, Enterprise Edition is displayed.

- The forced power-off (forced shutdown) procedure is necessary to turn off the power with the blue screen displayed. Keep pressing the POWER switch for about 4 seconds. Pressing the POWER switch quickly does not turn off the power in this case.

The server is not found on the network:

- ☐ Is the LAN cable connected?
 - Make sure to connect the LAN cable to the network port on the rear of the server. Also make sure to use the LAN cable that conforms to the network interface standard.
- ☐ Have the protocol and service already configured?
 - Install the distinctive network driver for the server. Make sure that the protocol, such as TCP/IP, and services are properly specified.
- ☐ Is the transfer speed correct?
 - The built-in LAN controller mounted as standard on this server can be used in network with the transfer speed of 1000Mbps, 100Mbps or 10Mbps. You can change the transfer speed or configure the setting from OS. However, do not use the "Auto Detect" function. Fix the setting of the transfer rate to the same with that of the connected hub. Also, check if the duplex mode is the same with that of the connected hub.

Fix the transfer speed by using Device Manager. Select and right-click the network adapter to change the transfer speed from the tree on Device Manager, and select [Properties] from the displayed menu. When the properties window appears, select the [Link] tab, and select the item that matches to the connected HUB from the list box of [Speed and Duplex]. If you click [OK], configuration selected in [Speed and Duplex] will be effective.

Icon of drive A is changed to that of removal disk:

- Does not cause any problem.

Machine repeats rebooting at startup:

- ☐ Is CHKDSK executed at machine startup?

→ Open the utility of the BIOS setup at rebooting and change the following settings:

(Change BIOS settings)

Change [Server] - [Monitoring Configuration] - [OS Boot Monitoring] to [Disable].

(For details, see page 4-24 “Monitoring Configuration.”)

* After completion of CHKDSK, restart the machine and change the above setting back to [Enable] and continue the operation.

CHKDSK is executed in the following conditions:

- (1) CHKDSK is scheduled to be executed at next system startup
- (2) Corruption of file system is detected since the previous startup until shutdown
- (3) Inconsistency (corruption) of file system is detected while mouting at system startup

- ☐ Is the value of [OS Boot Monitoring] in the BIOS setting appropriate?

→ Change the value of [OS Boot Monitoring] to suit your environment.


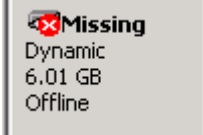

(For details, see page 4-24 “Monitoring Configuration.”)

Disk access LEDs on the disks are off:

→ The LEDs may seem to be off when an excessive amount of access causes the frequent blinking. Check if the LEDs are blinking green when the access is reduced.

Unavailable disks are displayed on Disk Management:

Follow the instruction below:

Disk Status	Description	Action
	A message [Foreign] is displayed when the dynamic disk used on another system is mounted.	<p>[To use data of the disk] Import the disk referring to Chapter 3 “Windows Setup and Operation.”</p> <p>[To make the disk usable] Initialization is required to use this disk. Initialize this disk to convert it to a usable disk.</p> <p><Note> The data on disks are lost when initialized. Make sure to back up the data before initializing disks.</p>
	A message [Missing] is displayed when the dynamic disk is broken or removed.	Delete the mirror on the disk when mirror volume is on missing disk. After deleting the mirror, right-click [Missing] disk and execute [Remove disk].
	A message [Not Initialized] is displayed when there is no signature on the disk.	Right-click on the disk and execute [Initialize Disk] to convert it to a usable disk.

CPU load ratio of SNMP Service (snmp.exe) increases:

- While monitoring the server from NEC ESMPRO Manager, the CPU load ratio of SNMP Service on the NEC ESMPRO Agent side may increase at every monitoring interval (default: 1 minute).
- NEC ESMPRO Manager and NEC ESMPRO Agent exchange information through SNMP Service. If the server status monitoring by NEC ESMPRO Manager is on (default: ON), NEC ESMPRO Manager regularly issues a request to NEC ESMPRO Agent to get the current status of the server. In response, NEC ESMPRO Agent checks the status of the server. As a result, the CPU load ratio of SNMP Service increases temporarily.
- If you have trouble of terminating a movie player application, turn off the server status monitoring by NEC ESMPRO Manager or extend the monitoring interval.

SNMP Service caused hang:

- SNMP Service has a module called “SNMP Extended Agent.” This module may be registered when you install some software that uses SNMP Service. If you start SNMP Service, SNMP Extended Agent is also loaded at the initialization. However, if the initialization is not completed within a specified period, SNMP Service will hang. It may take time to complete the initialization due to temporary high load on the system. In this case, wait for the system load become low enough before restarting SNMP Service.

Pop-up message of esmcmn.exe is displayed when starting the system:

- The following pop-up message may be displayed when you restart the system which NEC ESMPRO Agent is installed to and removal drives such as MO and DVD-RAM are mounted on, without closing Windows Explorer, after displaying the contents of media and removing the media by the software eject (by right-clicking the DVD drive on Windows Explorer and selecting [Eject]) The message (the drive name) displayed varies depending on the systems.
If the pop-up messages below are displayed, click [Cancel] or [Continue] to close the dialog box. If you do not close the dialog box, you cannot start the Workstation service and related services, causing unstable operation of the system. Also, if you restart the system, execute it after terminating the program such as Windows Explorer which displays a media.

<Example>



Memory dump (debug information) cannot be collected when a failure occurs:

- ☐ Is there any available storage space on a storage location?
 - Specify the drive in which there is an available storage space of more than a memory size on the server plus 12 MB (more than 2048 plus 12MB if a memory size is more than 2GB).
For details, see “Set Memory Dump (Debug Information)” of “Step 14: Make Settings for Failure Management” in Chapter 4 “Windows Setup” in the separate User’s Guide for setup.
- ☐ Is [Initial size] of the paging file of the OS partition smaller than [Recommended]?
 - If a value smaller than the [Recommended] value is set for [Initial Size] of the paging file, accurate memory dump (debug information) may not be collected. Be sure to create the file in the above size in the OS partition.
For details, see “Set Memory Dump (Debug Information)” of “Step 14: Make Settings for Failure Management” in Chapter 4 “Windows Setup” in the separate User’s Guide for setup.

Command prompt cannot be displayed in full screen:

In Fault Tolerant Server series, you cannot switch command prompt to full screen mode. Also, you cannot execute applications that use command prompt full screen mode. When you attempt to switch to full screen mode, the message below may appear. Click [OK] and close the window.

<Example message>



Exclamation mark “!” appears to “VGA Display Controller” under the “non-Plug and Play device” when changed the setting to show hidden devices in menu in the Device Manager:

This has to do with the server specification and there is no effect to the operation. Exclamation mark “!” appears to “VGA Display Controller” since OS Standard VGA driver is not activated in the server.

Warning message appears in POST after implementing ft Remote Management Card:

- ☐ Did you set “Initialize Remote Management Card”?

H/W Configuration of BMC is corrupted.

!! Update BMC H/W Configuration by configuration tool!!

!! Refer to BMC Configuration manual !!

If the message above appears, press **F1** key or wait for a while. Then POST proceeds. Insert EXPRESSBUILDER DVD attached to the server to the DVD-ROM drive to start EXPRESSBUILDER. Select [Tools] - [Initialize Remote Management Card] from its main menu to write the sensor information specific to the server to the card.

A CPU/IO module cannot be integrated:

When a componet fails and is reintegrated, the following message may be recorded to the system event log and the process is stopped. Such event indicates that the component’s MTBF is below the threshold and it is judged that repair is necessary. Thus the reintegration process cannot be completed. Generally replacement of the component will be required, so contact your sales representative. If reintegraating the component without repair is required for some reason, consult your sales agent. It is possible to perform reintegration forcefully.

Source: srabid
ID: 16395
Description: x is now STATE BROKEN / REASON_BELLOW_MTBF (“x” is a device number.)

When you integrate a PCI module when exchanging, starting and diagnosing the PCI module, follwing events may be recorded on [System] in [Event Viewer], and the duplex process may fail:

Source: srabid
ID: 16474
Description: Diagnostics failure of XX: ‘IO GbEnet OUI Verification 1, D821’ (Ftn=xxxx Info=xxxx,xxxx).
Source: srabid
ID: 16395
Description: XX is now STATE BROKEN/REASON_DIAGNOSTICS_FAILED

“XX” refers to the PCI module ID. If it is PCI module 1, it is shown as “10”; if it is PCI module 2, it is shown as “11.” As to “xxxx,” the value differs depending on circumstances when errors occur.

If the above events are recorded, follow the below procedure to integrate the PCI module.

- (1) Select the PCI module that failed to integrate on the ft Server Utility.
- (2) Select [Clear] under [MTBF clear].
- (3) Select [Start] to start the PCI module.

Screen under changing (distorted display) can be seen when screen resolution is changed:

If screen resolution is changed while the entire system is under high load, screen under changing (distorted display) may be seen.

This is because screen update is taking time to complete due to high load in the system. This is not because an error is occurring.

The screen will return to normal if you wait awhile.

Duplexed status is not displayed properly:

When one CPU/IO module is reintegrated after the other CPU/IO module is removed due to the failure or replacement, the status in ESMPRO or RDR Utility and status LED 2 on the CPU/IO module may not be displayed properly.

Restore normal display with the following procedure.

<Restoration procedure>

From [Start], click [Administrative Tools] and [Services] to start Services. Right-click [ftSys Maintenance and Diagnostics (MAD)] and click [Restart].

Unable to recognize the server from a managing PC:

- ☐ Did you configure [Initialize Remote Management Card]?
 - Start the server-accessory EXPRESSBUILDER, then go to [Tools] - [Initialize Remote Management Card] to write each server information in order to initialize the card.
- ☐ Does your management PC contain Java2 RuntimeEnvironment, Standard Edition 1.4.2_04 or later?
 - Java2 RuntimeEnvironment, Standard Edition 1.4.2_04 or later is required. Use the following procedure to install.
 - Start Windows on a management PC that you want to install the Java, then insert the EXPRESSBUILDER DVD into the DVD-ROM drive. Master control menu appears by the Autorun function.
 - Click [Software Setup] - [DianaScope]. Run the JRE installer in the DianaScope installation menu.
 - # If you would like to install the latest Java Runtime, go to the following website to download:
<http://java.sun.com/j2se/>
- ☐ Do you connect LAN cable appropriately?
 - Check if LAN cable is connected appropriately. The server sensors work properly only when the cable is connected properly. Make sure the cable isn't mistakenly connected to the server's LAN connector or to the serial port connector.
- ☐ Check if IP address is duplicated?
 - IP address for the management LAN port is configured as 192.168.1.1 at the factory default setting. Change the IP address if this one is already used on the network, as this one isn't recognized appropriately.

- ☐ Did you set ESMPRO/ServerAgent to monitor the server?

→ Change the ESMPRO setting. Start ESMPRO/ServerAgent in the Windows control panel, then go to [Express5800 Server] - [Monitor] from [System] tab, then click the check box. ([Unmonitored] is selected by default) After changing the setting, the server monitoring starts automatically. You do not have to reboot the server, but you need to restructure the tree if you still cannot monitor the server.

- ☐ Is network connection restricted by the firewall or the gateway?

→ Network connection may be restricted by a firewall setting. See if you can solve the problem by connecting the server and a client PC directly with a cross cable. Refer to Chapter 4 [Remote Management Function] - [BMC Configuration] - [Network Configuration], then check the port of the Remote Management Card and set the firewall or the gateway.

Server console screen does not appear on the web Remote KVM console screen:

- ☐ Did you set the server's screen resolution properly?

→ When you display the server screen by using the remote KVM in the Remote Management function, set the screen resolution 1024 x 768 and the refresh rate should be less than 75Hz.

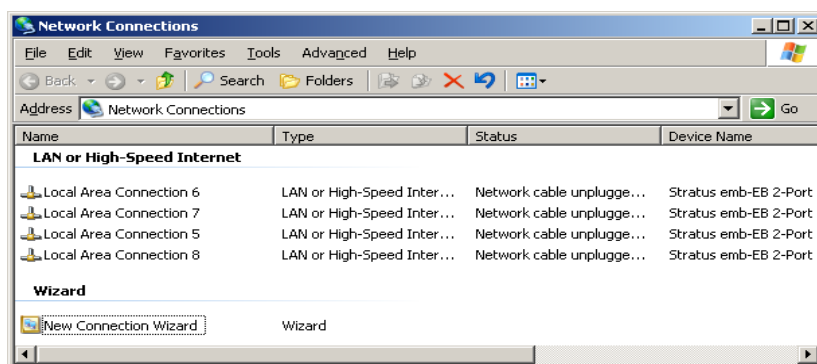
Forgot login name/password for the Remote Management Function on the web browser:

→ Refer to Chapter 4 on BMC configuration jumper. By changing the jumper position, the BMC configuration including the password returns to the factory default setting.

IMPORTANT:

After the operation, the BMC configuration for connecting to the DianaScope and to the server will be lost. If you are already using the DianaScope, save the configuration on FloppyDisk before this operation, then configure again. You can change/save the BMC configuration on the system management function of DianaScope or EXPRESSBUILDER.

On the Network Connections screen, the numbering of the Local Area Connection doesn't begin from "1":



→ This is because of the product feature and there this affects nothing on the operation. If you need to change the Local Area Connection name, right click the icon on the Network Connections screen and select [Change name].

Wake On LAN does not function:

- ☐ Does this happen to be right after the Alternate Current (AC) power supply started?
 - When you disconnect either or both of the AC cables on the server and the AC supply is stopped, the Wake On LAN becomes unavailable on the next system launch after the electricity supply starts. Connect the cables to both equipments to supply the electricity, and press the power switch to start the system.
- ☐ Is the AC power supplied to both AC cables?
 - If the AC power supplied to only one of the AC cables, Wake On LAN may become unavailable. Supply the AC power supply to both of the AC cables, and press the power switch to start the system.
- ☐ Is the network adapter configured on OS?
 - On the OS, go to [Start] - [Management Tool] - [Computer management] and select the Device Manager. Double click [Stratus emb-EB 2-Port Gigabit Adapter #n] under the network adapter, then select the following option from [Power Management] tab:

Wake on Magic Packet from power off state

TIPS:

Wake On Magic packet is unavailable even if it is checked.

- ☐ Is Hub/Client fixed as 1000M?
 - Check the following configurations:
 - Set the Hub as “Auto-Negotiation.”
 - Set the Client as “Auto-negotiate best speed.”

IMPORTANT:

For both Hub/Client, you cannot function Wake On LAN from standby with the 1000M fixed configuration.

- ☐ Do you happen to be sending Magic Packet to only one of the duplexed LAN?
 - If you use Wake On LAN under duplexed LAN, you need to send Magic Packet to all of the duplexed LAN pair(s).

Event Log

"The NMS Service terminated unexpectedly." is recorded in the system event log:

- Although the following log may be recorded in the system event log when starting the system, or after exchanging PCI modules, there is no real problem on operation. Change of a setup with PROSet II will become invalid if NMS service stops, but you can change a setup normally because NMS service will be automatically started when PROSet II is started.

Source: Service Control Manager

Event ID: 7031

Description: The NMS service terminated unexpectedly. This has occurred 1 time(s). The following corrective action will be taken in 0 milliseconds: No action.

iANSMiniport-related logs are recorded in the system event log:

- The logs of the source "iANSMiniport" are the logs about the duplex of the network. The following logs may be recorded in the system event log after starting the system or after setting duplex, but there is no problem on operation.

Source: iANSMiniport

Type: Warning

Event ID: 35

Description: Initializing "Virtual Team Adaptor" that lack adapter "Number of missed adaptors." Check if all adapters exist and function properly.

Source: iANSMiniport

Type: Warning

Event ID: 13

Description: "Physical Adaptor" is invalid in the team.

Source: iANSMiniport

Type: Warning

Event ID: 11

Description: The following adapter link is not connected: "Physical Adaptor."

