C122-E096-01EN

PRIMEQUEST
510A

REFERENCE MANUAL:
BASIC OPERATION/GUI/COMMANDS

FUJITSU

FOR SAFE OPERATION

This manual contains important information regarding the use and handling of this product. Read this manual thoroughly. Pay special attention to the section "NOTE ON SAFETY" Use the product according to the instructions and information available in this manual. Keep this manual handy for further reference.

Fujitsu makes every effort to prevent users and bystanders from being injured or from suffering damage to their property. Use the product according to this manual.

ABOUT THIS PRODUCT

This product is designed and manufactured for use in standard applications such as office work, personal device, household appliance, and general industrial applications. This product is not intended for use in nuclear-reactor control systems, aeronautical and space systems, air traffic control systems, mass transportation control systems, medical devices for life support, missile launch control systems or other specialized uses in which extremely high levels of reliability are required, the required levels of safety cannot be guaranteed, or a failure or operational error could be life-threatening or could cause physical injury (referred to hereafter as "high-risk" use). You shall not use this product without securing the sufficient safety required for high-risk use. If you wish to use this product for high-risk use, please consult with sales representatives in charge before such use.

RADIO FREQUENCY INTERFERENCE STATEMENT

The following notice is for EU users only.

WARNING: This is a product which meets Class A of EN55022. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

The following notice is for USA users only.

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.

Laser standards

This equipment includes Class 1 laser products and complies with FDA Radiation Performance Standards, 21 CFR 1040.10 and 1040.11, and the International Laser Safety Standards IEC60825-1: 2001.

TRADEMARK ACKNOWLEDGEMENTS

- Microsoft, Windows, MS, Windows NT, and Windows Server are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.
- Linux is a trademark or registered trademark of Linus Torvalds in the United States and other countries.
- Red Hat, RPM, and all Red-Hat-based marks and logos are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries.
- SUSE is a registered trademark of Novell Inc. in the United States and other countries.
- Intel, Xeon, and Itanium2 are trademarks or registered trademarks of Intel Corporation.
- Ethernet is a registered trademark of Fuji Xerox Co., Ltd. and Xerox Corporation in the United States and other countries.
- All other product names mentioned herein are the trademarks or registered trademarks of their respective owners.
- System and product names in this manual are not always noted with trademark or registered trademark symbols (™), (®).

TERMS AND CONDITIONS

The product includes software provided by third parties in addition to that provided by Fujitsu Ltd. You are granted permission to use the third parties' software subject to the terms and conditions below. If you acquire the source code of the software to which the following terms and conditions apply, refer to LICENSE1_EN.pdf and LICENSE2_EN.pdf, which are provided with the 'PRIMEQUEST Manuals' (C122-E013-C2).

THIS SOFTWARE IS PROVIDED "AS IS" AND FUJITSU LIMITED MAKES NO WARRANTIES, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER WHATSOEVER REGARDING TO THIS SOFTWARE, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE.

IN NO EVENT SHALL FUJITSU LIMITED BE LIABLE FOR ANY CLAIM FROM A THIRD PARTY, OR SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE, COPYING, MODIFICATION OR DISTRIBUTION OF THIS SOFTWARE.

The contents of this manual shall not be disclosed in any way or reproduced in any media without the express written permission of Fujitsu Limited.

All Rights Reserved, Copyright © FUJITSU LIMITED 2008

C122-E096-01EN

Revision History

(1/1)

Edition	Date	Revised section (Added/ Deleted/ Altered)(Note)	Details
01	2008-05-20	—	—

Note: In this table, the revised section is indicated by its section number in the current edition.
An asterisk (*) indicates a section in the previous edition.

Preface

This manual describes how to operate the system using the Web-UI and command line interface (CLI) provided with the PRIMEQUEST-series machine. Read this manual together with the manuals referenced in this manual.

This section explains:

- Structure and Contents of This Manual
- Other Reference Manuals
- Abbreviations
- Text Conventions
- Syntax of the Command Line Interface (CLI)
- Notes Regarding Notations Used in This Manual
- Conventions for Alert Messages
- Environmental Requirements for Using This Product
- Reader Feedback

Structure and Contents of This Manual

This manual is organized as described below:

Part I Basics

CHAPTER 1 Structure of This manual and How to Read It

Describes the structure of this manual and provides information about reading the manual.

CHAPTER 2 Overview of the Web-UI

Describes basic operations from the Web-UI provided with the PRIMEQUEST-series machine.

CHAPTER 3 Starting and Stopping the System

Explains how to turn on and turn off the main unit and partitions and also how to use LEDs to check the status.

Part II PRIMEQUEST Functions

CHAPTER 4 Overview of PRIMEQUEST Functions

Describes the PRIMEQUEST Server Agent (PSA) and management board (MMB) functions among the functions provided by PRIMEQUEST-series machines.

Part III MMB

CHAPTER 5 Web-UI Operations

Provides a list of menus and describes the windows and use of the MMB Web-UI for managing and operating the PRIMEQUEST-series machine.

CHAPTER 6 CLI Operations

Describes use of the CLI for managing and operating the PRIMEQUEST-series machine.

Part IV PSA

CHAPTER 7 Web-UI Operations

Provides a list of menus and describes the windows and use of the MMB Web-UI for PSA operations.

CHAPTER 8 CLI Operations

Describes use of the CLI for PSA operations.

Part V EFI

CHAPTER 9 EFI Overview

Provides an overview of the EFI.

CHAPTER 10 Boot Manager

Describes the EFI menu functions used to specify and change boot processing.

CHAPTER 11 EFI Shell and EFI Commands

Describes the EFI shell functions.

Glossary

Explains the terms used in this manual.

Index

Describes keywords and corresponding reference page numbers.

Other Reference Manuals

The following manuals are provided for reference:

a) PDF manuals included on the *PRIMEQUEST Manuals* CD-ROM disk (C122-E013-C2)

Title	Description	Manual code
PRIMEQUEST 510A System Design Guide	Explains requirements, considerations, and notes on the system operation design of the PRIMEQUEST 510A.	C122-B018EN
PRIMEQUEST 510A Installation Planning Manual	Explains specifications and requirements for installation sites that are applicable to the installation of the PRIMEQUEST 510A.	C122-H003EN
PRIMEQUEST 500A/500/400 Series Installation Manual	Explains the setup of the PRIMEQUEST, including the preparation for the installation, initial settings, and software installation.	C122-E001EN
PRIMEQUEST 510A Reference Manual: Basic Operation/GUI/ Commands	Explains operations, setup methods, and the system management method that are required for the system operation of the PRIMEQUEST. The explanation covers basic operations and functions of the MMB, PSA, and EFI.	C122-E096EN
PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/ Operation Information	Explains system maintenance, Hot Plug, REMCS, and LEDs and other information required for system operation. Also, the manual provides supplementary information such as information on the physical locations of components.	C122-E074EN
PRIMEQUEST 500A/500/400 Series Reference Manual: Messages/Logs	Explains measures to be taken against problems that occur during operation and describes various types of messages.	C122-E004EN
SPARC Enterprise/ PRIMEQUEST Common Installation Planning Manual	Explains basic information and policy on installation planning and facilities planning that are required for the installation of the SPARC Enterprise series and PRIMEQUEST series.	C120-H007EN

b) Printed manual

For the printed manual (sold separately), contact your certified service engineer.

- *PRIMEQUEST 500A/500/400 Series Installation Manual* (C122-E001EN)

Abbreviations

In this manual, the product names are abbreviated as follows:

Long title	Abbreviations
Red Hat® Enterprise Linux® AS (v.4 for Itanium) (*1)	Red Hat (*3)
Red Hat® Enterprise Linux® 5 (for Intel Itanium) (*2)	
Red Hat® Enterprise Linux®AS (v.4 for Itanium)	RHEL-AS4(IPF)
Red Hat® Enterprise Linux®5 (for Intel Itanium)	RHEL5(IPF) (*4)
SUSE™ Linux Enterprise Server 9 for Itanium Processor Family	SUSE
SUSE™ Linux Enterprise Server 10 for Itanium Processor Family	
SUSE™ Linux Enterprise Server 9 for Itanium Processor Family	SUSE9
SUSE™ Linux Enterprise Server 10 for Itanium Processor Family	SUSE10
Microsoft® Windows® XP Professional	Windows XP
Microsoft® Windows® XP Home Edition	
Microsoft® Windows Server® 2003, Enterprise Edition for Itanium-based Systems	Windows Windows Server 2003
Microsoft® Windows Server® 2003, Datacenter Edition for Itanium-based Systems	
Microsoft® Windows Server® 2008 for Itanium-Based Systems	Windows Windows Server 2008

*1: Supports Red Hat® Enterprise Linux® AS (v4.6 for Itanium) or later.

*2: Supports Red Hat® Enterprise Linux® 5.1 (for Intel Itanium) or later.

*3: Version-independent abbreviation

*4: description in the form of "RHEL5.x (IPF)" indicates an updated version.

Text Conventions

This manual uses the following symbols to express specific types of information:

Fonts/symbols	Meaning	Example
Italic	Indicates names of manuals.	See the *PRIMEQUEST 510A System Design Guide.*
" "	Indicates names of chapters, sections, items, buttons, or menus.	See Chapter 5, "System Maintenance.
[]	Indicates window names, window button names, tab names, and dropdown menu selections.	Click the [OK] button.

Syntax of the Command Line Interface (CLI)

The command syntax is described below.

Command syntax

The command syntax is as follows:

- A variable that requires input of a value must be enclosed in < >.
- An optional element must be enclosed in [ ].
- A group of options for an optional keyword must be enclosed in [ ] and delimited by |.
- A group of options for a mandatory keyword must be enclosed in { } and delimited by |.

```
The command syntax is shown in a frame such as this one.
```

Notes Regarding Notations Used in This Manual

- Items marked with "Linux" apply to both Red Hat® Enterprise Linux® AS (v.4 for Itanium), Red Hat® Enterprise Linux® 5 (for Intel Itanium) SUSE™ Linux Enterprise Server 9 for Itanium Processor Family and SUSE™ Linux Enterprise Server 10 for Itanium Processor Family (*).
  *: For details, contact a Fujitsu certified service engineer.
- The IO Unit is indicated as "IOU" in the MMB Web-UI and in the figures shown in this manual.

Conventions for Alert Messages

This manual uses the following conventions to show alert messages. An alert message consists of an alert signal and alert statements.

WARNING	This indicates a hazardous situation that could result in serious personal injury if the user does not perform the procedure correctly.
CAUTION	This indicates a hazardous situation that could result in minor or moderate personal injury if the user does not perform the procedure correctly. This signal also indicates that damage to the product or other property may occur if the user does not perform the procedure correctly.
IMPORTANT	This indicates information that could help the user to use the product more effectively.

Alert messages in the text

In the text, alert messages are indented to distinguish then from regular text. A wider space precedes and follows the message to show where the message begins and ends.

⚠WARNING

Certain tasks in this manual should only be performed by a certified service engineer. Users must not perform these tasks. Incorrect operation of these tasks may cause electric shock, injury, or fire.

- Installation and reinstallation of all components, and initial settings
- Removal of front or top covers
- Mounting/de-mounting of optional internal devices

The important alert messages are listed in the "Important Alert Messages" table in the section titled, "NOTE ON SAFETY" after "Preface."

Environmental Requirements for Using This Product

This product is a computer which is intended to be used in a computer room. For details on the operational environment, see the *PRIMEQUEST 510A Installation Planning Manual* (C122-H003EN).

Reader Feedback

- The screen images in this manual may be different from the actual screen images.
- If you find any errors or unclear statements in this manual, please fill in the "Reader's Comment Form" sheet at the back of this manual and forward it to the address indicated at the bottom of the sheet.
- This manual is subject to revision without prior notice.
- The PDF version of this manual is best viewed in Adobe® Reader® with a magnification of 100% and Single Page for the page layout.

NOTE ON SAFETY

Important Alert Messages

This manual provides the following important alert signals:

⚠ CAUTION

This indicates a hazardous situation that could result in minor or moderate personal injury if the user does not perform the procedure correctly. This signal also indicates that damage to the product or other property may occur if the user does not perform the procedure correctly.

Task	Warning	Page
Normal operation	**Malfunction** The MMB Web-UI supports the Web browsers listed below. Note that other browsers may not display Web-UI windows correctly. ● Microsoft® Internet Explorer (IE) v5.5 (SP2) and later ● Netscape v7.02 and later	P.2-1
	Data destruction When power to the main processing unit is turned off in an operation from the MMB, only the front MMB Ready is lit: Before turning off the main power (UPS, power distribution box, circuit breaker switches, etc.), be sure to confirm that all LEDs other than the front MMB Ready are off. Otherwise, turning off the main power may cause damage to data.	P.3-4
	Data destruction Before shutting down power, make sure the following events have occurred; otherwise, data may be destroyed: ● All applications have completed processing. ● No user is using a component. The Power LED on the operator panel is turned off when the main unit is turned off. Before shutting down main power (to the UPS, power distribution box, and circuit breakers), make sure that the LED is off. If necessary, back up files before shutting down the power.	P.3-6

Task	Warning	Page
Normal operation	**Malfunction** Before any of the following operations is performed, [Disable] must be set for the Boot Watchdog in the [Watchdog] window of PSA. ● Booting from a CD-ROM disk ● Booting the system in single-user mode (Linux) ● Booting the system in the safe mode (Windows) ● Backing up or restoring data by using SystemcastWizard If any of the above operations is performed with [Enable] set for the Boot Watchdog, OS restart is attempted repeatedly for the specified number of times. The system then takes the specified action (Stop rebooting and Power Off, Stop rebooting, or Diagnostic interrupt assert). The number of retries of the OS restart and the actions to be taken can be set in the [ASR Control] window for the MMB-UI. In the [ASR Control] window, check [Cancel Boot Watchdog], and click the [Apply] button. [Disable] can thus be forcibly set for the Boot Watchdog. For details about the [Watchdog] window of PSA, see Section 7.15.1, "[Watchdog] window," in Part IV, "PSA."	P.3-12 P.5-64
	Guarantee of operation Do not use this field. Doing so may lead to a malfunction and result in data corruption or a device failure.	P.5-47
	Guarantee of operation Fujitsu certified service engineers use the [Maintenance Wizard] window for maintenance. Customers should not use this window. Doing so may cause a failure.	P.5-135
	Mis-operation If the browser update button and the frame update function in the contextual menu are used in the PSA setting window that is displayed when settings are completed, settings may be made by simply confirming the previously made settings. Note that, in this case, the settings are made without displaying the corresponding confirmation dialog box. Note also that a window with the new settings is displayed when the settings have been made. However, to confirm that all settings are correct, Fujitsu recommends displaying the window again using the Refresh button. If no Refresh button is available, the window should be opened again by selecting the corresponding menu once again.	P.7-2

Task	Warning	Page
Normal operation	**Malfunction** Before any of the following operations is performed, [Disable] must be set for the Boot Watchdog. ● Booting from a CD-ROM disk ● Booting the system in single-user mode (Linux) ● Booting the system in safe mode (Windows) ● Backing up or restoring data by using SystemcastWizard If any of the above operations is performed with [Enable] set for the Boot Watchdog, OS restart is attempted repeatedly for the specified number of times. The system then takes the specified action (Stop rebooting and Power Off, Stop rebooting, or Diagnostic interrupt assert). The number of retries of the OS restart and the actions to be taken can be set in the [ASR Control] window for the MMB-UI. In the [ASR Control] window, check [Cancel Boot Watchdog], and click the [Apply] button. [Disable] can thus be forcibly set for the Boot Watchdog. For details about the [ASR (Automatic Server Restart) Control] window of MMB, see Section 5.2.17, "[ASR (Automatic Server Restart) Control] window," in Part III, "MMB." ● If 0 is specified for the value of Number-of-Restart-Tries in the [ASR (Automatic Server Restart) Control] window of the MMB, the specified action is not executed even after a lapse of the time at which a timeout should occur. Do not specify 0 for the value when you enable watchdog monitoring. For details of the [ASR (Automatic Server Restart) Control] window of the MMB, see Section 5.2.17, "[ASR (Automatic Server Restart) Control] window" in Part III, "MMB."	P.7-60

Product Handling

Maintenance

WARNING

Certain tasks in this manual should only be performed by a certified service engineer. Users must not perform these tasks. Incorrect operation of these tasks may cause electric shock, injury, or fire.

- Installation and reinstallation of all components, and initial settings
- Removal of front or top covers
- Mounting/de-mounting of optional internal devices
- Plugging or unplugging of external interface cards
- Maintenance and inspections (repairing, and regular diagnosis and maintenance)

CAUTION

The following tasks regarding this product and the optional products provided from Fujitsu should only be performed by a certified service engineer. Users must not perform these tasks. Incorrect operation of these tasks may cause malfunction.

- Unpacking optional adapters and such packages delivered to the users

Remodeling/Rebuilding

CAUTION

Do not make mechanical or electrical modifications to the equipment.
Using this product after modifying or overhauling may cause unexpected injury or damage to the property, the user, or bystanders.

Contents

Preface i
Structure and Contents of This Manual i
Other Reference Manuals iii
Abbreviations iv
Text Conventions iv
Syntax of the Command Line Interface (CLI) v
Notes Regarding Notations Used in This Manual v
Conventions for Alert Messages v
Environmental Requirements for Using This Product vi

NOTE ON SAFETY vii
Important Alert Messages vii

Product Handling xi
Maintenance xi
Remodeling/Rebuilding xi

Part I Basics

CHAPTER 1 Structure of This manual and How to Read It 1-1
1.1 Conventions Used in This Manual 1-2
1.2 Correspondence between Windows and Parts of This Manual 1-4

CHAPTER 2 Overview of the Web-UI 2-1
2.1 Web-UI Windows 2-1
2.2 Frame Configuration 2-3
2.3 Information Frame 2-4
2.4 Submenu Frame 2-6
2.5 Content Display Frame 2-7
2.6 Basic Operations in Web-UI Windows 2-9
2.7 User Privilege Levels 2-13
2.8 Switching to Operations with Software of Another Type 2-14

CHAPTER 3 Starting and Stopping the System 3-1
3.1 Component Names and Functions 3-1
3.2 Turning On and Turning Off the Main Power 3-3
3.2.1 Power-on procedure 3-3
3.2.2 Power-off procedure 3-4
3.3 Power Management Using MMB Web-UI 3-5

3.3.1 Power-on/power-off procedure using MMB Web-UI 3-5
3.3.2 Checking the power status and system status 3-8
3.3.3 Boot control 3-10
3.3.4 Power-on and power-off by scheduled operation 3-11
3.3.5 Setting for Automatic Restart 3-12
3.4 Power Management Using Command line interface (CLI) 3-15
3.5 Checking the System Power Status 3-17
3.6 Remote Shutdown 3-19
3.6.1 Remote shutdown of Windows 3-19
3.6.1.1 Remote shutdown via a LAN connection 3-20
3.6.1.2 Remote shutdown via a COM port connection 3-27
3.7 Checking Status with LEDs 3-31
3.8 UPS Operation. 3-32
3.8.1 UPS connections 3-32
3.8.2 Settings for UPS connections 3-34

Part II PRIMEQUEST Functions

CHAPTER 4 Overview of PRIMEQUEST Functions. 4-1

4.1 List of the Functions 4-1
4.2 MMB functions 4-6
4.3 Setting and Checking Log Information 4-10
4.3.1 Log information types 4-10
4.3.2 Checking a log of events that occurred in the PRIMEQUEST system. 4-10
4.3.2.1 Checking event logs 4-11
4.3.2.2 Clearing all events that are saved in the SEL 4-13
4.3.2.3 Downloading event data that is saved in the SEL 4-13
4.3.2.4 Filtering an event to be displayed 4-14
4.3.2.5 Displaying event details 4-16
4.4 Console Operation 4-18
4.4.1 Overview of console redirection 4-18
4.4.2 MMB settings of console redirection switch 4-19
4.4.3 Telnet/SSH user procedure 4-21
4.4.4 Buffering of console redirection 4-21
4.4.5 Console redirection to Web-UI 4-22
4.5 PSA Functions 4-25
4.5.1 Information managed by PSA 4-30
4.6 Collecting PSA Troubleshooting Information 4-31

Part III MMB

CHAPTER 5 Web-UI Operations 5-1

5.1 List of Menus in the Web-UI Window 5-1
5.1.1 List of menus for the PRIMEQUEST 510A 5-1
5.2 System Menu 5-5
5.2.1 [System Status] window 5-5
5.2.2 [System Event Log] window 5-7
5.2.2.1 [System Event Log Filtering Condition] window 5-10
5.2.2.2 [System Event Log (Detail)] window 5-13
5.2.3 [System Information] window 5-15
5.2.4 [Firmware Information] window 5-18
5.2.5 [System Setup] window 5-19
5.2.6 [LEDs] window 5-22
5.2.7 [Power Supply] window 5-23
5.2.8 [Fans] window 5-25
5.2.8.1 [Fans Status Clear] window 5-27
5.2.9 [Temperature] window 5-29
5.2.10 [BB] window 5-30
5.2.11 [BB Status Clear] window 5-38
5.2.12 [SASBP] window 5-45
5.2.13 [MMB] window 5-46
5.2.14 [Power Control] window 5-48
5.2.15 Schedule menu 5-52
5.2.15.1 [Schedule Control] window 5-52
5.2.15.2 [Schedule List] window 5-53
5.2.16 [Console Redirection] menu 5-60
5.2.16.1 [Console Redirection Switch] window 5-60
5.2.16.2 [Console Redirection] window 5-62
5.2.17 [ASR (Automatic Server Restart) Control] window 5-64
5.3 User Administration Menu 5-68
5.3.1 [User List] window 5-68
5.3.1.1 [Add User] window 5-70
5.3.1.2 [Edit User] window 5-73
5.3.2 [Change Password] window 5-75
5.3.3 [Who] window 5-77
5.4 Network Configuration Menu 5-78
5.4.1 [Date/Time] window 5-78
5.4.2 [Network Interface] window 5-81
5.4.3 [Management LAN Port Configuration] window 5-84
5.4.3.1 Setting the connection of management LAN hub 5-86

5.4.4 [Network Protocols] window 5-89
5.4.5 [Refresh Rate] window 5-92
5.4.6 SNMP Configuration menu 5-93
5.4.6.1 [SNMP Community] window 5-94
5.4.6.2 [SNMP Trap] window 5-97
5.4.6.3 [SNMP v3 Configuration] window 5-99
5.4.7 SSL menu 5-101
5.4.7.1 [Create CSR] window 5-101
5.4.7.2 [Export Key/CSR] window 5-104
5.4.7.3 [Import Certificate] window 5-105
5.4.7.4 [Create Selfsigned Certificate] window 5-106
5.4.8 SSH menu 5-108
5.4.8.1 [Create SSH Server Key] window 5-108
5.4.9 [Remote Server Management] window 5-110
5.4.9.1 [Edit User] window 5-112
5.4.10 [Access Control] window 5-114
5.4.10.1 [Add Filter] window/[Edit Filter] window 5-116
5.4.11 [Alarm E-Mail] window 5-118
5.4.11.1 [Alarm E-Mail Filtering Condition] window 5-120
5.5 Maintenance Menu 5-122
5.5.1 Firmware Update menu 5-122
5.5.1.1 [MMB Firmware Update] window 5-122
5.5.1.2 [PAL/SAL Firmware Update] window 5-125
5.5.1.3 [EFI Firmware Update] window 5-127
5.5.1.4 [BMC Firmware Update] window 5-129
5.5.2 Backup/Restore Configuration menu 5-131
5.5.2.1 [Backup/Restore MMB Configuration] window 5-131
5.5.2.2 [Backup/Restore EFI Configuration] window 5-133
5.5.3 [Maintenance Wizard] window 5-135
5.5.4 REMCS menu 5-135

CHAPTER 6 CLI Operations 6-1

6.1 Basic CLI Operations 6-1
6.1.1 Access through the serial interface 6-1
6.1.2 Access via the management LAN interface 6-2
6.1.3 List of CLI commands 6-2
6.2 Setting Commands 6-5
6.2.1 factory_default 6-6
6.2.2 clear access_control 6-6
6.2.3 clear ssh_key 6-7
6.2.4 power off 6-7
6.2.5 power on 6-8

6.2.6 download ssh_key 6-8
6.2.7 set date 6-9
6.2.8 set timezone 6-9
6.2.9 set gateway 6-12
6.2.10 set http 6-12
6.2.11 set http_port 6-13
6.2.12 set https 6-13
6.2.13 set https_port 6-14
6.2.14 set ssh 6-14
6.2.15 set ssh_port 6-15
6.2.16 set telnet 6-15
6.2.17 set telnet_port 6-16
6.2.18 set ip 6-16
6.2.19 set hostname 6-17
6.2.20 set remcs 6-17
6.3 Display Commands 6-19
6.3.1 show access_control 6-20
6.3.2 show date 6-20
6.3.3 show timezone 6-21
6.3.4 show gateway 6-21
6.3.5 show http 6-22
6.3.6 show http_port 6-22
6.3.7 show https 6-23
6.3.8 show https_port 6-23
6.3.9 show ip 6-24
6.3.10 show hostname 6-24
6.3.11 show ssh 6-25
6.3.12 show ssh_port 6-25
6.3.13 show telnet 6-26
6.3.14 show telnet_port 6-26
6.3.15 show network 6-27
6.3.16 show remcs 6-28
6.3.17 who 6-29
6.3.18 help 6-29
6.4 Update Commands 6-30
6.4.1 update MMB 6-30
6.4.2 update BMC 6-31
6.4.3 update EFI 6-32
6.4.4 update SAL 6-33
6.5 Other Commands 6-35
6.5.1 exit 6-35

6.5.2 passwd 6-36
6.5.3 ping 6-37

Part IV PSA

CHAPTER 7 Web-UI Operations 7-1

7.1 List of Menus in the Web-UI Window 7-3
7.2 [OS Information] Window 7-5
7.3 [CPUs] Window 7-7
7.4 [DIMMs] Window 7-8
7.5 [PCI Devices] Window 7-9
7.5.1 [Ethernet Controller] window 7-11
7.5.2 [Storage Controller] window 7-16
7.5.3 [Fibre Channel] window 7-21
7.5.4 [PCI Device] window 7-26
7.6 Network Menu 7-28
7.6.1 [Network Interfaces] window 7-28
7.6.2 [Network Routing] window 7-30
7.7 [Disk Partitions] Window 7-31
7.8 [Hard Disks] Window 7-32
7.9 [Process List] Window 7-34
7.10 [System File] (Selection) Window 7-38
7.10.1 [System File] (display) window 7-40
7.11 Inventory Menu 7-41
7.11.1 [Hardware Inventory] window 7-41
7.11.2 [Software Inventory] window 7-43
7.11.2.1 [Software Inventory -Detail-] window 7-45
7.12 [Agent Log] Window 7-47
7.12.1 [Agent Log Filtering Condition] window 7-50
7.13 [SEL] Window 7-53
7.14 [Export List] Window 7-54
7.14.1 [Export] window 7-57
7.15 Setup Menu 7-59
7.15.1 [Watchdog] window 7-59
7.15.2 [S.M.A.R.T.] window 7-64
7.16 [Expansion File Unit] Window 7-67
7.16.1 [SDU#x] window 7-68

CHAPTER 8 CLI Operations. 8-1

8.1 Basic CLI Operations 8-1
8.1.1 List of CLI commands 8-1

8.2 SAF-TE Operation Command (diskctrl) 8-3
8.3 PSA Start/Stop Command (y30FJSVpsa) 8-9
8.4 PSA Troubleshooting Data Collection Command (getopsa) 8-11
8.5 Filter Definition Update Commands (fltcpy, fltupdate) 8-13
8.6 Get Local Partition Number Command (getpartid) 8-18
8.7 Get Serial Number Command (getserialno) 8-20
8.8 SNMP Security Setting Command (setsnmpsec) 8-22
8.9 SAL/EFI Firmware Update Command (fjfwupdate) 8-23
8.10 Firmware Update Setup Command (fjfwup_setup) 8-41
8.11 Get Firmware Information Command (getfwinfo) 8-43

Part V EFI

CHAPTER 9 EFI Overview. 9-1

9.1 Boot Function 9-2
9.1.1 NVRAM variables for boot control 9-2
9.1.2 Boot processing order 9-3
9.1.3 Controlling auto-boot processing 9-4

CHAPTER 10 Boot Manager 10-1

10.1 Starting Boot Manager 10-1
10.2 Boot Manager Menu 10-2
10.3 Boot Option Maintenance Menu 10-4
10.3.1 [Boot From a File] window 10-5
10.3.2 [Add a Boot Option] window 10-6
10.3.3 [Delete Boot Option(s)] window 10-9
10.3.4 [Change Boot Order] window 10-11
10.3.5 [Set Auto Boot Timeout] window 10-13
10.3.6 Reset System 10-14
10.3.7 Exit 10-14
10.4 EFI Setup Menu 10-15
10.4.1 [EFI Configuration Utility] window 10-16
10.4.2 [Keyboard] window 10-17

CHAPTER 11 EFI Shell and EFI Commands 11-1

11.1 Auto-startup File 11-1
11.2 EFI Shell Command Syntax 11-2
11.3 Output Redirection 11-3
11.4 Batch Script 11-4

Glossary **GL-1**

Index **IN-1**

Figures

Figure 1.1 Software covered in this manual 1-1
Figure 1.2 Window and its corresponding section in this manual 1-4
Figure 2.1 Frame configuration 2-3
Figure 2.2 Information frame 2-4
Figure 2.3 Maintenance status 2-5
Figure 2.4 Submenu frame 2-6
Figure 2.5 Content display frame 2-7
Figure 2.6 Switching with Web-UI operations 2-14
Figure 3.1 PRIMEQUEST 510A 3-1
Figure 3.2 General configuration of the PRIMEQUEST 510A 3-2
Figure 3.3 ACS location 3-3
Figure 3.4 [Power Control] window 3-5
Figure 3.5 [Power Control] window 3-6
Figure 3.6 [Power Control] window 3-8
Figure 3.7 [Power Control] window 3-10
Figure 3.8 [ASR Control] window 3-12
Figure 3.9 [Power Supply] window 3-17
Figure 3.10 Execution of the Shutdown command 3-21
Figure 3.11 System Property sheet 3-22
Figure 3.12 [Computer Name Setting] dialog box 3-23
Figure 3.13 [Property] sheet 3-24
Figure 3.14 Example of entering the server name or IP address 3-25
Figure 3.15 Shutdown.exe command 3-26
Figure 3.16 Bootcfg.exe 3-28
Figure 3.17 Selecting an icon 3-29
Figure 3.18 Selecting the COM port and setting the baud rate 3-29
Figure 3.19 Concept of UPS connections 3-33
Figure 3.20 [System Setup] window 3-34
Figure 4.1 MMB main functions 4-6
Figure 4.2 [System Event Log] window 4-11
Figure 4.3 [System Event Log Filtering Condition] window 4-14
Figure 4.4 [System Event Log (Detail)] window 4-16
Figure 4.5 Concept of console redirection 4-18
Figure 4.6 [Console Redirection Switch] window 4-19
Figure 4.7 [Console Redirection] window (console output window) 4-23
Figure 4.8 [Console Redirection] window (when the output destination is set to the COM port) 4-24
Figure 4.9 Major PSA functions 4-25
Figure 5.1 [System Status] window 5-5

Figure 5.2 [System Event Log] window 5-7
Figure 5.3 [System Event Log Filtering Condition] window 5-10
Figure 5.4 [System Event Log (Detail)] window 5-13
Figure 5.5 [System Information] window 5-15
Figure 5.6 [Firmware Information] window 5-18
Figure 5.7 [System Setup] window 5-19
Figure 5.8 [LEDs] window 5-22
Figure 5.9 [Power Supply] window 5-23
Figure 5.10 [Fans] window 5-25
Figure 5.11 [Fans Status Clear] window 5-27
Figure 5.12 [Temperature] window 5-29
Figure 5.13 [BB] window (1/2) 5-30
Figure 5.13 [BB] window (2/2) 5-31
Figure 5.14 [BB Status Clear] window (1/2) 5-38
Figure 5.14 [BB Status Clear] window (2/2) 5-39
Figure 5.15 [SASBP] window 5-45
Figure 5.16 [MMB] window 5-46
Figure 5.17 [Power Control] window 5-48
Figure 5.18 [Schedule Control] window 5-52
Figure 5.19 [Schedule List] window 5-53
Figure 5.20 [Add Schedule] window 5-56
Figure 5.21 [Edit Schedule] window 5-58
Figure 5.22 [Console Redirection Switch] window 5-60
Figure 5.23 [Console Redirection-1] window 5-62
Figure 5.24 [Console Redirection-2] window 5-63
Figure 5.25 [ASR (Automatic Server Restart) Control] window 5-64
Figure 5.26 [User List] window 5-68
Figure 5.27 [Add User] window 5-70
Figure 5.28 [Edit User] window 5-73
Figure 5.29 [Change Password] window 5-75
Figure 5.30 [Who] window 5-77
Figure 5.31 [Date/Time] window 5-79
Figure 5.32 [Network Interface] window 5-82
Figure 5.33 [Management LAN Port Configuration] window 5-84
Figure 5.34 [Network Protocols] window 5-89
Figure 5.35 [Refresh Rate] window 5-92
Figure 5.36 [SNMP Community] window 5-94
Figure 5.37 [SNMP Trap] window 5-97
Figure 5.38 [SNMP v3 Configuration] window 5-99
Figure 5.39 [Create CSR] window 5-101
Figure 5.40 Create CSR (In Progress) indicator 5-102

Figure 5.41 [Export Key/CSR] window 5-104
Figure 5.42 [Import Certificate] window 5-105
Figure 5.43 [Create Selfsigned Certificate] window 5-106
Figure 5.44 [Create SSH Server Key] window 5-108
Figure 5.45 Create SSH Server Key (In Progress) indicator 5-108
Figure 5.46 [Remote Server Management] window 5-110
Figure 5.47 [Edit User] window 5-112
Figure 5.48 [Access Control] window 5-114
Figure 5.49 [Edit Filter] window 5-116
Figure 5.50 [Alarm E-Mail] window 5-118
Figure 5.51 [Alarm E-Mail Filtering Condition] window 5-120
Figure 5.52 [MMB Firmware Update] window (selection) 5-122
Figure 5.53 [PAL/SAL Firmware Update] window (selection) 5-125
Figure 5.54 [EFI Firmware Update] window 5-127
Figure 5.55 [BMC Firmware Update] window 5-129
Figure 5.56 [Backup/Restore MMB Configuration] window 5-131
Figure 5.57 [Backup/Restore EFI Configuration] window 5-133
Figure 5.58 [Maintenance Wizard] window 5-135
Figure 7.1 [OS Information] window (Linux) 7-5
Figure 7.2 [OS Information] window (Windows) 7-5
Figure 7.3 [CPUs] window 7-7
Figure 7.4 [DIMMs] window 7-8
Figure 7.5 [PCI Devices] window 7-9
Figure 7.6 [Ethernet Controller] window 7-11
Figure 7.7 [Storage controller] window 7-16
Figure 7.8 Fibre Channel window 7-21
Figure 7.9 [PCI Device] window 7-26
Figure 7.10 [Network Interfaces] window 7-28
Figure 7.11 [Network Routing] window 7-30
Figure 7.12 [Disk Partitions] window 7-31
Figure 7.13 [Hard Disks] window 7-32
Figure 7.14 [Process List] window 7-34
Figure 7.15 [System File] (selection) window 7-38
Figure 7.16 [System File] (selection) Error window 7-39
Figure 7.17 [System File] (display) window 7-40
Figure 7.18 [Hardware Inventory] window 7-41
Figure 7.19 [Software Inventory] window 7-43
Figure 7.20 [Software Inventory -Detail-] window 7-45
Figure 7.21 [Agent Log] window 7-47
Figure 7.22 [Agent Log Filtering Condition] window 7-50
Figure 7.23 [SEL] window 7-53