Source: iANSMiniport

Type: Error

Event ID: 16

Description: "Virtual Team Adaptor": the last adapter lost the link.

The team network lost the connection.

Source: iANSMiniport

Type: Warning

Event ID: 22

Description: The primary adapter did not detect the following probe: "Physical Adaptor." Reason: The team may be divided.

The log above gets output in the process of system start up or dual mode setting. When the log is recorded, there is no problem to the system by the above warning if the status of the adapter in the team is "Active" or "Standby." For the status of the adapter, check in properties of the team adapter from the device manager.

ESMCommonService related log is recorded in the system event log:

- Following event log is recorded while the system operation in some cases. The log indicates detection of an event that is not critical event for the server operation, and the event is amendable. This doesn't affect the system as long as the event never occurs repeatedly.

Source: ESMCommonService
 Type: Warning
 Event ID: 1309
 Description: ECC 1 bit error occurred on the system bus.

EvtAgnt log is recorded in the application event log:

- This event does not have any influence to the system not to SNMP services. Thus no measurement is required.

Source: EvtAgnt
 Event ID: 1003
 Description: TraceFileName parameter not located in registry; Default trace file used is .

Source: EvtAgnt
 ID: 1015
 Description: TraceLevel parameter not located in registry; Default trace level used is 32.

SCSI control error appears in the system event log:

- This symptom occurs, for example, when a SCSI chip receives a reset request from a different SCSI chip. The process will be continued properly by the retry function.

It is likely to occur when the server shifts from the simplex mode to the duplex mode at OS startup or during maintenance operations. If the number of the following errors recorded in the system event log is few, ignore the errors.

This error is logged about 5 to 50 times in two or three minutes when the server shifts from the simplex mode to the duplex mode during maintenance operations. Ignore these errors as well.

Source: adpu320
 Type: Error
 Event ID: 11
 Description: The driver detected a controller error on \Device\Scsi\adpu320xx.

If this error is recorded many times, the hard disk drive may be faulty. Contact your service representative.

SCSI device timeout appears in the system event log:

- This symptom occurs when the processing speed of HDDs is slower than the request from the operating system. The process will be continued properly by the retry function.

It is likely to occur when the server shifts from the simplex mode to the duplex mode at OS startup or during maintenance operations. If the number of the following errors recorded in the system event log is few, ignore the errors.

This error is logged about 5 times when the server shifts from the simplex mode to the duplex mode during maintenance operations. Ignore these errors as well.

Source: adpu320
 Type: Error
 EventID: 9
 Description: The device, \Device\Scsi\adpu320xx, did not respond within the timeout period.

Source: adpu320
 Type: Error
 EventID: 117
 Description: The driver for device \Device\Scsi\adpu320xx detected a port timeout due to prolonged inactivity. All associated busses were reset in an effort to clear the condition.

If this error is recorded many times, the hard disk drive may be faulty. Contact your service representative.

Event log which warn CPU load monitoring is registered:

- If NEC ESMPRO Agent cannot get performance information from the OS due to a temporary resource shortage or high load ratio on the system, it will record the following event log. However, there is no real problem on operation. (In the description, Y and X represent alphanumeric characters.)

Source: ESMCpuPerf

Type: Information

Event ID: 9005

Description: Cannot get system performance information now (YYYY Code=xxxx).

If NEC ESMPRO Agent cannot get information, it will treat the load ratio as 0%. So, if NEC ESMPRO Agent cannot get information continuously, the CPU load ratio may appear lower than the actual value.

Error log is registered on the OS start:

- The following event may be registered when the OS starts. This log may also be registered when the ftSys SSN service functions normally.

Source: Service Control Manager

Type: Error

Event ID: 7022

Description: Description: ft Sys SSN service hung on starting.

Verify the status of the ftSys SSN service by going to [Control Panel] - [Management Tool] - [Service] and start the Service Manager. If the status is [Start], there is no problem.

[Detected past event] is recorded

- Following event is recorded when MSCS is used, then the warning is sent to ESMPRO/Server Manager

Source: AlertManagerMainService

Event ID: 802

Description: Cannot get system performance information now (YYYY Code=xxxx).

- System time is modified.
- System was not shut down properly.
- Event log file is broken.

MSCS has a function which enables to see every event on the computer's cluster configuration. In some cases, however, events are not stored by date, when such as shutting down only one side, or launching only one side.

As ESMPRO/ServerAgent checks whether the events are stored by date, any events out of the date order is shown as "Past Event Detected."

Note that even when this event is recorded, the event log function continues to function properly for the events stored by date.

Fibre Channel related log is recorded in the System Event log

- The below events may be recorded when module switching, including module failure, occurs. This log indicates that the system has detected a non-fatal, correctable event for the server operation. This does not affect the system as long as this event is recorded consecutively.

Source: elxstor
 Type: Error
 Event ID: 11
 Description: Driver detected control error on \Device\Raid\Port?.

Data: Word
 0000: 0018000f 0068001 00000000 c00400b
 0010: 0000002a 00000000 00000000 00000000
 0020: 00000000 00000000 00000000 00000000
 0030: 00000000 c004000b 00000000 00000000

Note 1: “?” indicates the board number.

Note 2: When value is 0x0000002a that is indicated in 0x0010 word.

Error logs are recorded while maintenance operation

- While maintenance operation, such as detaching a I/O module, the following events may be recorded. These logs show that the I/O module was detached. This does not affect the system operation.

Source: srae1e51
 Type: Error
 Event ID: 805
 Description: Stratus emb-EB 2-Port Gigabit Adapter #n : PROBLEM :
 Unexpected adapter removal detected during check for hang.
 Was an I/O CRU short or removed?

Source: PlugPlayManager
 Type: Error
 Event ID: 12
 Description: The device ‘XXX’ disappeared from the system without first being prepared for removal.

Problems with EXPRESSBUILDER

When the server is not booted from the EXPRESSBUILDER DVD, check the following:

- ☐ Did you set the EXPRESSBUILDER DVD during POST and restart the server?
 - If you do not set the EXPRESSBUILDER DVD during POST and restart the server, an error message will appear or the OS will boot.
- ☐ Is BIOS configuration correct?
 - The boot device order may be specified with the BIOS setup utility of the server. Use the BIOS setup utility to change the boot device order to boot the system from the DVD-ROM drive first.
<Menu to check: [Boot]>
- ☐ If [OS installation ***default***] is selected at BOOT Selection screen, following message is displayed.

After this message appears, check the error and take the appropriate corrective action according to the error codes listed in the table below.

Message	Cause and Remedy
This EXPRESSBUILDER version was not designed for this computer. Insert the correct version and click [OK]. (When you click [OK], the computer reboots)	This EXPRESSBUILDER version was not designed for this server. Execute the EXPRESSBUILDER on the compliant server.
EXPRESSBUILDER could not get the hardware parameters written in this motherboard. This version is not designed for this computer or the motherboard may be broken. (When you click [OK], the computer reboots)	This message is shown when such as EXPRESSBUILDER could not find system-specific information because of motherboard exchanged.
The hardware parameters written in this motherboard are incorrect. This version is not designed for this computer or the motherboard may be broken. (When this error occurs just after changing the motherboard, configure the hardware information properly on the [Maintenance Utility])	

Problems with Master Control Menu

Failed to read online documentation:

- ☐ Is Adobe Acrobat Reader installed properly?
 - A part of online documentation is supplied in PDF file format. Install the Adobe Acrobat Reader (Version 4.05 or later) in your operating system. You can also install the Adobe Acrobat Reader using the EXPRESSBUILDER DVD. Launch the Master Control Menu and select [Setup] - [Adobe Acrobat Reader]. (After installation, launch Adobe Acrobat Reader and agree on license agreement before you use it).

Image of online documentation is not clear:

- ☐ Is your display unit set to display 256 colors or more?
 - Set the display unit to display 256 colors or more.

The master control menu fails to appear:

- ☐ Is your system Windows NT 4.0 or later, or Windows 95 or later?
 - The DVD Autorun feature is supported by Windows NT 4.0 and Windows 95. The older versions do not automatically start from the DVD.
- ☐ Is **Shift** pressed?
 - Setting the DVD with **Shift** pressed down cancels the Autorun feature.
- ☐ Is the system in the proper state?
 - The menu may not appear depending on the system registry setting or the timing to set the DVD. In such a case, start the Internet Explorer and run \MC\1ST.EXE in the DVD.

Menu items are grayed out:

- ☐ Is your computer environment proper?
 - Some software requires the administrative authority for operation or needs to operate on the server. Use that software in the appropriate computer environment.

Problems with Parameter File Creator

Failed to start Parameter File Creator:

- Parameter File Creator must be executed with “Microsoft® HTML Application host.” If this does not launch, follow the below procedure to associate Parameter File Creator with “Microsoft® HTML Application host.”
1. Go to Windows Start menu and select “Run”.
 2. Type %windir%\system32\mshta.exe \register and click OK.

Problems with NEC ESMPRO

NEC ESMPRO Manager

- See Chapter 5. See also online document in EXPRESSBUILDER DVD for troubleshooting and other supplementary information.

NEC ESMPRO Agent

Change in monitoring interval of file system and threshold value of free space monitoring do not reflect:

- Change in monitoring interval by the file system monitoring function of NEC ESMPRO Agent, threshold value of free space monitoring do not reflect immediately. The configuration change becomes effective in the next monitoring interval of monitoring service after changing the setting.

NEC ESMPRO Manager does not receive traps from NEC ESMPRO Agent properly:

- When the trap community which receives traps in the setting of NEC ESMPRO Manager is changed from the default setting “public”, SNMP service setting needs to be changed. See the separate user’s guide (Setup), and set the same community name configured in NEC ESMPRO Manager. For NEC ESMPRO Manager to receive traps from NEC ESMPRO Agent properly, both community names must be matched.

Alert is redundantly reported to NEC ESMPRO Manager:

- When NEC ESMPRO Manager’s IP address (or host name) assigned to SNMP service to send traps is assigned in the message manager (TCP/IP), a warning message for redundancy is displayed. Alert is redundantly reported when the same NEC ESMPRO Manager is assigned.

Cannot monitor from NEC ESMPRO Manager:

- When a community name besides “public” is entered in SNMP service trap properties sheet, see the separate user’s guide (Setup) and add the value to “Accepted community names” in security properties sheet. When the choice of “Accepted community names” is set other than “READ CREATE” or “READ WRITE”, monitoring from NEC ESMPRO Manager cannot be done.

NEC ESMPRO Agent cannot receive SNMP packet from NEC ESMPRO Manager:

- When you changed the community name which receive SNMP packet of SNMP service from the default name “public” to the desired name, you must register new community name of NEC ESMPRO Agent from the [Control Panel]. Follow the steps below:

1. Double-click the [NEC ESMPRO Agent] icon in [Control Panel].
2. Select a desired community name from the [SNMP Community] list box in [SNMP Setting] of the [General] sheet.

The community names to receive SNMP packets are listed in the [SNMP Community] list box.

3. Click the [OK] to terminate the operation.

The community name to send SNMP packet from NEC ESMPRO Manager and the community name to receive SNMP service in NEC ESMPRO Agent must be the same to receive SNMP packet properly.

NEC ESMPRO Agent does not operate properly:

- When SNMP service is added after applying service pack when OS is installed, apply service pack again. Otherwise, SNMP service does not run properly and NEC ESMPRO Agent may not run.
- SNMP service is necessary for NEC ESMPRO Agent to run. If you deleted SNMP service after installing NEC ESMPRO Agent, reinstall NEC ESMPRO Agent after installing SNMP service.
- SNMP service may be used among other software. If you install SNMP service and NEC ESMPRO Agent while such software is installed, NEC ESMPRO Agent service may not be able to start. In such case, delete SNMP service once and install it again. Then, reinstall NEC ESMPRO Agent and other software described above.

[Unknown] or illegal information is displayed in CPU information:

- If you select [CPU Module]–[CPU] in the [ft] tree of the data viewer, unknown or incorrect information appear in some information items.
- The CPU information can be viewed by selecting [System]–[CPU] in the [ESMPRO] tree.

Status of logical PCI slot:

- There is no effect to PCI module (IO module) since I/O hub and a display controller on PCI module (IO module) are logical PCI slot information. Hence, for [PCI slot (ID:0/10/102)] and [PCI slot (ID:0/10/103)] under [PCI module (ID:0/10)] of FT tree of the date viewer, “Status” becomes “Online” and the status color becomes green.

Message prompting to reconfigure a tree in the date viewer is displayed:

- If you dynamically change the configuration of the CPU or PCI module (IO module) in the relevant system during review of the server information by using the data viewer, the message prompting you to reconstruct the tree of the data viewer will appear. If you click the [Yes] button, the tree is reconstructed in the data viewer to reflect the change of the system configuration on the data viewer. If you click [No] button, the tree will not be reconstructed in the data viewer. If such case, the information in the data viewer may be different from the current system information because the change of the system configuration is not reflected on the data viewer.

Module status is shown “Fault”:

- PCI modules (IO modules), SCSI adapters, SCSI buses, and modules under the SCSI enclosure have impact on each other. For example, when the “Status” item of a module changes to “fault,” it may be caused by other module error. Check the status of the other modules referring to alert message.

Status color changes to different colors after mounting a hard disk drive:

- The status of hard disk drive and its upper component, SCSI enclosures change while generation of the mirror is completed after mounting a hard disk drive. In addition, it may take several minutes for OS to recognize the change of disk status and/or disk may need to be scanned again. A status color may turn to abnormal during the process, but it will return to normal color once a mirror is successfully generated.

Line fault and high line load are reported:

- The LAN monitoring function defines the line status depending on the number of transmission packets and the number of packet errors within a certain period of time. Thus, the LAN monitoring function may report a line fault or high line load only in a temporary high line impedance state. If a normal state recovery is immediately reported, temporal high line impedance may have occurred. Hence, there is no problem.

Threshold value of LAN monitoring does not reflect:

- Because the Fault Tolerant Server series detects hardware faults on the network in the driver level, NEC ESMPRO Agent does not monitor line faults. Thus, the value set for "Line fault occurrence rate" of a [LAN] tab of [NEC ESMPRO Agent properties] in the control panel is not used.

Remote shutdown function or change of threshold value function from NEC ESMPRO Manager cannot be used:

- Depending on your OS type or its version, settings for community, SNMP service’s security function, are not made, or default settings of authority are different. To enable the remote shutdown and threshold change functions via NEC ESMPRO Manager, make settings of community and set its authority to "READ CREATE" or "READ WRITE."

Machine in a sleep state cannot be monitored:

- NEC ESMPRO Manager cannot monitor the NEC ESMPRO Agent machine in the sleep state (system standby or system halt state).
- While NEC ESMPRO Manager monitors server shutdown, the relevant NEC ESMPRO Agent machine may be entered into the sleep state. If so, the report "server access disabled" is issued and the status color of the server icon becomes gray. This cannot indicate whether the NEC ESMPRO Agent machine is shut down or entered into the sleep state. Keep these in mind when operating the system where systems to be monitored may enter the sleep state.

Some items cannot be monitored in NEC ESMPRO Manager:

- NEC ESMPRO Manager Ver4.23 or later is necessary to monitor Fault Tolerant Server series. If you are using older version, install NEC ESMPRO Manager DVD that comes with the device.

Various logs cannot be referred in ESRAS Utility:

- ESRAS Utility is software that refers various logs, print out, output to a file, and initialization in Fault Tolerant Server series in which NEC ESMPRO Agent is installed. When ESRAS Utility of NEC ESMPRO Manager is used, there are some devices that cannot refer various logs.
- Use ESRAS Utility of NEC ESMPRO Agent. It is registered in DVD that comes with the device. Install it from related utility of ESMPRO setup.

Managing dual mode system:

- When managing dual mode system, install Operation/Standby separately to local disk. Installation of NEC ESMPRO Agent is same as normal installation except installing to two servers.

The monitoring event is not alerted:

- The alert function is based on the event information registered in the event log of the system. Thus, set the event log process on the event viewer to [Overwrite events as needed]. The monitoring event is not alerted in the setting other than that.
- The event registered in the monitoring event tree on the setting tool of alert function (Alert Manager) is not alerted to the manager if Alert Manager Main Service does not operate. Even when the service is operating, if the enabled/disabled flag of each alerting ways is disabled, the event is not alerted. The alert enabled/disabled flag is set by selecting [Base Setting] – [Report] Properties from [Setting] of Alert Manager. Also the event occurred before Eventlog Service started at the time of system startup cannot be alerted.
- You can set the time to the shutdown by selecting [Base Setting] – [Other] on the setting tool of the alert function (Alert Manager). The initial value is 20 seconds. When you set smaller value than this, the alert may not be performed at the time of shutdown.
- When an alert failure occurs at the time of alerting of monitoring target event, an error message is logged in the event log. If you newly log the error message which occurs at the time of alerting as a monitoring target event, the error at the time of alerting will be alerted again. As the result, large number of alerts will be sent when recovering the failure. This leads to the increase of system load and the degradation of the performance. Do not register the events especially which are produced by the following alert function services as the monitoring target.

Alert Manager ALIVE(S) Service
Alert Manager Main Service
Alert Manager Socket(S) Service

Printer Information's Available Time:

When you add a new printer, install its driver and make its settings, if you do not make settings for the available time from the properties window of the printer, the printer's available time (From and To) in [Printers and Faxes] are [00:00], on the other hand, NEC ESMPRO Manager's time are [9:00]. To display them properly, make the settings of printer from its properties window. The procedures are as follows:

1. From [Control Panel], click [Printers and Faxes], and open the properties window of a printer for making settings.
2. Select the [Advanced] tab.
3. Enter values in the available time ("Available from" and "To"), and click [OK] on the properties window to exit.

Now, you can see the correct information from NEC ESMPRO Manager, too.

The disk related works are desired while NEC ESMPRO Agent is running:

- The following works to disks (hard disk drive or magneto optical) are not allowed while NEC ESMPRO Agent is running.
- To format or delete a partition by Disk Administrator or by other means.
 - To request programmatically to remove media from removable disks such as MO, Zip and PD.

Please conduct these works by following the procedure written below.

1. Open [Control panel] – [Service].
2. Select a service named “ESM Common Service” and click [Stop].
3. Confirm that “ESM Common Service” is stopped, and close the [Service] in [Control Panel].
4. Do the disk-related works.
5. Open the [Service] in [Control Panel] again. Select “ESM Common Service” and click the [Start].
6. Confirm that “ESM Common Service” is started and close the [Service] and [Control Panel].

Changing the threshold of temperature/voltage/fan monitoring is desired:

- Displaying/changing the threshold of the temperature/voltage /fan from NEC ESMPRO Agent is not allowed. However, you can display the threshold on the data viewer of NEC ESMPRO Manager on some models. NEC ESMPRO Agent monitors using the appropriate threshold that is set for each model.

The detail information of alert is displayed as “Unknown”:

- Detail information of some alert displayed on the alert viewer may be displayed as “Unknown.”

Monitoring the failures of the tape device is desired:

- NEC ESMPRO Agent does not monitor the failures of the tape device. If you want to conduct monitoring, use backup software or tape monitoring application. Using the event monitoring function of NEC ESMPRO Agent allows you to monitor the event log of backup software or applications.

File system monitoring cannot be inherited on the system using NEC EXPRESSCLUSTER:

- When using NEC ESMPRO Agent in the cluster environment configured by NEC EXPRESSCLUSTER, there is the following limitation:
If a failover occurs, the settings of the threshold for the empty space monitoring function and the enable/disable of monitoring of the operating sever are not inherited to the standby server. Make sure to reset the threshold and the enable/disable of monitoring on the standby server.

Temperature/voltage/fan sensors appear in an incorrect manner:

- Some modes are equipped with temperature/voltage/fan sensors that do not have information on status, current values, rpm, threshold etc. Therefore, if you view such a sensor on NEC ESMPRO Manager, it may be displayed as follows:
- The status becomes “Unknown” (grayed out) on the data viewer.
 - The current value or rpm is displayed as “Unknown” on the data viewer.
 - The status is grayed out on the Web component data viewer.
 - The current value or rpm becomes blank on the Web component data viewer.

Even if the sensor is stated like stated above, it is monitoring the server.

Temperature/voltage error occurs on the CPU/PCI modules:

- At the time when a temperature or voltage error occurs on CPU/PCI module (CPU/IO module), necessary actions will differ depending on their status as shown below. You can check the status of each module from the data viewer of NEC ESMPRO Manager or ftServer Utility.

Status	Operation
Duplex	Stop the failed CPU/PCI module (CPU/IO module).
Simplex	Shut down the system.

- If the status is “Empty”, the module is not mounted. Sensor monitoring is not conducted.
- If disks are mounted on PCI modules (IO modules), the status of both modules is “Simplex” while the disks are mirrored. Temperature or voltage error occurring during disk mirroring will result in the system to shut down.

Network drive is not displayed in the data viewer:

- On WindowsXP or the OS released after it, the drive connected to network is not displayed under the file system tree in the data viewer of NEC ESMPRO Manager.

Shutdown monitoring:

- When performing shutdown monitoring, all shutdown processes are to be monitored. If there is an application that performs shutdown without rebooting OS or turning off the power, set the timeout value longer or disable the monitoring function.

The external clock of CPU is listed as “Unknown”:

- In [CPU information] of Data Viewer’s system tree, the external clock is listed as “Unknown.”

[ft] tree appears on data viewer in an incorrect manner:

- After the system starts up, the tree or the state of a Data Viewer may not be displayed correctly due to high load of the system. In about 20 minutes after the system startup, when a pop-up message which prompts you to reconstruct a Data Viewer appears, click [OK]. The Data Viewer will be reconstructed and the tree and the status will be displayed correctly.

The information on the floppy disk appears in an incorrect manner:

- After switching on and off the power of the CPU/IO module, the floppy disk drive name of [I/O Device] on Data Viewer may be different from the name that is recognized by the OS.

(Example: drive name on Data Viewer: “A”

drive name recognized by the OS “B”)

Check the floppy disk drive name on Explorer.

- If you add or delete floppy disk drive connected with USB while the system is running, the drive information under the [I/O Device] in the data viewer will be updated at the next system startup.

When the Displayed BIOS Information is Incorrect

Additional information of BIOS which is displayed by clicking [ft] - [CPU Module] - a CPU module - [General] - [BIOS Information] on a Data Viewer or by clicking a CPU module and clicking [BIOS Information] on ftServer Utility may not be displayed correctly. In such a case, display the BIOS information on a Data Viewer by clicking [ESMMIB] - [BIOS].

The status of Ethernet board is displayed as an error:

- If an Ethernet adapter is not used (not connected to cable), set it to “Disable” in [Network Connections] from Control Panel. If an Ethernet adapter are about to disable has dual LAN settings (AFT function), remove the dual LAN settings before disable it.

NEC ESMPRO Agent does not work properly in the environment where Oracle products and NEC ESMPRO Agent coexist:

- The installation of the Oracle products may change Startup type of SNMP Service into “Manual.” If so, change the setting back to “Automatic” and set up correctly according to the description of the Oracle product.

SCSI Status on a Data Viewer:

- “Unknown” is always displayed for the following items:
 - “Bus Mode” and “Backplane Config” in “General” of “SCSI Enclosure”
 - “Type,” “Threshold,” “Current,” “Faults,” “Time of last fault,” “Time of last run,” and “Result” in “Maintenance” of “SCSI Enclosure”
 - “Type,” “Reassign Block Count,” “Reassign Block threshold,” and “Path Information” in “General” of “SCSI Slot”
 - “Type,” “Threshold,” “Current,” “Faults,” and “Time of last fault” in “Maintenance” of “SCSI Slot”

SCSI Status while IO Module is Starting or being Stopped:

- While a PCI module is starting or being stopped, the status of SCSI adapters, SCSI bus, SCSI enclosure, SCSI slots, and mirror disks temporarily indicates an undefined status. Once the module is started or stopped, the status will return to normal.

Status of SCSI Slots and Mirrored Disks at High Load:

- When the system load is high, the status of SCSI slots and mirror disks may not be obtained, and incorrect status may be displayed temporarily.

“Warning” is displayed for a “Normal” mirror volume on Disk Management:

- If the combination of the disks that configure a mirror is different from the one described in “Disk Operations” in Chapter 3, “Warning” is displayed for a normal mirror volume.

Data viewer is not displayed normally when the PCI module (IO module) is running in the simplex mode.

- When only the PCI modules (IO modules) is running in the simplex mode (non-duplexed mode), the data viewer cannot display the status of the SCSI enclosure and mirror disk. To check if the duplex mode is changed to the simplex mode, check the event log or alert viewer log, or the status color of the PCI module by the data viewer.

COLLECTING TROUBLE LOGS

In the event of trouble, you can get information in the procedures described below:

IMPORTANT:

- You can perform the procedures described below only when you are asked by your maintenance personnel to get trouble logs.
 - When the system restarts after the trouble, it may show a message that there is a shortage of virtual memory. However, continue the system startup. If you reset and restart the system, you cannot get correct information.
-

Collection of Event Logs

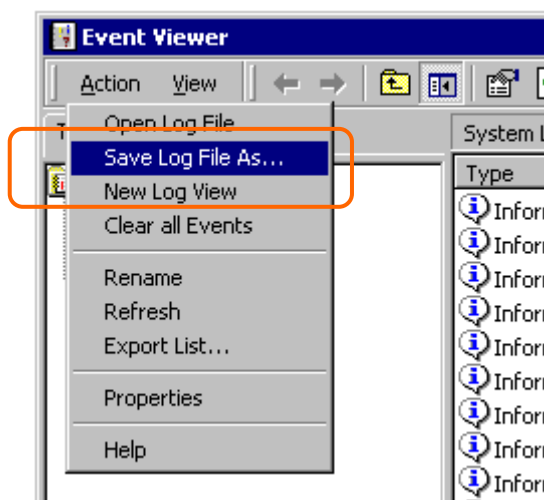
Collect the logs of various events that have occurred in the Fault Tolerant Server series. It is recommended that you collect all the logs of [Application Log], [Security Log] and [System log] by the following procedure.

IMPORTANT: If a STOP error or system error has occurred or the system has stalled, restart the system, and then start collecting event logs.

1. Click [Start] - [Settings] - [Control Panel] - [Administrative Tools] - [Event Viewer].
2. Select the type of the log to be collected.

[Application Log] contains events related to the applications that were active at occurrence of the events.
 [Security Log] contains security-related events. [System Log] contains events that occurred in system components of Windows Server 2003, Enterprise Edition.

3. Click [Save Log File As...] in the [Action] menu.



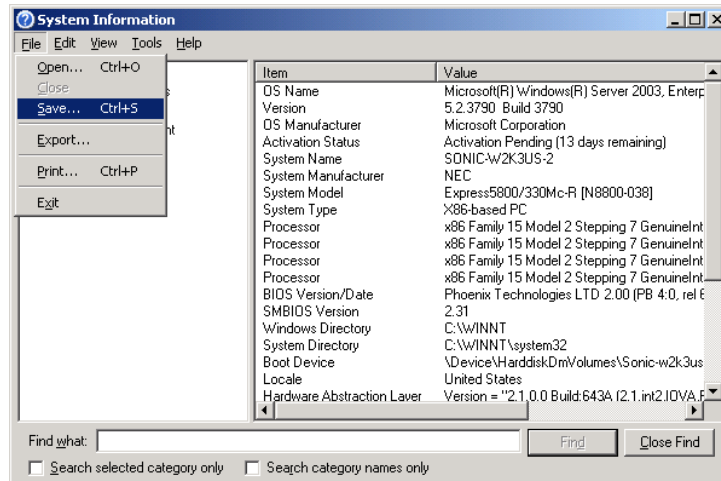
4. Enter the name of the target archive log file in the [File name] box.
5. Select the format of the target log file from the [Save as type] list box, and click [OK].

Collection of Configuration Information

Collect information such as the hardware configuration and internal setting information of the Fault Tolerant Server series.

IMPORTANT: If a STOP error or system error occurs or the system stalls, restart the system, and then start the work.

1. Click [Start] - [All Programs] - [Accessories] - [System Tools] - [System Information].
2. Select the [Save...] from the File menu.



3. Enter the name of the target file in the [File name] box.
4. Click [Save].

Collection of Diagnostic Information by Dr. Watson

Collect diagnostic information related to application errors by using Dr. Watson.

You can designate any destination to save diagnostic information.

For details, see help information. Click [Start] - [Run...], execute "drwtsn32.exe," and click [Help] in the [Dr. Watson for Windows] dialog box.

COLLECTING THE MEMORY DUMP

If a failure occurs, the memory data should be dumped to acquire the required information. If you stored the dump data in a DAT, label it so as to indicate the software (e.g. NTBackup) you used for storing it. You may save the diagnosis data to a desired destination.

IMPORTANT:

- Consult with your sales agent before dumping the memory. Executing memory dumping while the server is in the normal operation may affect the system operation.
 - Restarting the system due to an error may display a message indicating insufficient virtual memory. Ignore this message and proceed. Restarting the system again may result in dumping improper data.
 - Press the DUMP switch on the primary CPU/IO module, whose POWER LED has been blinking, for four to eight seconds. Use something sharp, such as curved clips to press the DUMP switch on CPU/IO module 1.
-

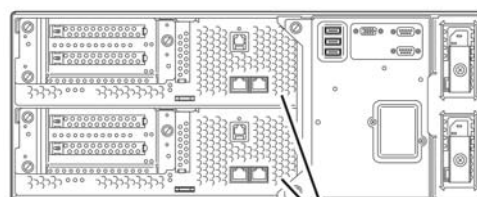
Preparing to collect Memory Dump

Memory dumping with the DUMP switch may disable the server to restart. In such a case, it is required to force the server to shut down.

Saving Dump Files

Press the DUMP (NMI) switch on the primary CPU/IO module to save the dump file when an error occurs. Insert something sharp-pointed like a pen into the switch hole to press the DUMP switch.

Pressing the DUMP switch saves the dump file in the specified directory. (Memory dumping may not be available when the CPU stalls.)



DUMP (NMI) switch

IMPORTANT: Do not use a toothpick or plastic stick that is easy to break.

Chapter 8

System Upgrade



This chapter describes procedures to add options and replace failed components.



IMPORTANT:

- Optional devices described in this chapter may be installed or removed by the user. However, The manufacturer does not assume any liability for damage to optional devices or the server or malfunctions of the server resulted from installation by the user. We recommend you ask your sales agent to install or remove any optional devices.
- Be sure to use only optional devices and cables designated by the manufacturer. Repair of the server due to malfunctions, failures, or damage resulted from installing undesignated devices or cables will be charged.

SAFETY PRECAUTIONS

Observe the following notes to install or remove optional devices safely and properly.

 WARNING	
	<p>Observe the following instructions to use the server safely. There are risks of death or serious personal injury. See “PRECAUTIONS FOR SAFETY” in Chapter 1 for details.</p> <ul style="list-style-type: none">• Do not disassemble, repair, or alter the server.• Do not look into the DVD-ROM drive.• Do not remove the lithium battery.• Disconnect the power plug before working with the server.

 CAUTION	
	<p>Observe the following instructions to use the server safely. There are risks of fire, personal injury, or property damage. See “PRECAUTIONS FOR SAFETY” in Chapter 1 for details.</p> <ul style="list-style-type: none">• Do not install or remove components by a single person.• Do not install the server leaving the cover removed.• Make sure to complete component installation.• Do not pinch your finger(s).• High temperature

ANTI-STATIC MEASURES

The server contains electronic components sensitive to static electricity. Avoid failures caused by static electricity when installing or removing any optional devices.

- Wear wrist straps (arm belts or anti-static gloves).

Wear wrist straps on your wrists. If no wrist strap is available, touch an unpainted metal part of the cabinet before touching a component to discharge static electricity from your body.