Figure 7.24 [Export List] window 7-54
Figure 7.25 [Export] window 7-57
Figure 7.26 [Watchdog] window 7-60
Figure 7.27 [S.M.A.R.T.] window 7-65
Figure 7.28 [Expansion File Unit] window 7-67
Figure 7.29 [SDU#x] window 7-68
Figure 9.1 EFI outline 9-1
Figure 10.1 Example of the displayed [Boot Manager Menu] window 10-2
Figure 10.2 Example of the displayed [Boot Option Maintenance Menu (Main Menu)] window. 10-4
Figure 10.3 Example of the displayed [Boot From a File] window 10-5
Figure 10.4 Example of the displayed [Add a Boot Option] window 10-6
Figure 10.5 Sample boot file (elilo.conf) 10-7
Figure 10.6 Boot option setting example 10-8
Figure 10.7 Boot Manager menu as it is displayed after a boot option is added 10-8
Figure 10.8 Example of the displayed [Delete Boot Option(s)] window 10-9
Figure 10.9 Example of the displayed [Change Boot Order] window. 10-11
Figure 10.10 Example of the displayed [Set Auto Boot Timeout] window 10-13
Figure 10.11 EFI Setup Menu as it is displayed immediately after startup 10-15
Figure 10.12 Example of the displayed [EFI Configuration Utility] window 10-16
Figure 10.13 Example of the displayed [Keyboard] window 10-17

Tables

Table 2.1 User privilege levels 2-13
Table 3.1 Displayed and setting items in the [Power Control] window. 3-7
Table 3.2 Displayed and setting items in the [Power Control] window. 3-9
Table 3.3 Displayed and setting items in the [Power Control] window. 3-11
Table 3.4 Displayed and setting items in the [ASR Control] window 3-13
Table 3.5 Terminal software setting 3-15
Table 3.6 Displayed and setting items in the [Power Supply] window 3-18
Table 3.7 Shutdown methods 3-20
Table 3.8 Displayed and setting items in the [System Setup] window 3-35
Table 4.1 Functions provided by MMB Web-UI (system) 4-1
Table 4.2 Functions provided by MMB Web-UI (user) 4-3
Table 4.3 Functions provided by MMB Web-UI (network/security) 4-4
Table 4.4 Functions provided by MMB Web-UI (maintenance). 4-5
Table 4.5 Displayed and setting items in the [System Event Log] window 4-12
Table 4.6 Displayed and setting items in the [System Event Log Filtering Condition] window 4-15
Table 4.7 Displayed and setting items in the [System Event Log (Detail)] window 4-17
Table 4.8 Displayed and setting items in the [Console Redirection Switch] window 4-20
Table 4.9 Log files 4-28
Table 4.10 Information managed by PSA 4-30
Table 5.1 Menus (PRIMEQUEST 510A) 5-1
Table 5.2 Displayed items in the [System Status] window 5-6
Table 5.3 Displayed items in the [System Event Log] window 5-8
Table 5.4 Buttons in the [System Event Log] window 5-8
Table 5.5 Displayed and setting items in the [System Event Log Filtering Condition] window 5-11
Table 5.6 Buttons in the [System Event Log Filtering Condition] window. 5-12
Table 5.7 Displayed items in the [System Event Log (Detail)] window. 5-13
Table 5.8 Buttons in the [System Event Log (Detail)] window. 5-14
Table 5.9 Displayed and setting items in the [System Information] window. 5-16
Table 5.10 Buttons in the [System Information] window 5-17
Table 5.11 Displayed items in the [Firmware Information] window. 5-18

Table 5.12 Displayed and setting items in the [System Setup] window 5-19
Table 5.13 Buttons in the [System Setup] window. 5-21
Table 5.14 Displayed and setting items in the [LEDs] window 5-22
Table 5.15 Displayed items in the [Power Supply] window 5-24
Table 5.16 Displayed items in the [Fans] window 5-25
Table 5.17 Button in the [Fans] window. 5-26
Table 5.18 Displayed and setting items in the [Fans Status Clear] window 5-27
Table 5.19 Buttons in the [Fans Status Clear] window 5-28
Table 5.20 Displayed items in the [Temperature] window 5-29
Table 5.21 Displayed and setting items in the [BB] window 5-32
Table 5.22 Button in the [BB] window 5-37
Table 5.23 Displayed and setting items in the [BB Status Clear] window 5-40
Table 5.24 Buttons in the [BB Status Clear] window 5-44
Table 5.25 Displayed and setting items in the [SASBP] window 5-45
Table 5.26 Displayed and setting items in the [MMB] window. 5-46
Table 5.27 Buttons in the [MMB] window. 5-47
Table 5.28 Displayed and setting items in the [Power Control] window 5-49
Table 5.29 Buttons in the [Power Control] window 5-51
Table 5.30 Displayed and setting items in the [Schedule Control] window 5-52
Table 5.31 Buttons in the [Schedule Control] window 5-52
Table 5.32 Displayed and setting items in the [Schedule List] window 5-54
Table 5.33 Buttons in the [Schedule List] window 5-54
Table 5.34 Displayed and setting items in the [Add Schedule] window 5-56
Table 5.35 Buttons in the [Add Schedule] window. 5-57
Table 5.36 Displayed and setting items in the [Edit Schedule] window 5-58
Table 5.37 Buttons in the [Edit Schedule] window. 5-59
Table 5.38 Displayed and setting items in the [Console Redirection Switch] window 5-60
Table 5.39 Buttons in the [Console Redirection Switch] window. 5-61
Table 5.40 Displayed and setting items in the [ASR (Automatic Server Restart) Control] window 5-65
Table 5.41 Buttons in the [ASR (Automatic Server Restart) Control] window 5-66
Table 5.42 Displayed and setting items in the [User List] window. 5-68
Table 5.43 Buttons in the [User List] window. 5-69
Table 5.44 Displayed and setting items in the [Add User] window 5-70
Table 5.45 User privilege levels and operation restrictions 5-71
Table 5.46 Buttons in the [Add User] window 5-72
Table 5.47 Displayed and setting items in the [Edit User] window 5-73
Table 5.48 User privilege levels and operation restrictions 5-74
Table 5.49 Buttons in the [Edit User] window 5-75

Table 5.50 Displayed and setting items in the [Change Password] window 5-76
Table 5.51 Buttons in the [Change Password] window 5-76
Table 5.52 Displayed items in the [Who] window 5-77
Table 5.53 Displayed and setting items in the [Date/Time] window 5-79
Table 5.54 Buttons in the [Date/Time] window 5-80
Table 5.55 Displayed and setting items in the [Network Interface] window 5-82
Table 5.56 Buttons in the [Network Interface] window 5-83
Table 5.57 Displayed and setting items in the [Management LAN Port Configuration] window. 5-85
Table 5.58 Buttons in the [Management LAN Port Configuration] window. 5-85
Table 5.59 Connection mode (when the check box is cleared). 5-87
Table 5.60 Disconnection mode (when the check box is selected) 5-88
Table 5.61 Displayed and setting items in the [Network Protocols] window 5-89
Table 5.62 Buttons in the [Network Protocols] window 5-91
Table 5.63 Displayed or setting item in the [Refresh Rate] window 5-92
Table 5.64 Buttons in the [Refresh Rate] window 5-92
Table 5.65 Displayed and setting items in the [SNMP Community] window 5-95
Table 5.66 Buttons in the [SNMP Community] window 5-96
Table 5.67 Displayed and setting items in the [SNMP Trap] window. 5-97
Table 5.68 Buttons in the [SNMP Trap] window 5-98
Table 5.69 Displayed and setting items in the [SNMP v3 Configuration] window 5-99
Table 5.70 Buttons in the [SNMP v3 Configuration] window 5-100
Table 5.71 Displayed and setting items in the [Create CSR] window 5-102
Table 5.72 Buttons in the [Create CSR] window 5-103
Table 5.73 Buttons in the [Export Key/CSR] window 5-104
Table 5.74 Buttons in the [Import Certificate] window 5-105
Table 5.75 Displayed and setting items in the [Create Selfsigned Certificate] window 5-106
Table 5.76 Buttons in the [Create Selfsigned Certificate] window. 5-107
Table 5.77 Displayed item in the [Create SSH Server Key] window 5-109
Table 5.78 Button in the [Create SSH Server Key] window 5-109
Table 5.79 Displayed and setting items in the [Remote Server Management] window 5-111
Table 5.80 Buttons in the [Remote Server Management] window 5-111
Table 5.81 Displayed and setting items in the [Edit User] window 5-112
Table 5.82 Buttons in the [Edit User] window 5-113
Table 5.83 Displayed and setting items in the [Access Control] window 5-114
Table 5.84 Buttons in the [Access Control] window 5-115

Table 5.85 Displayed and setting items in the [Edit Filter] window 5-117
Table 5.86 Buttons in the [Edit Filter] window 5-117
Table 5.87 Displayed and setting items in the [Alarm E-Mail] window 5-118
Table 5.88 Buttons in the [Alarm E-Mail] window 5-118
Table 5.89 Displayed and setting items in the [Alarm E-Mail Filtering Condition] window 5-120
Table 5.90 Buttons in the [Alarm E-Mail Filtering Condition] window 5-121
Table 5.91 Displayed and setting items in the [MMB Firmware Update] window 5-123
Table 5.92 Buttons in the [MMB Firmware Update] window 5-123
Table 5.93 Displayed and setting items in the [PAL/SAL Firmware Update] window (selection) 5-125
Table 5.94 Buttons in the [PAL/SAL Firmware Update] window 5-125
Table 5.95 Displayed and setting items in the [EFI Firmware Update] window 5-127
Table 5.96 Buttons in the [EFI Firmware Update] window 5-127
Table 5.97 Displayed and setting items in the [BMC Firmware Update] window 5-129
Table 5.98 Buttons in the [BMC Firmware Update] window 5-129
Table 5.99 Buttons in the [Backup/Restore MMB Configuration] window 5-132
Table 5.100 Buttons in the [Backup/Restore EFI Configuration] window 5-133
Table 5.101 Buttons in the [Maintenance Wizard] window 5-135
Table 6.1 Setting items of terminal software 6-1
Table 6.2 CLI commands 6-2
Table 6.3 Time zone settings 6-10
Table 7.1 Component status and background colors 7-1
Table 7.2 Menus 7-3
Table 7.3 Displayed items in the [OS Information] window 7-6
Table 7.4 Displayed items in the [CPUs] window 7-7
Table 7.5 Displayed items in the [DIMMs] window 7-8
Table 7.6 Displayed items in the [PCI Devices] window 7-10
Table 7.7 Buttons in the [PCI Devices] window 7-10
Table 7.8 Displayed and setting items in the [Ethernet Controller] window 7-12
Table 7.9 Buttons in the [Ethernet Controller] window 7-14
Table 7.10 Displayed and setting items in the [Storage Controller] window 7-17
Table 7.11 Buttons in the [Storage Controller] window 7-19
Table 7.12 Display and setting items of [Fibre Channel] window 7-22
Table 7.13 Buttons in [Fibre Channel] window 7-24
Table 7.14 Displayed and setting items in the [PCI Device] window 7-26
Table 7.15 Buttons in the [PCI Device] window 7-27
Table 7.16 Displayed items in the [Network Interfaces] window 7-29

Table 7.17 Displayed items in the [Network Routing] window 7-30
Table 7.18 Displayed items in the [Disk Partitions] window 7-31
Table 7.19 Display items of [Hard Disks] window 7-33
Table 7.20 Displayed and setting items in the [Process List] window 7-35
Table 7.21 Buttons in the [Process List] window 7-36
Table 7.22 Displayed item in the [System File] (selection) window 7-38
Table 7.23 Buttons in the [System File] (selection) window 7-39
Table 7.24 Error messages 7-39
Table 7.25 Button in the [System File] (display) window 7-40
Table 7.26 Displayed items in the [Hardware Inventory] window 7-41
Table 7.27 Displayed items in the [Software Inventory] window 7-44
Table 7.28 Buttons in the [Software Inventory] window. 7-44
Table 7.29 Displayed items in the [Software Inventory -Detail-] window. 7-45
Table 7.30 Button in [Software Inventory -Detail-] window 7-46
Table 7.31 Displayed and setting items in the [Agent Log] window. 7-48
Table 7.32 Buttons in the [Agent Log] window 7-49
Table 7.33 Displayed and setting items in the [Agent Log Filtering Condition] window 7-50
Table 7.34 Buttons in the [Agent Log Filtering Condition] window 7-52
Table 7.35 Buttons in the [SEL] window 7-53
Table 7.36 Displayed and setting items in the [Export List] window. 7-55
Table 7.37 Buttons in the [Export List] window 7-55
Table 7.38 Error messages 7-56
Table 7.39 Displayed and setting items in the [Export] window 7-57
Table 7.40 Buttons in the [Export] window 7-57
Table 7.41 Error messages 7-58
Table 7.42 Displayed and settings items in the [Watchdog] window 7-61
Table 7.43 Buttons in the [Watchdog] window 7-62
Table 7.44 Error messages 7-63
Table 7.45 Displayed and settings items in the [S.M.A.R.T.] window 7-65
Table 7.46 Buttons in the [S.M.A.R.T.] window 7-65
Table 7.47 Error messages 7-66
Table 7.48 Display items of [Expansion File Unit] window 7-67
Table 7.49 Buttons of [Expansion File Unit] window 7-68
Table 7.50 Display and setting items of [SDU#x] window 7-69
Table 7.51 Buttons of [SDU#x] window 7-71
Table 8.1 Commands 8-2
Table 8.2 SAF-TE operation command (diskctrl) massages 8-6
Table 8.3 Filter definition update command (fltcpy, fltupdate) messages. 8-16
Table 8.4 Get firmware information command (getfwinfo) messages 8-44

Table 10.1 Display items in the [Boot Manager Menu] window 10-2
Table 10.2 Keys used for Boot Manager operation 10-3
Table 10.3 Outline of functions available in the [Boot Option Maintenance Menu (Main Menu)] window 10-4
Table 10.4 Functions of submenus available in the Delete Boot Option(s) window 10-9
Table 10.5 Keys used for operation on the [Delete Boot Option(s)] window 10-10
Table 10.6 Functions of submenus available in the [Change Boot Order] window. 10-11
Table 10.7 Keys used for operation on the [Change Boot Order] window. 10-11
Table 10.8 Functions of submenus available in the [Set Auto Boot Timeout] window 10-13
Table 10.9 Functions of the EFI Setup Menu 10-15
Table 10.10 Symbols displayed for the [EFI Configuration Utility] window 10-17
Table 10.11 Items displayed in the [Keyboard] window. 10-18
Table 11.1 Wildcards 11-2
Table 11.2 Special strings 11-3

Part I Basics

CHAPTER 1 Structure of This manual and How to Read It

This manual describes operation of software on the PRIMEQUEST-series machine.

Figure 1.1 shows the main types of software running on this server:

- MMB firmware : Part III
- PSA : Part IV
- EFI firmware : Part V

Each part of the manual corresponds to one type of software.

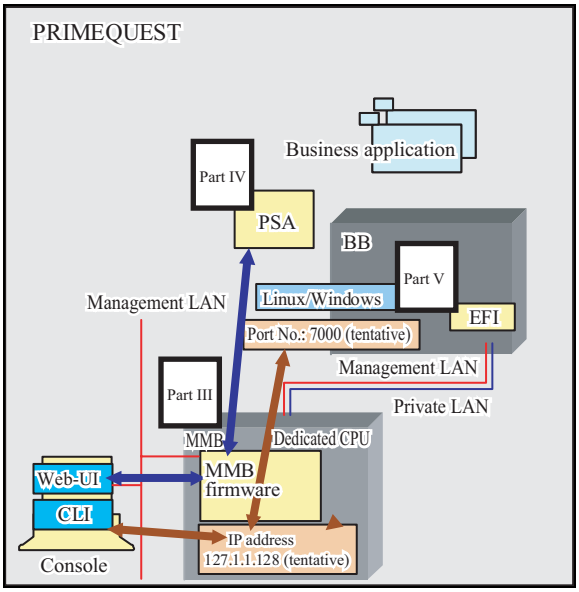


Figure 1.1 Software covered in this manual

1.1 Conventions Used in This Manual

MMB and PSA descriptions in Parts III and IV are organized in sections according to the windows and commands that are described.

This section describes the format of the descriptions in Parts III and IV.

Format of window descriptions

Each Web window description has the following format:

xx window

A window screenshot is provided. For a window whose display varies depending on the Web browser, the window displayed in Microsoft Internet Explorer is shown.

Item	Description
Name of item 1 in the window	Item 1 is described.
Name of item 2 in the window	Item 2 is described.
:	:

Names of displayed items in the window are listed together with their descriptions.

Button	Description
Name of button 1 in window	The function of button 1 is described.
Name of button 2 in window	The function of button 2 is described.
:	:

Names of displayed buttons in the window are listed together with their descriptions.

(1) Menu operation

The menu operating procedure for displaying the window is described.

(2) GUI operation

The operating procedure with the window is described.

Format of command descriptions

Each command description has the following format:

(1) Synopsis

The command syntax is described as follows:

- A variable to which a value must be assigned is enclosed in < >.
- An optional element is enclosed in [ ].
- A selection of optional keywords, which are delimited by |, is enclosed in [ ].
- A selection of required keywords, which are delimited by |, is enclosed in { }.

```
The command syntax is shown in a box.
```

(2) Options

Command options are described.

(3) Examples

Examples of using the command are shown.

```
Example of the command
```

Screen operation notations

Window operations are described as follows in this manual:

- Web UI menu operations
  [ ] → [ ]

  Example: Description of the operating procedure for displaying the [System Status] window
  Click [System] → [System Status]. (Select the items in the order shown.)

- Description of one of multiple components (They are actually represented by a number on the Web-UI.)
  Component-name#x

  Example: Description of a UPS number
  Click [UPC#] in the [Power Supply] window.

1.2 Correspondence between Windows and Parts of This Manual

Descriptions of operation from windows in this manual are based on the menu operations provided by the type of software used. This also applies to command descriptions in the manual.

Most operations of the PRIMEQUEST-series machine are performed from MMB Web-UI windows. Also, PSA Web-UI windows are used from the MMB Web-UI windows.

Figure 1.2 shows an example of the correspondence between windows and parts of the manual.

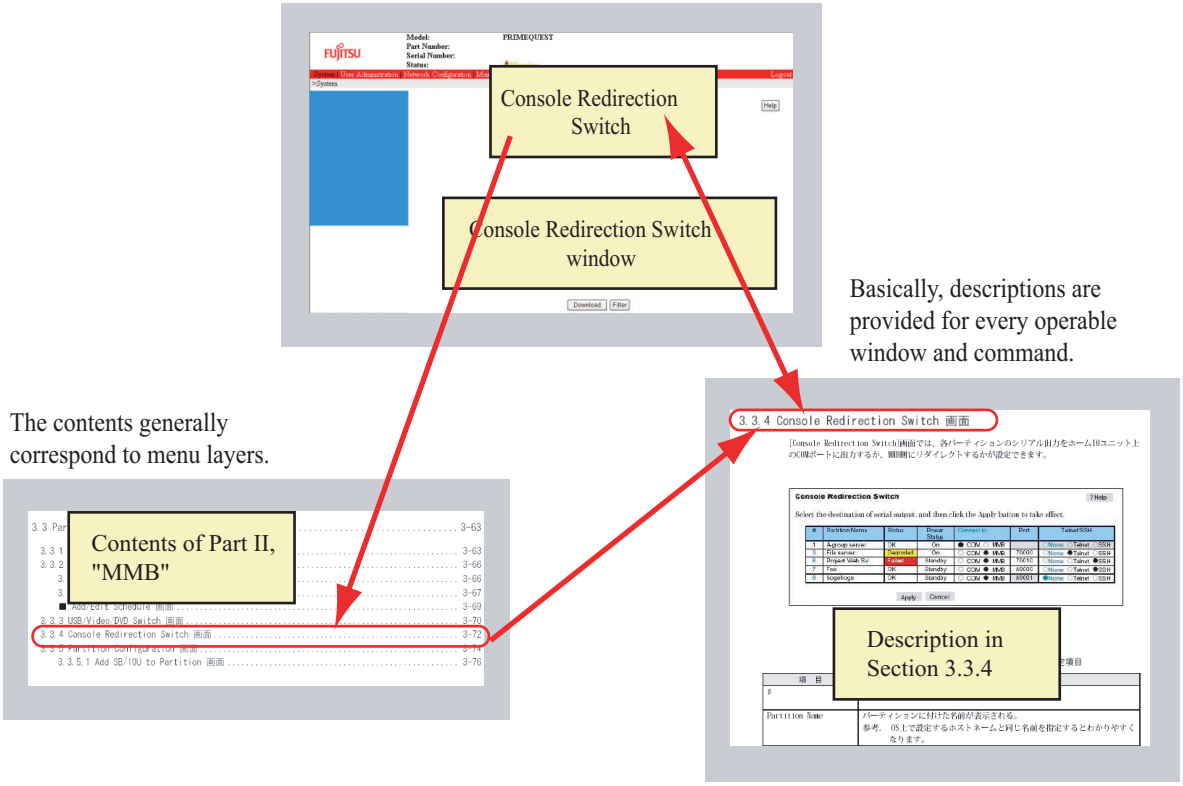


Figure 1.2 Window and its corresponding section in this manual

The contents of the manual generally correspond to menu layers.

Basically, the manual has operation descriptions for every operable window and command.

To find out the software corresponding to a window, check the submenu hierarchy (breadcrumb trail) that is displayed below the navigation bar in the window. The menu path to the displayed content is displayed there.

- An example of a submenu path is "System>PSA>Network>Network Interface".
- A submenu path that includes "PSA" indicates a PSA Web-UI window.
- A submenu path other than the above indicates an MMB Web-UI window.

CHAPTER 2 Overview of the Web-UI

The PRIMEQUEST-series machine provides two user interfaces for its server management board, referred to as the management board (MMB), containing a dedicated processor:

- The Web user interface (Web-UI) enables operation and management by the user through a Web browser running on a PC or workstation (referred to collectively as a PC, in this document).
- The command line interface (CLI) enables operation by the user through a serial port or remote PC connection via a management LAN.

This chapter describes common Web-UI window operations and basic operations with the MMB for management and operation of the PRIMEQUEST-series machine. Basic operations from the CLI are described in the chapter on CLI operations in each part of this manual.

CAUTION

Malfunction

The MMB Web-UI supports the Web browsers listed below. Note that other browsers may not display Web-UI windows correctly.

- Microsoft® Internet Explorer (IE) v5.5 (SP2) and later
- Netscape v7.02 and later

2.1 Web-UI Windows

The user can select the desired font size in these windows. The system status is indicated by text. It is also indicated by colors so that the user can easily recognize the current status. Three color patterns classify the status as normal, warning, or error:

- Normal status
  The window background color remains the same.
- Warning status
  Yellow indicates the warning status.
  For example, if a unit is in the warning status, the table frame that displays the status has a yellow background.

- Error status
  Red indicates the error status.
  For example, if a unit is in the error status, the table frame that displays the status has a red background.

If there is an occurrence of an MMB failure, MMB warning, or a similar problem indicated by one of the "operation interruption check conditions" below, do not attempt to perform any operation yourself. Contact a Fujitsu certified service engineer instead.

- Operation interruption check conditions
  - The Alarm LED of the MMB is on.
  - A connection could not be established to the MMB Web-UI.
  - The Alarm LEDs of multiple boards in the main unit are on.
  - "ReadError" is displayed by the MMB Web-UI.
  - "Not Present" is displayed for the status of every unit in the [System Status] window of the MMB Web-UI.

2.2 Frame Configuration

Each Web-UI window consists of three frames as shown below.

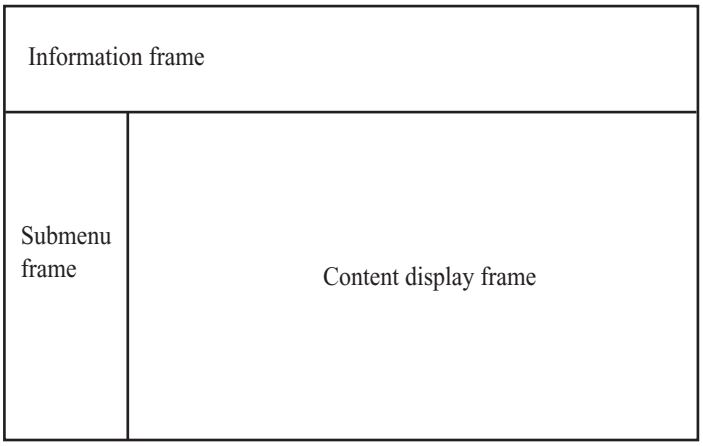


Figure 2.1 Frame configuration

- Information frame
  PRIMEQUEST-series machine information, such as a model name and part number, is displayed. The user can check this information to easily identify the system.
- Submenu frame
  A tree view menu is displayed. Selecting a menu item displays the corresponding window in the content display frame, which displays status information and is used to make settings.
- Content display frame
  A window for displaying status information and specifying functions is displayed.

2.3 Information Frame

This section describes the information that is always displayed in the information frame.

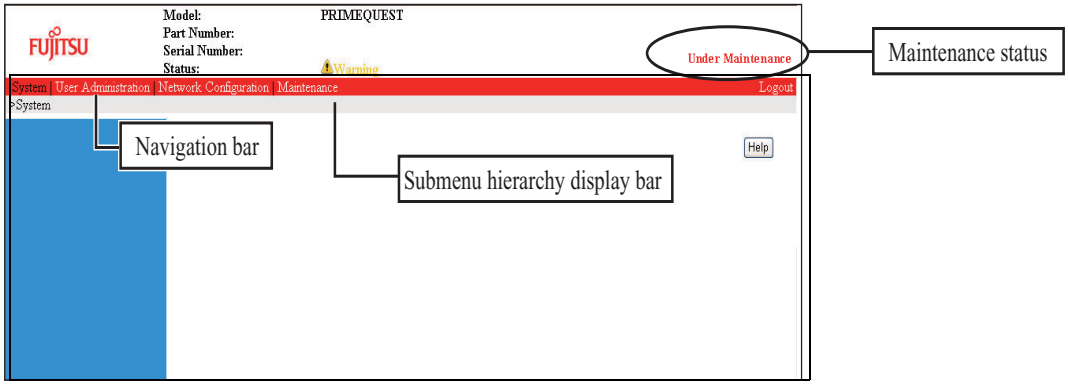


Figure 2.2 Information frame

- Model
  A PRIMEQUEST model name is displayed.
- Part Number
  A PRIMEQUEST part number is displayed.
  Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer.
- Serial Number
  A PRIMEQUEST serial number is displayed.
  Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer.
- Status
  The status of the PRIMEQUEST-series machine as a whole is displayed. The following three system statuses can be displayed.

Status	Displayed color	Icon
Normal	Green	(None)
Warning	Yellow	Black exclamation mark (!) in a yellow triangle
Error	Red	White X mark in a red circle

Clicking the system status displays the [System Event Log] window.

- Maintenance status
  "Under Maintenance" is displayed in orange while the PRIMEQUEST-series machine is being maintained by a maintenance engineer using the [Maintenance Wizard] menu.
  Nothing is displayed for this status when the PRIMEQUEST-series machine is not under maintenance.

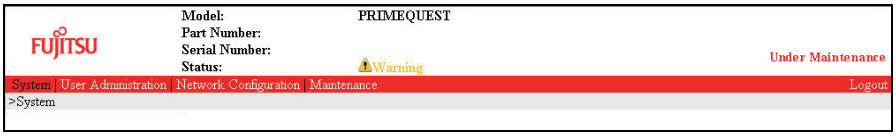


Figure 2.3 Maintenance status

- Navigation bar
  Any of the menus can be selected for display in the submenu frame.
  The name of the selected menu is displayed in black, and the names of the other menus, which are not selected, are displayed in white.
- Submenu hierarchy display bar
  The path to the submenu displayed in the submenu frame is displayed. Clicking a level in the path displays the corresponding window.
- [Logout]
  Clicking [Logout] results in logout from the Web-UI.

2.4 Submenu Frame

The submenu frame displays the menu selected from the navigation bar in the information frame.

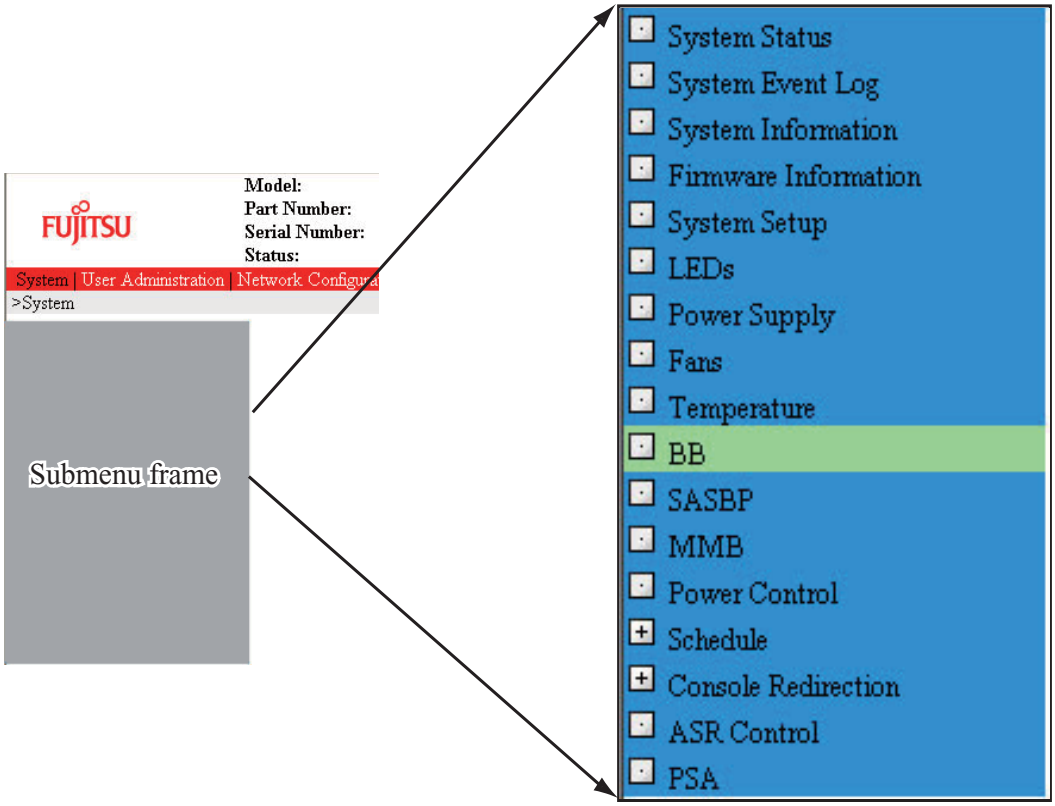


Figure 2.4 Submenu frame

The following applies to the displayed menu:

- Up to three layers of submenus are displayed.
- One of the following icons is displayed to the left of each submenu item to indicate whether the item has a lower layer:
  - [+] : The submenu item has a lower layer of items. :
  - [-] : The submenu item has a lower layer of items, and the expanded node displays these items.
  - [·] : The submenu item has no lower layer of items.
- A submenu item is displayed in reverse video when the cursor is placed on it.
- Selection of an item is indicated by a different background color.

2.5 Content Display Frame

The content display frame displays the window corresponding to the menu item selected from the navigation bar in the information frame or from the submenu in the submenu frame.

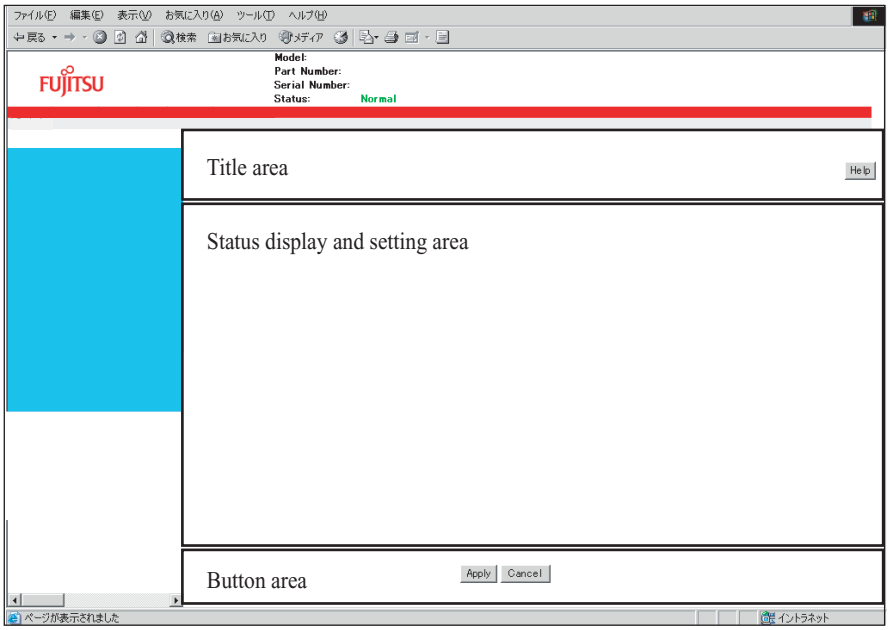


Figure 2.5 Content display frame

The content display frame is split into the following three areas:

- Title area
  This area displays the title of the displayed content. The area also has the [Help] button, which is used to display the Help for the content, and the [Refresh] button, which is used to reload data.
  Clicking the [Help] button displays the Help. The Help window is displayed when the button is clicked.
  The [Refresh] button reloads only the data in the content display frame. The [Refresh] button is displayed only in a window subject to automatic refresh, and it is not displayed in a window used only for configuring data settings without allowing automatic status changes.

- Status display and setting area
  This area displays status information and settings for the displayed content. Components such as input fields, radio buttons, and check boxes are grayed out for users who have only the privilege to display information, thereby preventing them from configuring settings.
- Button area
  This area displays buttons used for actions involving the data in the status display and setting area. The [Apply] and [Cancel] buttons are usually displayed.
  Note that the button area is not displayed in cases where the displayed content requires no input or the user has only the privilege to display information.
- Dialog box
  Dialog boxes appear in this area for content display frame operations, such as clicking the [Apply] button. A dialog box notifies the user of an error, prompts for confirmation, or prompts for input of subsequently required information. The following two types of dialog boxes can be displayed:
  - Warning dialog box
    This dialog box notifies the user of an error such as an input error.
    Example:

  - Confirmation dialog box
    This dialog box prompts the user to specify whether to continue processing.
    Example:

2.6 Basic Operations in Web-UI Windows

- Access procedure

The procedure for accessing the MMB from the Web-UI is described below.

1. Start a Web browser.
   Remarks:
   - JavaScript must be enabled on the browser because the MMB Web-UI uses JavaScript.
   - Download must be enabled on the browser because the MMB Web-UI is used to perform downloads.
2. Enter one of the following addresses:

Standard	http:// nodename:adminport
SSL	https:// nodename:adminport

   For "nodename," specify the virtual IP address, physical IP address, or corresponding FQDN of the active MMB.
   For "adminport," specify the port number assigned to the MMB management port (The default value is 8081 for Standard or 432 for SSL.)
3. Enter the following user account and password, and then click the [Login] button.
   Remarks:
   If the MMB is starting for the first time or its settings have not been changed, the following default user account and password are in effect and you are asked to change the default password.

User name ID	Administrator
Password	Password set by the Fujitsu certified service engineer at the time of device setup.

The procedure for displaying the desired Web-UI window is described below.

1. Select the appropriate menu item from the navigation bar in the information frame to display the corresponding menu in the submenu frame.
   The submenu frame then displays the menu.
2. Select the window from the submenu displayed in the submenu frame.
   The content display frame then displays the window.
3. Confirm and specify information in the window.
4. To return to the next higher layer of the menu, click the ← (back) button on the toolbar.
   The content display frame displays the window as the next higher layer of the menu.

Note: When using the MMB Web-UI on Internet Explorer, if it takes two minutes or longer to check the execution of processing and indicate the completion of processing with the related dialog box displayed, connection to the MMB Web-UI is cut off. In such case, log in again to the MMB Web-UI.

The step for exiting from the Web-UI window is described below.

1 Click [Logout] at the right end of the navigation bar in the information frame. This results in logout from the Web-UI.

- Displaying and using a Window

Each field in a window can be displayed and used as follows:

● Character string input field (text field)
A character string can be entered in the field.

Input of a character string

● Selection field (pulldown list)
Click the [▼] button to display the list from a pulldown menu, and select a value from the list.