Touch the metal part regularly when working with components to discharge static electricity.

- Select a suitable workspace.

- Work with the server on the anti-static or concrete floor.
- When you work with the server on a carpet where static electricity is likely to be generated, make sure take anti-static measures beforehand.

- Use a worktable.

Place the server on an anti-static mat to work with it.

- Clothes

- Do not wear a wool or synthetic cloth to work with the server.
- Wear anti-static shoes to work with the server.
- Take off any metal accessories you wear (ring, bracelet, or wristwatch) before working with the server.

- Handling of components

- Keep any component in an anti-static bag until you actually install it to the server.
- Hold a component by its edge to avoid touching any terminals or parts.
- To store or carry any component, place it in an anti-static bag.

PRE-UPGRADE VERIFICATION

If you add on optional devices onto this equipment, some devices require specific ft server software version (s).

If the optional asks for specific version number (s), refer to the following procedure before adding on the devices.

1. Confirm the required ft server control software's version, Refer to the sever-accessory User's Guide, check the manufacturer's website, or contact your sales representative.
2. Verify the version of the ft control software on your system.
3. After confirming it as the available version, add the device onto the server.

For more information on how to verify the working ft server utility's, refer to the separate User's Guide (setup) "Confirming the ft Server Control Software Version" (page 5-13).

PREPARING YOUR SYSTEM FOR UPGRADE

Note the following, when installing or replacing devices, to improve the performance of Fault Tolerant Server series.

- With the Fault Tolerant Server series, devices can be replaced during the continuous operation. Take extreme care for electric shock and damage to the component due to short-circuit.
- Optional devices cannot be installed or removed during continuous operation. When you shutdown Windows Server 2003, check that the server is powered off, disconnect all power cords and interface cables from the server before installing or removing the optional devices.
- To remove the CPU/IO module during the continuous operation, disable the intended module (place the module off-line) by using the ftServer Utility of the NEC ESMPRO Agent or the NEC ESMPRO Manager from the management PC on the network. After a new module is installed to the server, enable the module using the ftServer Utility or the NEC ESMPRO Manager.

TIPS:

The system is defaulted to automatically boot the module, once installed. For more information, see Chapter 5.

- Make sure to provide the same hardware configuration on both CPU/IO modules (except SCSI board).
- Use the same slots and sockets on both groups.
- Do not install those devices having different specifications, performance, or features.
- Before removing the set screws from the CPU/IO modules, place the desired module off-line using the ftServer Utility or the NEC ESMPRO Manager.

3.5-INCH HARD DISK DRIVE

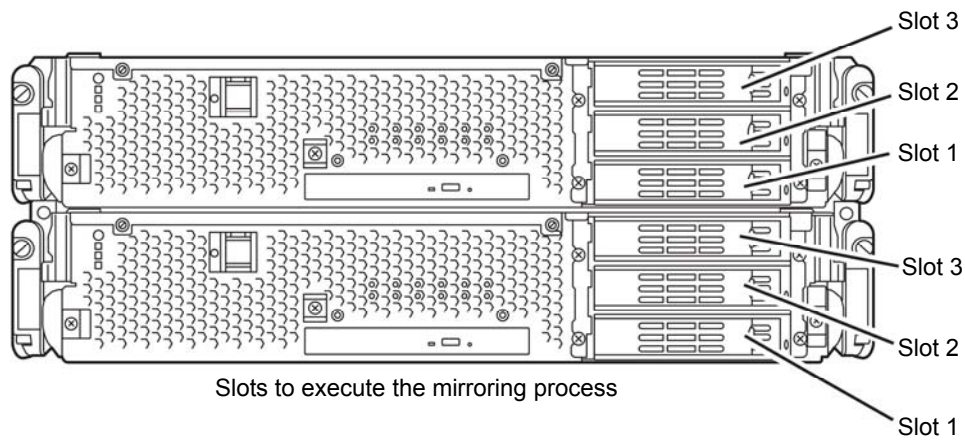
The 3.5-inch hard disk drive bay in front of the server contains six slots in which hard disks with the SAS interface are installed.

IMPORTANT:

Do not use any hard disks that are not authorized by the manufacturer. Installing a third-party hard disk may cause a failure of the server as well as the hard disk. Purchase hard disks of the same model in pair. Contact your sales agent for hard disk drives optimum for your server.

You can install 25.4mm (1-inch) high hard disk drives to six 3.5-inch hard disk drive bays on the server.

The hard disk drives installed on the slot 1, 2, and 3 of the CPU/IO module 0 and 1 are mirrored respectively. (The OS is installed on the mirror volumes that consist of the hard disks in the slot 1.)



Empty slots in the 3.5-inch hard disk drive bay contain dummy trays. The dummy trays are inserted to improve the cooling effect within the device. Always insert the dummy trays in the slots in which hard disks are not installed.

Installing 3.5-inch Hard Disk Drive

Follow the procedure below to install the hard disk. A hard disk may be installed in another slot in the same procedure.

IMPORTANT:

- Refer to “ANTI-STATIC MEASURES” and “PREPARING YOUR SYSTEM FOR UPGRADE” before starting installing or removing options.
- You must mount two HDDs that form dual disk configuration before starting Windows Server 2003.

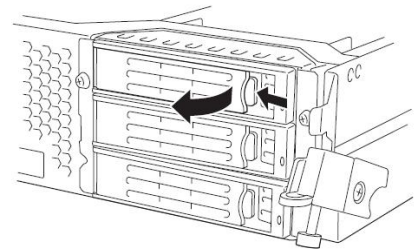
1. Shut down Windows Server 2003. The system turns off automatically.

2. Remove the front bezel.

3. Identify the slot to which you want to install the hard disk drive.

Install a hard disk in an empty slot in the group, starting from the lower slot. (In the order of slot 1, slot 2, and slot 3 in CPU/IO module 0 and 1)

4. Pull the lever toward you while pushing the green lock of the dummy tray to the left.



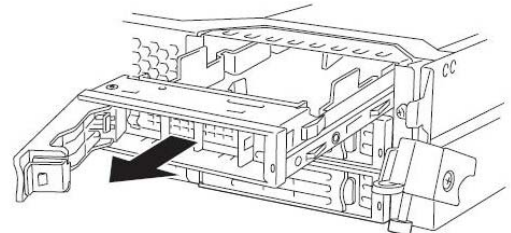
5. Hold the handle of the dummy tray to remove the tray.

IMPORTANT:

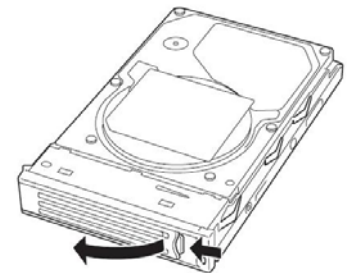
Keep and store the dummy tray with care.

TIPS:

The lever on the slot 3 may be hard to pull toward you. This does not become a problem for proper operation.



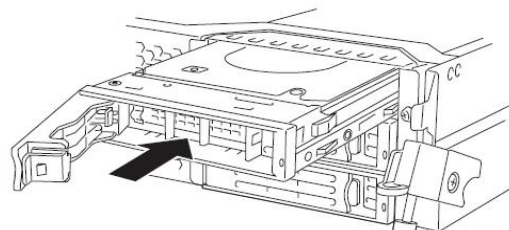
6. Unlock the hard disk to be added.



7. Firmly hold the handle of the hard disk to install and insert the hard disk into the slot.

TIPS:

- Insert the disk until the lever hook touches the server frame.
- Check the orientation of lever. Insert the hard disk with the lever unlocked.



8. Slowly close the lever.

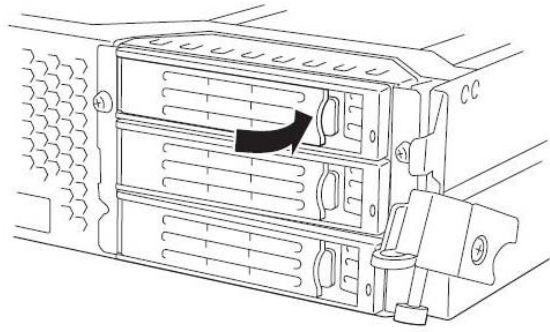
When the lever is locked, you will hear a click sound.

IMPORTANT:

Be careful not to pinch your finger(s) between the lever and handle.

TIPS:

Check the hook of the lever is engaged with the frame.



- 9.** Press the POWER switch to power on.
- 10.** Install the front bezel.
- 11.** Set the dual disk configuration (see “Step 8: Set Dual Disk Configuration” in Chapter 4 in the User’s Guide (Setup).).

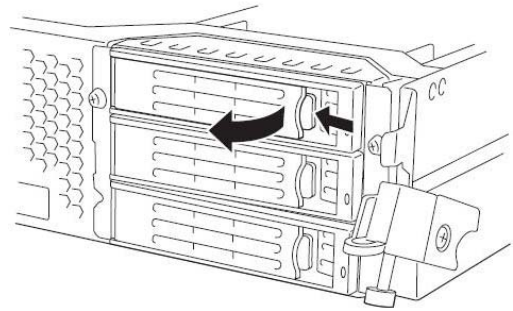
Removing 3.5-inch Hard Disk Drive

Follow the procedure below to remove the hard disk.

IMPORTANT:

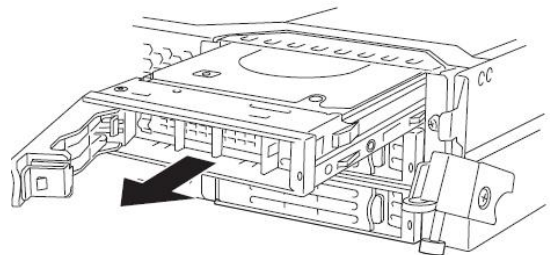
Make sure to read “ANTI-STATIC MEASURES” and “PREPARING YOUR SYSTEM FOR UPGRADE” before you take the following procedures.

1. Shut down Windows Server 2003.
The system turns off automatically.
2. Remove the front bezel.
3. Push the lever of the hard disk to unlock the handle.



4. Hold the handle and hard disk to pull them off.
5. Install the dummy tray in an empty tray according to procedures described in "Installation".

Make sure to install the dummy slot in the empty slot to improve the cooling effect within the device.



TIPS:

It may not be easy to pull the lever of slot 3 toward you, but it will not cause a problem for operation.

Replacing 3.5-inch Hard Disk Drive

Follow the procedure below to remove the failed hard disk. If the hard disk fails, it should be replaced with new device with the server powered-on.

IMPORTANT:

Make sure to read “ANTI-STATIC MEASURES” and “PREPARING YOUR SYSTEM FOR UPGRDE.” You can replace disks during continuous operation.

Replacing the Hard Disk Drive

1. Locate the failed hard disk.

When a hard disk fails, the DISK ACCESS LED on the hard disk drive’s handle illuminates amber.
2. Remove the failed hard disk referring to “Replacing Failed Hard Disk Drives” on page 3-21 and “Removing 3.5-inch Hard Disk Drive” on page 8-7.

No need to shut down Windows Server 2003.

3. Refer to the steps in “Installing 3.5-inch Hard Disk Drive” to install a new hard disk.

CHECK:

- The hard disk to be installed for replacement must have the same specifications as its mirroring hard disk.
 - After disk physical format, refer to “Disk Operation” in Chapter 3 and restore the dual configuration. For physical format, see “SAS BIOS Adaptec SAS/SATA Configuration Utility” in Chapter 4, “System Configuration,” and format disks with Disk Utilities. To format disks, select “Server,” “Monitoring Configuration” and set “Option ROM Scan Monitoring” to Disabled.” For how to configure the setting, see “System BIOS SETUP” in Chapter 4, “System Configuration.”
-

4. Restore the redundant configuration (see Chapter 3).

CPU/IO MODULE

To replace a CPU (processor, DIMM (memory), PCI card, you need to remove the CPU/IO module.

IMPORTANT:

- Ask your sales agent to replace the CPU/IO module and components of the CPU/IO module.
 - Make sure to read “ANTI-STATIC MEASURES” and “PREPARING YOUR SYSTEM FOR UPGRADE.”
 - To install or remove CPU or DIMM, first power off the server before removing the CPU/IO module.
 - Removing the module being operating may cause unexpected trouble. Use the management software (e.g., ftServer Utility or NEC ESMPRO Manager) to identify the module to be removed so that the module is removed when it is stopped, without fail.
Then remove the relevant module after verifying the Status LED on the CPU/IO module. See Chapter 2 “LEDs” for details of the Status LED.
-

Precautions

When replacing both CPU/IO modules, replace one module and wait until dual configuration is established to replace the other module. If you replace the both modules simultaneously, establishing dual CPU/IO module configuration can result in interruption of the whole system.

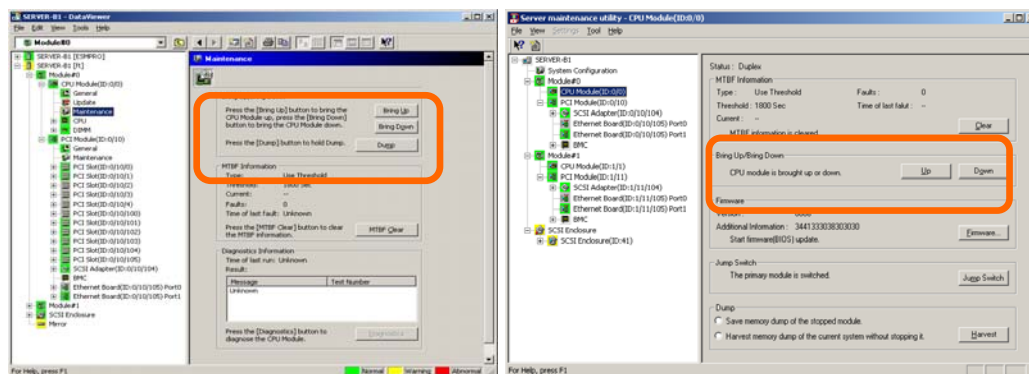
Removing CPU/IO Module

Follow the procedure below to remove the CPU/IO module.

1. Stop the CPU/IO module you want to remove.

To this end, use the ftServer Utility of the NEC ESMPRO Agent installed to your server or the Data Viewer of the NEC ESMPRO Manager.

For the detailed procedure, see “NEC ESMPRO Agent and Manager” – “Maintenance of Fault Tolerant Server series” in Chapter 5.



NEC ESMPRO Manager
Select [ft] - [CPU Module] - [CPU Module (to be removed)] - [Maintenance] - [Bring Up/Bring Down] - [Bring Down].

ftServer Utility
Select [FTServer] - [CPU Module] - [CPU Module (to be removed)] - [Bring Up/Bring Down] - [Down].

Repeat the operation mentioned above for the IO module (PCI module) and confirm that the status of the CPU/IO module and the IO module (PCI module) are “Removed.”

TIPS:

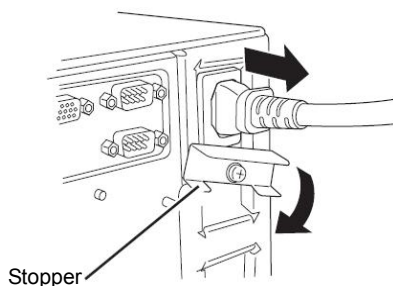
When removing CPU/IO modules 0, select [Bring Down] for CPU module (ID:0) and PCI module (ID:10)

2. Remove the front bezel

3. Hold the stopper, and disconnect the power cable of the module to be removed.
The stopper will return to the vertical position when you release it.

CHECK:

Leave your hands and make sure that the stopper returned to the vertical position. If you disconnect the cable and the stopper does not go back to this position, you cannot pull out the CPU/IO module in the next step.



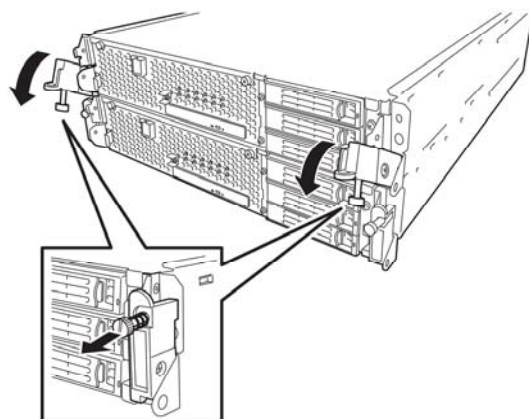
4. Loosen the screws securing the CPU/IO module handle to press down the handle.

IMPORTANT:

Before you pull out a CPU/IO module, check the rear of the server to make sure cables for connection with peripheral equipment or network are disconnected. If any cables are connected, keep a record of where the cables are connected and disconnect all cables connected to the module you are to pull out.

TIPS:

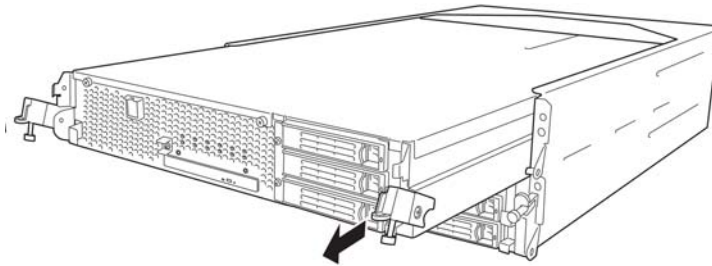
If you cannot disconnect the LAN cable easily, disconnect while pressing the latch with a slotted screwdriver.



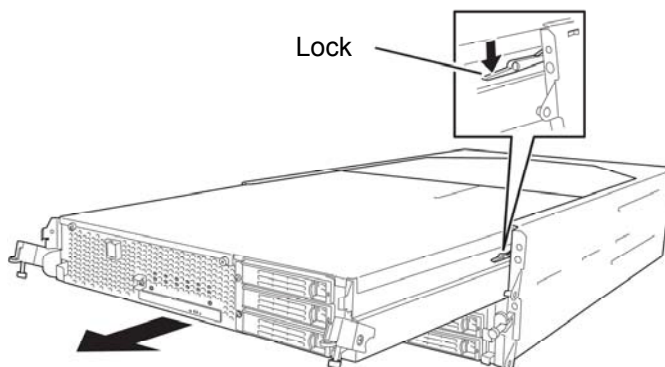
5. Hold the black levers of the CPU/IO module and pull it off. Pull it off until it is locked and stopped.

IMPORTANT:

- Do not hold part other than the handle to pull the module.
 - Handle the CPU/IO module carefully. Do not drop the module or bump it against parts in the device when you remove it.
-



6. The CPU/IO module is locked on the way and cannot be pulled out. Lower the lock on the side of CPU/IO module and unlock it, and then pull it out.



7. Pull out the CPU/IO module gently and carefully place it on a flat and sturdy table. Avoid the dusty or humid place.

This allows you to access the devices in the CPU/IO module. For more information on how to handle these devices, see the associated sections.

Installing CPU/IO Module

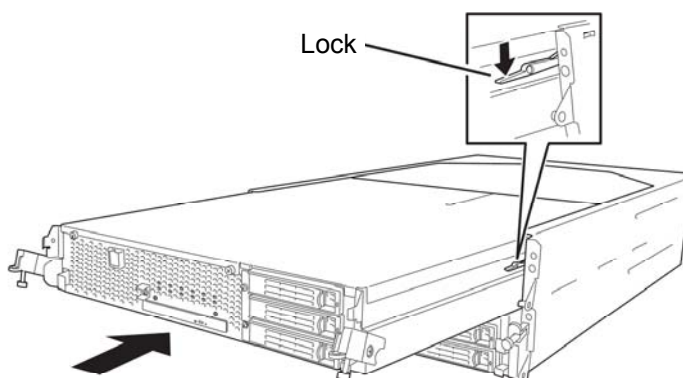
Follow the procedure below to install the CPU/IO module:

IMPORTANT:

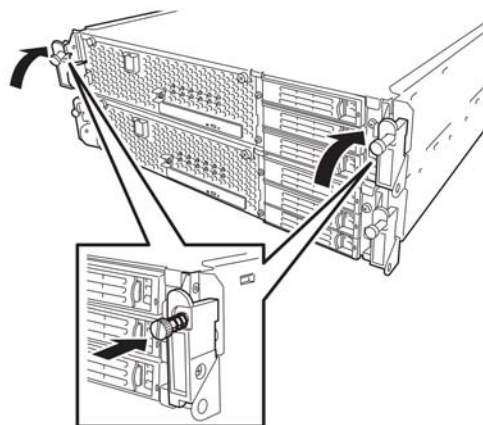
Make sure to read “ANTI-STATIC MEASURES” and “PREPARING YOUR SYSTEM FOR UPGRADE.” Insert the black lever slowly and fasten the screws tightly. Be careful not to cause a shock to the device at this time.

1. Firmly hold the CPU/IO module with both hands and insert it into the rack.

Hold the CPU/IO module in such a way that its back panel connector faces the back of the rack and engage the guides of the module and chassis, and insert it slowly.



2. Push up the black levers placed on the left and right sides of the front of the CPU/IO module, and fasten them with screws.



IMPORTANT:

- Secure the handle with the screws. If it is not secured by the screws, the operation of the CPU/IO module will be unstable.
 - In some system statuses or settings, auto start up or integration does not take place when the module is connected. In such a case, check the status by using the fitServer Utility or NEC ESMPro Manager data viewer, and then start up the CPU/IO modules.
-

3. Connect the cables for connecting the peripheral devices and network.
4. Hold the stopper with your hand and insert the cable of the installed module.
5. The installed CPU/IO module will be automatically started.

DIMM

The DIMM (dual inline memory module) is installed to the DIMM socket in the CPU/IO module on the Fault Tolerant Server series.

The CPU/IO module board is equipped with six sockets. A DIMM is installed on the CH0 slot 0 and CH1 slot 0 as standard equipment. (The standard DIMMs can be replaced with other DIMMs.)

Fault Tolerant Server: 1GB DIMM×2

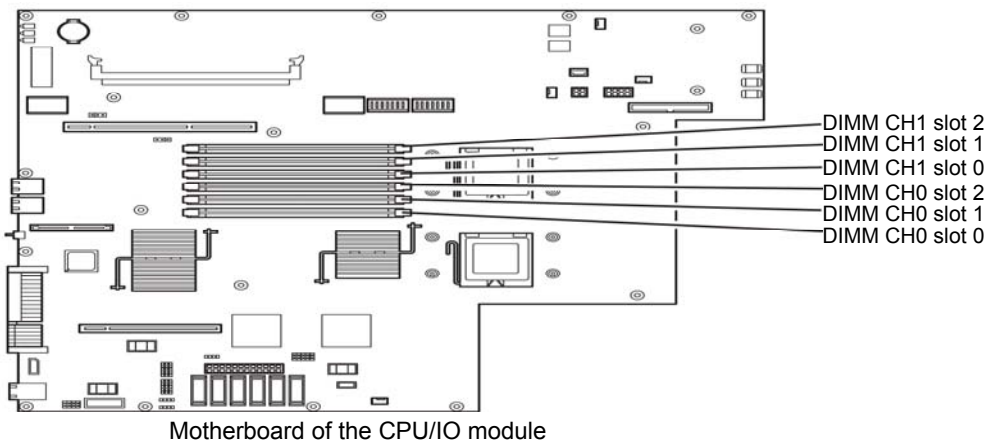
DIMMs should be installed in a set of 2 DIMMs, starting from the lowest socket number.

TIPS:

- You can add memory up to 24 GB (4GB x 6).
In the error messages and logs in POST NEC ESM PRO, or Off-line Maintenance Utility, the DIMM connector may be described as “group.” The number next to “group” corresponds to the slot number shown in the figure on the next page.
-

IMPORTANT:

- The DIMM is extremely sensitive to static electricity. Make sure to touch the metal frame of the server to discharge static electricity from your body before handling the DIMM. Do not touch the DIMM terminals or onboard parts with a bare hand or place the DIMM directly on the desk. For more information on static electricity, see “ANTI-STATIC MEASURES.”
 - Make sure to use the DIMM authorized by the manufacturer. Installing a third-party DIMM may cause a failure of the DIMM as well as the server. Repair of the server due to failures or damage resulted from installing such a board will be charged.
 - Before adding or removing DIMMs, power off the server and detach the CPU/IO module.
 - Make sure to read “ANTI-STATIC MEASURES” and “PREPARING YOUR SYSTEM FOR UPGRADE” before installing/removing DIMM.
-



Precautions

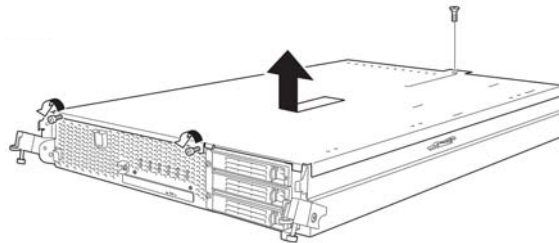
Note the following to install or replace DIMM.

- The DIMMs with the same slot number are linked between the CH1 and CH0.. When a DIMM is added to one CH, another identical DIMM should be installed to the slot with the same number in another CH. This rule is applied to the case of removal.
- The linked DIMMs between CHs should be of the same product with the same performance.
- DIMMs should be installed in sockets from the lowest slot number to the highest slot number.
- To install DIMM, install the product with the same serial number to the same CHs and slots of the CPU/IO modules 0 and 1.

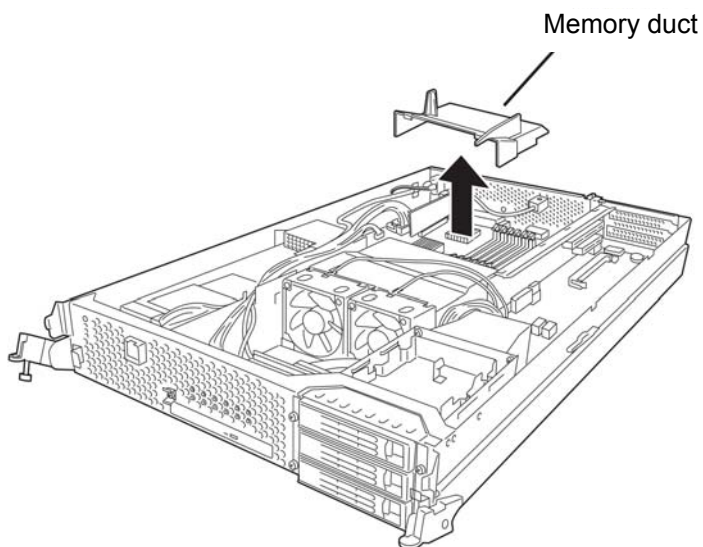
Installing DIMM

Follow the procedure below to install the DIMM.

1. Shut down OS.
The sever turns off automatically.
2. Disconnect the power cords from the outlets.
3. Remove the CPU/IO module referring to page 8-10.
4. Remove the screw, and remove the top cover of the CPU/IO module.



5. Remove the memory duct.



6. Check to be sure in which socket you are mounting the DIMM

7. Remove the DIMM connector cover from the socket in which the DIMM is installed.

A DIMM connector cover is installed to the open socket. When the levers on both ends of the connector are opened, the DIMM connector cover is unlocked and you can remove the cover.

IMPORTANT:

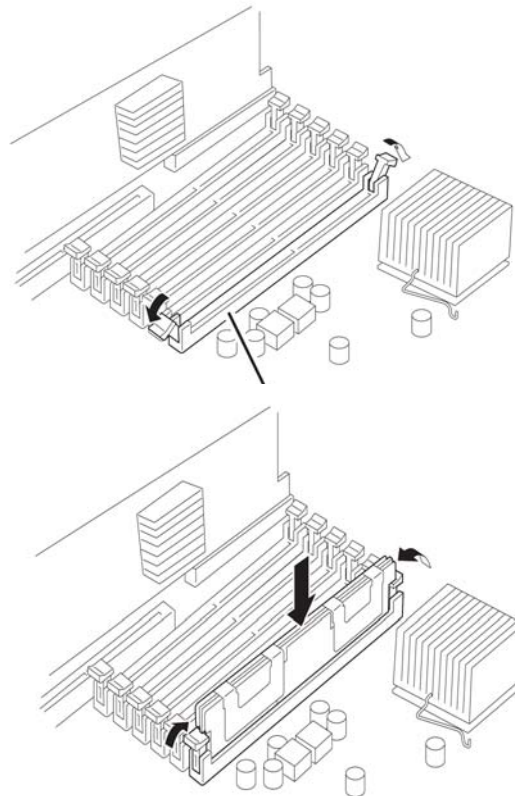
Keep the removed DIMM connector cover.

8. Insert a DIMM into the DIMM socket vertically.

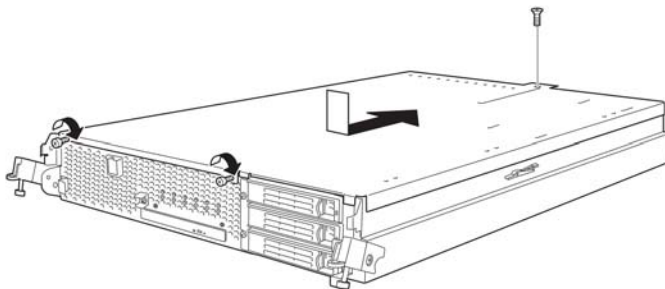
TIPS:

Pay attention to the orientation of the DIMM. The terminal of the DIMM has a cutout to prevent misinsertion.

After the DIMM is completely inserted into the socket, the levers are automatically closed.



9. Attach the memory duct
10. Place the top cover of the CPU/IO module and secure it with the screws.



11. Refer to page 8-13 and install the CPU/IO module.
12. Connect the power cords.
13. Press the POWER switch to power on the server.
14. Verify that POST displays no error message.
If POST displays an error message, write it down and see the POST error message list on page 7-4.
15. After starting the OS, set the paging file size to at least the recommended value (1.5 times the installed memory size). (See “Size of the Partition to be Created” in Chapter 4 of the User’s Guide (Setup).)

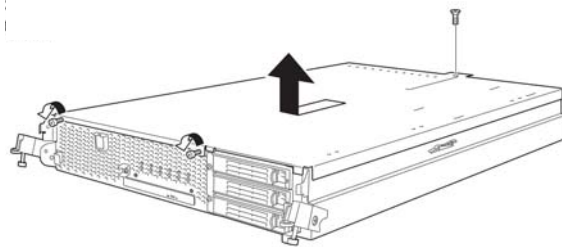
Removing DIMM

Follow the procedure below to remove the DIMM.

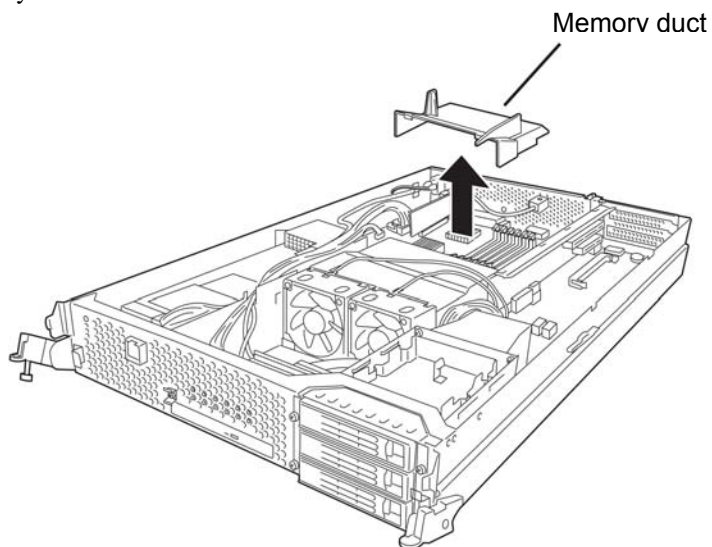
IMPORTANT:

This server works only when there are at least two DIMMs installed.