Selection ▼

● Setting button (button)

Apply Cancel

- [Apply] button
When this button is clicked, the system checks the validity of the data entered in character string input fields and selected values in the selection fields and other specified data in the window. If invalid data is found, a warning dialog box appears.
For example, if the [Apply] button is clicked with an invalid IP address such as 255.255.255.255 entered in the IP address input field, the warning dialog box shown below appears.

When the [OK] button is clicked in the warning dialog box, the window scrolls until the input error location is displayed, and the cursor is displayed at the input error location.

If the entered data may have a significant effect on the system, a confirmation dialog box for continuing processing is displayed.

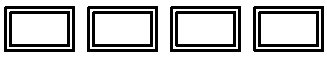
- [Cancel] button
  When this button is clicked, the data entered in the character string input fields and selected values in the selection fields are not applied in the system, and the state prior to entry of the data is restored.
- Selection of a single option (radio button)
  Clicking [○], an option button, selects the corresponding element. Only one button can be selected in the field.
  Clicking [○] (off) changes it to [●] (on).

Select	● ○ ○ ○

- Selection of multiple options (check box)
  Clicking [□], a check box, selects the corresponding field.
  Clicking [□] (off) changes it to [■] (on).

Select	■ □ □ ■

- Link
  Clicking a link results in a jump to the destination window.
  LINK
- IP address input field
  A number ranging from 0 to 255 can be entered in each input field.



- MAC address input field
  A hexadecimal number ranging from 00 to FF can be entered in each input field. Case sensitivity is not considered for the hexadecimal numbers A, B, C, D, E, and F.

Note: During a download operation through the MMB Web-UI using Internet Explorer running under Windows XP SP2 or later, the dialog box for confirming the download destination may be blocked from opening. In this event, do as follows:

1 Click [Tool] → [Internet Option] → [Privacy] → [Block Popups].
2 In the [Block Popups] dialog box, add the MMB URL to the addresses at "Address of Web site to allow."

2.7 User Privilege Levels

The following table lists the user privilege levels used to restrict operation of the PRIMEQUEST-series machine.

Table 2.1 User privilege levels

Privilege level	Description
User	Permitted only to refer to the PRIMEQUEST-series machine status.
CE	Permitted to refer to the PRIMEQUEST-series machine status. Changes to user management and network settings are not permitted. Maintenance operations are permitted.
Operator	Permitted to refer to the system status and configure system settings. Changes to user management settings or the LAN configuration are not permitted. The following operations are not permitted: • Operating power from the [Power Control] window • Changing the fan status
Administrator	Permitted to perform every type of operation.

2.8 Switching to Operations with Software of Another Type

This section describes how to switch to operations with software of another type among the following types of software:

- MMB firmware
- PSA
- EFI firmware

The Web-UI or CLI can be used to issue instructions for this operation from a PC connected to the management LAN.

Switching with Web-UI operations and switching with CLI operations are briefly described below.

Switching with Web-UI operations

Figure 2.6 shows an outline of switching with Web-UI operations.

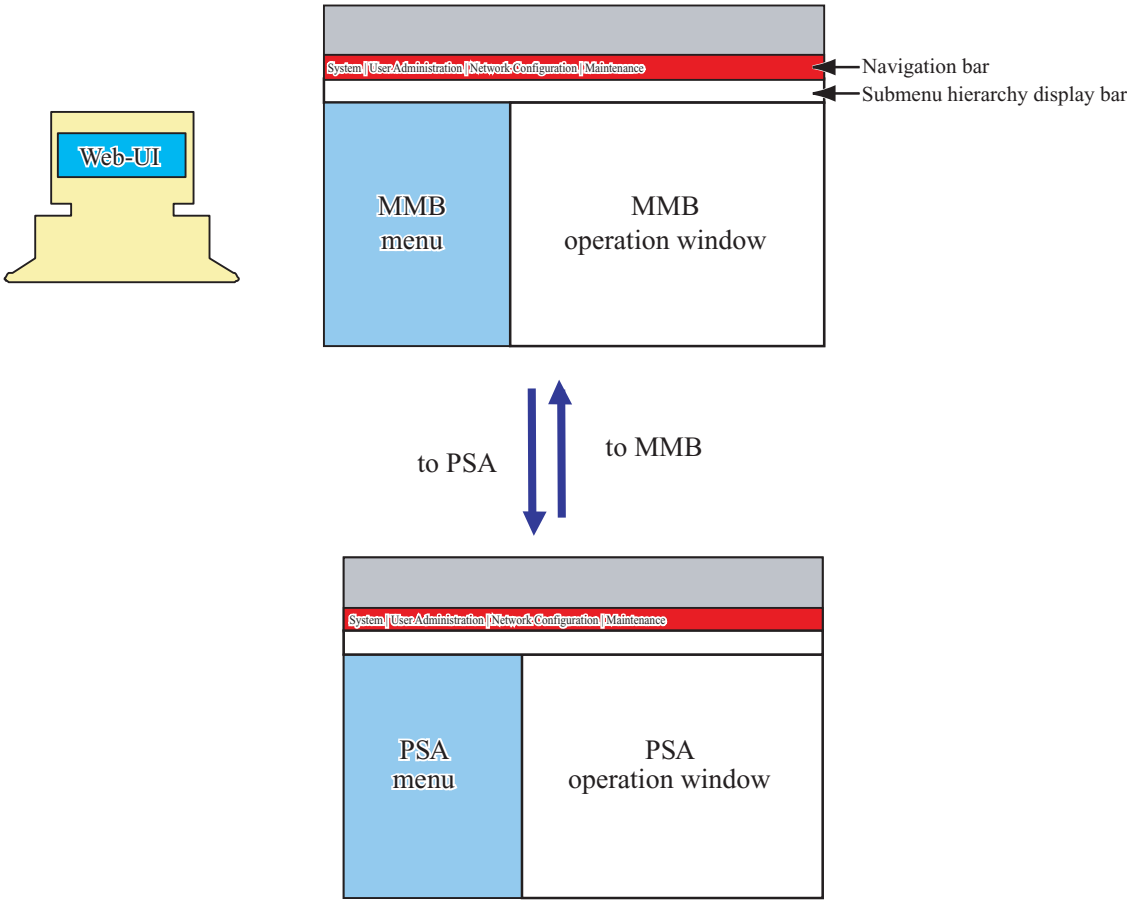


Figure 2.6 Switching with Web-UI operations

The navigation bar and menus are used for switching.

The current software used for operations can be determined from the submenu hierarchy display bar, which shows the menu path to the displayed window.

to PSA

1 Click [System] on the navigation bar.
2 Select [PSA] from the System menu.
→ The PSA menu of the selected System is displayed.

to MMB

1 Click [System] on the navigation bar.
→ The MMB menu is displayed.

Switching with CLI operations

An outline of switching with CLI operations is provided below.

The Telnet or SSH command from a PC connected to the management LAN is used in CLI operations to switch to the target software for particular operations. The basic operating procedure is to log in to the OS or firmware of the target of this operation by executing the Telnet or SSH command with the corresponding IP address specified. Information required for remote login, such as an IP address, an account ID, and a password, must be specified in advance.

Logging in to the MMB

Specify the MMB IP address, and log in with a remote connection.

Note: To log in to the MMB using telnet or SSH from an external device, click [Network Configuration] → [Network Protocols], and set [Enable] for the necessary parameters in the [Network Protocols] window.

Logging in to the EFI

The EFI is used for special cases such as for changing boot control.

1 Click [System] → [Power Control] on the MMB Web-UI, and the [Boot Control] window is diaplayed.
2 Click [Boot Selector] → [Force EFI Boot Manager] and click the [Apply] button.

CHAPTER 3 Starting and Stopping the System

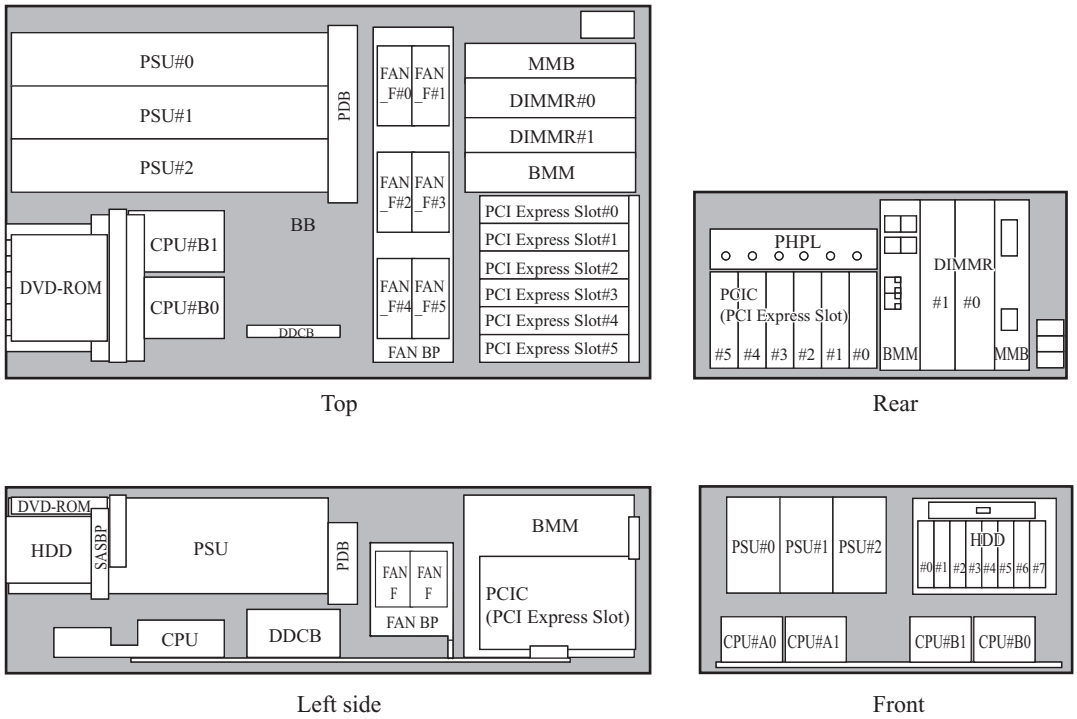
3.1 Component Names and Functions

The following figures show the appearances of the PRIMEQUEST 510A.

Figure 3.1 PRIMEQUEST 510A

The names and functions of individual PRIMEQUEST components are listed below.

The PRIMEQUEST 510A components are installed as shown below.



PSU:	Power Supply Unit	DIMMR:	Riser board for mounting DIMM
CPU:	Central Processing Unit	BMM:	BMC module
HDD:	Hard Disk Drive	BB:	Base Board
FAN:	Fan	PCI Express Slot:	PCI Express slot
MMB:	Management Board	PDB:	Power Distribution Board

Figure 3.2 General configuration of the PRIMEQUEST 510A

3.2 Turning On and Turning Off the Main Power

This section explains how to turn on and turn off the main power as follows:

- Power-on procedure (→ 3.2.1)
- Power-off procedure (→ 3.2.2)

3.2.1 Power-on procedure

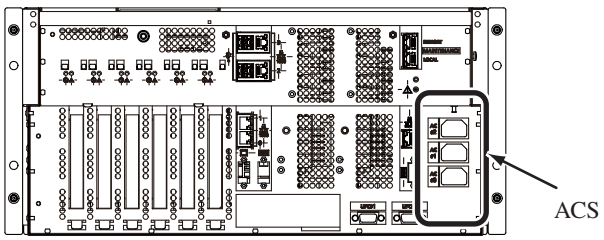
Remarks: Wait at least 10 seconds before reconnecting the power cable to the ACS after disconnecting it.

If the power distribution box is switched off due to the detection of overcurrent, a failure (e.g., short circuit) may have occurred in the main unit. Switching the power distribution box back on again in that status may also switch off the power distribution board circuit breaker or cause burnout in the main unit. Therefore, if the power distribution box is switched off due to the detection of overcurrent, contact a Fujitsu certified service engineer without switching the power distribution box back on.

Power-on procedure

1 Connect the power cable to the ACS of the main unit, and then connect the power cable to the power distribution box.

Note: When connecting power cables to the ACS, connect them sequentially from the bottom.



Rear view

Figure 3.3 ACS location

3.2.2 Power-off procedure

Power-off procedure

CAUTION

Data destruction

When power to the main processing unit is turned off in an operation from the MMB, only the front MMB Ready is lit:
Before turning off the main power (UPS, power distribution box, circuit breaker switches, etc.), be sure to confirm that all LEDs other than the front MMB Ready are off. Otherwise, turning off the main power may cause damage to data.

1. Turn off the main unit.
   Use the management board (MMB) for the power-off operation. For details, see Section 3.3.1, "Power-on/power-off procedure using MMB Web-UI."
2. Confirm that only the front MMB Ready is lit:
3. Disconnect the power cable from the power distribution box.

3.3 Power Management Using MMB Web-UI

This section explains power-on and power-off procedures using the MMB Web-UI window.

CHAPTER 2 explains the basic operations of the MMB Web-UI screen. See Section 2.6, "Basic Operations in Web-UI Windows" as required.

3.3.1 Power-on/power-off procedure using MMB Web-UI

- Power-on procedure

1 Switch on the power switches on the MMB and peripherals.

2 Log in to MMB Web-UI.
The MMB Web-UI window is displayed.

3 Click [System] → [Power Control] from the Web-UI menu.
The [Power Control] window is displayed.

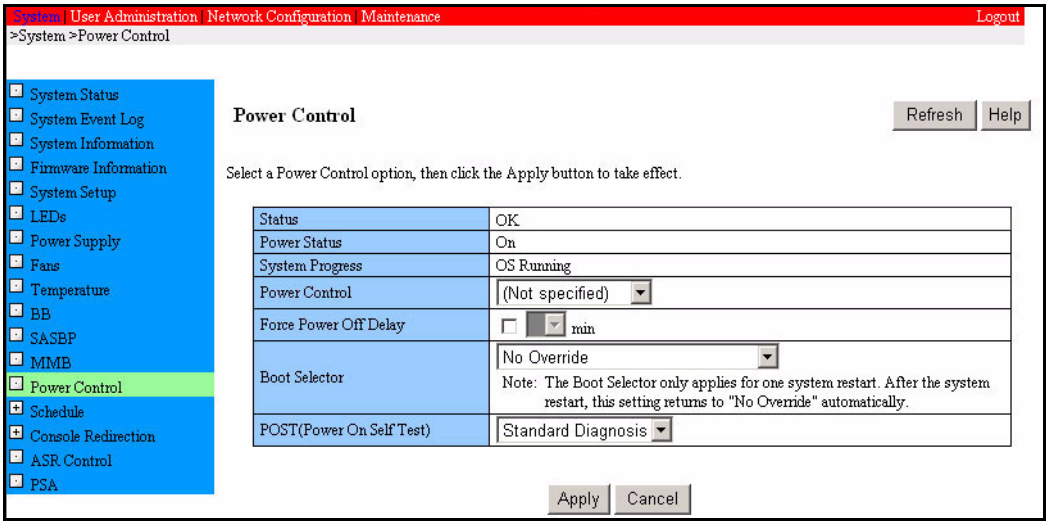


Figure 3.4 [Power Control] window

4 Select [Power On] in the [Power Control] list, and then click the [Apply] button.
System power is turned on.

- Power-off procedure

CAUTION

Data destruction

Before shutting down power, make sure the following events have occurred; otherwise, data may be destroyed:

- All applications have completed processing.
- No user is using a component.

The Power LED on the operator panel is turned off when the main unit is turned off. Before shutting down main power (to the UPS, power distribution box, and circuit breakers), make sure that the LED is off. If necessary, back up files before shutting down the power.

Note: Use the OS shutdown function to shut down the system normally. Only in emergency situations, such as when no response is obtained from the system, should MMB Power-Off (Force Power Off) be used to turn off the power.

1 Log in to MMB Web-UI.
The MMB Web-UI window is displayed.

2 Click [System] → [Power Control] from the Web-UI menu.
The [Power Control] window is displayed.

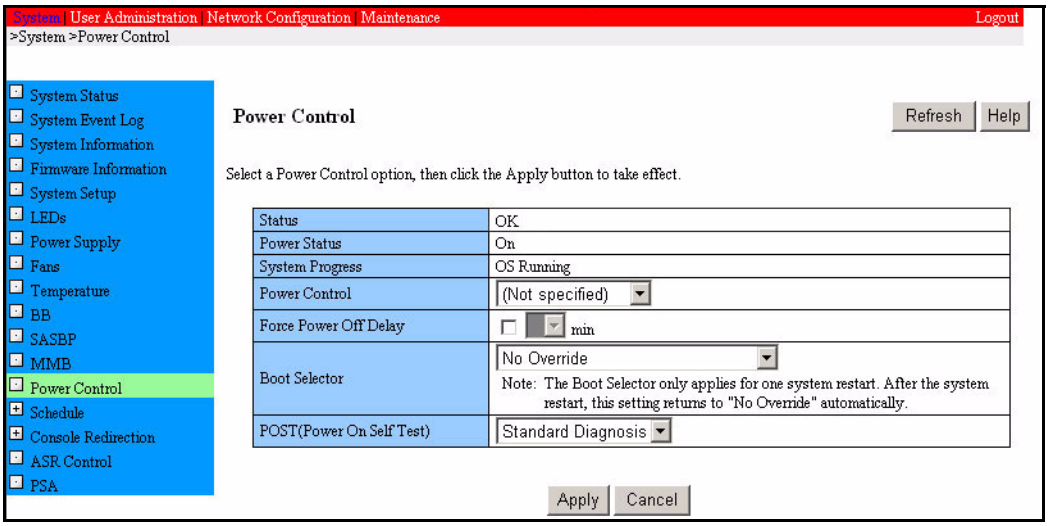


Figure 3.5 [Power Control] window

3 Click [Power Off] or [Force Power Off] in the [Power Control] list, and click the [Apply] button.
System power is turned off.
Remarks:
If [Force Power Off] is selected, power is turned off without shutting down any OS.

- Explanation of the [Power Control] window

Table 3.1 Displayed and setting items in the [Power Control] window

Item	Description
Status	System status: • OK: Operating normally • Degraded: Component failure (The faulty component can be isolated to continue operation.) • Warning: Warning status (A problem will possibly occur.) • Failed: Failure
Power Control	Select a power control setting. The [Power On] selection is not displayed when the power is on. Conversely, the [Power Off], [Reset], [INIT], [Power Cycle], and [Force Power Off] selections are not displayed when the power is off. • Power On: Powers on. • Power Off: Powers off. • Power Cycle: Forcibly powers off and powers it on again. • Reset: Resets the system. • INIT: Generates an INIT interrupt and generates a dump. • Force Power Off: Forcibly powers off a partition. • (Not specified): Issues no instruction. Note: Executing INIT forcibly terminates applications running in the system. Before executing INIT, stop important applications. Also, unmount unnecessary file systems.
Force Power Off Delay	Specify whether to forcibly power off the system in the event that the system is not powered off by a shutdown instruction issued to its OS during the [Power Off]. When Force Power Off is specified with a check mark in the check box, a specified time (one to nine minutes) can be set. When this specified time has passed, the power to the partition is forcibly turned off. Default: Force Power Off check box is unchecked.

3.3.2 Checking the power status and system status

This section explains how to check the power status and system status.

1 Log in to MMB Web-UI.
The MMB Web-UI window is displayed.

2 Click [System] → [Power Control] from the Web-UI menu.
The [Power Control] window is displayed.

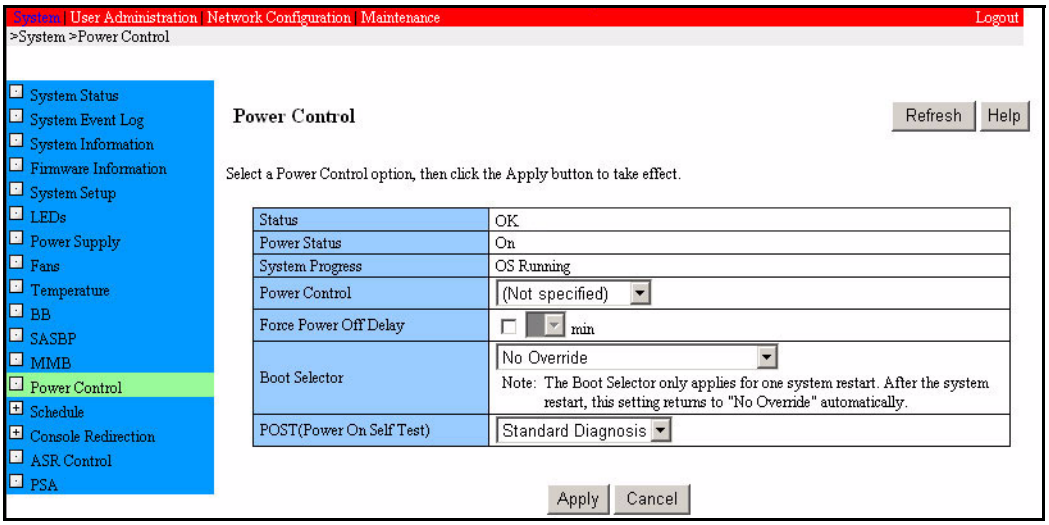


Figure 3.6 [Power Control] window

[Power Status] displays the power status, and [System Progress] displays the system status.

Table 3.2 Displayed and setting items in the [Power Control] window

Item	Description
Power Status	The cabinet power status is displayed as follows: • [On]: Power is on. • [Standby]: The system is in the standby state.
System Progress	The system status is displayed as follows: • Power Off: System power is off. • Power On In Progress: The system is in power-on sequence. • Reset: The system is reset. • POST XXXXh: Indicates that the system has started POST Code=XXXXh processing. • Boot: The system is in one of the following states: - The system is being booted. - PSA is not installed. - Installation is in progress. - Backup or restoration using Systemcast Wizard is in progress. • OS Running: The OS is active. • OS Shutdown: The OS is shut down. • Panic: The system is in panic state. • Power Off In Progress: The system is in power-off sequence. • Check Stop: The system is stopped. • Initiate soft-shutdown: Starts countdown to Force Power Off.

3.3.3 Boot control

This section explains the boot control such as a boot device specification. The boot control can be set with administrator/operator authority only.

1 Log in to MMB Web-UI.
The MMB Web-UI window is displayed.

2 Select [System] → [Power Control] from the Web-UI menu.
The [Boot Control] window is displayed.

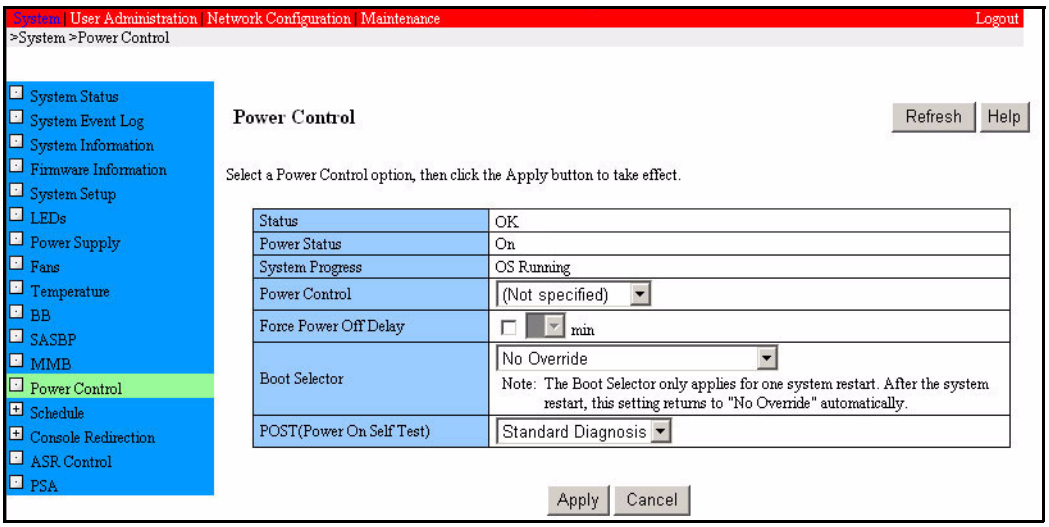


Figure 3.7 [Power Control] window

3 Specify the boot setting.

Table 3.3 Displayed and setting items in the [Power Control] window

Item	Description
Boot Selector	Specify the boot device by overwriting the EFI Boot Manager settings. Select the boot device from the pulldown menu: • No Overwrite: The EFI Boot Manager settings are used to boot the system. • Force boot into EFI Boot Manager: EFI Boot Manager is started, and it then waits for input. EFI Boot Manager can thereby be used to select a boot device and boot the system. • Force PXE: The EFI Boot Manager settings are overwritten, and PXE is forcibly executed. • Force boot from DVD: The EFI Boot Manager settings are overwritten, and a forced boot of the system from the DVD is attempted. The default is [No Overwrite].
Post (Power On Self Test)	Select the type of Power On Self Test (POST) from the pulldown menu: • Fast Boot: Fast boot with minimal diagnosis • Standard Diagnosis: Standard diagnosis • Full Diagnosis: Complete diagnosis with all diagnostic items The default is [Standard Diagnosis].

4 Click the [Apply] button.

3.3.4 Power-on and power-off by scheduled operation

The power can be turned on and off by a scheduled operation (auto power control). If a scheduled operation is defined, the power is turned on at the specified time. A daily, weekly, or monthly schedule or the schedule for a specific day can be set. For details on schedule setting, see Section 5.2.15, "Schedule menu."

Remarks: Power-off by a scheduled operation is supported only by Linux.

3.3.5 Setting for Automatic Restart

This section explains how to specify the conditions for automatic restart.
Setting for automatic restart requires Administrator authority.

CAUTION

Malfunction

Before any of the following operations is performed, [Disable] must be set for the Boot Watchdog in the [Watchdog] window of PSA.

- Booting from a CD-ROM disk
- Booting the system in single-user mode (Linux)
- Booting the system in the safe mode (Windows)
- Backing up or restoring data by using SystemcastWizard

If any of the above operations is performed with [Enable] set for the Boot Watchdog, OS restart is attempted repeatedly for the specified number of times. The system then takes the specified action (Stop rebooting and Power Off, Stop rebooting, or Diagnostic interrupt assert). The number of retries of the OS restart and the actions to be taken can be set in the [ASR Control] window for the MMB-UI.
In the [ASR Control] window, check [Cancel Boot Watchdog], and click the [Apply] button. [Disable] can thus be forcibly set for the Boot Watchdog.
For details about the [Watchdog] window of PSA, see Section 7.15.1, "[Watchdog] window," in Part IV, "PSA."

Procedure

1. Log in to MMB Web-UI.
   The MMB Web-UI window is displayed.
2. Click [System] → [ASR Control].
   The [ASR Control] window is displayed.

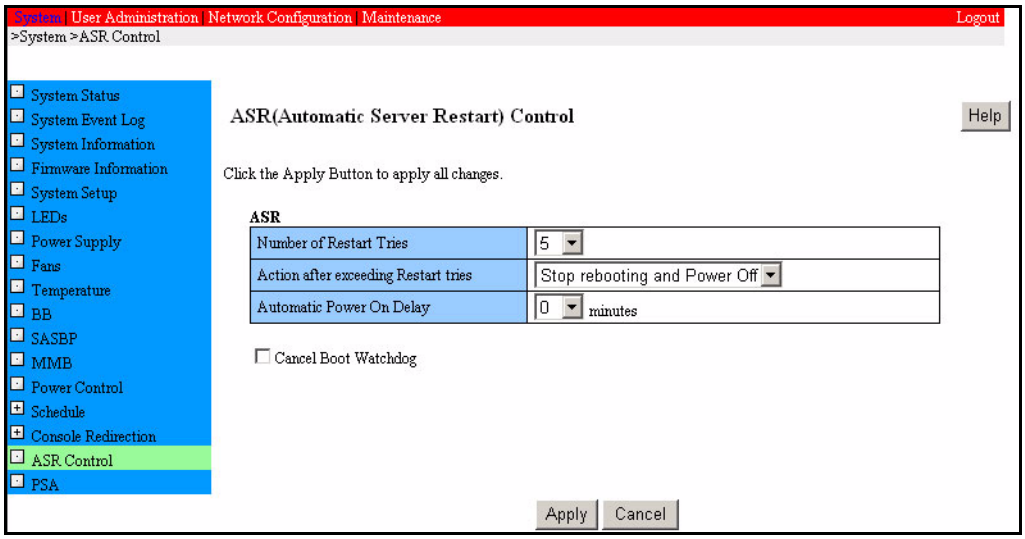


Figure 3.8 [ASR Control] window

3 Specify the conditions for the automatic restart (Action after exceeding Restart tries).
4 To cancel Boot Watchdog, check the [Cancel Boot Watchdog] check box.
5 Click the [Apply] button.

Explanation of the [ASR Control] window

Table 3.4 Displayed and setting items in the [ASR Control] window

Item	Description
Number of Restart Tries	Specify the number of times the OS is restarted after Boot Watchdog or PSA Software Watchdog detects a timeout. A number ranging from 0 to 10 can be specified. Default: 5
Action after exceeding Restart tries	Specify the action that is taken if the above Number of Restart Tries is exceeded by the number of restarts that are repeated because of a Watchdog timeout. One of the following actions can be specified: • Stop rebooting and Power Off • Stop rebooting • Diagnostic Interrupt assert Default: Stop rebooting and Power Off
Automatic Power On Delay	Specify the delay time for the power-on operation by automatic restart. A value ranging from 0 to 10 minutes can be specified. Default: 0

Item	Description
Cancel Boot Watchdog	This cancels OS Boot Watchdog. If the Boot Watchdog is canceled in this window, the system does not initiate OS boot monitoring until [Enable] is set again for the Boot Watchdog in the [Watchdog] window of PSA. For details about the [Watchdog] window of PSA, see Section 7.15.1, "[Watchdog] window," in Part IV, "PSA." Remarks: OS boot monitoring is a PSA function. The monitoring starts when the Boot Watchdog timeout time is set in the PSA window. If the specified Boot Watchdog timeout time is too short, however, a timeout may occur before the system starts PSA, which can stop the Boot Watchdog timer. As a result, repeated reboots may occur. In such cases, PSA has not yet started, and the PSA page that provides the Boot Watchdog function cannot be displayed, so the Boot Watchdog cannot be displayed. Likewise, if any of the following operations is performed, PSA will not boot, resulting in any of the aforementioned problems: • Booting from a CD-ROM disk • Booting the system in single-user mode Booting the system in the safe mode • Backing up or restoring data by using SystemcastWizard Provided as a measure against this problem, this check box disables the Boot Watchdog without using PSA. Default: Check box unchecked

3.4 Power Management Using Command line interface (CLI)

This section explains how to use the MMB command line interface (CLI) for power control over the entire system. These operations require Administrator authority.

Accessing the CLI

The following two methods of CLI access can be used. Use one of them to access the CLI.

- Access via an MMB serial port
- Access from a remote PC via an MMB management LAN

- Access via a serial interface

1. Connect the MMB to a terminal (e.g., notebook PC) by using an RS-232C cross cable.
2. Start terminal software (e.g., Windows HyperTerminal) on the terminal, and set up the terminal software as follows.

Table 3.5 Terminal software setting

Setting item	Value
Transfer rate (bps)	19200
Data bit	8
Parity	None
Stop bit	1
Flow control	No
Emulation	VT100

3. A login prompt is displayed. Enter your user name and password to log in.

- Access via a management LAN interface

1. Connect the MMB to a remote PC by using a straight LAN cable.
2. Start Telnet or SSH Client on the remote PC, and enter the MMB IP address and a Telnet or SSH port number to establish a connection.
3. Enter the account and password to log in.

Notes:
MMB supports only the connection functions available under the SSH V2 protocol. Therefore, to establish a connection with the MMB using the SSH protocol, terminal software compatible with SSH V2 must be prepared.

Power-on operation using the CLI

The system can be turned on.

- Command syntax

```
power on
```

  - The command turns on the entire system.

Power-off operation using the CLI

The entire system can be turned off.

- Command syntax

```
power off [force]
```

- Option

  force: Indicates that the power has been forcibly turned off without shutting down the operating system of the partition.

3.5 Checking the System Power Status

This section explains how to check the system power status.

Checking the system power status by using MMB

1 Log in to MMB Web-UI.
The MMB Web-UI window is displayed.

2 Select [System] → [Power Supply] from the Web-UI menu.
The [Power Supply] window is displayed.

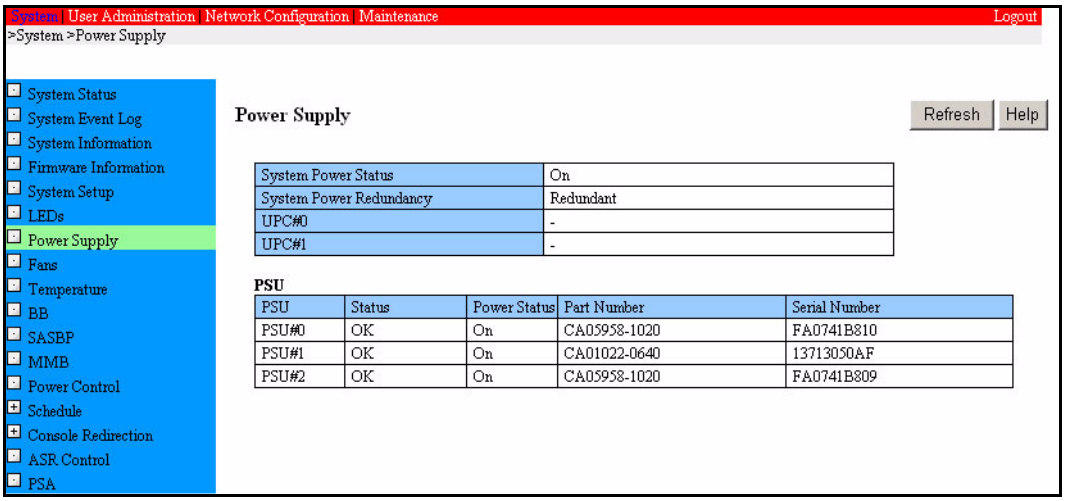


Figure 3.9 [Power Supply] window

The PRIMEQUEST 510A power status is displayed at [System Power Status].

Explanation of displayed information

Table 3.6 Displayed and setting items in the [Power Supply] window

Item	Description
System Power Status	The system (cabinet) power status is displayed as follows: • [On]: Power is on. • [Standby]: The system is in the standby state.
System Power Redundancy	The redundancy status of the power supply unit is displayed as follows: • [Redundant] The PSU is redundant. • [Non-redundant: Sufficient Resources] PSU redundancy has been lost, but there are enough PSUs for system operation. • [Non-redundant: Insufficient Resources] PSU redundancy has been lost, and there are not enough PSUs for system operation.
UPS#x	The status of a UPS detected by the UPC interface is displayed as follows: • [AC Lost]: Power failure • [Battery Lost]: The battery has been depleted. • [Failed]: Failure has occurred. • [-]: Normal status or the UPS is not connected. Notes: The UPC interface could not recognize a UPS, if it is connected. Therefore, when no problem is detected, "-" is displayed.
Status	The PSU status is displayed as follows: • [OK]: Normal • [Not present]: Not mounted. • [Failed]: Failure has occurred. • [Predictive Fail]: Expecting a failure. • [A/C Lost]: Power failure.
Power Status	This indicates whether a PSU is on or off.
Part Number	The part number of a PSU is displayed. Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer.
Serial Number	The serial number of a PSU is displayed. Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer

3.6 Remote Shutdown

3.6.1 Remote shutdown of Windows

This section explains how to shut down the system on which Windows Server 2003 is installed, from a remote management terminal.

The management terminal establishes a connection to the unit to shut it down. The following two connection modes can be used:

- Remote shutdown via a LAN connection (→ 3.6.1.1)
- Remote shutdown via a COM port connection (→ 3.6.1.2)

Basically, the remote shutdown is executed via a LAN. However, select the appropriate connection mode and shutdown method, depending on the operating environment of the system.

Note:

If the following condition occurs, contact your Fujitsu certified service engineer.

A remote shutdown is executed, and the operation is not completed even after a long time has elapsed. Furthermore, an attempt to display the status of each component in the MMB Web-UI window causes "Read Error" to be displayed for [Part Number] or [Serial Number].

3.6.1.1 Remote shutdown via a LAN connection

The following three methods may be used to shut down the system through its LAN port connection to the management terminal.

Table 3.7 Shutdown methods

	Management terminal OS	
	Windows OS	Linux/Unix OS
A) Shutdown.exe command	Y*1	N
B) Remote Desktop Connection	Y*1	N
C) Telnet connection	Y*1	Y

Y: Can be used N: Cannot be used

*1 The applicable Windows versions are limited. For details, see the respective shutdown method explanations.

Some of these methods require preparations or different operating conditions. Use the methods properly according to your operating environment.

a) Shutdown with the Shutdown.exe command

The Shutdown.exe command is a standard command in Windows XP and Windows Server 2003. Entering this command in response to the command prompt on the management terminal can shut down the system.

- Prerequisites:
  - The management terminal is connected to the unit via a LAN.
  - The management terminal OS is Windows XP or Windows Server 2003, both of which support shutdown.exe.
  - The management terminal has the same log-in account information, user name, and password as Windows. (example: user name: Administrator, password: primequest)
- Procedure:
  - Steps on the management terminal (Windows XP)
    1. Click [Start] button → [Programs] → [Accessory] → [Command Prompt] to start the command prompt.
    2. Enter the following command:

```
C: \>shutdown -s -m\\Servername
```

Specify the computer name in *Servername*, and execute the Shutdown command.

```
C:\WINDOWS\system32\cmd.exe

C:\>shutdown /?
Usage: shutdown [/i | /l | /s | /r | /a | /p | /h | /e] [/f]
    [/m \\computer][/t xxx][/d [p:]xx:yy [/c "comment"]]

    No args    Display help. This is the same as typing /?
    /?         Display help. This is the same as not typing any options
    /i         Display the graphical user interface (GUI).
               This must be the first option
    /l         Log off. This cannot be used with /m or /d option
    /s         Shutdown the computer
    /r         Shutdown and restart the computer
    /a         Abort a system shutdown.
               This can only be used during the time-out period
    /p         Turn off the local computer with no time-out or warning.
               This can only be used with /d option
    /h         Hibernate the local computer.
               This can only be used with the /f option
    /e         Document the reason for an unexpected shutdown of a computer
    /m \\computer Specify the target computer
    /t xxx     Set time-out period before shutdown to xxx seconds.
               The valid range is 0-600, with a default of 30
    /c "comment" Comment on the reason for the restart or shutdown.
               Maximum of 127 characters allowed
    /f         Force running applications to close without forewarning users
    /d [p:]xx:yy  Provide the reason for the restart or shutdown
               p indicates that the restart or shutdown is planned
               xx is the major reason number (positive integer less than 256)
               yy is the minor reason number (positive integer less than 65536)
```

Figure 3.10 Execution of the Shutdown command

The command shown above has 30 seconds (default) specified in the -s option for the shutdown time. Both the restart and the shutdown times can be specified. For details on command operations, display Help as shown above.

Remarks:

The command can be used similarly under Windows Server 2003.

b) Shutdown through Remote Desktop Connection

Remote Desktop Connection is similar to Terminal Service Connection, which is usually used under Windows 2000 Server. The user can use this function from the management terminal to log in via the GUI base to the system, on which Windows Server 2003 is installed, and implement different types of operations, including shutdown. Although Remote Desktop Connection is installed by default with Windows Server 2003, it is disabled by default. To use it, therefore, enable it after installation of the OS.

In addition, the management terminal requires a client application to establish a connection to Remote Desktop of Windows Server 2003. If the management terminal OS is Windows XP or Windows Server 2003, a connection client application has been installed by default. However, if another Windows OS is installed on the terminal, a connection client application must be installed after installation of the OS. A connection client application can be obtained free of charge from the Microsoft website. See the following URLs.

Reference URL:
- Remote Desktop Connection for Windows Server 2003 [5.2.3790] (connection client application)

http://www.microsoft.com/windowsxp/downloads/tools/rdclientdl.mspx
- Enabling and configuring Remote Desktop for management under Windows Server 2003

http://support.microsoft.com/kb/814590/

- Prerequisites:
  - The management terminal is connected to the unit via a LAN.
  - A Remote Desktop client application is installed on the management terminal.
    Remarks:
    If the remote management terminal OS is Windows XP or Windows Server 2003, a Remote Desktop client application has been installed by default on the management terminal.
- Procedure:
  - Prepare the system (Windows Server 2003) as follows (setup is required only once, in initial operation)
    If you perform batch installation using the batch installer included in the High-reliability Tools, this procedure is unnecessary.
    1. Click [Control Panel] button → [System].
    2. Select the [Remote] tab, and check the [Enable Remote Desktop on this computer] check box.

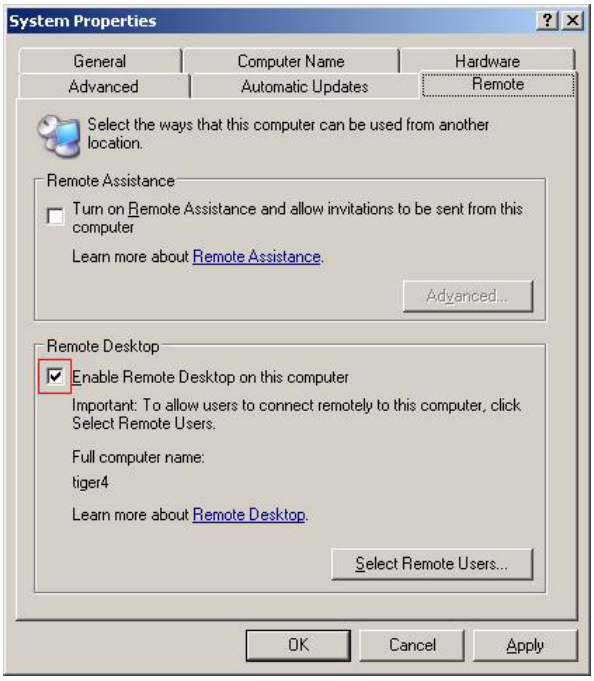


Figure 3.11 System Property sheet

Remarks:
Click the [Select Remote User] button to allow you, as required, to place a restriction regarding users who can remotely log in.

3 Click the [OK] button to enable Remote Desktop Connection.
Remarks:
If the firewall is enabled, select "Windows Firewall" and check and make the settings as follows:
- Select the [General] tab, and confirm that [Don't allow exceptions] is unchecked.
- Select the [Exceptions] tab, and check [Remote Desktop].

● Steps on the management terminal (Windows XP)

If the terminal uses a Windows version other than Windows XP, the method of starting the application may be different but the operating procedure other than the procedure of starting the application is basically the same.

1 Click [Start] button → [Programs] → [Accessories] → [Communication] → [Remote Desktop Connection].

2 Specify the computer name or IP address of the PRIMEQUEST-series machine in [Computer], and click the [Connect] button.

Figure 3.12 [Computer Name Setting] dialog box

3 The normal Windows login dialog box opens. Enter your user name and password to log in to the system.

4 As in the normal Windows shutdown procedure, click [Start] button → [Shutdown] to shut down the system.

c) Shutdown with Telnet

The user can use Telnet from the management terminal to log in via the CUI base to the system and implement operations such as shutdown.
Although the telnet service is installed by default with Windows Server 2003, it is disabled by default. Therefore, set the telnet service to auto start so that the service is enabled every time Windows Server 2003 starts. The rest of this section explains how to enable the telnet service and how to log in from the management terminal.

- Prerequisites:
  - The management terminal is connected to the unit via a LAN.
  - A Telnet connection client application is installed on the management terminal (it is installed by default with Windows 98 and later versions, but the operating method may differ slightly depending on the version).
- Procedure:
  - Prepare the system (Windows Server 2003) as follows:
    1. Click [Start] button → [Program] → [Management Tool] → [Service].
    2. Select telnet from the service list, and right-click it to display the Property sheet.

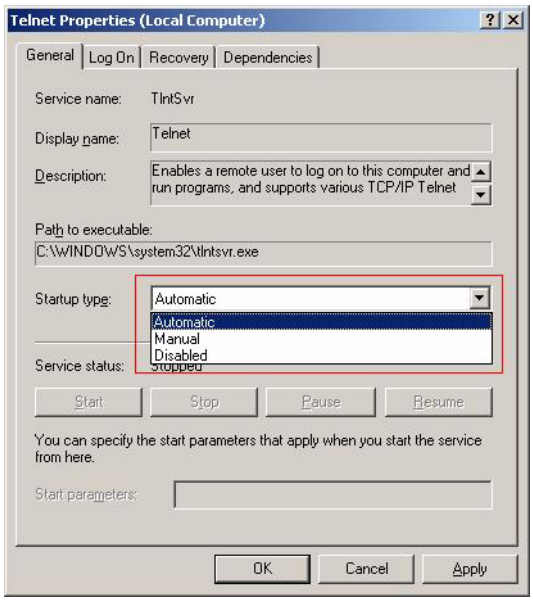


Figure 3.13 [Property] sheet

3 Select [Auto] from [Startup type].

Notes:

[Disable] is selected by default. Do not select [Manual] because the service must be started every time the server starts.

4 Click the [Start] button.

- Connection from the management terminal (Windows XP)

1 Click [Start] button → [Run], enter "telnet.exe", and click the [OK] button to start the service.

(Alternatively, start the command prompt, and enter "telnet.exe".)

2 Enter the following command to establish a connection:

```
Microsoft Telnet> o Servername (or IP Address)
```

Specify the computer name or IP address in *Servername*, (at the bottom of the window).

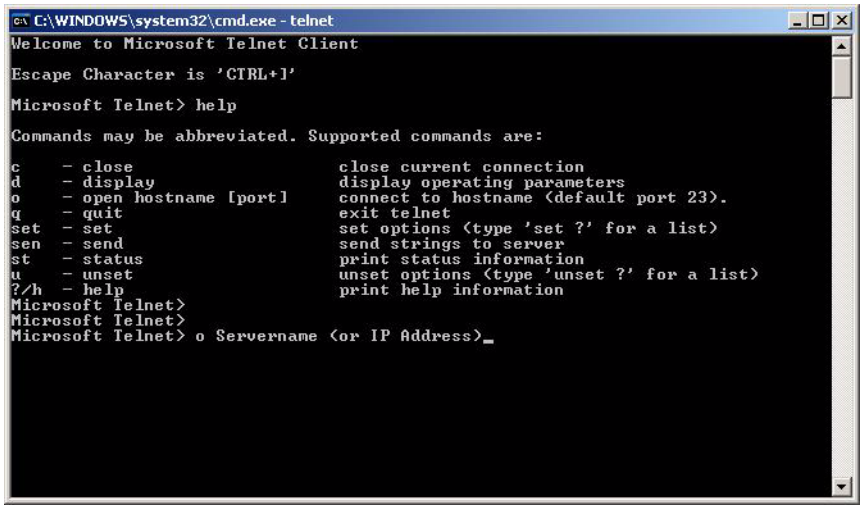


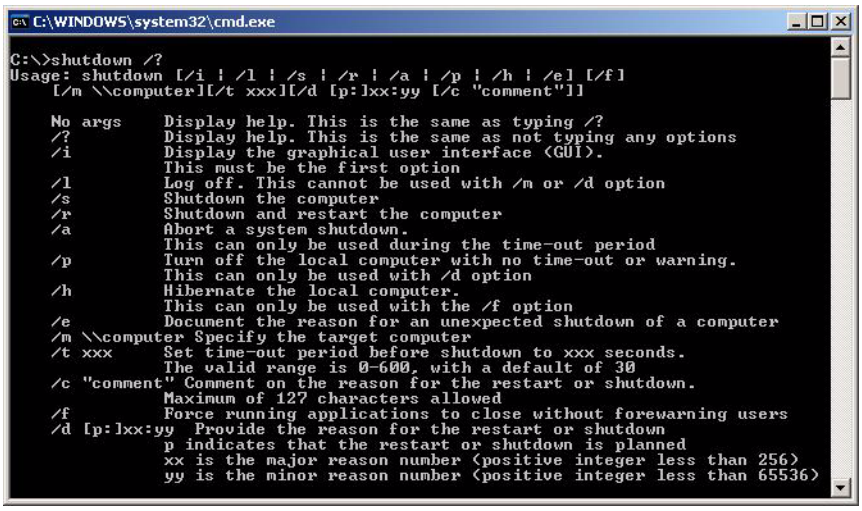
Figure 3.14 Example of entering the server name or IP address

For details on Telnet operation, display Help as shown above.

3 When a connection has been successfully established, enter your login ID and password to log in.

4 Enter the Shutdown.exe command as follows to shut down the system:

```
C: \>shutdown -s
```



```
C:\WINDOWS\system32\cmd.exe

C:\>shutdown /?
Usage: shutdown [/i | /l | /s | /r | /a | /p | /h | /e] [/f]
    [/m \\computer][/t xxx][/d [p:]xx:yy [/c "comment"]]

    No args    Display help. This is the same as typing /?
    /?         Display help. This is the same as not typing any options
    /i         Display the graphical user interface (GUI).
               This must be the first option
    /l         Log off. This cannot be used with /m or /d option
    /s         Shutdown the computer
    /r         Shutdown and restart the computer
    /a         Abort a system shutdown.
               This can only be used during the time-out period
    /p         Turn off the local computer with no time-out or warning.
               This can only be used with /d option
    /h         Hibernate the local computer.
               This can only be used with the /f option
    /e         Document the reason for an unexpected shutdown of a computer
    /m \\computer Specify the target computer
    /t xxx     Set time-out period before shutdown to xxx seconds.
               The valid range is 0-600, with a default of 30
    /c "comment" Comment on the reason for the restart or shutdown.
               Maximum of 127 characters allowed
    /f         Force running applications to close without forewarning users
    /d [p:]xx:yy  Provide the reason for the restart or shutdown
               p indicates that the restart or shutdown is planned
               xx is the major reason number (positive integer less than 256)
               yy is the minor reason number (positive integer less than 65536)
```

Figure 3.15 Shutdown.exe command

The command shown above causes a shutdown in 30 seconds. Shutdown/restart or the shutdown/restart time can be specified. For details on command operations, display Help as shown above.

3.6.1.2 Remote shutdown via a COM port connection

In special cases where the unit cannot be connected to the local area via a LAN, shutdown can be implemented by connecting the unit to the management terminal, using a serial cable via the COM port, to enable redirection to the management terminal console.

- Shutdown via an Emergency Management Service (EMS) connection

Shutdown via an EMS connection

EMS is a new Windows function added to Windows Server 2003. EMS connects the unit to the management terminal via the COM port to implement specific kinds of operations, such as shutting down the system.
To use EMS, it must be enabled on the system. It can be enabled during or after installation. This section explains how to enable it after installation. For details on how to enable it during installation, search Help in Windows Server 2003 for the explanation on how to enable EMS.

- Prerequisites:
  - The unit is connected with a serial cable to the management terminal via the COM port.
  - There is no conflict between COM port that connects the unit to management terminal and another port used by the system.
  - * Connect the COM cable to the COM port of the IO Unit

- Procedure:
  - Prepare the system (Windows Server 2003) as follows:
    1. Before enabling the EMS function, decide the boot entry(*1) in which EMS is to be enabled. (Boot entries can be listed by entering Bootcfg.exe at the command prompt.)
    2. Start the command prompt, and execute Bootcfg.exe to set EMS to ON.

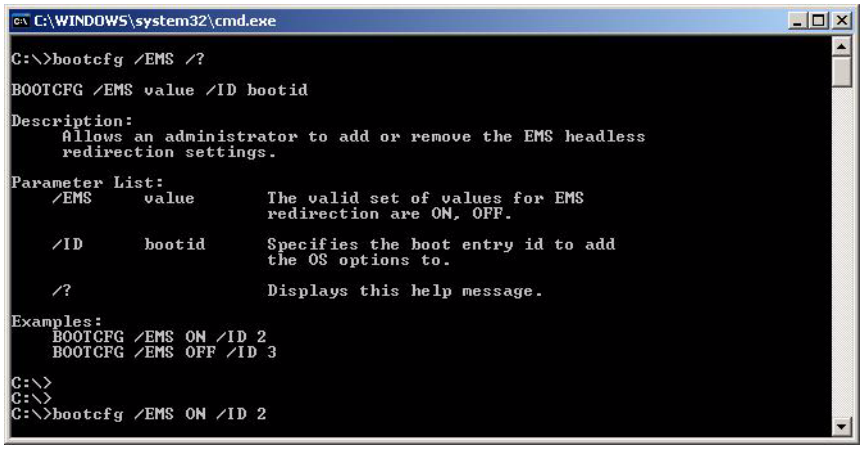


Figure 3.16 Bootcfg.exe

The command shown above enables the EMS function in boot entry ID 2.

*1 For details on editing boot entries, display Help for Bootcfg.exe. Alternatively, the EFI Shell in the boot entry selection window can similarly be used for editing. For details, see Using EFI Shell at the following URL:

Related URL:
● Using EFI Shell
http://www.intel.com/software/products/college/efishell/

- Steps on the management terminal (Windows Server 2003) (*1)

1 Click [Start] button → [Programs] → [Accessories] → [Communication], and start HyperTerminal.
Remarks:
HyperTerminal must be installed separately.

2 Enter an arbitrary name for the connection name, and select an icon.

Figure 3.17 Selecting an icon

3 Select the COM port, and set the baud rate.

- Specify the COM port to which the serial cable is connected (in the red rectangular field in the left figure below).
- Set the baud rate (in the red rectangular field in the right figure below).

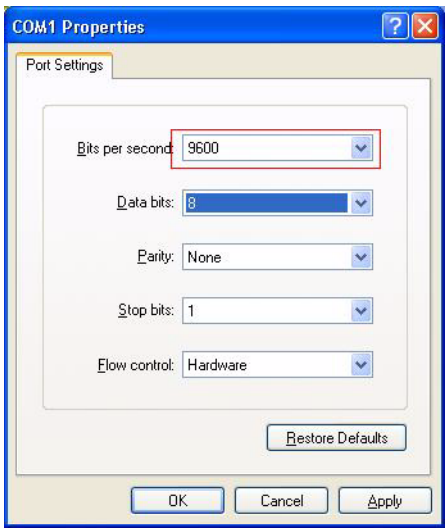


Figure 3.18 Selecting the COM port and setting the baud rate

Note:

- Set the communication speed to 19200 bits per second.
- Preset values for the port settings depend on the environment.

4 When step 3 is completed, turn on the PRIMEQUEST-series machine, and select the boot entry in which EMS is ON to boot the system.

5 Control passes to HyperTerminal, and the SAC (*2) commands can be used on the Special Administration Console. To shut down the PRIMEQUEST-series machine, enter the Shutdown command.

*1 Although steps in this procedure use HyperTerminal in Windows Server 2003, the same steps can also be performed in cases with a standard terminal connection. However, because HyperTerminal does not support UTF-8, the Japanese language is not correctly displayed. It is recommended that the other terminal software products that support UTF-8 be used.

*2 For details about the Special Administration Console and SAC commands, see Help in Windows Server 2003.

3.7 Checking Status with LEDs

The PRIMEQUEST-series machine uses LEDs to indicate information on power-on, power-off, failures, and the physical locations of components. Detailed status information on each component can be checked in the management window.
Note that all ALARM LEDs are turned on when AC power is turned on. This does not indicate any failure.

Each component is equipped with the following LEDs:

- Power LED (Green)

This LED indicates the component power status or that hot swapping of the component is in progress. A hot-swappable component can be removed while the LED is off.

- Alarm LED (Orange)

This LED indicates whether the component is faulty.

- Location LED (Blue)

This LED indicates the mounting location of the component. The LED is equipped with display functions to assist hot swapping, and the user can set each function to ON or OFF.

Remarks:

See the *PRIMEQUEST 510A System Design Guide* (C122-B018EN) for details on the meanings of the LED status display. Also, see Chapter 2, "Physical Locations of Components" in the *PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/ Operation Information* (C122-E074EN) for details on the physical installation location of each component, and Chapter 10, "Status Confirmation from LED" in the *PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/Operation Information* (C122-E074EN) for details on checking the LED status on the system.

3.8 UPS Operation

This section explains as follows connections of an uninterruptible power supply unit (UPS) for a means of power-off:

- UPS connections (→ 3.8.1)
- Settings for UPS connections (→ 3.8.2)

3.8.1 UPS connections

The PRIMEQUEST 510A has ports on the baseboard (BB) as interfaces for external UPSs. Two ports are provided to support dual power feed.
The PRIMEQUEST-series machine supports dual power feed as an option. When connecting a UPS to use this option, connect the UPS to the respective power supply system.

- Single power feed

Connect a UPS to the UPC0 connector on the main unit of the PRIMEQUEST-series machine.

- Dual power feed

Connect one UPS to each of the UPC0 and UPC1 connectors on the BB. The UPS connected to the UPC0 connector functions as a System 0 UPS, and the one connected to the UPC1 connector functions as a System 1 UPS. In other words, the UPS connected to UPC0 connector on the BB must be connected to the System 0 AC connector on the main unit of the PRIMEQUEST, using an AC cable. The one connected to UPC1 connector must be connected to the System 1 AC connector on the main unit of the PRIMEQUEST, using an AC cable.

The following figure shows the concept of UPS connections.

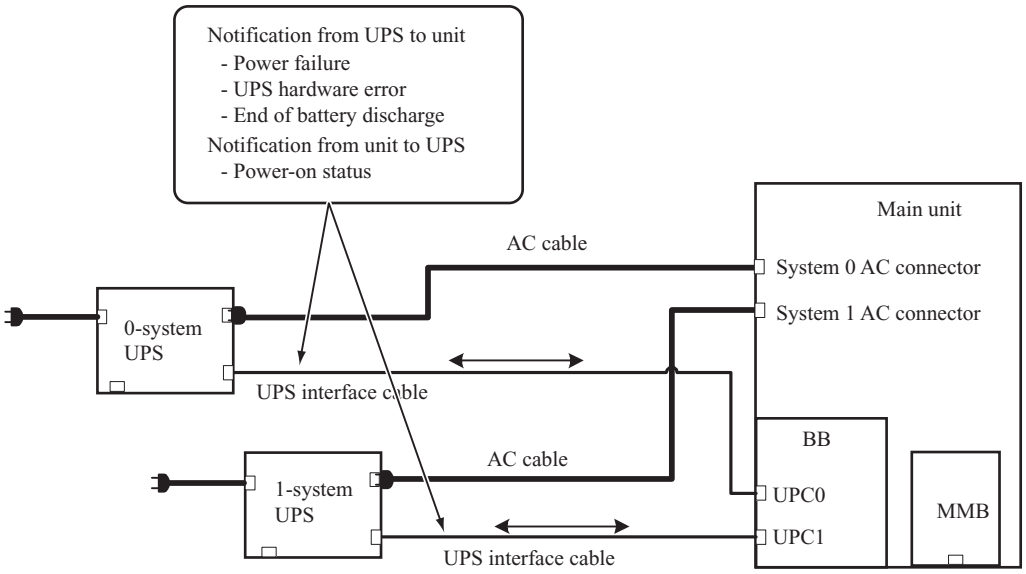


Figure 3.19 Concept of UPS connections

Remarks: For details on the UPS connections, see the *PRIMEQUEST 510A Installation Planning Manual* (C122-H003EN).

3.8.2 Settings for UPS connections

This section explains how to make settings for UPS connections.

Procedure

1 Log in to MMB Web-UI.
The MMB Web-UI window is displayed.

2 Select [System] → [System Setup] from the MMB menu.
The [System Setup] window is displayed.

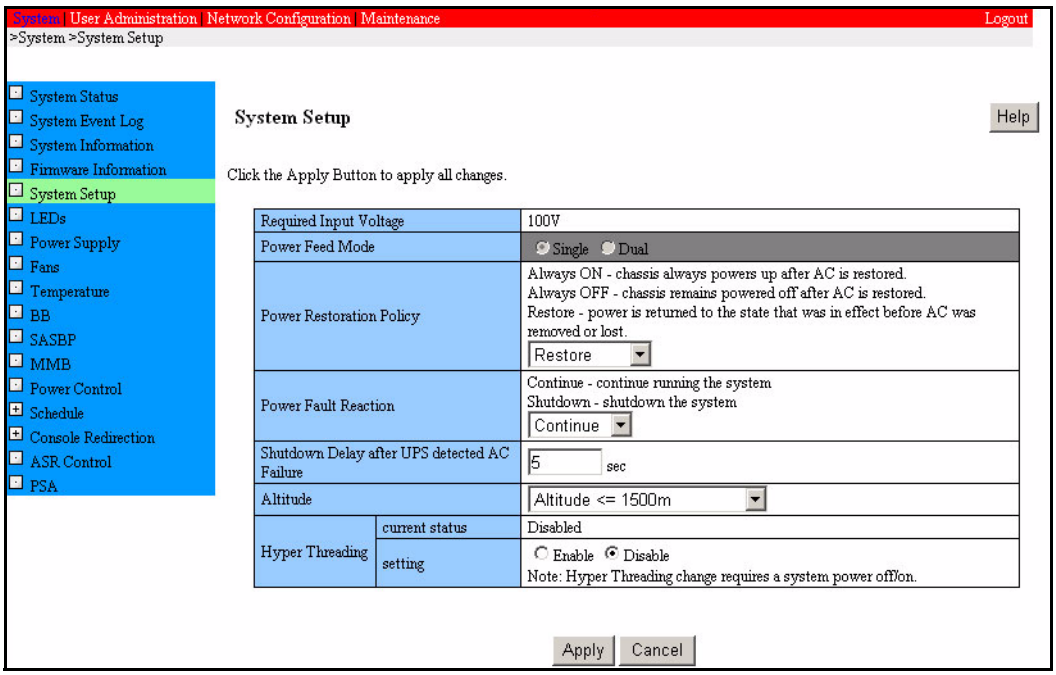


Figure 3.20 [System Setup] window

3 Set the time in [Shutdown Delay after UPS detects AC Failure], and click the [Apply] button.

Explanation of the [System Setup] window

Table 3.8 Displayed and setting items in the [System Setup] window

Item	Description
Power Feed Mode	Specify the power feed mode (single power feed or dual power feed) of the PRIMEQUEST system: • [Single] (single power feed mode) • [Dual] (dual power feed mode) Note: Dual (dual power feed) is valid only when the input voltage is 200 V. When the input voltage is 100 V, Power Feed Mode is grayed out and cannot be selected. Remarks: This operation is performed by a Fujitsu certified service engineer. Default: [Single]
Power Restoration Policy	Specify the power operation performed after power recovery following power outage: • [Always off]: Keep the power off after power recovery. • [Always on]: Turn the power on after power recovery, regardless of whether it was on or off at the time of power outage. • [Restore]: Restore the power state in effect at the time of power outage. In other words, if the power was on at that time, turn the power on again, and if the power was off, keep the power off. Default: [Restore]
Power Fault Reaction	Specify the action to be performed if redundancy is lost (or the system displays the action): • continue: Continue server operation even if redundancy is lost. • shutdown: Shut down the system if redundancy is lost. Default: [continue]
Shutdown Delay after UPS detected AC Failure	Specify the delay between UPS detection of power outage and OS shutdown start. If AC recovery is completed within this delay time, the OS shutdown is not performed. Specify a number ranging from 0 to 9999 seconds. Default: 5 s

Item	Description
Altitude	Specify in units of 100 meters the altitude at which the PRIMEQUEST system is to be installed. • Altitude < = 1500 m • 1500 m < Altitude < = 2000 m • 2000 m < Altitude < = 2500 m • 2500 m < Altitude Default: Altitude < = 1500 m Remarks: Setting an altitude enables precise detection of abnormal intake temperatures.

Part II PRIMEQUEST Functions

CHAPTER 4 Overview of PRIMEQUEST Functions

4.1 List of the Functions

Since the MMB performs integrated management for PSA and the GSWB in the PRIMEQUEST-series machine, the user can operate the PRIMEQUEST-series machine via the MMB Web-UI from a general-purpose PC connected to the management LAN without using a special console.

The MMB Web-UI provides the system administrator and user with functions for operating the PRIMEQUEST-series machine. This section describes the functions provided by the Web-UI of the PRIMEQUEST-series machine.

System

Table 4.1 Functions provided by MMB Web-UI (system)

Function	Reference
Displays the status of the entire system.	5.2.1, "[System Status] window"
Displays events that are saved in the SEL (System Event Log) of the MMB.	5.2.2, "[System Event Log] window"
• Displays information on the PRIMEQUEST system. • Set a name for the PRIMEQUEST system (cabinet) • Set asset tag.	5.2.3, "[System Information] window"
Displays a firmware version.	5.2.4, "[Firmware Information] window"
Sets a system setup.	5.2.5, "[System Setup] window"
Displays LED status.	5.2.6, "[LEDs] window"
• Displays the status of system internal power supply unit. • Displays reaction to a power supply unit failure.	5.2.7, "[Power Supply] window"

Function	Reference
• Displays the status of system internal fan. • Displays reaction to a fan failure.	5.2.8, "[Fans] window"
• Displays the temperature of system internal temperature sensor • Displays reaction to an abnormal temperature.	5.2.9, "[Temperature] window"
Displays and sets the status of BB board.	5.2.10, "[BB] window"
Displays and sets the status of SASBP board.	5.2.12, "[SASBP] window"
Displays MMB related information.	5.2.13, "[MMB] window"
• Performs power control. • Controls system boot.	5.2.14, "[Power Control] window"
Specifies whether the system is put in scheduled operation.	5.2.15.1, "[Schedule Control] window"
Sets the power-on/off schedule for the system.	5.2.15.2, "[Schedule List] window"
Sets the serial output destination of the system.	5.2.16.1, "[Console Redirection Switch] window"
Displays system console output.	5.2.16.2, "[Console Redirection] window"
Sets conditions for executing system automatic reboot.	5.2.17, "[ASR (Automatic Server Restart) Control] window"
Displays an outline of system and OS information.	7.2, "[OS Information] Window"
Lists CPU information.	7.3, "[CPUs] Window"
Lists memory information.	7.4, "[DIMMs] Window"
Displays information on the connected PCI devices.	7.5, "[PCI Devices] Window"
Displays the network status in the system.	7.6.1, "[Network Interfaces] window"
Displays the routing status in the system.	7.6.2, "[Network Routing] window"
Displays disk partition information.	7.7, "[Disk Partitions] Window"
List hard disk information	7.8, "[Hard Disks] Window"
• Lists process information • Transmits signals to the specified process.	7.9, "[Process List] Window"

Function	Reference
Displays the contents of major system files.	7.10, "[System File] (Selection) Window"
Lists the system hardware components (BB, CPU, DIMM, PCI device).	7.11.1, "[Hardware Inventory] window"
• Displays OS versions, displays a listing of RPM packages with detail information • Downloads RPM package list information to the terminal.	7.11.2, "[Software Inventory] window"
Logs various PSA actions (log output, REMCS transmission, SNMPtrap transmission etc.)	7.12, "[Agent Log] Window"
Downloads the SEL files held by the system.	7.13, "[SEL] Window"
• Saves the current configuration and status in the system to a file on the system. • Downloads an export file to the terminal.	7.14, "[Export List] Window"
Makes settings for Software Watchdog and Boot Watchdog.	7.15.1, "[Watchdog] window"
Specifies whether to enable the hard disk's S.M.A.R.T function for monitoring and detect predictive signs of failure.	7.15.2, "[S.M.A.R.T.] window"
Displays information on the connected expansion file unit.	7.16, "[Expansion File Unit] Window"

User

Table 4.2 Functions provided by MMB Web-UI (user)

Function	Reference
Displays, edits, and deletes a list of registered user accounts.	5.3.1, "[User List] window"
Information on currently registered user accounts is displayed.	5.3.2, "[Change Password] window"
Displays a user who is connected to MMB Web-UI.	5.3.3, "[Who] window"

Network/Security

Table 4.3 Functions provided by MMB Web-UI (network/security)

Function	Reference
Sets the MMB date and time.	5.4.1, "[Date/Time] window"
Sets an IP address for accessing the MMB.	5.4.2, "[Network Interface] window"
Sets an MMB-HUB port	5.4.3, "[Management LAN Port Configuration] window"
Makes settings related to MMB network protocol.	5.4.4, "[Network Protocols] window"
Sets an HTTP/HTTPS screen-refresh rate.	5.4.5, "[Refresh Rate] window"
Sets SNMP community.	5.4.6.1, "[SNMP Community] window"
Sets a destination to send an SNMP trap.	5.4.6.2, "[SNMP Trap] window"
Sets an SNMP v3 specific engine ID and user.	5.4.6.3, "[SNMP v3 Configuration] window"
Creates a private key and then creates a CSR (signature request) for it.	5.4.7.1, "[Create CSR] window"
Exports a private or CSR (signature request) key stored on the MMB.	5.4.7.2, "[Export Key/CSR] window"
Imports to the MMB an electronic certificate with a signature sent from the certification authority.	5.4.7.3, "[Import Certificate] window"
Creates a self-signed certificate.	5.4.7.4, "[Create Selfsigned Certificate] window"
Creates an SSH server private key.	5.4.8.1, "[Create SSH Server Key] window"
Sets a user required to control the MMB from a remote terminal with RMCP.	5.4.9, "[Remote Server Management] window"
Sets IP filtering to enable connection.	5.4.10, "[Access Control] window"
Sets notification by e-mail for an event occurrence in the system.	5.4.11, "[Alarm E-Mail] window"

Maintenance

Table 4.4 Functions provided by MMB Web-UI (maintenance)

Function	Reference
Updates MMB firmware. (*1)	5.5.1.1, "[MMB Firmware Update] window"
Updates PAL and SAL. (*1)	5.5.1.2, "[PAL/SAL Firmware Update] window"
Updates EFI. (*1)	5.5.1.3, "[EFI Firmware Update] window"
Updates BMC firmware. (*1)	5.5.1.4, "[BMC Firmware Update] window"
Backs up and restores MMB configuration information.	5.5.2.1, "[Backup/Restore MMB Configuration] window"
Backs up EFI configuration information.	5.5.2.2, "[Backup/Restore EFI Configuration] window"
Maintenance in wizard format	5.5.3, "[Maintenance Wizard] window"
Specifies settings for the Remote Customer Support System (REMCS) service.	5.5.4, "REMCS menu"

*1: This function is used by Fujitsu certified engineer.

4.2 MMB functions

Figure 4.1 shows the PRIMEQUEST main functions. The "MMB" part at left of the figure shows the MMB main functions.

This section explains each function of the MMB.

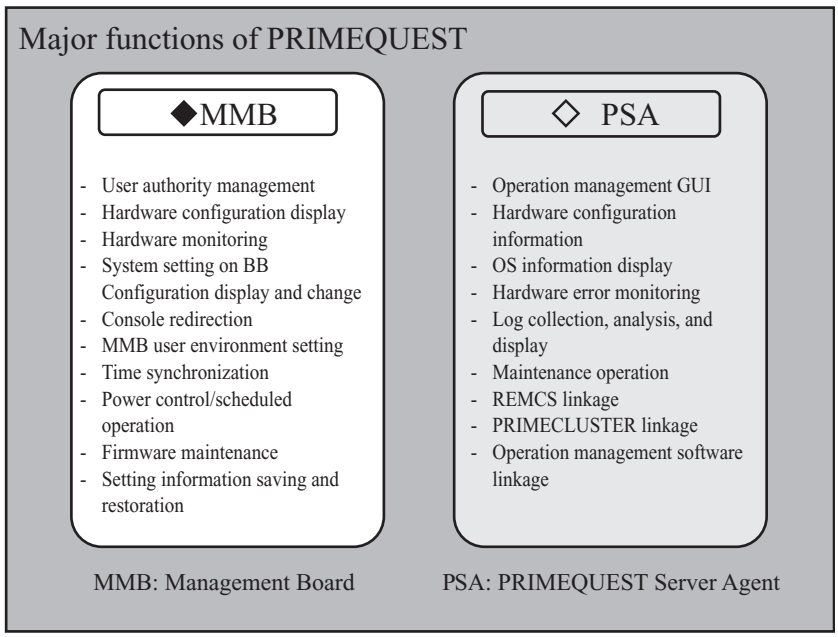


Figure 4.1 MMB main functions

User authority management

The user authorities for accessing the MMB are classified into "User," "CE," "Operator," and "Administrator," where a system account such as a user name and authority needs to have been registered. An operator can use functions that correspond to his or her authority. See Section 2.7, "User Privilege Levels" for details.