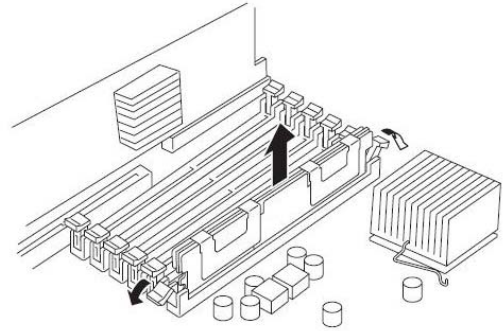
1. Shutdown OS.
The system turns off automatically.
2. Disconnect the power cords from the outlets.
3. Remove the CPU/IO module referring to page 8-10.
4. Remove the screws and the top cover of the CPU/IO module.



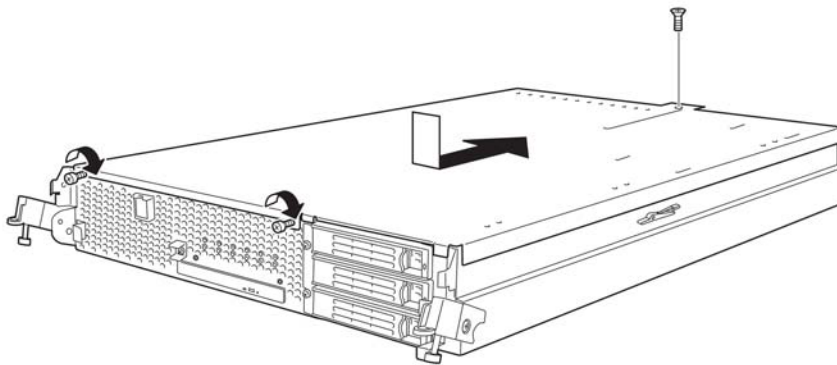
5. Remove the memory duct.



6. Open the levers attached on both sides of the socket of the DIMM to be removed. It will be unlocked and the DIMM can be removed.



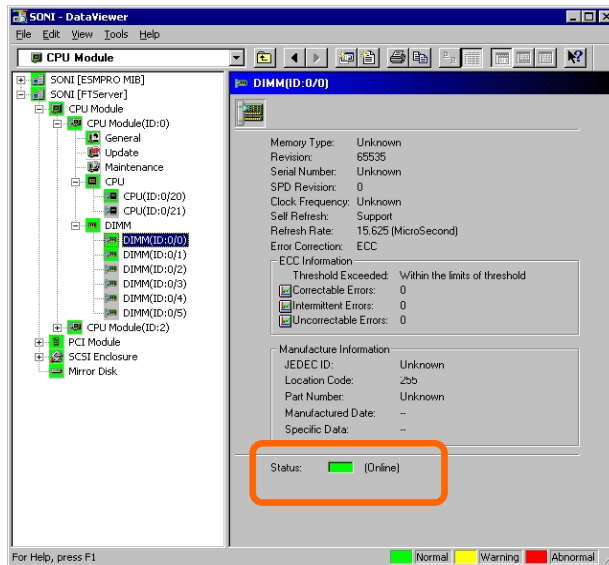
7. Attach the memory duct.
8. Attach the top cover of the CPU/IO module and secure it with screws.



9. Refer to page 8-13 and install the CPU/IO module.
10. Connect the power cords.
11. Press the POWER switch to power on the server.
12. Verify that POST displays no error message.
If POST displays an error message, write it down and see the POST error message list on page 7-4.

Replacing DIMM

Follow the procedure below to replace a failed DIMM.



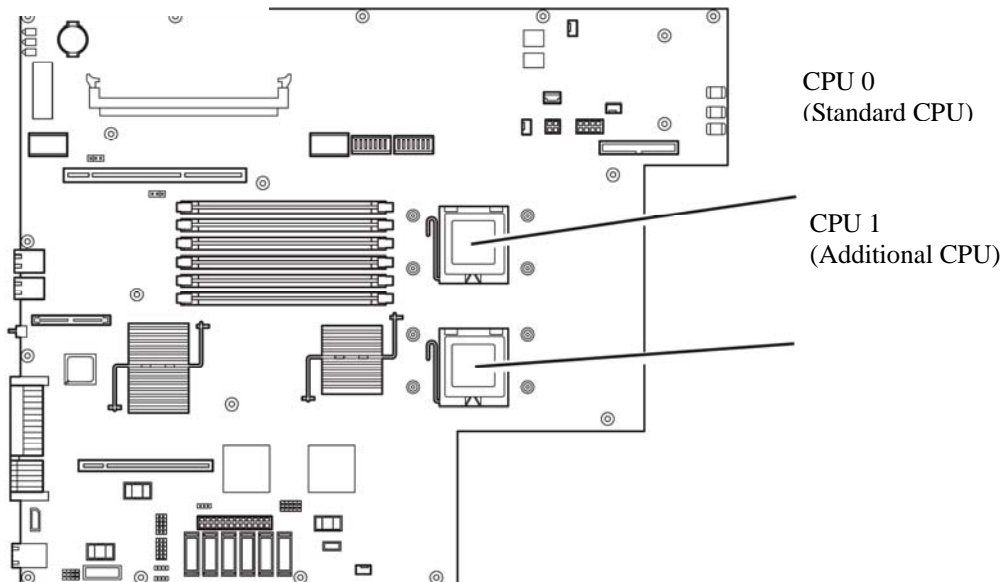
1. Identify the failed DIMM using the Data Viewer of NEC ESMPRO Manager.
2. Remove the CPU/IO module referring to page 8-10.
3. Replace the DIMM.
4. Install the CPU/IO module referring to page 8-13.
5. Start up the CPU/IO module using NEC ESMPRO Manager or ftServer Utility.

PROCESSOR (CPU)

In addition to the standard CPU (Quad-Core Intel® Xeon™ Processor), you can operate the system by adding one CPU.

IMPORTANT:

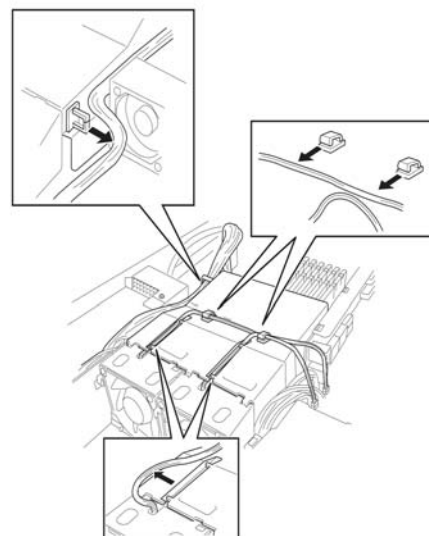
- The CPU is extremely sensitive to static electricity. Make sure to touch the metal frame of the server to discharge static electricity from your body before handling the CPU. Do not touch the CPU terminals or onboard parts with a bare hand or place the CPU directly on the desk. For more information on static electricity, see “ANTI-STATIC MEASURES.”
 - Do not use the system before checking to see it works correctly.
 - Make sure to use the CPU specified by the manufacturer. Installing a third-party CPU may cause a failure of the CPU as well as the server. Repairing the server due to failures or damage resulting from these products will be charged even if it is under guarantee.
 - Before adding or removing a CPU, power off the server and then remove the CPU/IO module.
-



Installing CPU

Follow the steps below to install a CPU (model with air-cooling kit).

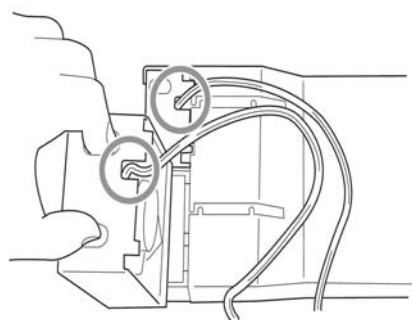
1. Shut down the OS.
The server is automatically powered off.
2. Unplug the power cords.
3. Remove the CPU/IO module referring to page 8-10.
4. Remove the cable connected to the CPU duct cover.



IMPORTANT:

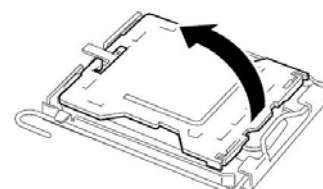
Remove the cable without adding pressure to the bases of the fan cable.

5. Remove the CPU duct cover.



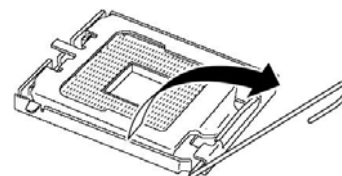
6. Check to be sure of the location of the CPU socket.
7. Detach the socket cover on the CPU socket.

IMPORTANT: Keep the socket cover.

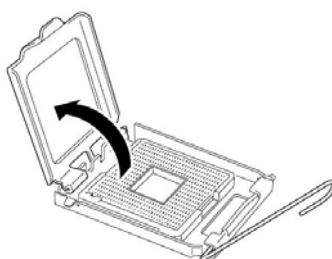


8. Lift the socket lever.

IMPORTANT: Open the lever fully. It can be opened 120° or more.



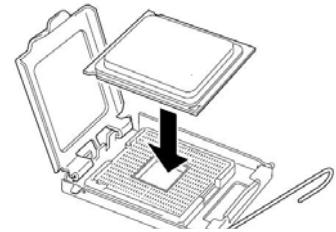
9. Lift the CPU socket holder.



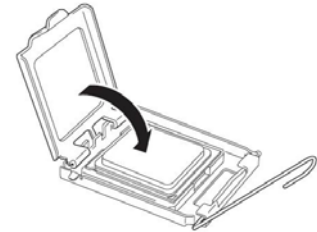
- 10.** Place the CPU on the socket carefully.

TIPS:

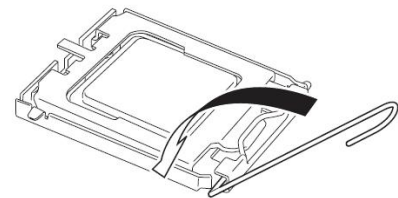
Pay attention to the orientation of the CPU. The CPU and socket have pin marks to prevent misinsertion. Check the pin marks of the CPU and the socket and insert the CPU correctly.



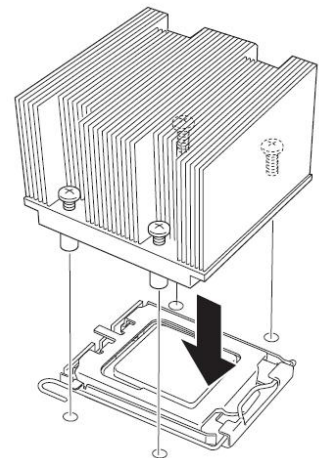
- 11.** After pressing the CPU softly against the socket, place the CPI socket holder back to its original place.



- 12.** Return the socket lever back to its original place.

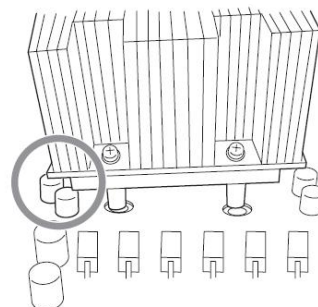


- 13.** Place the heat sink on the CPU and secure it with 4 screws. Loosely fasten the screws in the cross-coupling way, and then fasten them tightly.



IMPORTANT:

Place the heat sink so that its corners will not bump against the parts on the motherboard.



14. Check that the heat sink is attached to the mother board horizontally.

IMPORTANT:

- If the heat sink is tilted, remove the heat sink and then attach it again.
If the heat sink is not attached horizontally, it may be caused by the following.
 - The CPU is not attached correctly.
 - Screws are not secured tightly enough.
 - Do not move around the heat sink fastened.
-

15. Connect the duct cover.

16. Fasten the cable to the duct cover.

17. Refer to page 8-13 and attach install the CPU/IO module.

18. Connect the power cord.

19. Turn on the power by pressing the POWER switch.

20. Verify that POST displays no error message. If an error message is displayed, write it down and check it in the error message list on page 7-4.

Removing CPU

Removal of a heat sink and CPU is the reverse procedure of installation.

PCI BOARD

Up to three PCI boards can be installed to the CPU/IO module.

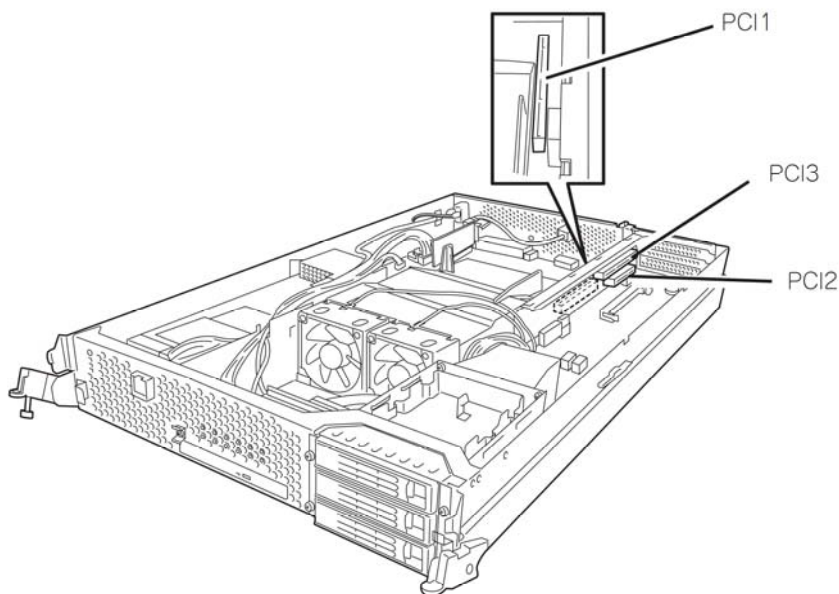
IMPORTANT:

- The PCI board is extremely sensitive to static electricity. Make sure to touch the metal frame of the server to discharge static electricity from your body before handling the PCI board. Do not touch the PCI board terminals or onboard parts by a bare hand or place the PCI board directly on the desk. For more information on static electricity, see "ANTI-STATIC MEASURES" on page 8-2.
 - Make sure to read "ANTI-STATIC MEASURES" and "PREPARING YOUR SYSTEM FOR UPGRADE."
-

Note the following to install or replace PCI board.

- To make a dual PCI board configuration, install the same type of board (i.e., having the same specifications and performance) to the same slot for each group.

When a PCI board is installed to one group, another identical PCI board should be installed to the same slot in another group. This rule is applied to the case of removal.



List of option PCI boards and installable slots:

List of optional PCI boards and installable slots:

Product name	PCI-1	PCI-2	PCI-3	Remarks
PCI slot performance	PCI-X 133MHz/64bit	PCI Express X4 lane	PCI-X 133MHz/ 64bit	
Slot size	Low Profile	Full Height		
PCI board type	3.3V	x8 socket	3.3V	
Mountable board size	MD2	Full Size		
1000BASE-T 1ch board set	○			Mount exactly the same board into the same slot on each CPU/IO module 0, 1. Up to 1 board when 1000BASE-T 2ch board set or Fibre Channel board set is already mounted.
1000BASE-SX 1ch board set	○			
1000BASE-T 2ch board set			○	Up to 1 board. Mount exactly the same board into the same slot on each CPU/IO module 0, 1. Up to 2 boards can be mounted when combined with other boards. But this board must not be mixed with 1000BASE-T 2ch board set or Fibre Channel board.
SCSI board	○		○	Up to 1 board. Mount exactly the same board into the same slot on each CPU/IO module 0, 1.
Fibre Channel board set		○		Mount exactly the same board into the same slot on each CPU/IO module 0, 1. Up to 2 boards can be mounted when combined with other boards. But this board must not be mixed with 1000BASE-T 2ch board set or Fibre Channel board.