Hardware configuration display

This function displays the hardware configurations and status.

The function displays the configurations of all components such as SBs and IO Units and of CPU, memory, and HDD units in each component, including fans and power system units mounted on PRIMEQUEST series machines.

The configuration information also displays the status of each component. This status information includes, for example, the indication of normal and abnormal states. The display of some of these states may require corrective action on the part of the system administrator and the maintenance engineer. Detailed information can be displayed by following a link in the display item column.

Hardware monitoring

This function monitors the system for hardware failures and abnormalities.

Hardware failures and abnormalities are detected with a variety of checkup features and sensors. When a failure or abnormality is detected, the required corrective action is taken according to such hardware configuration conditions as the detection location and redundant configuration. The system collects all logs including those for cases where processing can be resumed by replacing or disconnecting the pertinent hardware components and logs error messages.

An LED will go on depending on the extent of the failure or abnormality. The error is posted by e-mail if there is a setting for this type of posting. The indication destinations include a system administrator, the operation management application, and the REMCS center.

All logs and messages can be displayed with a filter to reduce the size of the display. The conditions under which abnormal states are to be detected can also be set.

Console redirection

This function switches the input-output destination of the console information over to the management LAN. The two methods below are available for implementing OS input-output.

- Using the BMM COM port
- Using the management LAN that is connected via the MMB

To redirect to the management LAN, the terminal connected to it can be used as a console.

Setting of MMB user environment

This function sets and changes the MMB user environment.

- Unification of system accounts
  The MMB have interfaces such as a Telnet and Web-UI whose system account is collectively managed by the MMB.

- User management
  This function manages user authorities for accessing the MMB.
- Network environment setting and change
  This function sets the MMB user environments such as a HTTP and Telnet.
- Access control
  To maintain security, this function sets an IP filter to enable MMB access (to set a usable IP address for each protocol). Only set IP addresses enable MMB access.
- SSL support
  This function encrypts Web and Telnet access with SSL (Secure Sockets Layer). It creates a private key and an electronic certificate.

Time synchronization

Synchronizes the time.

By using the NTP server function or NTP client function, the system time can be synchronized with the MMB time. Also, by accessing an external NTP server, the time can also be synchronized with another NTP server time.

Power control/scheduled operation

This function sets a schedule for turning on and off the power to the system and automatically controlling the operation according to such schedule.

Firmware maintenance

This function updates a variety of firmware. The update operation is performed by a certified service engineer. The following firmware is subject to updating.

- MMB firmware (mounted on the MMB)
- BMC firmware
- PAL/SAL/EFI firmware

Saving and restoring setting information

These functions save and restore the EFI setting information and the MMB setting information.

The MMB provides a function for setting and restoring the EFI setting information.

These functions can be used to do the following:

- After the EFI is set from the EFI Boot Manager menu, the EFI setting information can be saved.
- If a problem occurs with a BB and the BB is replaced, the system can be recovered from the saved EFI setting information.
- The configuration information saved in a system can be restored or copied to another system.

The saved information can be stored on a remote terminal. The data saved to the remote terminal can also be restored.

In addition to the function for the EFI configuration information, a save/restore function for the MMB configuration information is also provided.

4.3 Setting and Checking Log Information

This section explains how to operate log information.

4.3.1 Log information types

The events that occurred in the PRIMEQUEST system are saved in the SEL (System Event Log) of the MMB and can be checked in the Event Log window.

4.3.2 Checking a log of events that occurred in the PRIMEQUEST system

Out of the events that occurred in the PRIMEQUEST system, those that are currently saved in the SEL (System Event Log) of the MMB can be checked.

The SEL can save 1,000 or more events. When a system event log becomes full of entries, the oldest event log is deleted and the newly generated event log is saved in the SEL.

In the [System Event log] window, it is possible to filter an event to be displayed in the window, download event data that is saved in the SEL, and clear all events that are saved in the SEL.

The functions are explained in the following procedures.

- Checking event logs
  (→ 5.2.2, "[System Event Log] window")
- Clearing all events that are saved in the SEL
  (→ 5.2.2, "[System Event Log] window")
- Downloading event data that is saved in the SEL
  (→ 5.2.2, "[System Event Log] window")
- Filtering an event to be displayed
  (→ 5.2.2.1, "[System Event Log Filtering Condition] window")
- Displaying event details
  (→ 5.2.2.2, "[System Event Log (Detail)] window")

4.3.2.1 Checking event logs

Procedure

1 Click [System] → [System Event Log].
The [System Event Log] window is displayed.

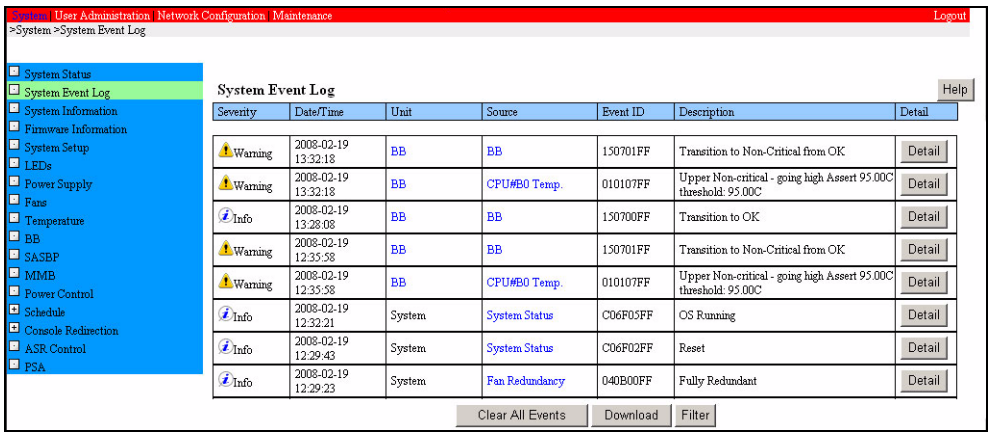


Figure 4.2 [System Event Log] window

2 Check the description.
To clear all events that are saved in the SEL, click the [Clear All Events] button.
To download event data that is saved in the SEL, click the [Download] button. To select an event to be displayed in the window, click the [Filter] button.
Click the [Detail] button to display the detailed window of the events corresponding to the button.
See Sections 4.3.2.2 to 4.3.2.5 for details on each operation.
To cancel these settings to return to the previous state, click the [Cancel] button.

Remarks:
An error that occurred during operation can be reported by e-mail. See Section 5.4.11, "[Alarm E-Mail] window" for details on specifying whether to report errors and setting the error level and report destination.

Explanation of [System Event Log] window

Table 4.5 Displayed and setting items in the [System Event Log] window

Item	Description
Severity	Displays the severity of an event and error. • [Error]: Important problem such as hardware problem • [Warning]: Event not always important but likely to be a problem in the future • [Info]: Event as information
Date/Time	Displays in the local time the date and time when an event or error occurred. Format: yyyy-MM-dd HH:mm:ss
Unit	Displays the unit containing a sensor by which an event or error was detected. Example: If an error occurred in CPU #A0, "BB" is displayed. Clicking on the indicated unit displays the information window (the window indicating the individual parts number and serial number of the unit) for that unit.
Source	Displays the name of the sensor that detected an event or an error. Clicking on the indicated sensor name displays either a window indicating the sensor status, or the information window for the unit containing the sensor.
Event ID	Displays an ID (eight-digit hexadecimal number) that identifies an event. If no suitable ID exists, "-" is displayed.
Description	Displays event or error details. For a sensor for which something other than [Trig Offset] is indicated for event data, the event data itself is displayed. Example: Sensors for which [R] and [T] is indicated: The reading and limit values at the time an event occurred are displayed. Notes: If the event involves board insertion or removal, the part number and serial number of the board are displayed.
Detail	Detail button of each event

4.3.2.2 Clearing all events that are saved in the SEL

Procedure

1. Click the [Clear All Events] button in the [System Event Log] window.
   A confirmation dialog box is displayed.
2. Click [OK].
   All events are cleared.
   To cancel the clearance, click [Cancel].

4.3.2.3 Downloading event data that is saved in the SEL

The event data that is saved in the SEL is required for a Fujitsu certified service engineer to analyze the system status.

Remarks:
You may be requested to download the event data and submit it to the Fujitsu certified service engineer.

Procedure

1. Click the [Download] button in the [System Event Log] window.
   A dialog box for specifying a saving file path name is displayed.
2. Enter the path name.
   Event data that is saved in the SEL is downloaded onto a PC with the Web-UI window displayed.

4.3.2.4 Filtering an event to be displayed

Procedure

1 Click the [Filter] button in the [System Event Log] window.
The [System Event Log Filtering Condition] window is displayed.

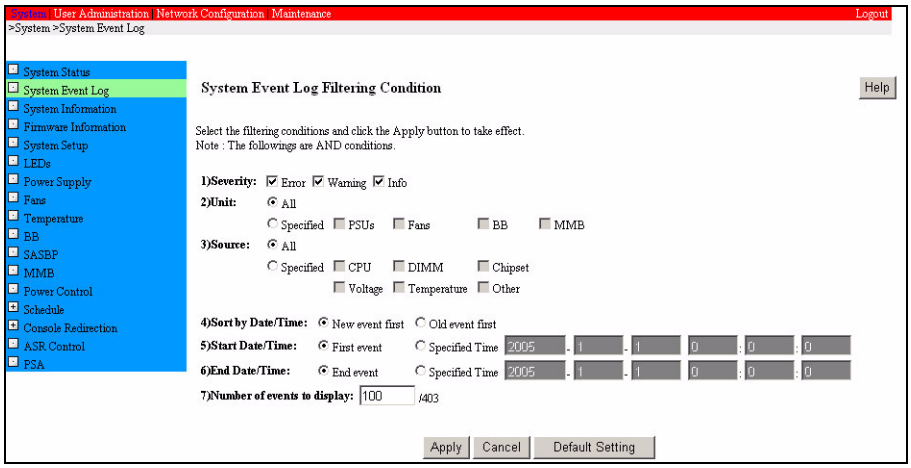


Figure 4.3 [System Event Log Filtering Condition] window

2 Specify filtering conditions and click the [Apply] button.
The [System Event Log] window is restored showing the events that satisfy the selection conditions.
Click the [Cancel] button to cancel the specified selection conditions and redisplay the [System Event Log] window.

Explanation of [System Event Log Filtering Condition] window

Table 4.6 Displayed and setting items in the [System Event Log Filtering Condition] window

Item	Description
Severity	Selects with a check box the severity level to be displayed. More than one can be selected. • [Error]: Important problem such as hardware problem • [Warning]: Event not always important but likely to be a problem in the future • [Info]: Normal event Default: All
Unit	Selects units to be displayed using the radio button of [All] or [Specified]. • Select [All] to not implement filtering by unit. • When [Specified] is selected, filtering by unit can be set; select the check box of a unit whose event you want to display. Default: [All]
Source	Selects a source to be displayed. Select [All] or [Specified] with the radio button. • Select [All] to not implement filtering by source. • When [Specified] is selected, filtering by source can be set; select the check box of a source whose event you want to display. Default: [All]
Sort by Date/ Time	Selects the radio button for "Sorting from oldest to most recent" or "Sorting from most recent to oldest." Default: New event first
Start Date/Time	Specifies the start time for the range of events to be displayed. The first event or Date/Time can be selected with a radio button. Default: First event
End Date/Time	Specifies the end time for the range of events to be displayed. The last event or Date/Time can be selected with a radio button. Default: End event
Number of events to display	Specifies the number of logs to be displayed. The denominator displays the total number of events logged. The total number of saved events can be displayed. Default: 100 logs

4.3.2.5 Displaying event details

Procedure

1 Click the [Detail] button of an event whose details are to be displayed.
The [System Event Log (Detail)] window is displayed.

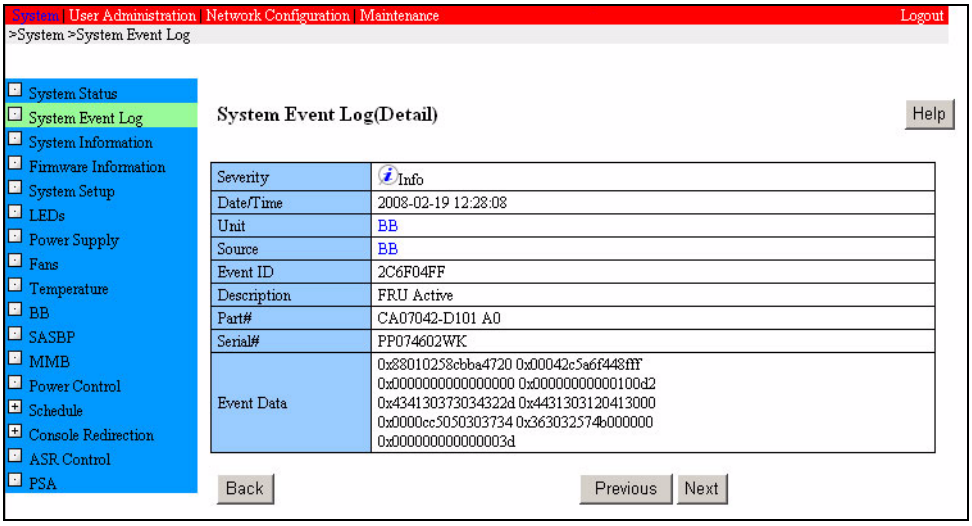


Figure 4.4 [System Event Log (Detail)] window

2 Click a corresponding operator button.
[Back] button: Returns to the System Event Log window.
[Previous] button: Displays the detail information of the previous event in the System Event Log window. Instead of the order of events in the actual SEL, only the events displayed in the System Event Log window are handled.
[Next] button: Displays the detail information of the next event in the System Event Log window.

Explanation of [System Event Log (Detail)] window

Table 4.7 Displayed and setting items in the [System Event Log (Detail)] window

Item	Description
Severity	Displays events and error severities. • [Error]: Important problem such as hardware error • [Warning]: Event that is not always important but may lead to a problem in the future • [Info]: Normal event
Date/Time	Displays in the local time the date and time when an event or error occurred. Format: yyyy-MM-dd HH:mm:ss
Source	Displays the unit containing a sensor by which an event or error was detected. Example: If an error occurred in CPU #A0, "BB" is displayed. Clicking on the indicated unit displays the information window (the window indicating the individual parts number and serial number of the unit) for that unit.
Unit	Displays the name of the sensor that detected an event or an error. Clicking on the indicated sensor name displays either a window indicating the sensor status, or the information window for the unit containing the sensor.
Event ID	Displays an ID (eight-digit hexadecimal number) that identifies an event. If no suitable ID exists, "-" is displayed.
Description	Displays event or error details. If the event involves board insertion or removal, the part number and serial number of the board are displayed.
Part#	Part# of a component whose event is created. If Part# is not available, "-" is displayed.
Serial#	Serial number of a component whose event is created
Event Data	Hexadecimal display of [Event Data]

4.4 Console Operation

This section explains console redirection.

4.4.1 Overview of console redirection

Console redirection function

This function redirects console output and EFI console output for the COM port of the OS, to a Telnet/SSH client via the MMB.

Console redirection configuration

A Zircon chip mounted on the BMM board provides a serial interface for the OS and EFI. The OS and EFI provide console output to the serial interface in the same manner as for the usual serial output.

The MMB performs a serial over LAN conversion for the serial output onto a private LAN and reports the serial output to the MMB.

The MMB sends the serial output to the Telnet/SSH client. Conversely, input from the Telnet/SSH client is reported to the OS and EFI via the Zircon.

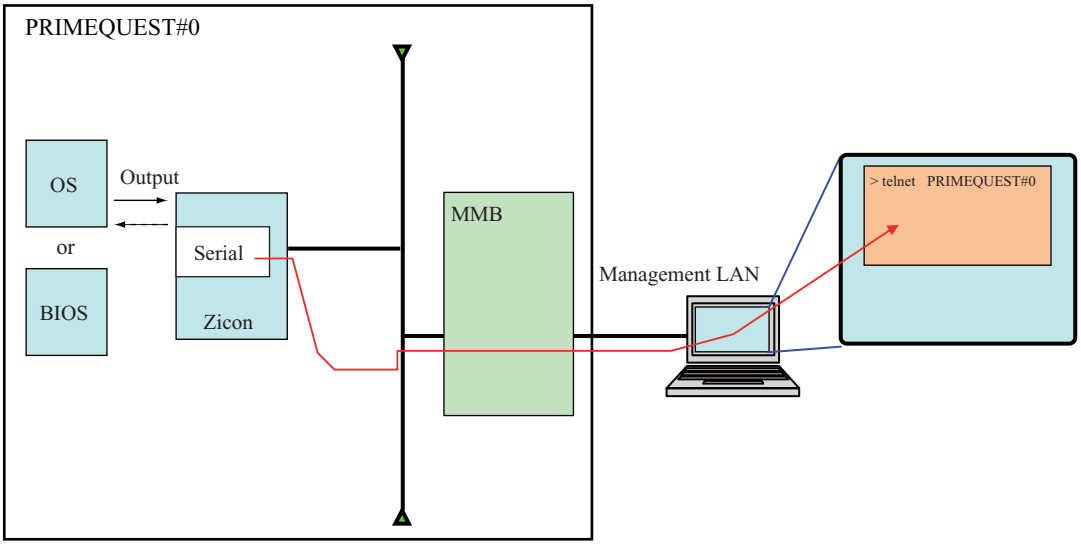


Figure 4.5 Concept of console redirection

4.4.2 MMB settings of console redirection switch

A console redirection switch is set to redirect the serial output of the system to the MMB side.

1 Click [System] → [Console Redirection] → [Console Redirection Switch].
The [Console Redirection Switch] window is displayed.

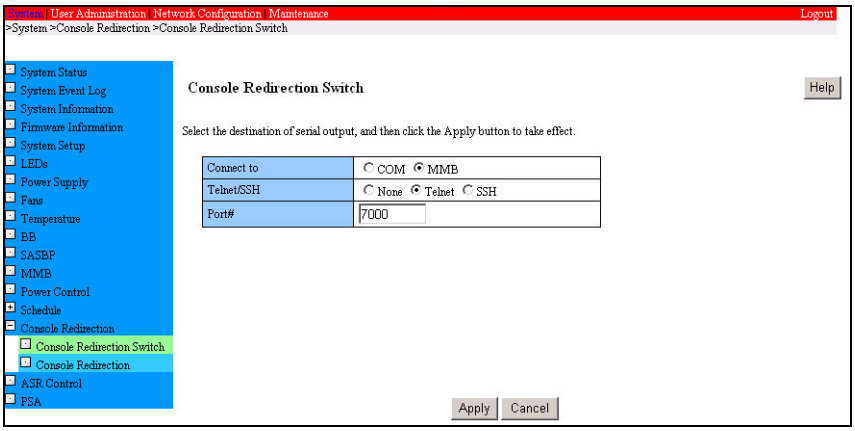


Figure 4.6 [Console Redirection Switch] window

2 Enter the required items.
Remarks:
To display the console redirection window from the MMB Web-UI, select an MMB in [Connect to].

3 Click the [Apply] button.

Explanation of [Console Redirection Switch] window

Table 4.8 Displayed and setting items in the [Console Redirection Switch] window

Item	Description
Connect to	Specifies whether to send an OS serial output to an IO Unit COM port or redirect it to a remoter client via an MMB. • [COM]: Outputs to COM port. • [MMB]: Redirects to remote client via MMB. Default: [COM]
Telnet/SSH	Select from Telnet/SSH a protocol used for remote client to connect to the console redirection. • [Telnet] • [SSH] • [None] If [None] is selected, only the Web-UI console redirection window can be displayed.
Port	As port numbers for remote client to connect to the console redirection, 1,024 or more port numbers can be entered.

Remarks:

To connect to the console redirection in Figure 4.6, enter the command as indicated below in the terminal software of the remote client.

```
#
# telnet <IP-address-of-MMB> 7000
```

4.4.3 Telnet/SSH user procedure

This section explains the procedure for referring to the serial output via an MMB using Telnet/SSH from the remote PC.

1 Specify the relevant port number.
The login prompt for certification is displayed from the MMB.
Remarks:
When using Telnet/SSH, specify the port number assigned to the MMB IP address. Set the relevant port number in advance using [Console Redirection Switch].
Example: Enter the port number as follows.

```
telnet <IP-address-of-MMB> <port-number>
```

2 Enter the MMB account/password.
Input-output to the COM port is enabled.

4.4.4 Buffering of console redirection

The MMB has a screen buffer for the console redirection. The screen buffer size that can be set on the client terminal is as follows:

- Screen width: 80 only
- Screen height: Up to 512 lines

When the screen buffer is used to connect to the console redirection, the screen image that was output before to the COM port from the system can be displayed.

Example: When Linux, which was operating, failed

Connect to the console redirection via the MMB by using Telnet/SSH from the remote PC.

When the connection to the console redirection is completed, the MMB sends to the Telnet/SSH client on the remote PC, the screen buffer output that is set in the system.

Even if the connection to the console redirection is made later by using this function, the earlier COM port output can be viewed with the preset screen buffer output.

4.4.5 Console redirection to Web-UI

A console redirection to the Web-UI is provided as an interface to view only the console redirection output.

Note:

The Console Redirection window may not be displayed normally because the following restrictions apply to it:

- Because the Console Redirection window outputs escape sequences without modification, the window display is not the same as that output on the terminal in the following cases:
  - Operation is performed using the delete, back space, page up or page down keys.
  - The ls command is executed on the OS Console (the beginning of the prompt is not normally displayed).
  - Colored characters are displayed.
- The Console Redirection window is displayed using character code set ISO-8859-1. If any character that is not supported is included in the display window, the contents of the [Console Redirection] window may not be displayed normally.

The COM port output that is buffered on the MMB side can be viewed.

Because this output is not automatically updated, it is necessary to manually refresh the screen to view the latest information or enable the automatic refreshing function.

Remarks:

Specify a refresh rate in [Refresh Rate] in the [Network Configuration] menu. By default, "Automatic Refresh = Disable" is selected. See Section 5.4.5, "[Refresh Rate] window," for details on the operation.

1 Click [System] → [Console Redirection] → [Console Redirection] in the MMB menu.
The system console output is displayed. The console enables the output, but not the input.

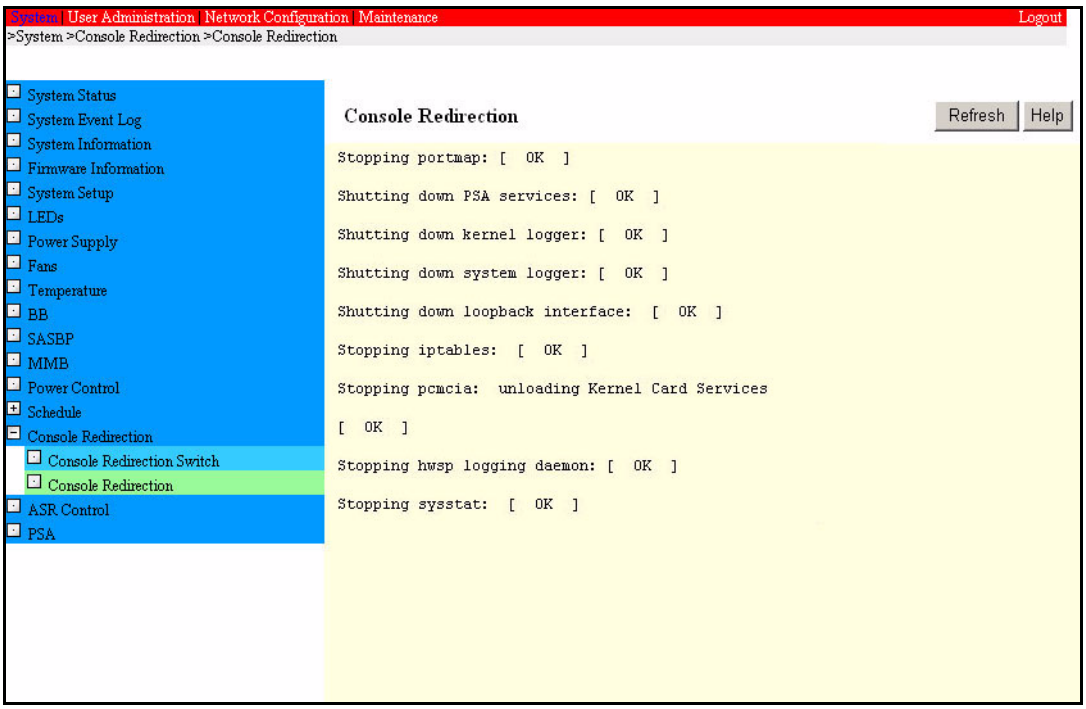


Figure 4.7 [Console Redirection] window (console output window)

Remarks:
If the output destination of the serial output port is set to the COM port instead of the MMB, the console output cannot be displayed; therefore, the following window is displayed.

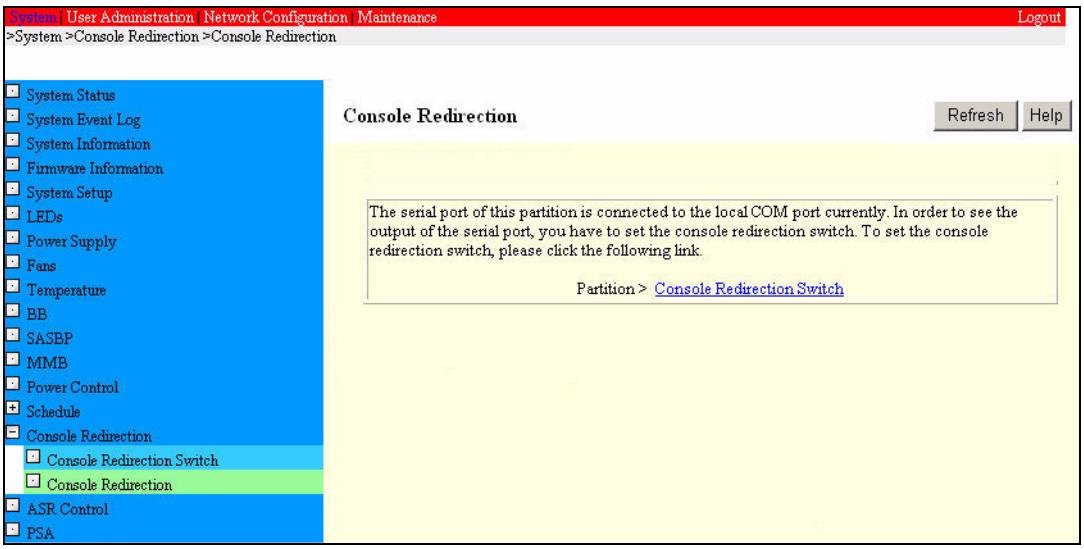


Figure 4.8 [Console Redirection] window (when the output destination is set to the COM port)

.

4.5 PSA Functions

Figure 4.9 shows the major functions of PRIMEQUEST. The major PSA functions are shown in the right column in the figure.

This section explains the PSA functions individually.

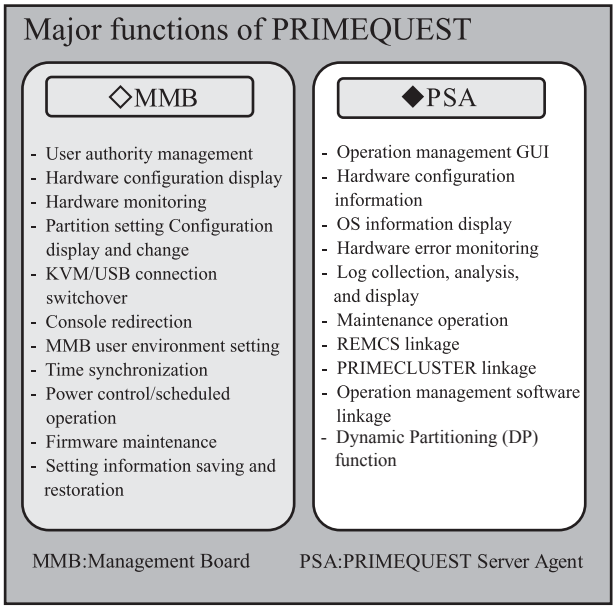


Figure 4.9 Major PSA functions

Operation management GUI

The operation management GUI is a Web-UI function used for OS operation control.

PSA that is installed on the OS cooperates with MMB firmware, by which system information on the BB can be displayed and controlled from the MMB Web-UI, without the need for the system on the BB to have the Web server function.

Upon receipt of a request from the user, MMB firmware distributes the corresponding Web screen. PSA further collects information according to the request from the system on the BB and displays it on the Web screen.

Remarks:

The functions listed below are supported by the Command Line Interface (CLI) so that command line operation and script operation can be performed from the OS console. For more information, see CHAPTER 6, "CLI Operations."

- SAF_TE operator command (used by a Fujitsu certified service engineer for disk hot-swapping)

- PSA start/stop command
- PSA investigation data collection command
- Filter definition update command
- Local partition number acquisition command
- Serial number acquisition command
- SNMP security setting command
- Get firmware information command

Hardware configuration management

This function displays the hardware resources. The following types of configuration information can be displayed:

- BB configuration
- CPU configuration (maximum number of CPUs that can be mounted, CPU mounting locations, and CPU identification information)
- Memory configuration (memory mounting locations and detail information including memory types)
- PCI configuration (PCI card installation, PCI device installation, detail information including PCI device types, and error status)
- SCSI/FC connection device configuration (HDD, tape, and others)
- Network configuration (network interface, and error status)

OS information display

This function displays information on the installed OS.
The following types of information can be displayed:

- OS information (OS type, OS version, and package installation information)
- Storage configuration information (device and capacity)
- Network configuration information (interface, connection status, speed, and routing information)
- OS status (operating hours and number of logins)
- Process list display

Hardware error monitoring

This function monitors the system for hardware errors.

PSA monitors PCI cards, error information output by SAS device drivers, the power supply of expansion file units, and FAN errors, and periodically monitors for predictive signs of errors detected by the S.M.A.R.T. (Self-Monitoring Analysis and Reporting Technology) function of hard disks.

When an error is detected, PSA analyzes it, identifies the unit where the error occurred, records that unit as log information, and reports to the MMB and upper management software.

As for errors of expansion file units, PSA monitors them in five-minute intervals.

PSA also monitors various logs of errors the OS or firmware detects in the CPU, memory, chip sets, and inter-chip busses.

Log collection, analysis, and display

This function executes log collection, analysis, and display for the hardware predictive function.

When notified of various types of log information from firmware, various drivers, and the OS, the function saves error messages to log files and displays them. The function also executes event filtering and predefined actions such as notification by e-mail or via the REMCS, issuing an SNMP trap, and saving a log.

Once a hardware error is detected and reported by e-mail, via the REMCS, or with an SNMP trap, any errors detected at the same location are not reported. (However, such errors would be displayed and recorded in a log file).

This suppression of reporting is canceled when:

- the suppression period (1 hour in Japan or 24 hours outside Japan) expires,
- the hardware unit is removed or replaced,
- the error status is cleared through the Web-UI,
- the operating system is rebooted, or
- PSA is restarted.

The table below lists the PSA log files with outlines of the files.

Table 4.9 Log files

Log file	Outline
Agent log	PSA action events (e.g., saving to OS log files and issuing SNMP traps) are stored as agent log data (except for events whose event ID ranges from 00000 to 09999). This type of log can be displayed in GUI and downloaded through GUI as a CSV format file.
Error log	Information on the errors detected by firmware is logged by the OS machine check handler. PSA monitors the error information logged by the OS machine check handler and stores it in the OS log file.
System Event Log	The system event log is stored on the MMB. PSA periodically polls the system event log and stores the logged data in the OS log file. The logged data thus stored can be downloaded through the GUI as a binary format file.

Remarks:
For details of the agent log, see the *PRIMEQUEST 500A/500/400 Series Reference Manual: Messages/Logs* (C122-E004EN).

Note:

If the time zone is changed when PSA is active, the local time in PSA is not updated. To update the local time, restart PSA.

Maintenance operation

This function supports hot swapping of hard disks.

The SAS controller of the hard disk used for the PRIMEQUEST enables power-on/off and insertion/extraction of the disk by using the SCSI Accessed Fault-Tolerant Enclosure (SAF-TE) function. PSA provides SAF-TE operator commands that allow the user to use the SAF-TE function to safely carry out disk replacement or disk expansion when a hardware fault is detected.

REMCS linkage

This function reports the resource information and errors to the REMCS center, by linking with the MMB.

REMCS Agent reports PRIMEQUEST system errors and log information to the REMCS Center via the Internet or a P-to-P connection.

PRIMEQUEST REMCS Agent consists of MMB firmware and a PSA and an SIRMS. PSA reports errors detected by the OS and available hardware resources, to the REMCS center via MMB firmware. PSA also reports software configuration information and software error information detected by SIRMS, to the REMCS center via MMB firmware.

See Chapter 7, "REMCS" in the *PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/Operation Information* (C122-E074EN) for details on the REMCS.

PRIMECLUSTER linkage

This function enables linkage with PRIMECLUSTER (clustering system).

The function allows for a clustering configuration that works with PRIMECLUSTER. A cluster consisting of multiple nodes (PRIMEQUEST) can form a redundant configuration having active and standby systems.

If the active system becomes unusable such as because of a fault, the operation by the active system can be taken over by the standby system.

The PRIMECLUSTER linkage function is installed in MMB firmware and PSA to support the following functions:

- System status monitor/display: Monitors and displays the status of the specified node.
- System status notification: Notifies a remote node, which makes up a cluster, of a status change of the local node.
- Event reception from another system: Receives a status change of a remote node.
- Instruction to another system: Issues an instruction to the specified remote node.

Linkage with upper-level operation management software

This function enables a linkage with upper-level operation management software.

The function enables PSA to work with Systemwalker. It uses SNMP (Simple Network Management Protocol) as a linkage means.

4.5.1 Information managed by PSA

Table 4.10 Information managed by PSA

Type of information	Description	
Hardware information	Model information	CPU information: Mounting information, type, version, frequency
		Memory information: Mounting information, type (size)
		BB information: Mounting information
		PCI card information: Mounting information, adapter name, detail information
		Connection I/O information: Mounting information, type, detail information
System information	Operating System: OS type, version	
	Disk-related information: File system setup, etc.	
	Network-related information: Interface Name, Network Type, MACAddress, Interface Speed, Current Status (up/down/link down), Packet Size	
	Other I/O information	

Note:

MMB Web-UI supports the following browsers. Note that the Web-UI window may not be displayed normally if another browser is being used.

- Microsoft ® IE (Internet Explorer) v5.5 (SP2) or later
- Netscape v7.02 or later

4.6 Collecting PSA Troubleshooting Information

If an error occurs in PSA, collect PSA troubleshooting information by using the following methods:

- For Linux
  Use the system data output tool (fjsnap) to collect system information and PSA troubleshooting information.
  See Section 1.5, "Collecting Maintenance Data (Linux)" in the P*RIMEQUEST 500A/500/400 Series Reference Manual: Tools/Operation Information* (C122-E074EN) for details on using the tool.
- For Windows
  Use the Software Support Guide to collect system information and PSA troubleshooting information. For how to use the Software Support Guide and other details, refer to the Software Support Guide manual.

To collect troubleshooting information for PSA only according to a support group request, use the PSA troubleshooting information collection command (getopsa). See Section 8.4, "PSA Troubleshooting Data Collection Command (getopsa)," for details on using getopsa.

Part III MMB

CHAPTER 5 Web-UI Operations

This chapter describes how to operate and manage the PRIMEQUEST-series machine from the MMB Web-UI, and it provides a list of menus in the MMB Web-UI window and describes the associated windows and operations.

5.1 List of Menus in the Web-UI Window

This section provides a list of menus for the Web-UI.

The abbreviations in the Privilege column mean the following:

- RW : The user can read and write in the window concerned.
- RO : The user can only read in the window concerned.
- N/A : The window and submenu concerned are not displayed.

5.1.1 List of menus for the PRIMEQUEST 510A

Table 5.1 Menus (PRIMEQUEST 510A)

Navigation Bar submenus					Privilege				Remarks
Level 1	Level 2	Level 3	Level 4	Level 5	Admin	Operator	User	CE	
System									
	System Status				RO	RO	RO	RO	Displays the status of the entire system.
	System Event Log				RW	RO	RO	RO	Displays the system event log.
	System Information				RW	RO	RO	RO	Displays system information such as system and product names.
	Firmware Information				RO	RO	RO	RO	Displays firmware version information.
	System Setup				RW	RO	RO	RW	Specifies the system configuration.
	LEDs				RW	RW	RW	RW	Displays LED statuses.

Navigation Bar submenus					Privilege				Remarks
Level 1	Level 2	Level 3	Level 4	Level 5	Admin	Operator	User	CE	
	Power Supply				RW	RO	RO	RO	Displays the power status.
	Fans				RW	RO	RO	RW	Displays fan statuses.
	Temperature				RO	RO	RO	RO	Displays the readings from temperature sensors in the PRIMEQUEST-series machine.
	BB								Displays only the submenus for the installed BB.
	SASBP				RO	RO	RO	RO	Displays SASBP status.
	MMB				RW	RW	RO	RW	Displays MMB information.
	Power Control				RW	RW	RO	RO	Power control
	Schedule								
		Schedule Control			RW	RW	RO	RO	Specifies information for scheduled operations.
		Schedule List			RW	RW	RO	RO	Sets the power-on and power-off schedule.
	Console Redirection Switch								
		Console Redirection Switch			RW	RW	RO	RW	Specifies the output destination of console redirection.
		Console Redirection			RO	RO	RO	RO	Displays console output (input not allowed).
	ASR Control				RW	RO	RO	RO	Specifies the automatic restart conditions.
	PSA				See Part IV, "PSA."				
User Administration									
	User List				RW	N/A	N/A	N/A	Displays a list of registered user accounts, deletes these accounts, and is used to edit the accounts.
	Change Password				RW	RW	RW	RW	Changes the password of the current user account.

Navigation Bar submenus					Privilege				Remarks
Level 1	Level 2	Level 3	Level 4	Level 5	Admin	Operator	User	CE	
	Who				RO	RO	RO	RO	Displays the users connected to the MMB Web-UI.
Network Configuration									
	Date/Time				RW	RO	RO	RO	Specifies the MMB date and time.
	Network Interface				RW	RO	RO	RO	Specifies the IP address used to access the MMB, etc.
	Management LAN Port Configuration				RW	N/A	N/A	N/A	Specifies the MMB port, and specifies the disconnection between the MMB port and system.
	Network Protocols				RW	RO	RO	RO	Specifies the network protocols of the MMB.
	Refresh Rate				RW	RW	RW	RW	Specifies the refresh rate of an HTTP/HTTP page.
	SNMP Configuration				RW	N/A	N/A	N/A	This submenu is displayed only if [Enable] is set for SNMP in [Network Protocols].
		SNMP Community			RW	N/A	N/A	N/A	Specifies the SNMP community.
		SNMP Trap			RW	N/A	N/A	N/A	Specifies the trap transmission destination.
		SNMPv3 Configuration			RW	N/A	N/A	N/A	Specifies the engine ID and users unique to SNMP v3.
	SSL								
		Create CSR			RW	N/A	N/A	N/A	Creates private keys and CSRs.
		Export Key/CSR			RW	N/A	N/A	N/A	Exports private keys and CSRs.
		Import Certificate			RW	N/A	N/A	N/A	Installs a certificate.
		Create Selfsigned Certificate			RW	N/A	N/A	N/A	Creates a self-signed certificate.
	SSH								

Navigation Bar submenus					Privilege				Remarks
Level 1	Level 2	Level 3	Level 4	Level 5	Admin	Operator	User	CE	
		Create SSH Server Key			RW	N/A	N/A	N/A	Creates SSH server private keys.
	Remote Server Management				RW	N/A	N/A	N/A	Specifies the user configuration used to control the MMB using RMCP.
	Access Control				RW	N/A	N/A	N/A	Defines the IP filter to enable access.
	Alarm E-Mail				RW	N/A	N/A	N/A	Defines e-mail notification for events.
Maintenance									
	Firmware Update								
		MMB Firmware Update			RW	N/A	N/A	RW	Updates MMB firmware.
		PAL/SAL Firmware Update			RW	N/A	N/A	RW	Updates PAL/SAL firmware to the MMB.
		EFI Firmware Update			RW	N/A	N/A	RW	Updates EFI firmware.
		BMC Firmware Update			RW	N/A	N/A	RW	Updates the BMC firmware.
	Backup/Restore Configuration								Backup/Restore of setting values.
		Backup/Restore MMB Configuration			RW	N/A	N/A	RW	Backs up and restores MMB configuration information.
		Backup/Restore EFI Configuration			RW	N/A	N/A	RW	Backs up and restores EFI configuration information.
	Maintenance Wizard				RW	N/A	N/A	RW	Wizard-based maintenance
	REMCS								See Chapter 7, "REMCS" in the *PRIMEQUEST 500A/ 500/400 Series Reference Manual: Tools/Operation Information* (C122-E074EN).
		REMCS			RW	N/A	N/A	RW	
		Detailed Setup			RW	N/A	N/A	RW	

5.2 System Menu

From the [System] menu, the status of PRIMEQUEST hardware components can be displayed and settings can be made for these components.

Note: If "Read Error" is displayed for [Part Number] or [Serial Number] in the MMB Web-UI window (content display frame and information frame), contact your Fujitsu certified service engineer.

Do not execute [Reset] or [Force Power Off] from the Power Control window while "Read Error" is displayed. Also, do not perform power-off using the power cable.

5.2.1 [System Status] window

The [System Status] window displays the status of the entire PRIMEQUEST-series machine.

Clicking the box containing a unit name in this window displays the detailed status view window for the unit.

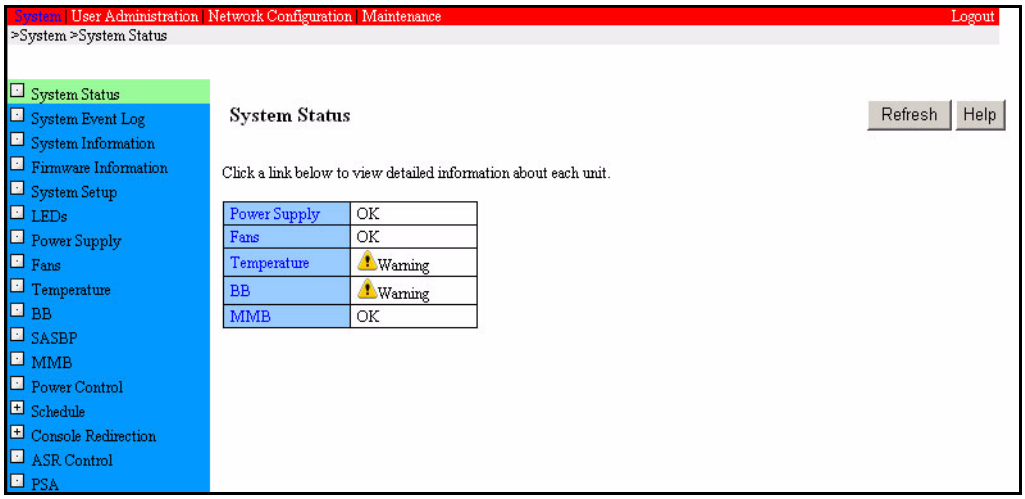


Figure 5.1 [System Status] window

This window displays the statuses of all devices in the PRIMEQUEST-series machine. The displayed status means the following:

Clicking the display frame of a unit displays the detail status information window of the unit.

OK: The device has no defect and it is operating normally.

Not-present: This unit is not installed. This status is grayed out.

Warning: The device has encountered an event that is not serious IO Units but will possibly develop into a problem. The accompanying icon is .

Failed: The device has failed and must be isolated. The accompanying icon is .

Degraded: The device contains a faulty component but can continue operating when the faulty component has been isolated. The accompanying icon is .

Table 5.2 Displayed items in the [System Status] window

Item	Description
Power Supply	Status of power supply units in the PRIMEQUEST-series machine
Fans	Status of fans in the PRIMEQUEST-series machine
Temperature	Status of temperature sensors in the PRIMEQUEST-series machine
BB	Statuses of BB in the PRIMEQUEST-series machine
MMB	Statuses of MMB in the PRIMEQUEST-series machine

(1) Menu operation

[System] → [System Status]

(2) GUI operation

1 To check the status of a device in detail, click the box containing its unit name.
A detailed status view window for the device is displayed.

Remarks: To display the detailed status of a unit, you can select the menu for the unit directly from the [System] submenu. For details on this operation, see Section 5.2.6 to Section 5.2.14.

5.2.2 [System Event Log] window

The [System Event Log] window displays events that occurred in the PRIMEQUEST-series machine and are stored in the system event log of the MMB.

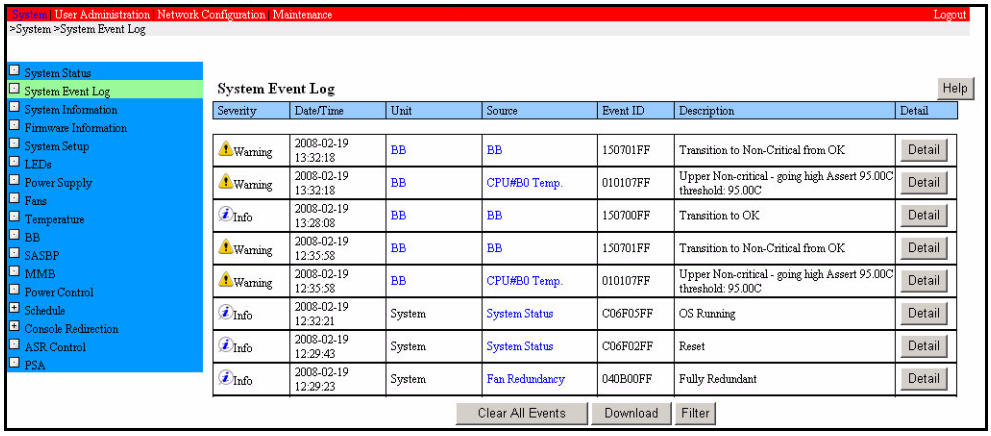
More than 1,000 events can be stored in the system event log. When the system event log reaches the maximum number of entries, new events are saved in the system event log as the oldest events are deleted. Clicking the [Detail] button displays the detailed information on each event.

Note: In Windows Server 2008, the following system event log item is displayed for operating system startup, but it does not affect operation.

Severity: Info

Unit/Source/Event ID: None

Description: Binary character string



Severity	Date/Time	Unit	Source	Event ID	Description	Detail
Warning	2008-02-19 13:32:18	BB	BB	150701FF	Transition to Non-Critical from OK	Detail
Warning	2008-02-19 13:32:18	BB	CPU#B0 Temp.	010107FF	Upper Non-critical - going high Assert 95.00C threshold: 95.00C	Detail
Info	2008-02-19 13:28:08	BB	BB	150700FF	Transition to OK	Detail
Warning	2008-02-19 12:35:58	BB	BB	150701FF	Transition to Non-Critical from OK	Detail
Warning	2008-02-19 12:35:58	BB	CPU#B0 Temp.	010107FF	Upper Non-critical - going high Assert 95.00C threshold: 95.00C	Detail
Info	2008-02-19 12:32:21	System	System Status	C06F05FF	OS Running	Detail
Info	2008-02-19 12:29:43	System	System Status	C06F02FF	Reset	Detail
Info	2008-02-19 12:29:23	System	Fan Redundancy	040B00FF	Fully Redundant	Detail

Figure 5.2 [System Event Log] window

The title row in the table remains visible during scrolling, and only the table body is scrolled.

Table 5.3 Displayed items in the [System Event Log] window

Item	Description
Severity	Severity of an event or error: • Error: Serious IO Units problem such as a hardware failure • Warning: Event that is not serious IO Units but will possibly develop into a problem • Info: Normal event
Date/Time	Local date and time at which an event or error occurred. Format: yyyy-MM-dd HH:mm:ss
Unit	Unit with the sensor that detected an event or error. For example, "BB" is displayed for an error that occurred in CPU#A0. Clicking a displayed unit name displays the corresponding unit information window (whose information includes the part number and serial number of the unit).
Source	Name of the sensor that detected an event or error. Clicking a displayed sensor name displays the corresponding sensor status window or the unit information window of the unit containing the sensor.
Event ID	ID (eight-digit hexadecimal number) that identifies an event. For details on event ID assignment, see the *PRIMEQUEST 500A/500/400 Series Reference Manual: Messages/Logs* (C122-E004EN).
Description	Description of an event or error. If the event involves board insertion or removal, the part number and serial number of the board are displayed.

Table 5.4 Buttons in the [System Event Log] window

Button	Description
Clear All Events	Click the [Clear All Events] button to clear all of the events stored in the system event log. A confirmation dialog box opens for confirmation to clear the events.
Download	Click the [Download] button to download the event data stored in the system event log to the PC whose browser is displaying the Web-UI. The [Save File] dialog box opens before downloading begins. Specify the save destination directory and a file name.
Filter	Click the [Filter] button to open the [System Event Log Filtering Condition] window for entering filtering conditions. Enter filtering conditions, and click the [Apply] button. The [System Event Log] window is then displayed with the data that satisfies the entered filtering conditions.

Button	Description
Detail	Click the [Detail] button to display details on the selected event in the [System Event Log (Detail)] window.

(1) Menu operation

[System] → [System Event Log]

(2) GUI operation

- Clearing all of the events stored in the system event log
  1. Click the [Clear All Events] button.
     A confirmation dialog box opens for confirmation to clear all of the events.
- Downloading the event data stored in the system event log
  1. Click the [Download] button.
     A dialog box is displayed to allow you to enter a save file path. Download the event data to the PC that displays the Web-UI.
- Filtering the events displayed in the window
  1. Click the [Filter] button.
     The [System Event Log Filtering Condition] window for entering filtering conditions opens.
  2. Enter filtering conditions in the [System Event Log Filtering Condition] window, and click the [Apply] button.
     The [System Event Log] window is then displayed again, with only the events that satisfy the specified conditions.
- Displaying details on an event displayed in the window
  1. Click the applicable [Detail] button.
     The [System Event Log (Detail)] window is displayed with details on the event.

5.2.2.1 [System Event Log Filtering Condition] window

The [System Event Log Filtering Condition] window can be used to identify events that occurred in the PRIMEQUEST-series machine. If conditions are entered in this window, the caller window displays the events that satisfy the entered conditions when it is redisplayed.

This filtering uses the AND operator for entered conditions.

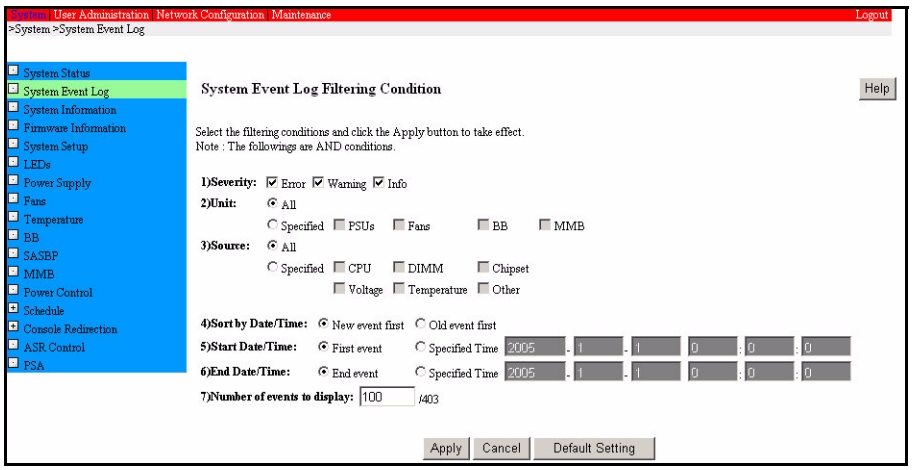


Figure 5.3 [System Event Log Filtering Condition] window

Table 5.5 Displayed and setting items in the [System Event Log Filtering Condition] window

Item	Description
Severity	Select the severities of the system events to be displayed for the system event log by checking the corresponding check boxes. More than one severity option can be selected. • Error: Serious IO Units problem such as a hardware failure • Warning: Event that is not serious IO Units but will possibly develop into a problem • Info: Normal event By default, all of the options are selected.
Unit	Select units whose events are to be displayed. Select either [All] or [Specified] by clicking its radio button. Selecting [All] disables filtering of units. Selecting [Specified] enables filtering of units and checking of check boxes, so units can be selected. The default setting is [All].
Source	Select the sensors (e.g., CPU, DIMM) used to display the sources of any events and errors that occur. Select either [All] or [Specified] by clicking its radio button. Selecting [All] disables filtering of sources. Selecting [Specified] enables filtering and checking of check boxes, so the sources can be selected. The default setting is [All].
Sort by Date/Time	Specify the order for displaying events, from new events to old events or vice versa, by clicking a radio button. The default setting is [New event first].
Start Date/Time	Specify a time range for the event logs to be displayed. Select either [First event] or [Specified time] as the start time by clicking a radio button. If [Specified time] is selected, the start time can be entered. The default setting is [First event].
End Date/Time	Specify a time range for the event logs to be displayed. Select either [End event] or [Specified time] as the end time by clicking a radio button. If [Specified time] is selected, the end time can be entered. The default setting is [End event].
Number of events to display	Specify the number of events to be displayed for the log. The default setting is 100. The denominator indicates the number of events stored in the log.

Table 5.6 Buttons in the [System Event Log Filtering Condition] window

Button	Description
Apply	Specify conditions such as [Severity] and [Unit], and click the [Apply] button. The specified filtering conditions are then set, and the [System Event Log] window is displayed again. The window displays events that satisfy the filtering conditions.
Cancel	Click the [Cancel] button to return to the [System Event Log] window. The events displayed in the window remain the same.
Default Setting	Click the [Default Setting] button to reset all items in this window to their default values.

(1) Menu operation

[System] → [System Event Log] → [Filter] button

(2) GUI operation

- To display the [System Event Log] window in specified filtering conditions:
  1. Specify conditions and click the [Apply] button.
     The [System Event Log] window reappears. It displays a list of messages limited to those which fulfill the specified conditions. If no message that fulfills the conditions exists, the window displays its title and a message stating that there is no log to be displayed.
- To return to the [System Event Log] window:
  1. Click the [Cancel] button. The specified conditions are canceled and the [System Event Log] window reappears.
- To return the selected values to the default values:
  1. Click the [Default Setting] button. The conditions selected for all parameters are cleared and the parameters revert to their default values.

5.2.2.2 [System Event Log (Detail)] window

The [System Event Log (Detail)] window displays detailed information on an event displayed in the [System Event Log] window.

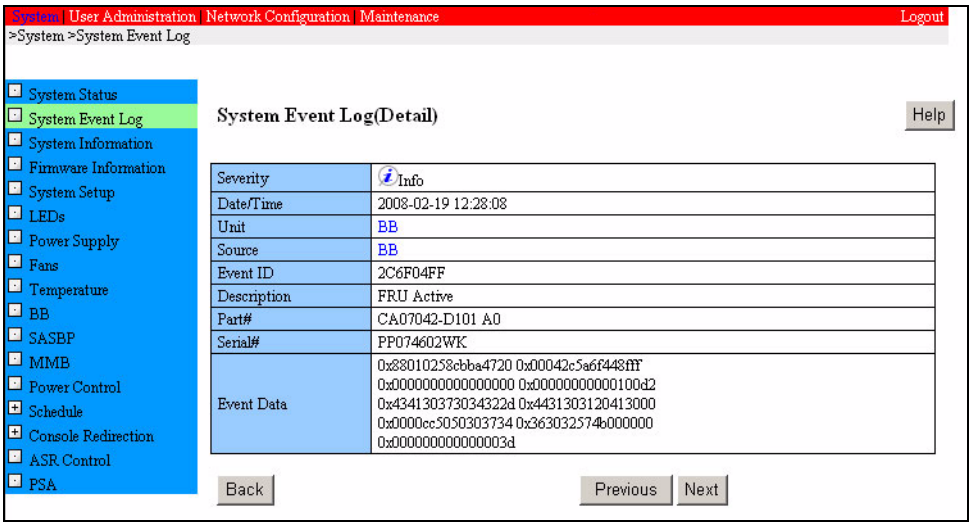


Figure 5.4 [System Event Log (Detail)] window

Table 5.7 Displayed items in the [System Event Log (Detail)] window

Item	Description
Severity	Severity of the event or error: • Error: Serious IO Units problem such as a hardware failure • Warning: Event that is not serious IO Units but will possibly develop into a problem • Info: Normal event
Date/Time	Local date and time at which the event or error occurred. Format: yyyy-MM-dd HH:mm:ss
Unit	Unit with the sensor that detected the event or error. For example, "BB" is displayed for an error that occurred in CPU#A0. Clicking the displayed unit name displays the corresponding unit information window (whose information includes the part number and serial number of the unit).
Source	Name of the sensor that detected the event or error. Clicking a displayed sensor name displays the corresponding sensor status window or the unit information window of the unit containing the sensor.
Event ID	ID (eight-digit hexadecimal number) that identifies the event. For details on ID assignment, see the *PRIMEQUEST 500A/500/400 Series Reference Manual: Messages/Logs*. (C122-E004EN)

Item	Description
Description	Description of the event or error. If the event involves board insertion or removal, the part number and serial number of the board are displayed.
Part Number	Part number of the source or unit where the event occurred
Serial Number	Serial number of the source or unit where the event occurred
Event Data	Event data in hexadecimal notation

Table 5.8 Buttons in the [System Event Log (Detail)] window

Button	Description
Back	Redisplays the [System Event Log] window.
Previous	Displays detailed information on the previous IO Units event according to the display order in the [System Event Log] window.
Next	Displays detailed information on the next event according to the display order in the [System Event Log] window.

(1) Menu operation

[System] → [System Event Log] → [Detail] on each log

(2) GUI operation

- Returning to the [System Event Log] window

  1 Click the [Back] button.
  The [System Event Log] window is displayed again.

- Displaying detailed information on the previous IO Units event

  1 Click the [Previous] button.
  The window displays detailed information on the previous IO Units event according to the display order in the [System Event Log] window.

- Displaying detailed information on the next event

  1 Click the [Next] button.
  The window displays detailed information on the next event according to the display order in the [System Event Log] window.

5.2.3 [System Information] window

The [System Information] window displays information about the PRIMEQUEST-series machine, such as the system name, product name.

The PRIMEQUEST-series machine (cabinet) name and the asset tag (asset management number) can be specified from this window. The name specified here is also used in [System Name] for communication using SNMP.

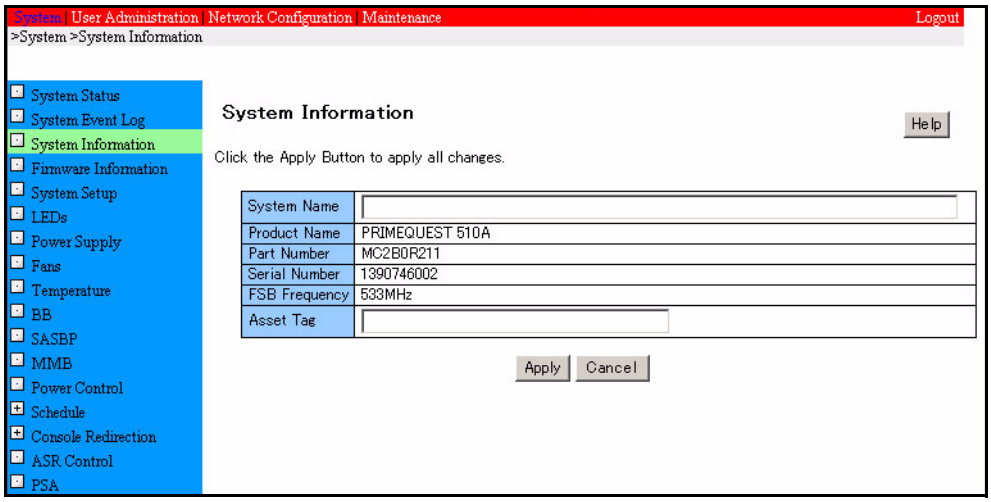


Figure 5.5 [System Information] window

Table 5.9 Displayed and setting items in the [System Information] window

Item	Description
System Name	System name. A user with the Admin privilege can change the system name to a name consisting of up to 64 characters. This system name is also used as an SNMP system name. Remarks: Any of the following characters can be used: [0-9], [a-z], [A-Z], " "(en-size space), !" (double quotation mark) # $ % & ' (single quotation mark) ( ) = - ^ ~ \ (or back slash) @ ` [ ] { } : * ; + ? < . > , / _ |. However, the following restrictions apply: - The following characters cannot be used at the beginning of a string: # (en-size space) - The following character cannot be used at the end of the string: (en-size space) This system name is also used as the SNMP system name. The system name set here is displayed in the [SNMP Configuration] window but cannot be changed in the [SNMP Configuration] window. The default name is <PRIMEQUEST + serial_number>.
Product Name	Product name Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer.
Part Number	Part number Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer.
Serial Number	Serial number Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer.
FSB Frequency	Frequency.
Asset Tag	Asset management information (Asset Tag). A user with Administrator privilege can change asset management information. Up to 32 byte characters can be entered. You can use the following characters for system names: 0-9, a-z, A-Z, - (hyphen), _ (underscore), and en-size space. However, the first character must be one of a-z and A-Z.

Table 5.10 Buttons in the [System Information] window

Button	Description
Apply	Sets the values entered in [System Name] and [Asset Tag].
Cancel	Reverts to the original settings in [System Name] and [Asset Tag].

(1) Menu operation

[System] → [System Information]

(2) GUI operation

1 Change the values in [System Name] and [Asset Tag], and click the [Apply] button.
The entered values are then set.

5.2.4 [Firmware Information] window

The [Firmware Information] window displays version information on firmware running on the system.

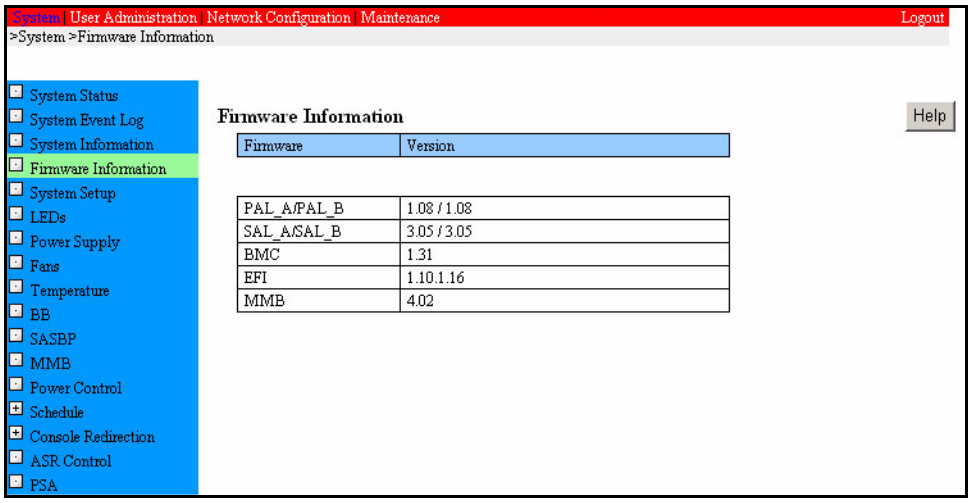


Figure 5.6 [Firmware Information] window

Table 5.11 Displayed items in the [Firmware Information] window

Item	Description
Firmware	Firmware type
Version	Firmware version. "-" is displayed for an unknown version.

(1) Menu operation

[System] → [Firmware Information]

(2) GUI operation

None

5.2.5 [System Setup] window

The [System Setup] window allows you to specify PRIMEQUEST Power Feed mode settings and Power Restore actions.

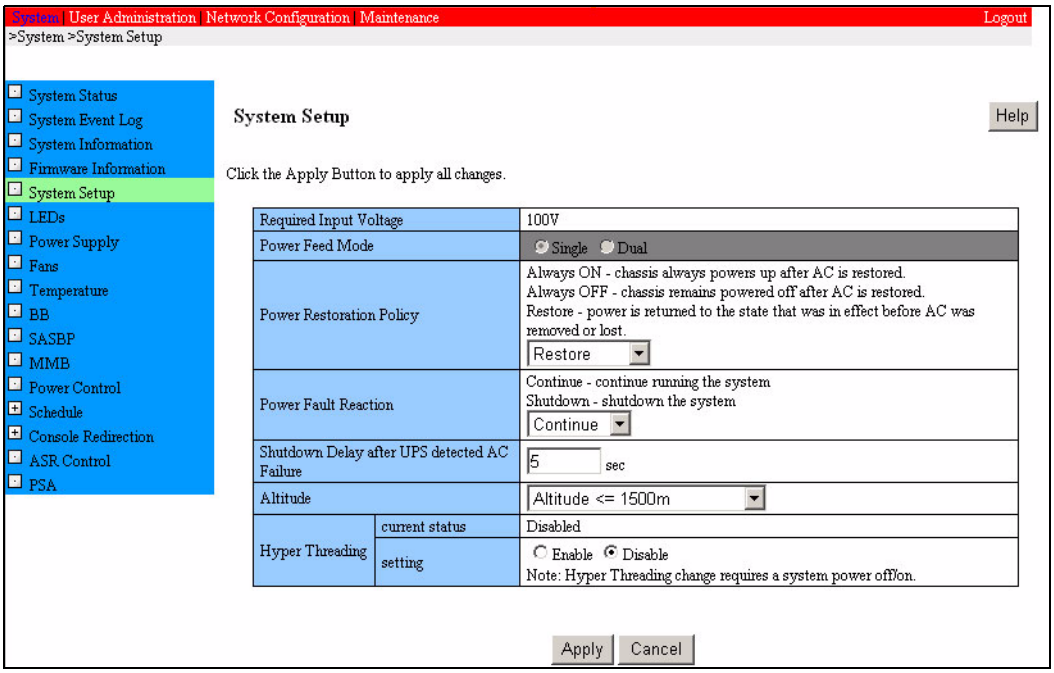


Figure 5.7 [System Setup] window

Table 5.12 Displayed and setting items in the [System Setup] window

Item	Description
Required Input Voltage	Displays the required input voltage.
Power Feed Mode	The user can set either single power feed mode or dual power feed mode for the power supply to the PRIMEQUEST-series machine: • Single: Single power feed mode • Dual: Dual power feed mode Note: Dual (dual power feed) is valid only when the input voltage is 200 V. When the input voltage is 100 V, Power Feed Mode is grayed out and cannot be selected. Remarks: This operation is performed by a Fujitsu certified service engineer. The default setting is [Single].

Item	Description
Power Restoration Policy	The user can specify the action taken for power recovery in the event of a power failure, and this setting is displayed: • Always off: Keeps power off after power recovery. • Always on: Turns power on after power recovery regardless of the status at the time of the power failure. • Restore: Restores the status at the time of the power failure. That is, if power was on at the time of the power failure, power is turned on, and if power was off, power is kept off. The default setting is [Restore].
Power Fault Reaction	The user can specify the action taken in the event of lost redundancy, and this setting is displayed: • continue: Keeps servers operating continuously when redundancy is lost. • shutdown: Shuts down the servers when redundancy is lost. Note: When the input voltage is 100 V and two PSUs (no redundant)are used, use the default value of this parameter. The default value is [continue].
Shutdown Delay after UPS detected AC Failure	The user can specify the grace period from UPS detection of a power failure until the start of an OS shutdown. If power recovery is completed within this time, the OS shutdown does not start. The setting range is 0 to 9999 seconds. The default setting is 5 seconds.
Altitude	The user can specify the altitude of the PRIMEQUEST-series machine installation location. • Altitude <= 1500 m • 1500 m < Altitude <= 2000 m • 2000 m < Altitude <= 2500 m • 2500 m < Altitude The default setting is Altitude <= 1500 meters. Remarks: Setting an altitude enables precise detection of abnormal intake temperatures.
Hyper Threading (current status)	Spedifies whether to enable the Hyper Threading function/ • Enabled: Hyper Threading is enabled/ • Disabled: Hyper Threading is disabled
Hyper Threading (setting)	Specifies whether to enable the Hyper Threading function. • Enable (enable Hyper Threading). • Disable (disabling Hyper Threading) The default setting is [Disable] (disabling Hyper Threading.)

Table 5.13 Buttons in the [System Setup] window

Button	Description
Apply	Specify [Power Feed Mode], [Power Restore Policy], and other items, and click the [Apply] button to set the specified values.
Cancel	When you click the [Cancel] button, modifications or additions to items are not made effective, but the items are returned to their previous state.

(1) Menu operation

[System] → [System Setup]

(2) GUI operation

1 Specify [Power Feed Mode], [Power Restoration Policy], and other items in this window, and click the [Apply] button.
Then, the specified values are made effective.
Note: When the "Hyper Threading" setting is changed in the [System Setup] window, clicking the [Apply] button with the power supplied to the system displays the dialog box with a warning.
To change the type of Hyper Threading, the cabinet power must be turned off and turned on again.

5.2.6 [LEDs] window

The [LEDs] window displays LEDs statuses in the system.

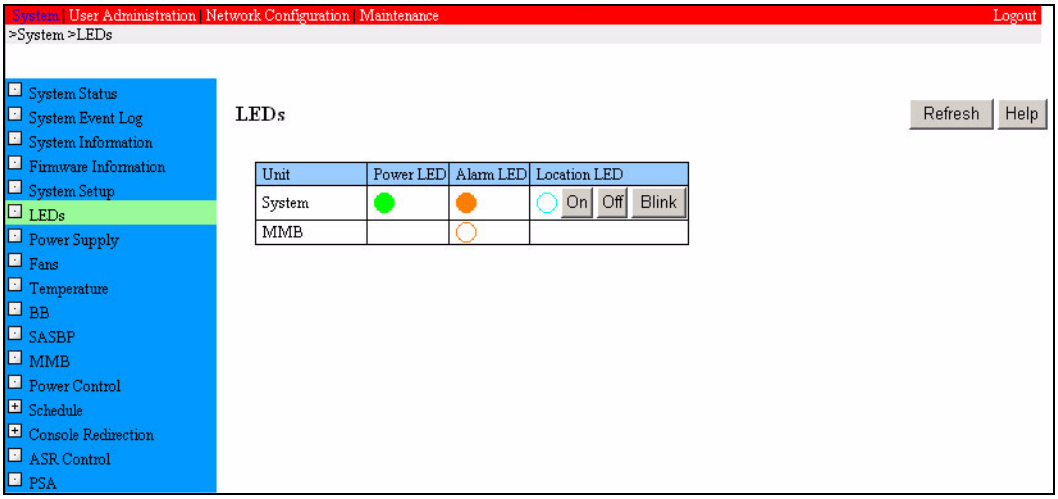


Figure 5.8 [LEDs] window

Table 5.14 Displayed and setting items in the [LEDs] window

Item	Description
Unit	Unit name.
Power LED	Power status
Alarm LED	Indication of whether the unit operating normally or abnormally
Location LED	Used to indicate the location or status of the unit corresponding to the LED

(1) Menu operation

[System] → [LEDs]

(2) GUI operation

1 Click the [On], [Off], or [Blink] button.
All location LEDs in the target unit are turned on, turned off, or blink.

5.2.7 [Power Supply] window

The [Power Supply] window displays power supply unit statuses in the PRIMEQUEST-series machine.