Installing PCI Board

Follow the procedure below to install the board to be connected to the PCI board slot.

TIPS:

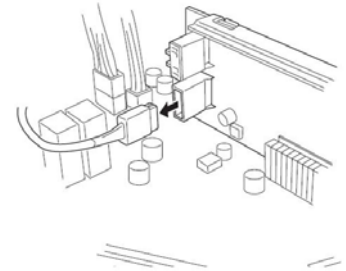
To install the PCI board, make sure the shape of the board connector matches with the shape of the PCI board slot connector.

1. Remove the CPU/IO module referring to the page 8-10.

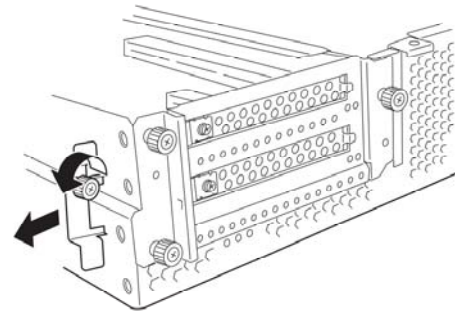
The following steps explain how to install a PCI board on the PCI board slot (PCI-X slot 2, PCI-X slot 3) of the riser card.

Go to step 10 to install a PCI board on the PCI board slot (PCI-X slot 1).

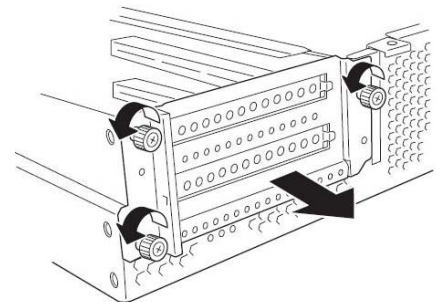
2. Disconnect the cable from the connector of the riser card.



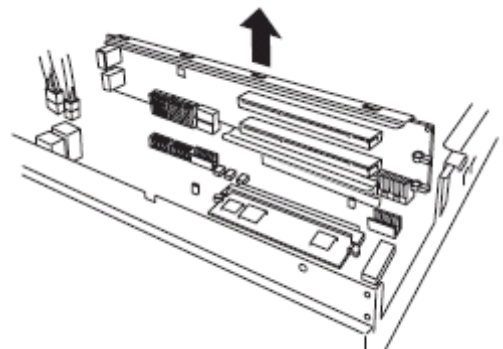
3. Loosen a fixed screw on the PCI stopper on the rear side of the device, and remove the PCI stopper.



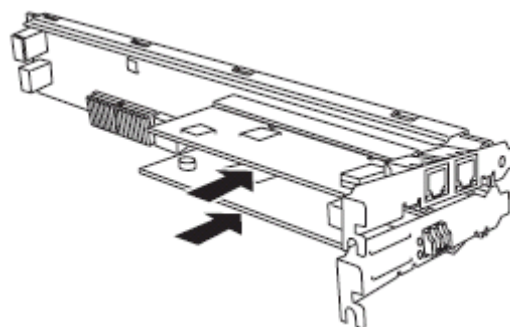
4. Loosen the 3 fixed screws on the PCI bracket on the rear side of the device, and remove the PCI bracket.



5. Remove the riser card from the motherboard.



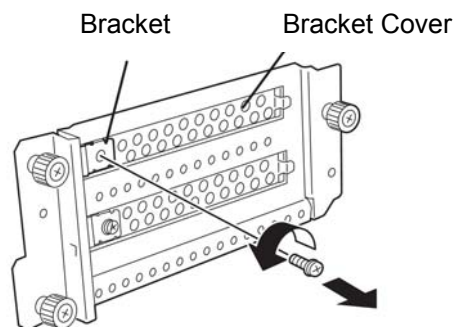
6. Insert optional PCI boards into the two PCI slots of the riser card.



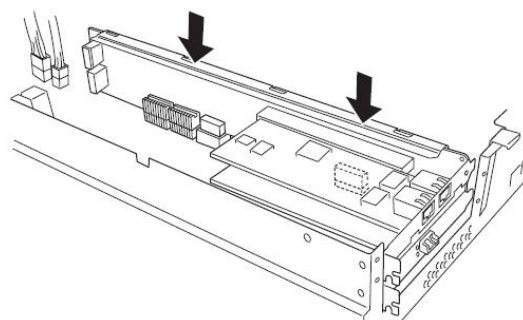
7. Remove the bracket cover (for two slots) from the PCI bracket.

IMPORTANT:

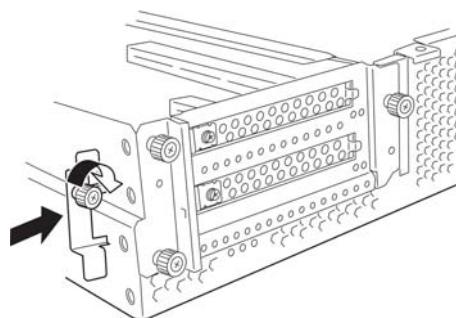
Carefully keep the removed PCI bracket.



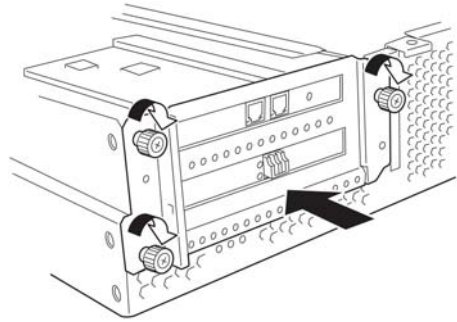
8. Install the riser card on which the PCI board is installed on the motherboard.



9. Fix screws on the PCI stopper on the rear side of the device, and slide to attach the PCI stopper.



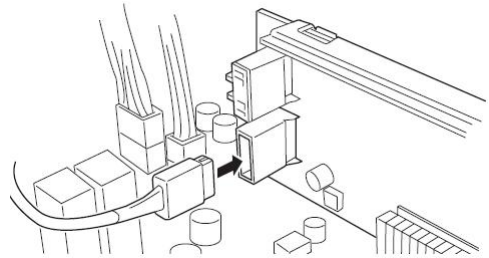
10. Secure the PCI brackets with 3 screws.



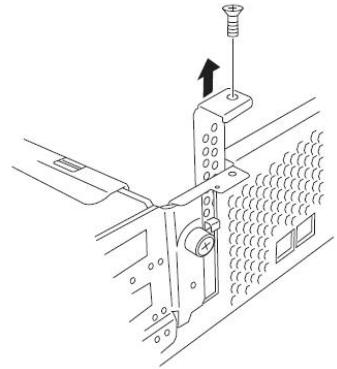
11. Connect the disconnected cable to the connector of the riser card.

IMPORTANT:

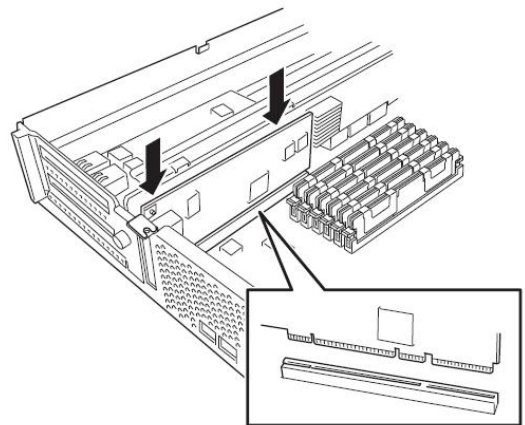
Connect the cable to the connector on the lower part.



12. Loosen the fixed screw on the bracket cover that corresponds to another PCI slot that is hidden behind the riser card, and remove the bracket cover.



13. Install the optional PCI board to another PCI slot hidden behind the riser card.



14. Secure the PCI board with a fixed screw.

Removing PCI Board

To remove PCI board card, follow the reverse procedure of the installation and install the expansion slot cover.

Replacing PCI Board

Follow the procedure below to replace the failed PCI board.

1. Check the failed board from the event log.
2. Remove the CPU/IO module referring to the page 8-10.
3. Remove the PCI bracket, then remove the PCI board.
4. Replace the board and fasten it.
5. Install the CPU/IO module referring to the page 8-13.
6. Connect the network cable and cables for PCI boards.
7. The installed CPU/IO module will start automatically.
8. Confirm that the PCI board is correctly recognized by POST and OS.

Setup of Optional PCI Board

IMPORTANT:

- To enable the fault-tolerant feature of the optional device, the identical PCI boards must be installed to the slots with the same number in CPU/IO module 0 and CPU/IO module 1.
 - The BIOS settings need to be modified when mounting some optional PCI boards. To change the BIOS settings, start the BIOS setup utility to change the [OS Boot Monitoring] configuration in [Server] – [Monitoring Configuration]. See page 4-24 for more details.
 - For the supported connecting devices, contact your sales agent.
-

1000BASE-T 1ch board set

1000BASE-SX 1ch board set

1000BASE-T 2ch board set

IMPORTANT:

For LAN cable's connector, use a RJ-45 connector which is compliant with IEC8877 standard. If any other connector is used, it may not be removed easily.

- List of slots to install optional PCI boards
Refer to "List of option PCI boards and installable slots" on page 8-25.
- Driver installation procedure

TIPS:

To perform this procedure, you have to log on the system as an Administrator or a member of the Administrators group.

For Fault Tolerant Server series, use two option PCI boards in a pair to make dual configuration.

After installing OS, install drivers in the following procedure and make dual configuration of the PCI boards.

Follow the steps below to install the driver and establish a dual configuration:

1. Mount the PCI boards to the slots with the same number in CPU/IO modules 0 and 1, and then start Windows Server 2003.
2. Insert the “EXPRESSBUILDER” DVD into the DVD-ROM drive and run the following command after starting Command Prompt.

Run either of the below command depending on the OS:

<32bit> Optical disc drive: \001\win\has\w2k3\HASSETUP\LAN\INSTALL.VBS

<64bit> Optical disc drive: \001\win\has\w2k3amd64\HASSETUP\LAN\INSTALL.VBS

3. Configure transmitting speed and Duplex mode for the driver

TIPS:

If the check box in [Internet Protocol (TCP/IP)] is unchecked, first check an then configure the IP address.

- (1) Launch Device Manager
- (2) Expand network adapter and double click [Stratus emb-EB 2-Port Gigabit Adapter].
- (3) Double click [Link speed] tab, then configure [Speed and Duplex] to match the value on the hub.
- (4) On network adapter property, click [OK] at dialog box.
- (5) By the same procedure, configure another [Stratus emb-EB 2-Port Gigabit Adapter #2]

Add/delete protocol or services if needed. On [Network Connections], go to Local Area connection property's dialog box.

TIPS:

[Network monitor] is recommended to add as one of the services. [Network monitor] can monitor frames (or packets) sent and received a computer that installs [Network monitor]. This is a useful tool to analyze network failure. Refer to [Setup for failure managing] for the installation procedure.

As to the setup of another network port, [Managing port], refer to the online document [EDPRESSSCOPE Engine 2 User's guide] stored in the EXPRESSBUILDER DVD.

4. Set a dual LAN configuration.

Refer to “DUAL LAN CONFIGURATION” on page 3-24.

Now the 1000BASE-T 1ch board set, 1000BASE-SX 1ch board set, or 1000BASE-T 2ch board set is installed.

SCSI Board

- The lists of slots to install optional PCI boards

Refer to the table “List of option PCI boards and installable slots” on page 8-25.

- Driver installation procedure

TIPS:

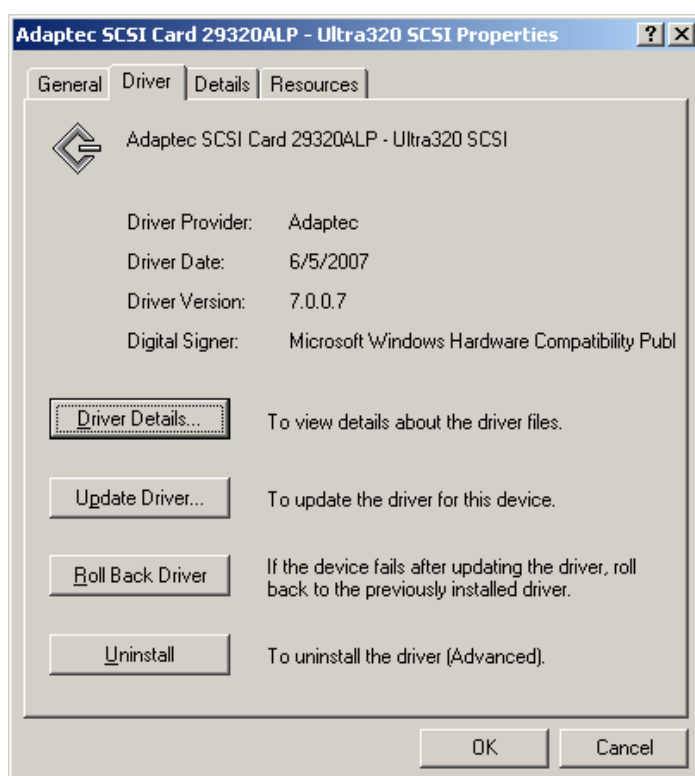
To perform this procedure, you have to log on the system as an Administrator or a member of the Administrators group.

1. Mount the SCSI board and start Windows Server 2003. When this launches, [New Hardware Detected] window appear and the driver will be installed automatically. However, the standard driver for the OS is not applicable on the ft server. Therefore, update the driver with the following procedure.
2. Insert the “EXPRESSBUILDER” DVD into the DVD-ROM drive and run the following command after starting the command prompt.

Run either of the below command depending on the OS:

<32bit> Optical disc drive: \001\win\has\w2k3\HASSETUP\LAN\INSTALL.VBS
 <64bit> Optical disc drive: \001\win\has\w2k3amd64\HASSETUP\LAN\INSTALL.VBS

3. Confirm the driver's version.
 From [Device Manager], select [SCSI and RAID Controller]. Right-click [Adaptec SCSI Card 29320ALP-Ultra320 SCSI] and display the property. Click [Driver] tag and confirm whether the driver version is 7.0.0.7. (see below).



Fibre Channel Board Set

- List of slots to install optional PCI boards

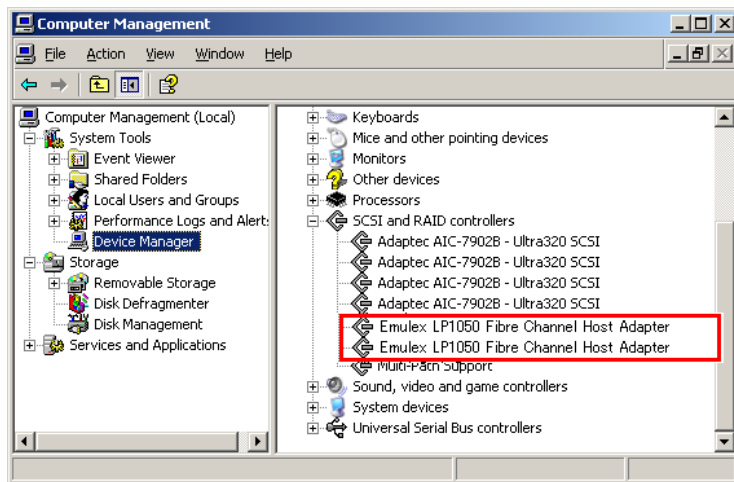
“List of option PCI boards and installable slots:” on page 8-25.

- Driver installation procedure

TIPS:

To perform this procedure, you have to log on the system as an Administrator or a member of the Administrators group.

1. Mount a the Fibre Channel board set, and then start the system.
2. Start Device Manager from [Start] - [Program] - [Administrative Tool] - [Computer Management], and check if “Fibre Channel Controller” appears under the [Other devices] as many as mounted.



3. Load EXPRESSBUILDER DVD on the optical disc drive, then open command prompt and run following commands:

TIPS:

Do not break a line when you enter the commands.