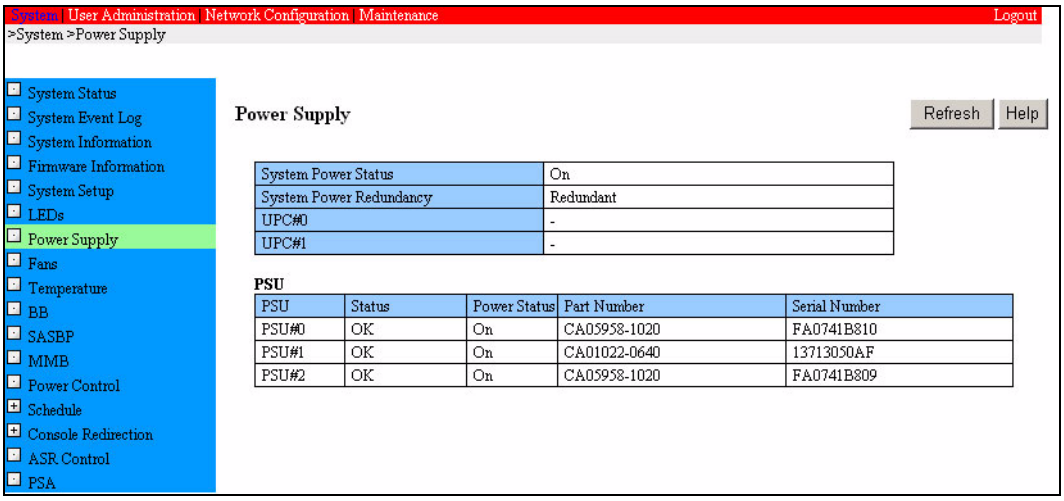


Figure 5.9 [Power Supply] window

Table 5.15 Displayed items in the [Power Supply] window

Item	Description
System Power Status	Power status of the PRIMEQUEST-series machine (system): • On: Powered on • Standby: Standby mode
Power Supply Redundancy	Redundancy status of power supply units: • Redundant: PSU redundancy is maintained. • [Non-redundant: Sufficient Resources]: PSU redundancy is lost, but there are enough PSUs to continue system operation. • [Non-redundant: Insufficient Resources]: PSU redundancy is lost, and there are not enough PSUs to continue system operation.
UPC#x	UPS status detected by the UPC interface: • AC Lost: Power is off. • Battery Lost: The battery has been depleted. • Failed: The system has failed. • -: Normal status or the UPS is not connected.

PSU

PSU	PSU number
Status	PSU status: • OK: Operating normally • Not-present: Not installed • Failed: Failure • Predictive Fail: Expecting a failure. • A/C Lost: Power failure
Power Status	Indication of whether PSU power is On or Off
Part Number	PSU part number Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer.
Serial Number	PSU serial number Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer.

(1) Menu operation

[System] → [Power Supply]

(2) GUI operation

None

5.2.8 [Fans] window

The [Fans] window displays fan statuses in the PRIMEQUEST-series machine, and the fan statuses can be cleared using this window.

If the user is granted no appropriate privilege, the [Status Clear] button is not displayed.

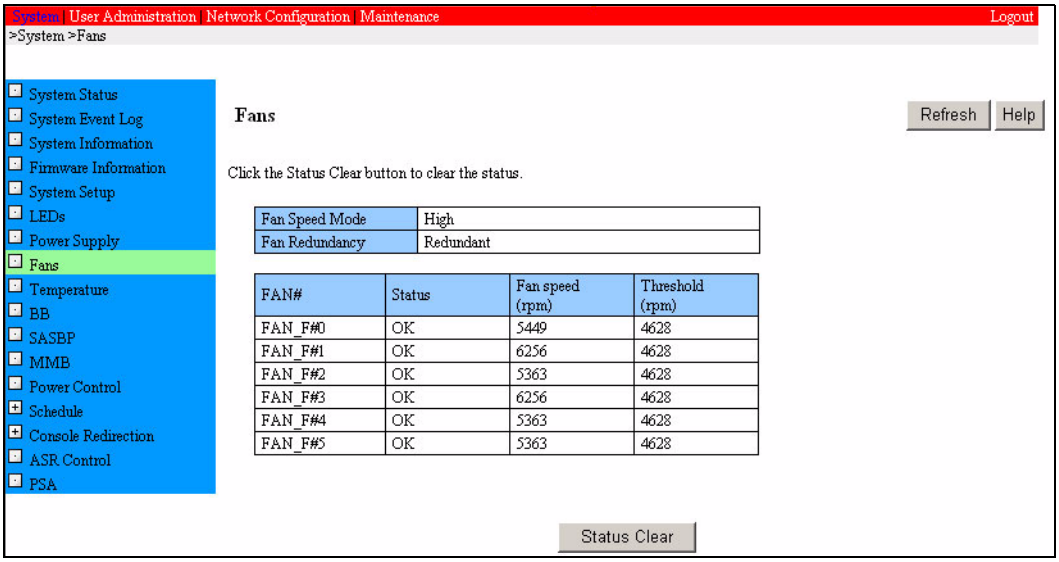


Figure 5.10 [Fans] window

Table 5.16 Displayed items in the [Fans] window

Item	Description
Fan Speed Mode	Fan speed mode: • Normal: Normal rotational speed • High: High rotational speed (The fan entered high-speed mode because of an abnormal temperature or lost redundancy.) • Low: Low rotational speed
Fan Redundancy	Fan redundancy status: • Redundant: Fan redundancy is maintained. • Non-redundant: Sufficient Resource Fan redundancy is lost, but there are enough fans to continue system operation. • Non-redundant:Insufficient Resources: Fan redundancy is lost, and there are not enough fans to continue system operation.
FAN#	Fan number
Status	Fan status: • OK: Operating normally • Not present: Not installed • Failed: Fan failure

Item	Description
Fan Speed(rpm)	Fan speed (rpm).
Threshold(rpm)	Lower limit of the fan speed (Any speed lower than this setting is abnormal.)

Table 5.17 Button in the [Fans] window

Button	Description
Status Clear	Click the [Status Clear] button to display the [Fans Status Clear] window. This window enables clearing of the fan statuses.

(1) Menu operation

[System] → [Fans]

(2) GUI operation

1 Click the [Status Clear] button.
The [Fans Status Clear] window is displayed.

2 Follow the clearing process in the [Fans Status Clear] window.
The fan statuses are cleared.

5.2.8.1 [Fans Status Clear] window

Once an abnormality is detected in a fan, the fan remains in the abnormal status until the fan is replaced or the abnormal status is cleared.

The abnormal status of a fan can be cleared using the [Fans Status Clear] window.

Remarks:

- After the abnormal status of a fan is cleared, if an abnormal fan speed is detected in the fan, the fan is placed in the [Failed] status again. Clearing the status of a fan with an abnormal fan speed does not change its status from [Failed].

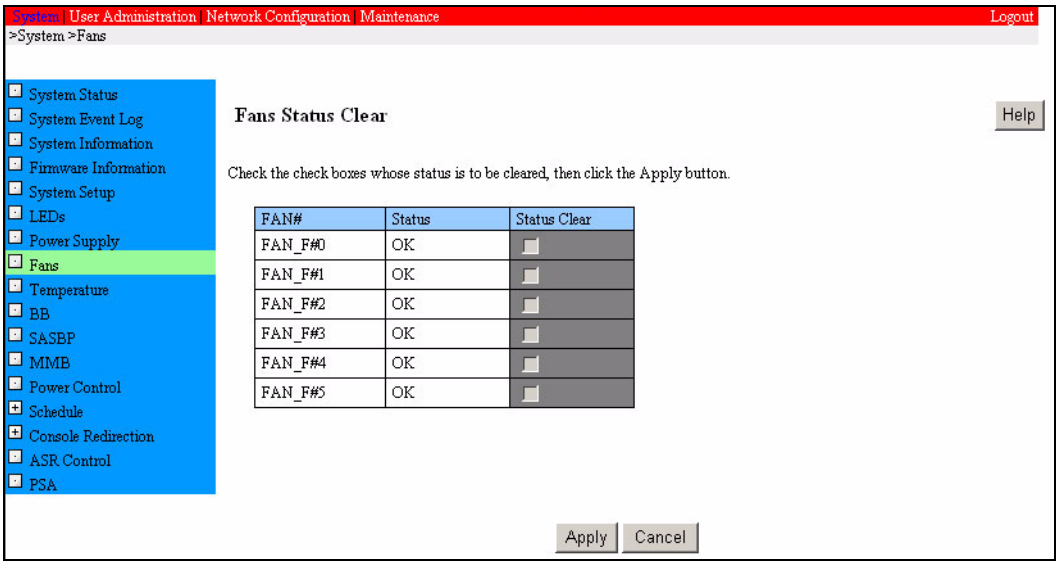


Figure 5.11 [Fans Status Clear] window

Normal fans are grayed out and cannot be selected.

Table 5.18 Displayed and setting items in the [Fans Status Clear] window

Item	Description
FAN#	Fan number
Status	Fan status: • OK: Operating normally • Not-present: Not installed • Failed: Fan failure
Status Clear	To clear the status of a fan, select it.

Table 5.19 Buttons in the [Fans Status Clear] window

Button	Description
Apply	To clear the status of a fan, select the fan, and click the [Apply] button. The abnormal status of the selected fan is then cleared.
Cancel	Click the [Cancel] button to not change information and not clear the abnormal status of a fan.

(1) Menu operation

[System] → [Fans]

(2) GUI operation

1 To clear the status of a fan, select the fan by checking its [Status Clear] check box, and click the [Apply] button.
The fan status is then cleared.

5.2.9 [Temperature] window

The [Temperature] window displays readings from the inlet air temperature sensor in the PRIMEQUEST-series machine and CPU temperature sensors.

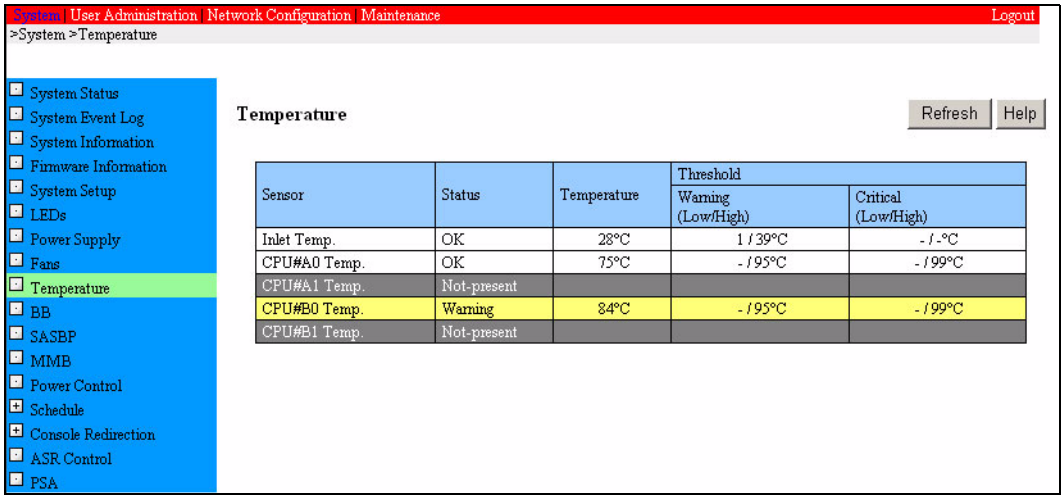


Figure 5.12 [Temperature] window

Table 5.20 Displayed items in the [Temperature] window

Item		Description
Sensor		Temperature sensor name.
Status		Temperature sensor status: • OK: Operating normally • Not present: Not installed • Warning: Warning status • Critical: Critical status
Temperature		Temperature sensor reading
Threshold	Warning (Low/High)	Lower and upper limits of the warning-status temperature stored in a temperature sensor
	Critical (Low/High)	Lower and upper limits of the critical-status temperature stored in a temperature sensor

(1) Menu operation

[System] → [Temperature]

(2) GUI operation

None

5.2.10 [BB] window

In the [BB] window, the user can clear the status information and error information on the BB board.

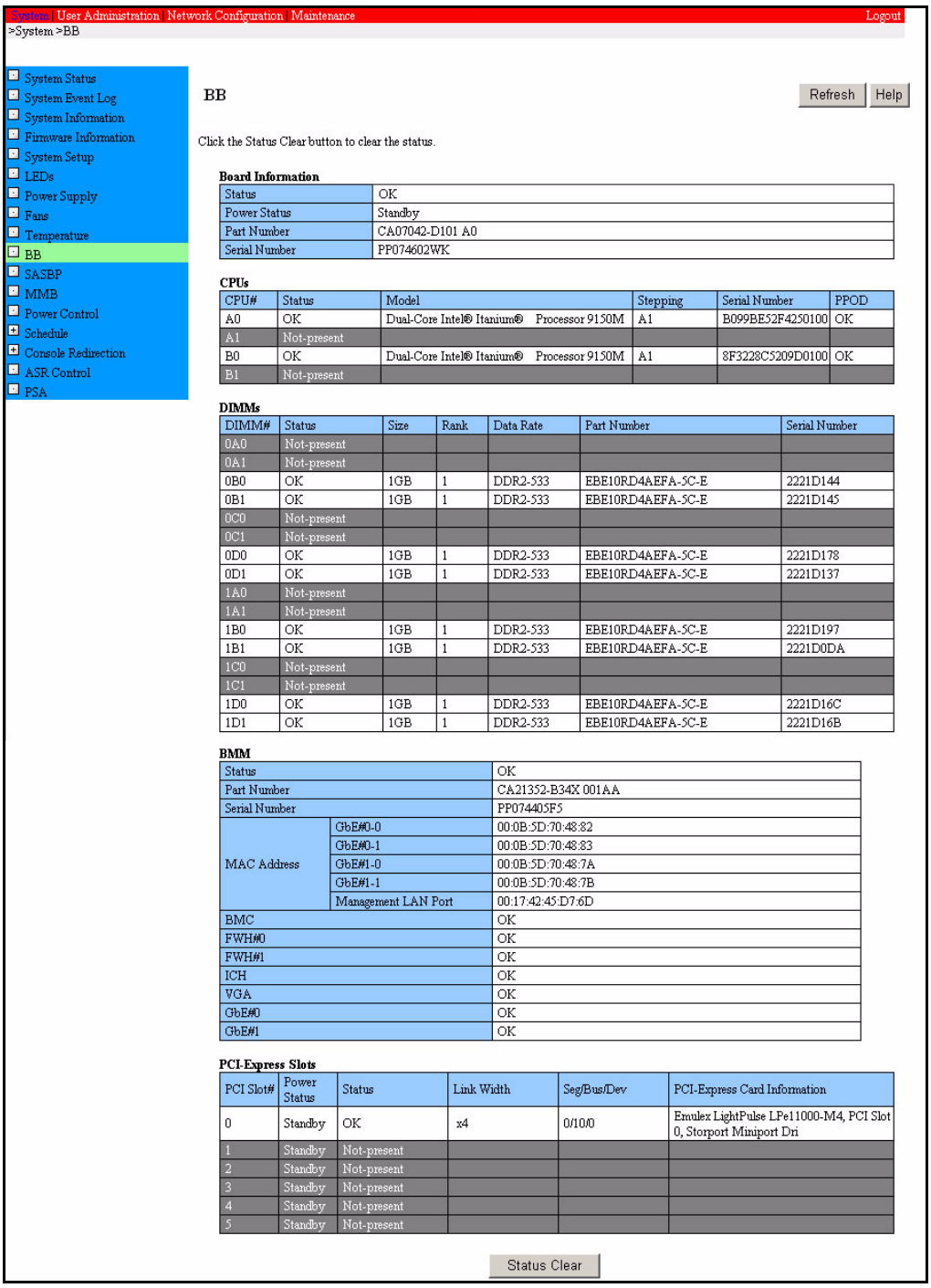


Figure 5.13 [BB] window (1/2)

A line with an uninstalled CPU or DIMM is grayed out.

If the user is granted no appropriate privilege, the [Status Clear] button is not displayed.

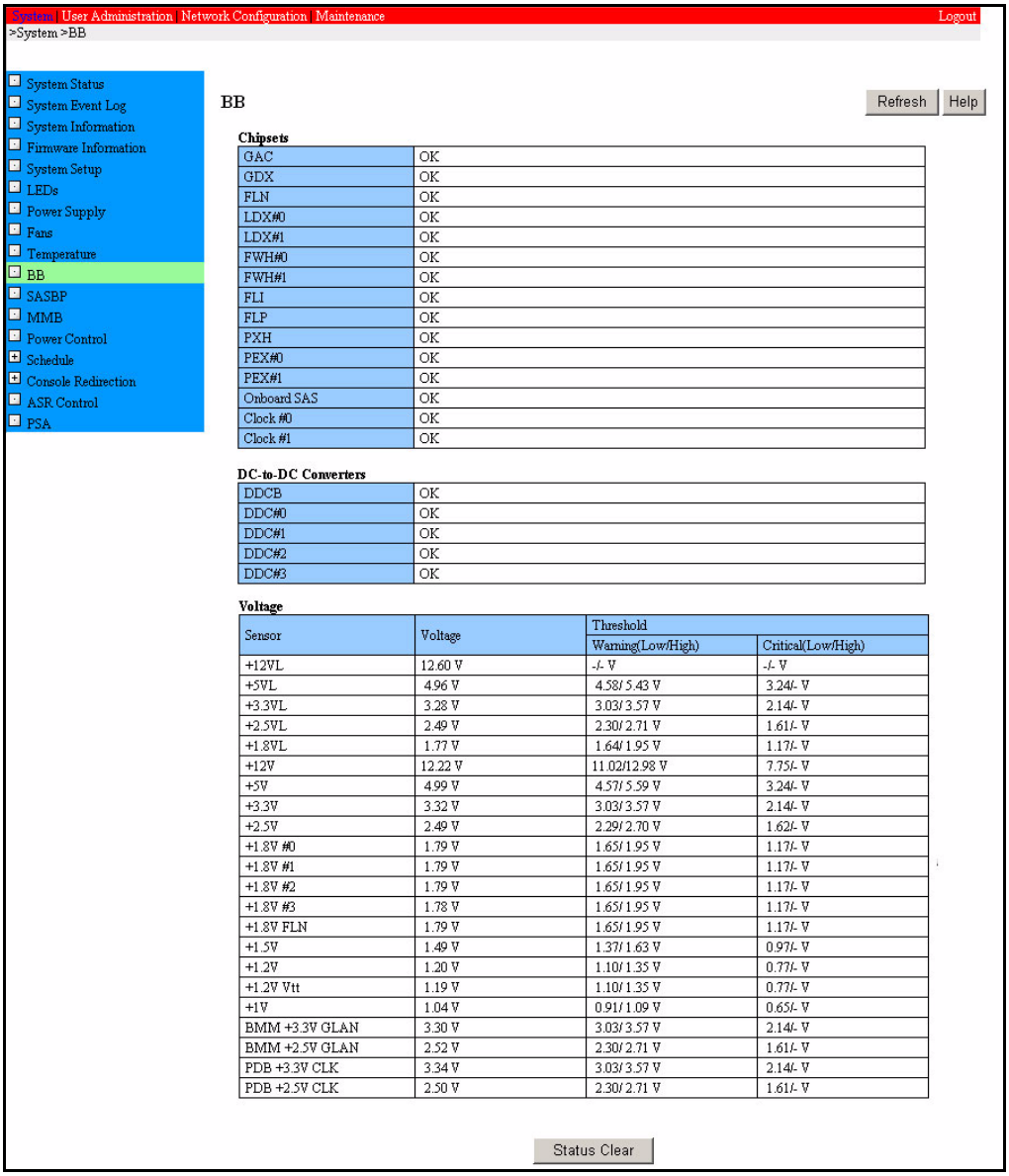


Figure 5.13 [BB] window (2/2)

Table 5.21 Displayed and setting items in the [BB] window

Item	Description
Board Information	
Status	BB status. • OK: Operating normally • Not-present: No BB is mounted. • Warning: A warning was detected for a component mounted on the BB, such as the CPU or memory. • Degraded: A failure has occurred on the CPU, memory, or other component on the BB. (The faulty component can be shut down to continue operation of the entire BB system.) • Failed: Failure
Power Status	BB power status: • On: Powered on • Standby: Standby mode
Part Number	BB part number Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer.
Serial Number	BB serial number Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer.
CPUs	
CPU#	CPU number
Status	CPU status: • OK: Operating normally • Not present: Not installed • Disabled: Normal, but not in use. • Warning: Operating but requires maintenance (Contact a certified service engineer.) • Failed: Failure
Model	CPU product name. Example: Intel® Itanium® 2 Processor 1.50 GHz with 6MB L3 Cache
Stepping	CPU stepping.
Serial Number	CPU serial number Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer.
PPOD	Status of the power pod corresponding to a CPU: • OK • NG

Item	Description
DIMMs	
DIMM#	DIMM number
Status	DIMM status: • OK: Operating normally • Not present: Not installed • Warning: Warning status: (A problem will possibly occur.) • Uncorrectable error: An error (uncorrectable) occurred. • Disabled: Set to the non-operational status • Configuration error: Configuration error • Not supported: Not supported • Unknown: Unknown
Size	DIMM size: • 1GB • 2GB • 4GB If the DIMM [Status] is "Not present," "Not-supported," or "Unknown," this field remains blank.
Rank	DIMM rank number (1 or 2). If the DIMM [Status] is "Not present," "Not-supported," or "Unknown," this field remains blank.
Date Rate	DIMM data rate: • DDR2-533 • DDR2-667 If the DIMM [Status] is "Not present," "Not-supported," or "Unknown," this field remains blank.
Part Number	DIMM part number. If the DIMM [Status] is "Not present," "Not-supported," or "Unknown," this field remains blank.
Serial Number	DIMM serial number. If the DIMM [Status] is "Not present," "Not-supported," or "Unknown," this field remains blank.
BMM	
Status	BMM status: • OK: Operating normally • Not present: Not installed • Failed: Failure
Part Number	BMM part number Note: If "Read Error" is displayed, contact a Fujitsu certified service engineer.

Item		Description
Serial Number		BMM serial number Note: If "Read Error" is displayed, contact a Fujitsu certified service engineer.
MAC Address	GbE#0-0, #0-1 GbE#1-0, #1-1	MAC address of GbE
	Manage-ment LAN port	MAC address of Management LAN port
BMC		BMC status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
FWH#0, FWH#1		FWH#0 and FWH#1 status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
ICH		ICH status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
VGA		VGA status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
GbE#0, GbE#1		GbE status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure

PCI Express Slots

PCI Slot#	PCI Express slot number
Power Status	Power status of the PCI Express slot: • On: Powered on • Standby: Standby mode

Item	Description
Status	PCI Express slot status: • OK: Operating normally • Not-present: Not installed • Failed: Failure • Disabled: Set to the non-operational status
Link Width	Data width of PCI Express slot • PCI-Express x4 • PCI-Express x8
Seg/Bus/Dev	Segment number, bus number, and device number of PCI device
PCI-Express Card Information	PCI-Express card information (64 byte, ASCII)

Chipsets

GAC	GAC status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
GDX	GDX status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
FLN	FLN status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a certified service engineer.) • Failed: Failure
LDX#0, #1	LDX status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a certified service engineer.) • Failed: Failure
FWH#0, #1	FWH status • OK: Operating normally • Warning: Operating but requires maintenance (Contact a certified service engineer.) • Failed: Failure

Item	Description
FLI	FLI status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
FLP	FLP status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
PXH	PXH status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
PEX#0, #1	PEX status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
Onboard SAS	SAS status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
Clock#0, #1	System clock status: • OK: Operating normally • Failed: Failure

DC-to-DC Converters

DDCB	Statuses of DC-to-DC Converter B: • OK: Operating normally • Not present: Not installed • Configuration error: Configuration error • Failed: Failure
DDC#0 to #3	Statuses of DC-to-DC Converters 0 to 3. These statuses are displayed in the same way as the statuses of DC-to-DC Converter B.

Item		Description
Voltage		
Sensor		Voltage sensor type
Voltage		Current voltage reading
Threshold	Warning (Low/High)	Lower and upper limits of the warning-level voltage. If no limit is set, "-" is displayed.
	Critical (Low/High)	Lower and upper limits of the critical-level voltage. If no limit is set, "-" is displayed.

Table 5.22 Button in the [BB] window

Button	Description
Status Clear	Click the [Status Clear] button to display the [BB Status Clear] window. This window enables clearing of the error status of a BB component whose failure was detected.

(1) Menu operation

[System] → [BB]

(2) GUI operation

- Clearing the error status of a component on which an error has been detected

1. Click the [Status Clear] button.
   The [BB Status Clear] window is displayed.
2. The [BB Status Clear] window enables clearing of the error status of a component whose failure was detected.

5.2.11 [BB Status Clear] window

Once an abnormality is detected in a component, the component remains in the abnormal status until the status is cleared.

The [BB Status Clear] window allows you to clear the error status of a component on which an abnormality has been detected. Radio buttons are provided to ensure that you can specify whether to clear all error statuses on the BB at the same time or clear the error status of individual components.

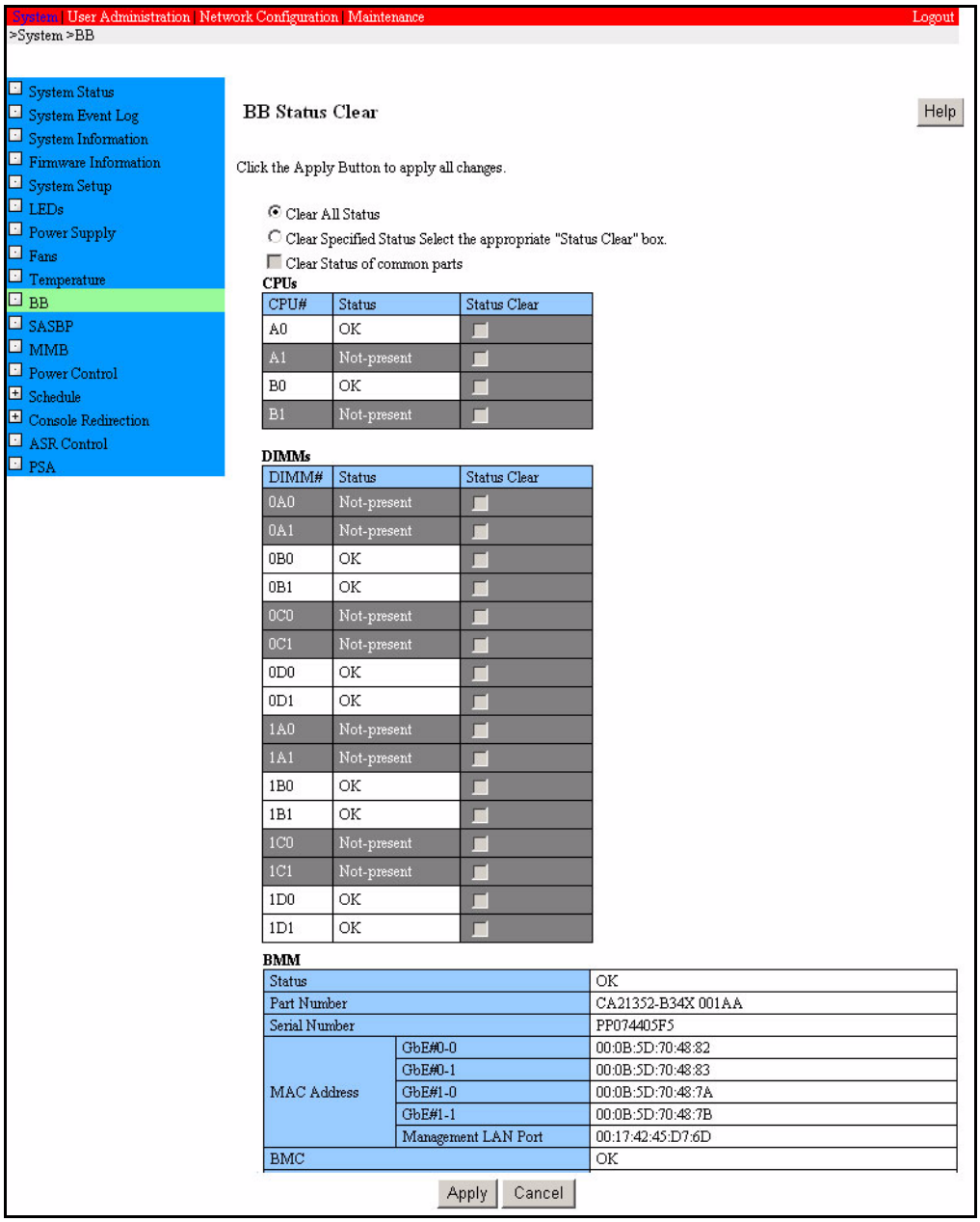


Figure 5.14 [BB Status Clear] window (1/2)

System | User Administration | Network Configuration | Maintenance Logout
>System >BB

- System Status
- System Event Log
- System Information
- Firmware Information
- System Setup
- LEDs
- Power Supply
- Fans
- Temperature
- BB
- SASBP
- MMB
- Power Control
- Schedule
- Console Redirection
- ASR Control
- PSA

BB Status Clear Help

PCI-Express Slots

PCI Slot#	Power Status	Status	Link Width	Seg/Bus/Dev	PCI-Express Card Information
0	On	OK	x4	0/10/0	Unknown
1	Standby	Not-present			
2	Standby	Not-present			
3	Standby	Not-present			
4	Standby	Not-present			
5	Standby	Not-present			

Chipsets

GAC	OK
GDX	OK
FLN	OK
LDX#0	OK
LDX#1	OK
FWH#0	OK
FWH#1	OK
FLI	OK
FLP	OK
PXH	OK
PEX#0	OK
PEX#1	OK
Onboard SAS	OK
Clock #0	OK
Clock #1	OK

DC-to-DC Converters

DDCB	OK
DDC#0	OK
DDC#1	OK
DDC#2	OK
DDC#3	OK

Voltage

Sensor	Voltage	Threshold	
		Warning(Low/High)	Critical(Low/High)
+12VL	12.60 V	-/- V	-/- V
+5VL	4.96 V	4.58/ 5.43 V	3.24/- V
+3.3VL	3.28 V	3.03/ 3.57 V	2.14/- V
+2.5VL	2.49 V	2.30/ 2.71 V	1.61/- V
+1.8VL	1.77 V	1.64/ 1.95 V	1.17/- V
+12V	12.22 V	11.02/12.98 V	7.75/- V
+5V	4.99 V	4.57/ 5.59 V	3.24/- V
+3.3V	3.32 V	3.03/ 3.57 V	2.14/- V
+2.5V	2.49 V	2.29/ 2.70 V	1.62/- V
+1.8V #0	1.79 V	1.65/ 1.95 V	1.17/- V
+1.8V #1	1.79 V	1.65/ 1.95 V	1.17/- V
+1.8V #2	1.79 V	1.65/ 1.95 V	1.17/- V
+1.8V #3	1.78 V	1.65/ 1.95 V	1.17/- V
+1.8V FLN	1.79 V	1.65/ 1.95 V	1.17/- V
+1.5V	1.49 V	1.37/ 1.63 V	0.97/- V
+1.2V	1.20 V	1.10/ 1.35 V	0.77/- V
+1.2V Vtt	1.19 V	1.10/ 1.35 V	0.77/- V
+1V	1.03 V	0.91/ 1.09 V	0.65/- V
BMM +3.3V GLAN	3.30 V	3.03/ 3.57 V	2.14/- V
BMM +2.5V GLAN	2.52 V	2.30/ 2.71 V	1.61/- V
PDB +3.3V CLK	3.34 V	3.03/ 3.57 V	2.14/- V
PDB +2.5V CLK	2.50 V	2.30/ 2.71 V	1.61/- V

Apply Cancel

Figure 5.14 [BB Status Clear] window (2/2)

Table 5.23 Displayed and setting items in the [BB Status Clear] window

Item	Description
Clear All Status	Select this item to clear all error statuses at the same time.
Clear Specified Status Select the appropriate "Status Clear" box.	Select this item to clear the error status of each component individually.
Clear Status of common parts	Select [Clear Status of common parts] to clear the statuses of common parts.
CPUs	
CPU#	CPU number
Status	CPU status: • OK: Operating normally • Not present: Not installed • Disabled: Normal, but not in use. • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
Status Clear	To clear the status of a CPU, select the CPU.
DIMMs	
DIMM#	DIMM number
Status	DIMM status: • OK: Operating normally • Not-present: Not installed • Warning: Warning status: (A problem will possibly occur.) • Uncorrectable error: An error (uncorrectable) occurred. • Disabled: Set to the non-operational status • Configuration error: Configuration error • Not supported: Not supported • Unknown: Unknown
Status Clear	Select the DIMM on which you want to clear the error status.
BMM	
Status	BMM status: • OK: Operating normally • Not present: Not installed • Failed: Failure
Part Number	BMM part number Note: If "Read Error" is displayed, contact a Fujitsu certified service engineer.
Serial Number	BMM serial number Note: If "Read Error" is displayed, contact a Fujitsu certified service engineer.

Item		Description
MAC Address	GbE#0-0, #0-1 GbE#1-0, #1-1	MAC address of GbE
	Manage-ment LAN port	MAC address of Management LAN port
BMC		BMC status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
FWH#0, FWH#1		FWH#0 and FWH#1 status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
ICH		ICH status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
VGA		VGA status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
GbE#0, GbE#1		GbE status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
PCI Express Slots#		PCI Express slot number
Power Status		Power status of the PCI Express slot: • On: Powered on • Standby: Standby mode
Status		PCI Express slot status: • OK: Operating normally • Not-present: Not installed • Failed: Failure • Disabled: Set to the non-operational status

Item	Description
Link Width	Data width of PCI Express slot • PCI-Express x4 • PCI-Express x8
Seg/Bus/Dev	Segment number, bus number, and device number of PCI device
PCI-Express Card Information	PCI-Express card information (64 byte, ASCII)

Chipsets

GAC	GAC status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
GDX	GDX status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
FLN	FLN status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a certified service engineer.) • Failed: Failure
LDX#0, #1	LDX status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a certified service engineer.) • Failed: Failure
FWH#0, #1	FWH status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a certified service engineer.) • Failed: Failure
FLI	FLI status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure

Item	Description
FLP	FLP status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
PXH	PXH status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
PEX#0, #1	PEX status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
Onboard SAS	SAS status: • OK: Operating normally • Warning: Operating but requires maintenance (Contact a Fujitsu certified service engineer) • Failed: Failure
Clock#0, #1	System clock status: • OK: Operating normally • Failed: Failure
DC-to-DC Converters	
DDCB	Statuses of DC-to-DC converter B: • OK: Operating normally • Not-present: Not installed • Configuration error: Configuration error • Failed: Failure
DDC#0 to #3	Statuses of DC-to-DC converters #0 to #3. These statuses are displayed in the same way as the redundancy statuses of DC-to-DC converter B.

Voltage

Sensor		Voltage sensor type
Voltage		Current voltage reading
Threshold	Warning (Low/High)	Lower and upper limits of the warning-level voltage. If no limit is set, a hyphen (-) is displayed.
	Critical (Low/High)	Lower and upper limit of the critical-level voltage. If no limit is set, a hyphen (-) is displayed.

Table 5.24 Buttons in the [BB Status Clear] window

Button	Description
Apply	To clear the status of a component, select the component, and click the [Apply] button.
Cancel	Click the [Cancel] button to not change information and not clear the status of a component.

(1) Menu operation

[System] → [BB] → [Status Clear]

(2) GUI operation

1 Make a selection for component status clearing as follows:

- Click [Clear All Status] to clear the statuses of all components.
- To clear the statuses of components individually, click [Clear Specified Status] and click [Status Clear] on the component on which you want to clear the error status.
- Click [Clear Status of common parts] to clear the statuses of common parts.

2 Click the [Apply] button.
The statuses of the specified components are then cleared.

5.2.12 [SASBP] window

The [SASBP] window allows you to view and set the status of the SASBP board.