<32bit>

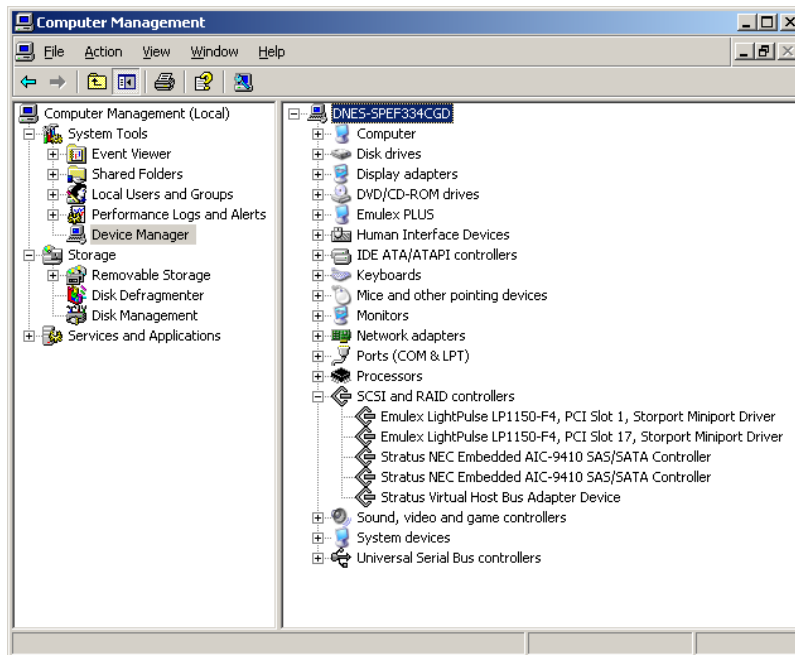
DVD-ROM drive: \001\win\has\w2k3\HASSETUP\FC\FCINST DVD-ROM
drive:\001\win\has\w2k3\HASSETUP\FC

<64bit>

DVD-ROM drive: \001\win\has\w2k3amd64\HASSETUP\FC\FCINST DVD-ROM
drive:\001\win\has\w2k3amd64\HASSETUP\FC

You can confirm the completion of the installation when [Install Completed Successfully!] appears. Close command prompt and reboot the system.

4. After the system is rebooted, start Device Manager from [Start] - [Program] - [Administrative Tool] - [Computer Management], and check that “Emulex LightPulse LP1150-F4, PCI Slot n, Storport Miniport Driver” are displayed under the [SCSI and RAID Controllers] as many as installed.



IMPORTANT:

- StoragePathSavior is necessary to connect to a Storage using the Fiber Channel boards.
 - Mount the Fiber Channel boards after completing the OS installation. They are used in a pair. Mount each controller on the slot of the same position of each PCI module.
-

ft Remote Management Card

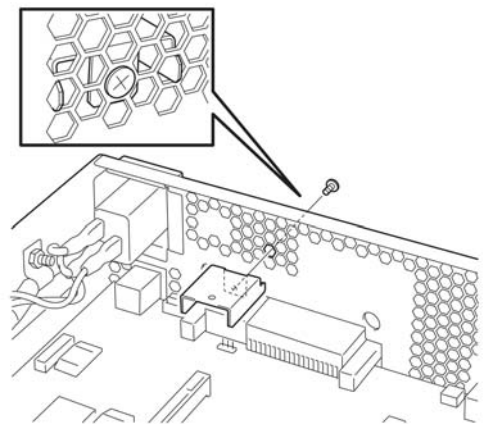
Each CPU/IO module can mount one ft Remote Management Card.

IMPORTANT:

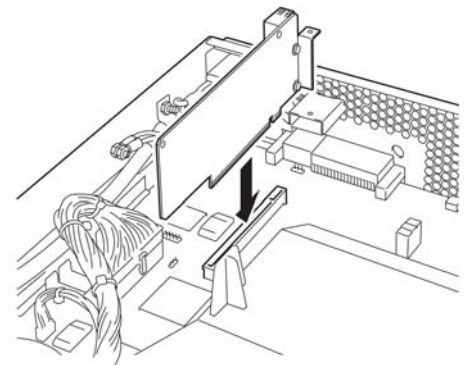
- The ft Remote Management Card is extremely sensitive to static electricity. Make sure to touch the metal frame of the server to discharge static electricity from your body before handling the card. Do not touch the card terminals or onboard parts with a bare hand or place the card directly on the desk. For more information on static electricity, see “ANTI-STATIC MEASURES.”
 - Make sure to read “ANTI-STATIC MEASURES” and “PREPARING YOUR SYSTEM FOR UPGRADE” before mounting the ft Remote Management Card.
-

Mounting the ft Remote Management Card

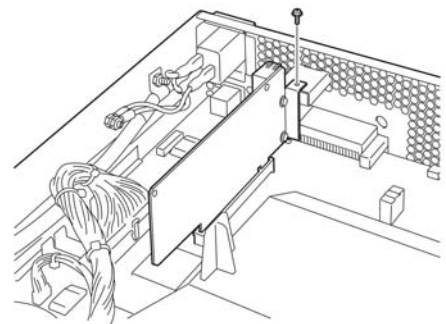
1. Refer to 8-12 and remove the CPU/IO module.
2. Hitch the bracket to a hole on the back of the 2U chassis and fix with a flat head screw.



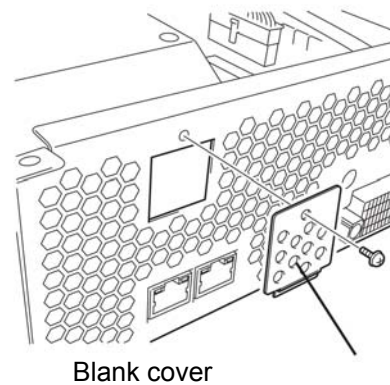
3. Mount the ft Remote Management Card.



4. Fix the card and the bracket with a screw.

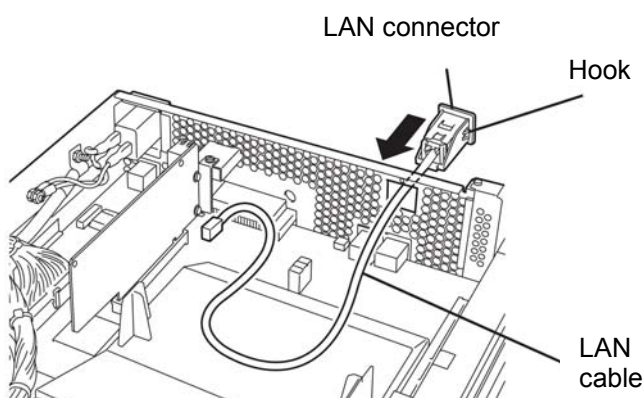


5. Remove the blank cover by removing the screw.

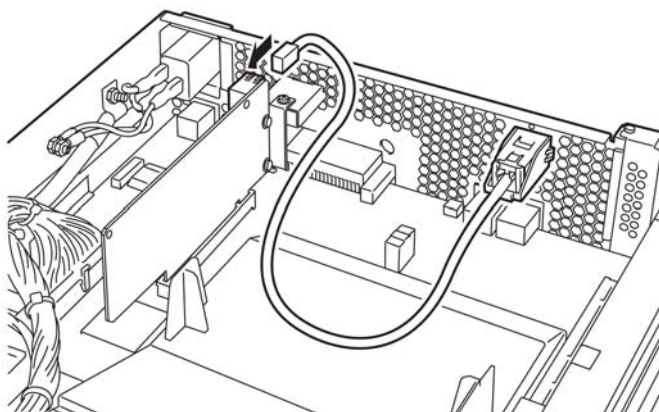


6. Put a LAN cable through a hole from outside the server and plug the LAN connector (the bigger connector) to the back of the chassis.

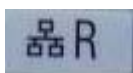
Make sure you see two hooks on the both sides of the LAN connector and hear the snap sound as you fix the LAN connector.



7. Attach the smaller connector to the LAN connector on the ft Remote Management card.



8. Attach the below label above the LAN connector on the outside of the chassis.



This page is intentionally left blank.

Appendix A

Specifications

Item		Fault Tolerant Server-LR	Fault Tolerant Server-MR
Factory-set model		Install model	
CPU	Type	Quad-Core Intel® Xeon® Processor 2.00GHz	Quad-Core Intel® Xeon® Processor 3.00GHz
	Clock/second cache	1333MHz/4MB × 2	
	Number of processors	1 processor (the number of processors installed per module)	
	Standard	Up to 1 processors (the number of processors installed per module)	
	Maximum	Up to 2 processors (the number of processors installed per module)	
Chipset		Intel Blackford + ESB2M	
Memory	Standard	2GB (1GB × 2*) * the number of memory per module	
	Maximum	24GB (The standard DIMM must be replaced.)	
	Expansion unit	2 DIMMs	
	Memory module	DDR II SDRAM DIMM (Fully Buffered)	
	Error check	ECC	
Graphics (VRAM)		ATI ES1000	
Auxiliary input device	Floppy disk (option)	3.5 inch drive x 1 (USB)	
	DVD-ROM (standard)	DVD Combo (Load type: tray. Speed: x6)	
	Hard disk (standard)	None	
	Hard disk (maximum)	1.8TB* (300GB × 6) * The user area is reduced to a half of the physical capacity due to software mirroring.	
File bay (3.5 inch)		6 slots	
Additional slot		1 slot (Low profile : PCI-X 133MHz, 64 bit), 1 slot (Full height, full length : PCI-X 100MHz, 64 bit), 1 slot (PCI-Express x4 lane x8)	
LAN interface		1000BASE-T/100BASE-TX/10BASE-T (2 ports)	
External interface	USB	4-pin connector (3 ports) Keyboard occupies one port.	
	Network	RJ-45 (2 ports)	
	Display	MINI D-sub 5-pin (1 port)	
Cabinet design		Rack-mount type	
External dimensions		483 (w) × 178 (h) × 762 (d) mm	
Weight		47.5 kg (Max. 53.5kg)	
Power supply		100 to 240 VAC ±10%, 50/60 Hz ±1 Hz	
Power consumption		1202VA / 1200W	
Environmental requirements	In operation	Temperature 10 to 35°C Humidity 20 to 80% RH (non-condensing)	
	In storage	Temperature -10 to 55°C Humidity 20 to 80% RH (non-condensing)	
Bundled standard software		RDR	

This page is intentionally left blank.

Appendix B

I/O Port Addresses

The factory-set I/O port addresses for the server are assigned as follows:

Address	Chip in Use
0x00000000-0x00000CF7	Direct memory access controller
0x00000010-0x0000001F	Motherboard resources
0x00000020-0x00000021	Programmable interrupt controller
0x00000024-0x00000025	Motherboard resources
0x00000028-0x00000029	Motherboard resources
0x0000002C-0x0000002D	Motherboard resources
0x0000002E-0x0000002F	Motherboard resources
0x00000030-0x00000037	Motherboard resources
0x00000038-0x00000039	Motherboard resources
0x0000003C-0x0000003D	Motherboard resources
0x00000040-0x00000043	System timer
0x00000050-0x00000053	Motherboard resources
0x00000060-0x00000060	Motherboard resources
0x00000061-0x00000061	System speaker
0x00000062-0x00000063	Motherboard resources
0x00000064-0x00000064	Motherboard resources
0x00000066-0x00000067	Motherboard resources
0x00000070-0x00000073	System CMOS/real time clock
0x00000074-0x00000077	Motherboard resources
0x00000080-0x00000080	Motherboard resources
0x00000081-0x0000008F	Direct memory access controller
0x00000090-0x0000009F	Motherboard resources
0x000000A0-0x000000A1	Programmable interrupt controller
0x000000A4-0x000000A5	Motherboard resources
0x000000A8-0x000000A9	Motherboard resources
0x000000AC-0x000000AD	Motherboard resources
0x000000B0-0x000000B5	Motherboard resources
0x000000B8-0x000000B9	Motherboard resources
0x000000BC-0x000000BD	Motherboard resources
0x000000C0-0x000000DF	Direct memory access controller
0x000000E0-0x000000E3	Motherboard resources
0x000000E4-0x000000E6	Stratus BMC Device
0x000000E7-0x000000EF	Motherboard resources
0x00000120-0x00000120	Stratus Virtual ATI Video
0x00000274-0x00000277	ISAPNP Read Data Port
0x00000279-0x00000279	ISAPNP Read Data Port
0x000002F8-0x000002FF	Communications Port (COM2)
0x000003B0-0x000003BB	PCI standard PCI-to-PCI bridge
0x000003B0-0x000003BB	Stratus Fault Tolerant North PCI to PCI Bridge
0x000003B0-0x000003BB	Stratus Fault Tolerant East/West PCI to PCI Bridge
0x000003B0-0x000003BB	Stratus Fault Tolerant Core

Address	Chip in Use
0x000003B0-0x000003BB	Intel(R) 82801 PCI Bridge - 244E
0x000003B0-0x000003BB	Stratus Virtual ATI Video
0x000003C0-0x000003DF	PCI standard PCI-to-PCI bridge
0x000003C0-0x000003DF	Stratus Fault Tolerant North PCI to PCI Bridge
0x000003C0-0x000003DF	Stratus Fault Tolerant East/West PCI to PCI Bridge
0x000003C0-0x000003DF	Stratus Fault Tolerant Core
0x000003C0-0x000003DF	Intel(R) 82801 PCI Bridge - 244E
0x000003C0-0x000003DF	Stratus Virtual ATI Video
0x0000040B-0x0000040B	Direct memory access controller
0x000004D0-0x000004D1	Programmable interrupt controller
0x000004D6-0x000004D6	Direct memory access controller
0x00000500-0x0000057F	Motherboard resources
0x00000580-0x0000059F	Motherboard resources
0x000005A0-0x000005BF	Motherboard resources
0x00000A79-0x00000A79	ISAPNP Read Data Port
0x00000C00-0x00000C01	Programmable interrupt controller
0x00000CA2-0x00000CA2	Stratus BMC Device
0x00000CA3-0x00000CA3	Stratus BMC Device
0x00000CA4-0x00000CA7	Stratus BMC Device

Technical publication remarks form

Title: NovaScale R630 E1 User's Guide

Reference: 86 A1 38FA 00

Date: June 2008

ERRORS IN PUBLICATION

SUGGESTIONS FOR IMPROVEMENT TO PUBLICATION

Your comments will be promptly investigated by qualified technical personnel and action will be taken as required.
If you require a written reply, please include your complete mailing address below.

NAME: _____ DATE: _____

COMPANY: _____

ADDRESS: _____

Please give this technical publication remarks form to your BULL representative or mail to:

Bull - Documentation Dept.
1 Rue de Provence
BP 208
38432 ECHIROLLES CEDEX
FRANCE
info@frec.bull.fr

Technical publications ordering form

To order additional publications, please fill in a copy of this form and send it via mail to:

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

Phone:
FAX:
E-Mail:

+33 (0) 2 41 73 72 66
+33 (0) 2 41 73 70 66
srv.Duplicopy@bull.net

Reference	Designation	Qty
_____ [_ _]		
_____ [_ _]		
_____ [_ _]		
_____ [_ _]		
_____ [_ _]		
_____ [_ _]		
_____ [_ _]		
_____ [_ _]		
_____ [_ _]		
_____ [_ _]		
_____ [_ _]		
_____ [_ _]		
_____ [_ _]		
[_ _] : The latest revision will be provided if no revision number is given.		

NAME: _____ DATE: _____

COMPANY: _____

ADDRESS: _____

PHONE: _____ FAX: _____

E-MAIL: _____

For Bull Subsidiaries:

Identification: _____

For Bull Affiliated Customers:

Customer Code: _____

For Bull Internal Customers:

Budgetary Section: _____

For Others: Please ask your Bull representative.

BULL CEDOC
357 AVENUE PATTON
B.P.20845
49008 ANGERS CEDEX 01
FRANCE

REFERENCE
86 A1 38FA 00