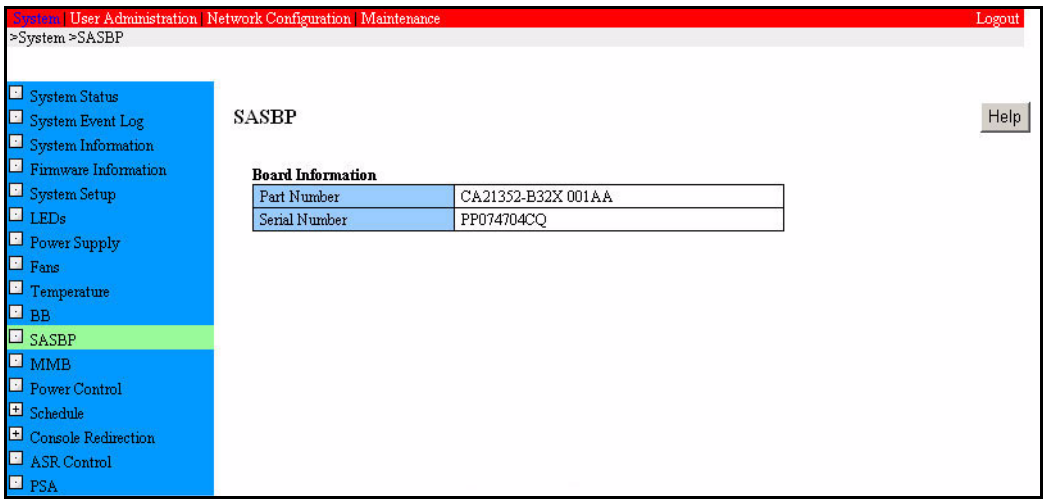


Figure 5.15 [SASBP] window

Table 5.25 Displayed and setting items in the [SASBP] window

Item	Description
Board Information	
Part Number	SASBP part number Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer.
Serial Number	SASBP serial number Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer.

(1) Menu operation

[System] → [SASBP]

(2) GUI operation

None

5.2.13 [MMB] window

The [MMB] window displays MMB information.

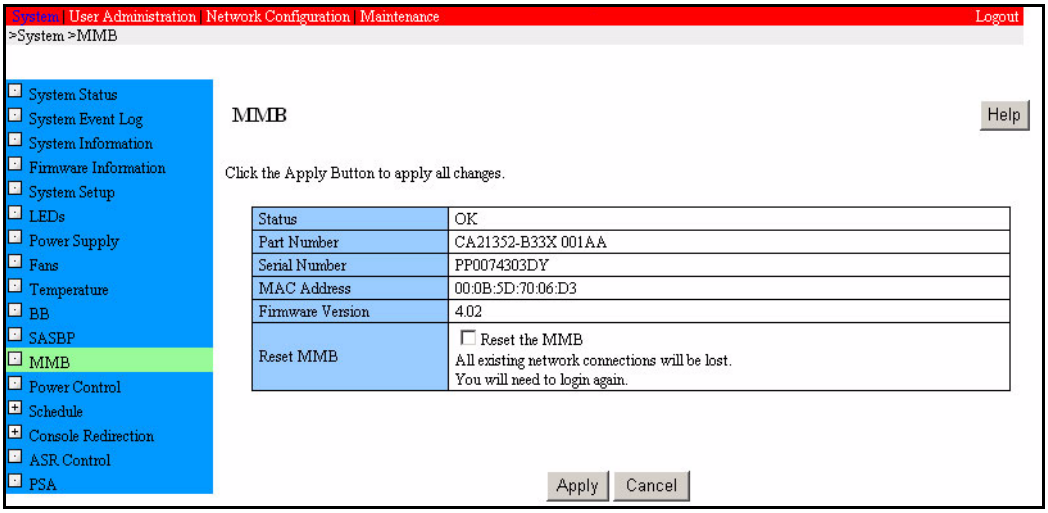


Figure 5.16 [MMB] window

Table 5.26 Displayed and setting items in the [MMB] window

Item		Description
Status		MMB status: • OK: Operating normally • Not present: Not installed • Degraded: Component failure (The faulty component can be isolated to continue operation.) • Failed: Failure
Part Number		MMB part number Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer.
Serial Number		MMB serial number Notes: If "Read Error" is displayed, contact a Fujitsu certified service engineer.
MAC Address	User/Maintenance port	MAC address of the MMB management port.
	REMCS port	MAC address of the MMB REMCS port.
Firmware Version		MMB firmware version

Item	Description
Reset MMB	⚠CAUTION **Guarantee of operation** Do not use this field. Doing so may lead to a malfunction and result in data corruption or a device failure. Check this check box to reset the MMB.

Table 5.27 Buttons in the [MMB] window

Button	Description
Apply	Specify control information, and click the [Apply] button to set the specified information.
Cancel	Click the [Cancel] button to revert to the original settings.

(1) Menu operation

[System] → [MMB]

(2) GUI operation

1 Specify information to change the MMB status, and click the [Apply] button. The specified information is then set to change the MMB status accordingly.

5.2.14 [Power Control] window

The [Power Control] window allows you to perform power control of the entire PRIMEQUEST.

Notes:

- Use the OS shutdown function to shut down the system normally. Only in emergency situations, such as when no response is obtained from the system, should MMB Power-Off (Force Power Off) be used to turn off power.
- If the following condition occurs, contact your Fujitsu certified service engineer. [Power off], [Reset], or [Force Power Off] is executed or a shutdown is executed from the operating system, and, as a result, "Error" is displayed for [Status] in the MMB Web-UI window (information frame). Furthermore, an attempt to display the status of each component in the MMB Web-UI window causes "Read Error" to be displayed for [Part Number] or [Serial Number].

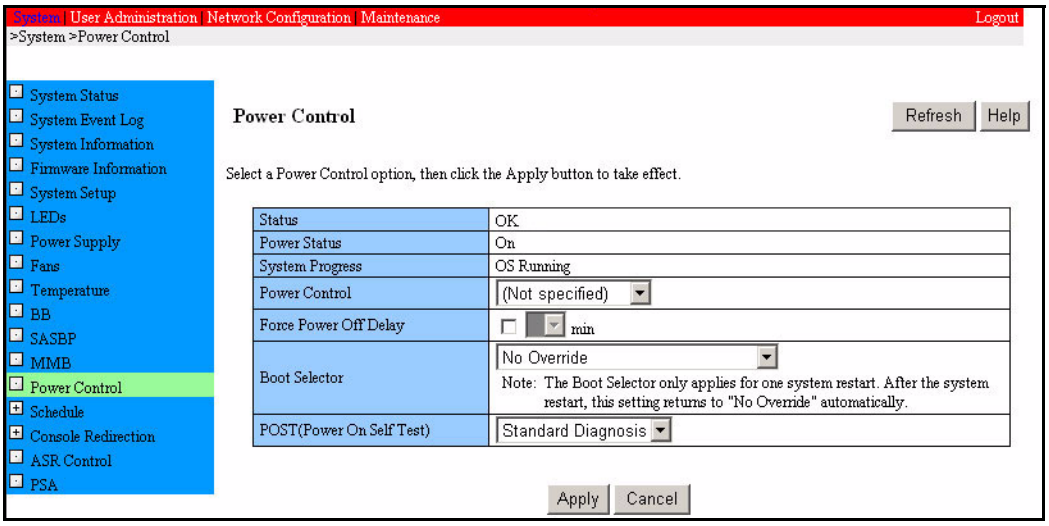


Figure 5.17 [Power Control] window

Table 5.28 Displayed and setting items in the [Power Control] window

Item	Description
Status	System status: • OK: Operating normally • Degraded: Component failure (The faulty component can be isolated to continue operation.) • Warning: Warning status (A problem will possibly occur.) • Failed: Failure
Power Status	System power status: • On: Powered on • Standby: Standby mode
System Progress	Indicates the current status of the system. • Power Off: Power is off. • Power On In Progress: The system is in power-on sequence. • Reset: The system is being reset. • POST XXXXh enter: The process identified by POST Code = XXXXh has started. • Boot: The system is in one of the following states: - The system is being booted. - PSA is not installed. - Installation is in progress. - Backup or restoration using Systemcast Wizard is in progress. • OS Running: The OS is running. • OS Shutdown: The OS is shutting down. • Panic: The system is in panic state. • Power Off In Progress: The system is in power-off sequence. • Check Stop: The system is stopped. • Initiate soft-shutdown: The count-down for forced power-off has started.

Item	Description
Power Control	If the power is already on, the [Power On] selection is not displayed. Conversely, if the power is already off, the [Power Off], [Reset], [INIT], [Power Cycle], and [Force Power Off] selections are not displayed. • Power On: Turns on the power. • Power Off: Turns off the power. • Power Cycle: Forcibly turns off the power and then turns the power on again. • Reset: Resets the system. • INIT: Causes an INIT interrupt to generate a dump. • Force Power Off: Forcibly turns off the power. • Not specified: Select this item when issuing no instructions. Note: Executing INIT forcibly terminates applications running in the system. Before executing INIT, stop important applications. Also, unmount unnecessary file systems.
Force Power Off Delay	Specify whether to forcibly power off the system in the event that the system is not powered off by a shutdown instruction issued to its OS during the power-off sequence. If [Power Off] is specified in [Power Control], the delay time can be specified (range: 1 to 9 minutes). The system is powered off when the specified delay time has elapsed. The default setting is no forcible power-off.
Boot Selector	Specify the boot device by overwriting the EFI Boot Manager settings. Select the boot device from the pulldown menu: • No Overwrite: The EFI Boot Manager settings are used to boot the system. • Force boot into EFI Boot Manager: EFI Boot Manager is started, and it then waits for input. EFI Boot Manager can thereby be used to select a boot device and boot the system. • Force PXE: The EFI Boot Manager settings are overwritten, and PXE is forcibly executed. • Force boot from DVD: The EFI Boot Manager settings are overwritten, and a forced boot of the system from the DVD is attempted. The default is [No Overwrite].

Item	Description
POST	Select the type of Power On Self Test (POST) from the pulldown menu: • Fast Boot: Fast boot with minimal diagnosis • Standard Diagnosis: Standard diagnosis • Full Diagnosis: Complete diagnosis with all diagnostic items The default is [Standard Diagnosis].

Table 5.29 Buttons in the [Power Control] window

Button	Description
Apply	To set the values specified in the power control items, click the [Apply] button. A confirmation dialog box then opens. Click [OK] in the dialog box to set the values.
Cancel	Click the [Cancel] button to revert to the original settings in the power control items.

(1) Menu operation

[System] → [Power Control]

(2) GUI operation

- Power control setting

  1 Select from the [Power Control] pulldown list and specify a power control item, and click the [Apply] button.
  A confirmation dialog box opens.

  2 Click the [OK] button to set the specified values.
  Additional note: If specified power control action fails, a warning dialog box about that failure opens.

  Remarks: If control of the specified power supply fails, a warning dialog box opens.

- Boot device setting

  1 Select the boot device by overwriting the EFI Boot Manager settings (select the boot device from the pulldown list of [Boot Selector]), and click the [Apply] button. The boot device is now set.

5.2.15 Schedule menu

The [Schedule] menu provides the [Schedule Control] window and [Schedule List] window. This section describes these windows and their operations.

5.2.15.1 [Schedule Control] window

Information for scheduled operation can be specified in the [Schedule Control] window.

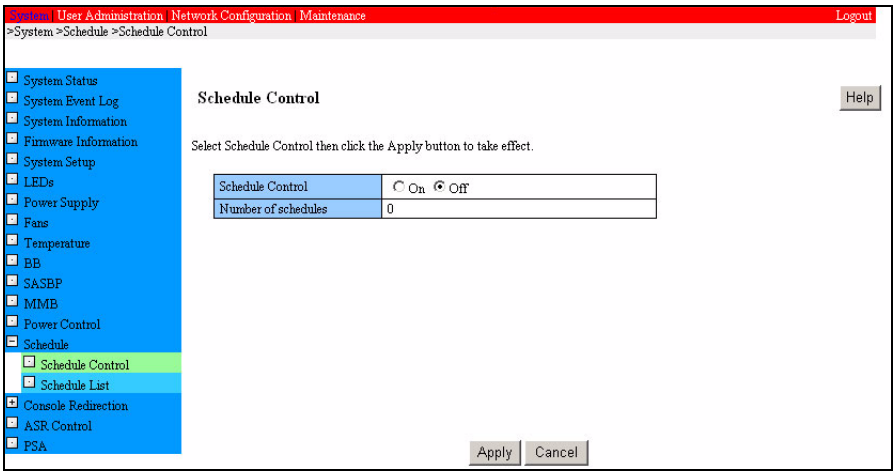


Figure 5.18 [Schedule Control] window

Table 5.30 Displayed and setting items in the [Schedule Control] window

Item	Description
Schedule Control	Specify whether to enable scheduled operation: • On: Enables scheduled operation. • Off: Disables scheduled operation.
Number of schedules	Number of schedules that have been set

Table 5.31 Buttons in the [Schedule Control] window

Button	Description
Apply	Sets the specified values for scheduled operation.
Cancel	Reverts to the original settings for scheduled operation.

(1) Menu operation

[System] → [Schedule] → [Schedule Control]

(2) GUI operation

1 Specify whether to enable scheduled operation by clicking a radio button, and click the [Apply] button.
The specified values for scheduled operation are then set.

5.2.15.2 [Schedule List] window

The power-on and power-off schedule for the system can be set from the [Schedule List] window.

Remarks:

- The power-off function may not work in the system in which Windows is installed as the OS.
- This window displays the power-on and power-off schedule in ascending order of the starting date of Term. The title row in the table remains visible during scrolling.

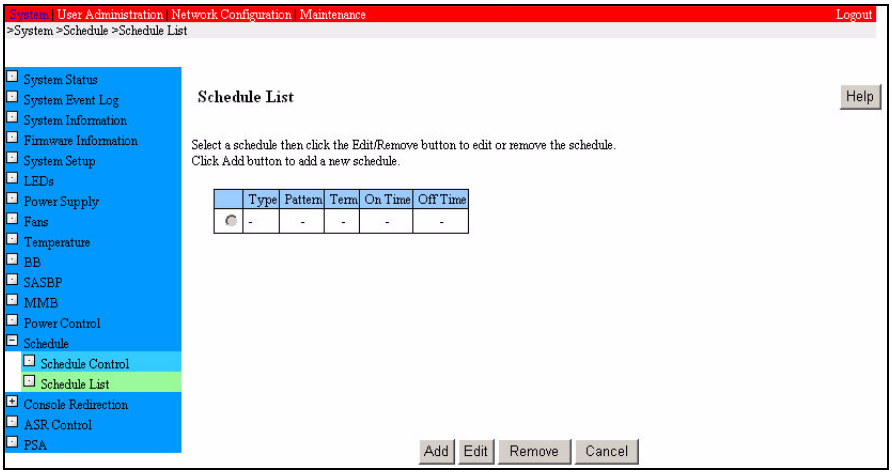


Figure 5.19 [Schedule List] window

Table 5.32 Displayed and setting items in the [Schedule List] window

Item	Description
(Radio buttons)	Select the schedule to be edited or deleted.
Type	Schedule type specified: • Daily: Daily operation • Weekly: Weekly operation • Monthly: Monthly operation • Special: Operation on specific dates For details on the types, see Figure 5.20, "[Add Schedule] window." below.
Pattern	Schedule pattern, such as days of the week, the repetition cycle, and specific dates. For details on the patterns, see Figure 5.20, "[Add Schedule] window." below.
Term	Term as particular months or specified dates. For details on display of this item, see Figure 5.20, "[Add Schedule] window." below.
On Time	Power-on time. For details on display of this item, see Figure 5.20, "[Add Schedule] window." below.
Off Time	Power-off time. For details on display of this item, see Figure 5.20, "[Add Schedule] window." below.

Table 5.33 Buttons in the [Schedule List] window

Button	Description
Add	Click the [Add] button to display the [Add/Edit Schedule] window. A new schedule can be added from this window. For details, see Figure 5.20, "[Add Schedule] window." below.
Edit	Select an existing schedule by clicking its radio button, and click the [Edit] button to display the [Add/Edit Schedule] window. The existing schedule can be changed in this window. For details, see Figure 5.20, "[Add Schedule] window." below.
Remove	Select a schedule by clicking its radio button, click the [Remove] button, and a confirmation dialog box opens. Click the [OK] button to delete the schedule.
Cancel	Click the [Cancel] button to not change information and to cancel adding, changing, or deleting of any schedule.

(1) Menu operation

[System] → [Schedule] → [Schedule List]

(2) GUI operation

- Adding a new schedule
  1. Click the [Add] button.
     The [Add Schedule] window is displayed.
  2. Add a schedule in the [Add Schedule] window.
- Changing a schedule
  1. To change a schedule, select the schedule by selecting its radio button in the column on the left end of the schedule list, and click the [Edit] button.
     The [Edit Schedule] window is displayed.
  2. Edit the schedule in the [Edit Schedule] window.
- Deleting a schedule
  1. To delete a schedule, select the schedule by selecting its radio button in the column on the left end of the schedule list, and click the [Delete] button.
     A confirmation dialog box opens.
  2. To delete the schedule, click the [OK] button in the dialog box.
     The schedule is deleted.

[Add Schedule] window

A new power-on or power-off schedule can be added in the [Add Schedule] window.

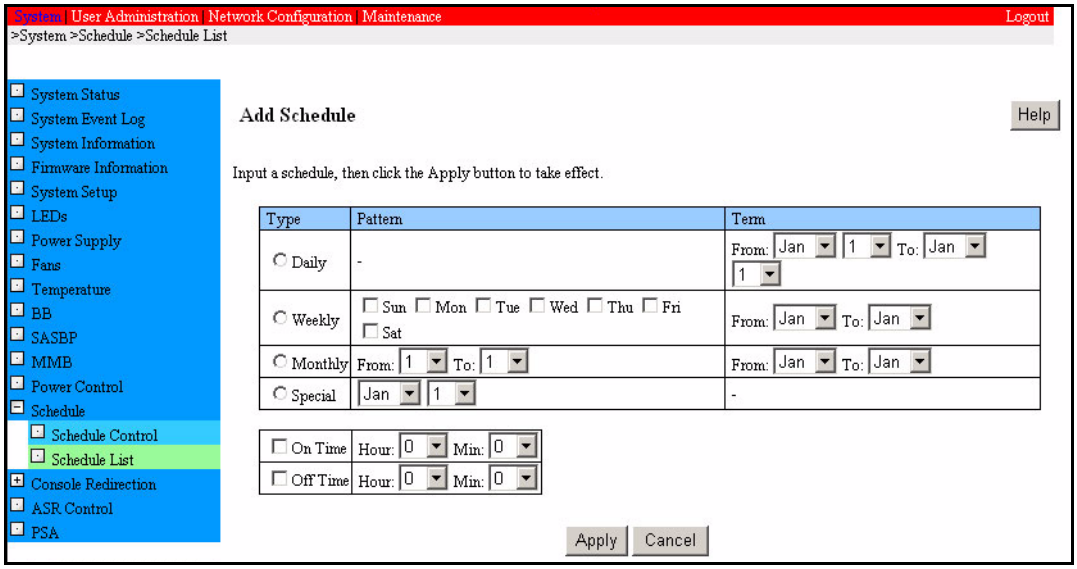


Figure 5.20 [Add Schedule] window

Table 5.34 Displayed and setting items in the [Add Schedule] window

Item	Description
Type	For a schedule selected, specify one of the following schedule types: • Daily: Select [Daily] to schedule daily operation. Additionally, specify the start and end dates of this daily operation period. • Weekly: Select [Weekly] to schedule weekly operation, and specify the days of the week for scheduled operation. Additionally, specify the start and end months of this weekly operation period. • Monthly: Select [Monthly] to schedule monthly operation, and specify the start and end days in the month. Additionally, specify the start and end months of this monthly operation period. • Special: Select [Special] for scheduled operation on a specific date every year, and specify the date.
Pattern	Depending on the schedule type, specify a schedule pattern, such as days of the week, the repetition cycle, or a specific date.
Term	Depending on the schedule type and pattern, specify the months or dates of this period.

Item	Description
On Time	Specify whether the power-on processing is performed on a scheduled day of operation. For power-on processing, specify the power-on time. The setting range for the hour is 24 or less, and the setting range for the minutes is 00, 10, 20, 30, 40, or 50.
Off Time	Specify whether the power-off processing is performed on a scheduled day of operation. For power-off processing, specify the power-off time. The setting range for the hour is 24 or less, and the setting range for the minutes is 00, 10, 20, 30, 40, or 50.

Table 5.35 Buttons in the [Add Schedule] window

Button	Description
Apply	Sets the specified values for the schedule items.
Cancel	Reverts to the original settings in the schedule items.

(1) Menu operation

[System] → [Schedule] → [Schedule List] → [Add] button

(2) GUI operation

1 Select a schedule type by clicking a radio button, specify values in [Pattern], [Term], [On Time], and [Off Time], and click the [Apply] button.
The specified values for the schedule items are then set.

[Edit Schedule] window

An existing schedule of power-on or power-off can be changed in the [Edit Schedule] window.

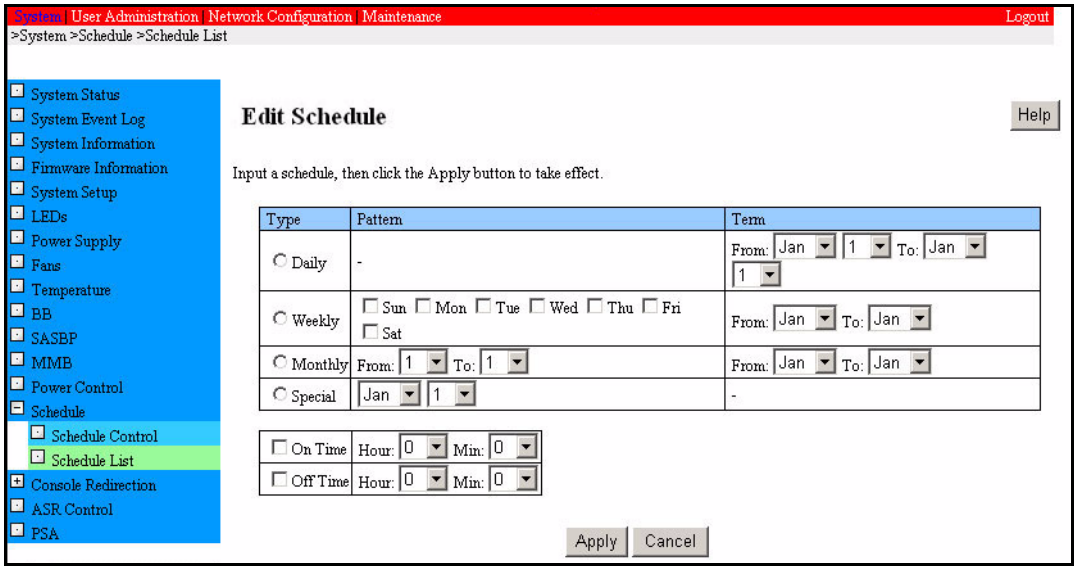


Figure 5.21 [Edit Schedule] window

Table 5.36 Displayed and setting items in the [Edit Schedule] window

Item	Description
Type	Specify one of the following schedule types: • Daily: Select [Daily] to schedule daily operation. Additionally, specify the start and end dates of this daily operation period. • Weekly: Select [Weekly] to schedule weekly operation, and specify the days of the week for scheduled operation. Additionally, specify the start and end months of this weekly operation period. • Monthly: Select [Monthly] to schedule monthly operation, and specify the start and end days in the month. Additionally, specify the start and end months of this monthly operation period. • Special: Select [Special] for scheduled operation on a specific date every year, and specify the date.
Pattern	Depending on the schedule type, specify a schedule pattern, such as days of the week, the repetition cycle, or a specific date.
Term	Depending on the schedule type and pattern, specify the months or dates of this period.

Item	Description
On Time	Specify whether the power-on processing is performed on a scheduled day of operation. For power-on processing, specify the power-on time. The setting range for the hour is 24 or less, and the setting range for the minutes is 00, 10, 20, 30, 40, or 50.
Off Time	Specify whether the power-off processing is performed on a scheduled day of operation. For power-off processing, specify the power-off time. The setting range for the hour is 24 or less, and the setting range for the minutes is 00, 10, 20, 30, 40, or 50.

Table 5.37 Buttons in the [Edit Schedule] window

Button	Description
Apply	Sets the specified values for the schedule items.
Cancel	Reverts to the original settings in the schedule items.

(1) Menu operation

[System] → [Schedule] → [Schedule List] → [Edit] button

(2) GUI operation

1 Select a schedule type by clicking a radio button, specify values in [Pattern], [Term], [On Time], and [Off Time], and click the [Apply] button.
The specified values for the schedule items are then set.

5.2.16 [Console Redirection] menu

The [Console Redirection] menu provides the [Console Redirection Switch] window and [Console Redirection] window. This section describes these windows and their operations.

5.2.16.1 [Console Redirection Switch] window

The [Console Redirection Switch] window can be used to connect serial output to the COM port or redirect it to the MMB.

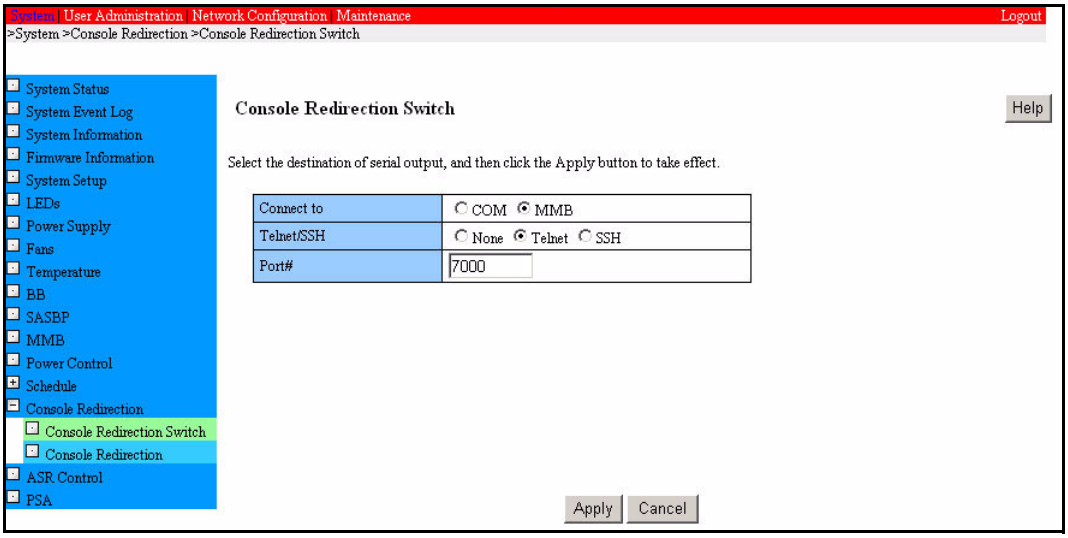


Figure 5.22 [Console Redirection Switch] window

Table 5.38 Displayed and setting items in the [Console Redirection Switch] window

Item	Description
Connect to	For serial output from the OS, select either a connection to the COM port or redirection to a remote client via the MMB: • COM: Output to the COM port • MMB: Redirected to a remote client via the MMB The default setting is [COM].
Telnet/SSH	Either [Telnet] or [SSH] can be selected for the protocol used in a connection to a remote client for [Console Redirection]. If [None] is selected, only the [Console Redirection] window of the Web-UI can be displayed. • Telnet • SSH • None

Item	Description
Port	A port number of 1024 or higher can be specified for a connection to a remote client for [Console Redirection]. The default is [7000].

Table 5.39 Buttons in the [Console Redirection Switch] window

Button	Description
Apply	Specify a redirection method and a port number, click the [Apply] button, and the specified values are set.
Cancel	Click the [Cancel] button to revert to the original settings.

(1) Menu operation

[System] → [Console Redirection] → [Console Redirection Switch]

(2) GUI operation

1 Select settings in [Console Redirection Switch] and the [Telnet/SSH] by clicking radio buttons, and click the [Apply] button.
The specified switch values are then set.

- Example of operation with terminal software on a remote client

For a [Console Redirection] connection in Figure 5.22, enter the following command:

```
#
# telnet <MMB_IP_address> 7000
```

5.2.16.2 [Console Redirection] window

The [Console Redirection] window displays console output. This console is for output only and does not accept any input.

Note: The [Console Redirection] window may not be displayed normally because of the following restrictions:

- The displayed window is not the same as that output to the terminal in the following cases because the [Console Redirection] window outputs escape sequences without modification:
  - An operation is performed with the [Delete], [Backspace], [Page Up], or [Page Down] key.
  - The ls command is executed on the OS console (the beginning of the prompt is normally not displayed).
  - Colored characters are displayed.
- The [Console Redirection] window supports the ISO-8859-1 character code set. If the displayed window includes any character that is not supported, the [Console Redirection] window contents may not be normally displayed.

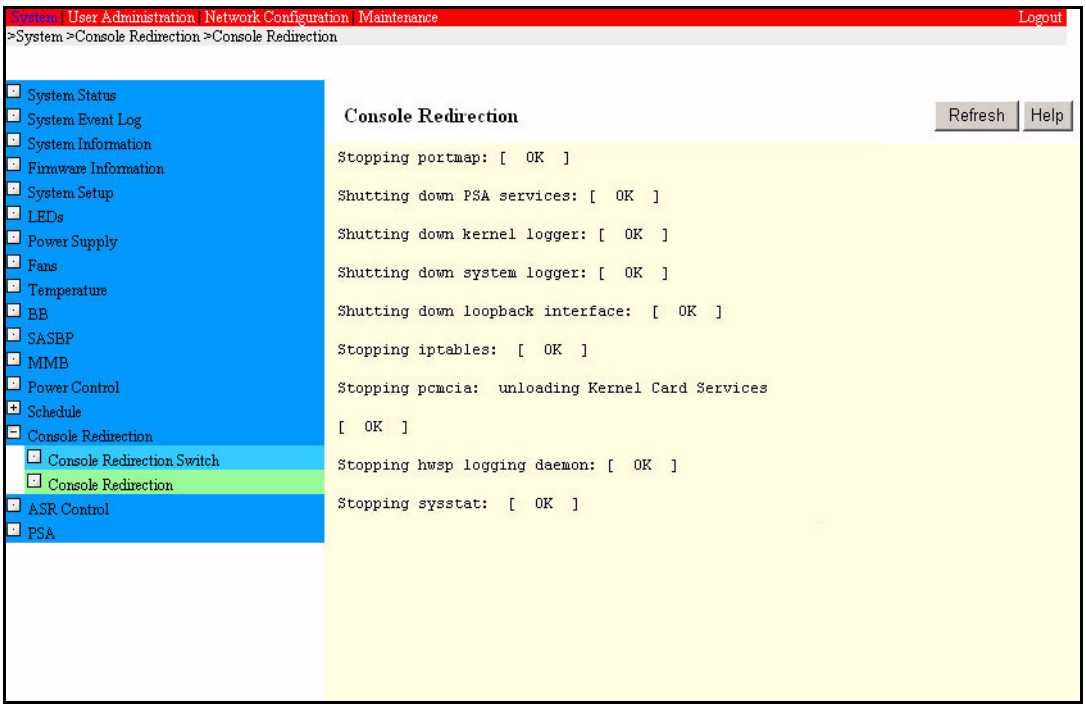


Figure 5.23 [Console Redirection-1] window

Console output is displayed with the latest line as the bottom line. Past data can be viewed by scrolling up in the window.

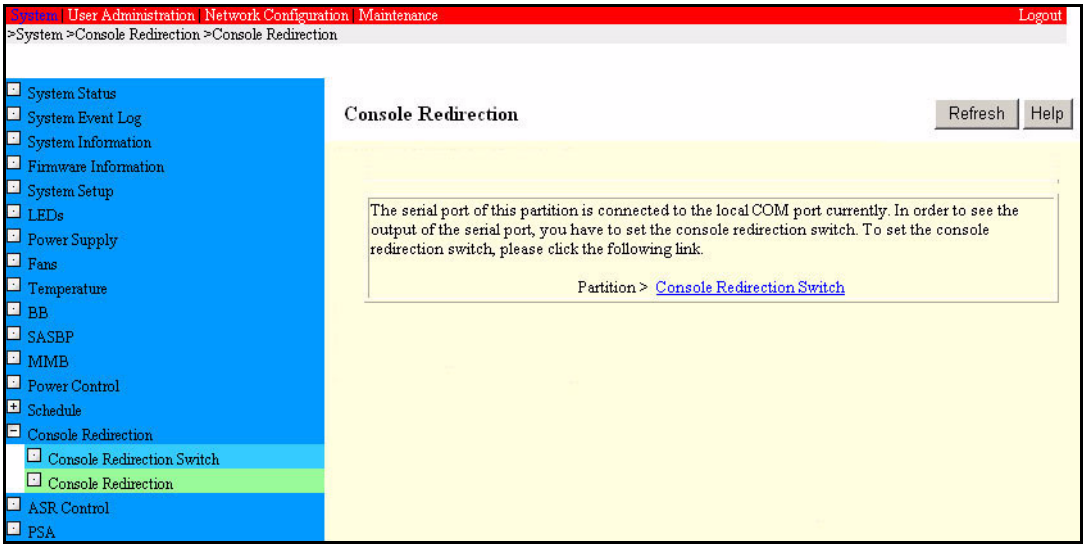


Figure 5.24 [Console Redirection-2] window

If the output serial port is connected to a COM port instead of the MMB, the above window is displayed because console output cannot be displayed.

For details, see Section 5.2.16.1, "[Console Redirection Switch] window."

(1) Menu operation

[System] → [Console Redirection] → [Console Redirection]

(2) GUI operation

None

5.2.17 [ASR (Automatic Server Restart) Control] window

The conditions for automatic restart can be specified in the [ASR (Automatic Server Restart) Control] window.

CAUTION

Malfunction

Before any of the following operations is performed, [Disable] must be set for the Boot Watchdog in the [Watchdog] window of PSA.

- Booting from a CD-ROM disk
- Booting the system in single-user mode (Linux)
- Booting the system in safe mode (Windows)
- Backing up or restoring data by using SystemcastWizard

If any of the above operations is performed with [Enable] set for the Boot Watchdog, OS restart is attempted repeatedly for the specified number of times. The system then takes the specified action (Stop rebooting and Power Off, Stop rebooting, or Diagnostic interrupt assert). The number of retries of the OS restart and the actions to be taken can be set in the [ASR Control] window for the MMB-UI.

In the [ASR Control] window, check [Cancel Boot Watchdog], and click the [Apply] button. [Disable] can thus be forcibly set for the Boot Watchdog.

For details about the [Watchdog] window of PSA, see Section 7.15.1, "[Watchdog] window," in Part IV, "PSA."

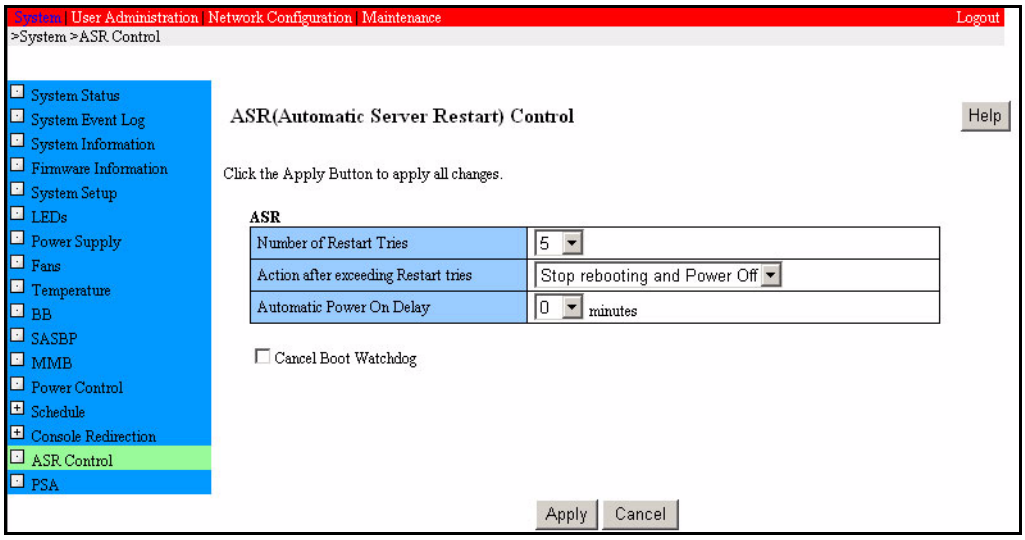


Figure 5.25 [ASR (Automatic Server Restart) Control] window

Table 5.40 Displayed and setting items in the [ASR (Automatic Server Restart) Control] window

Item	Description
Number of Restart Tries	Specify the number of OS restarts attempted following a timeout due to the Boot Watchdog or PSA software watchdog. The setting range is 0 to 10. The default setting is 5. • If 0 is specified, the specified action is not executed even after a lapse of the time at which a timeout should occur. Do not specify 0 when watchdog monitoring is being performed. • If 0 is specified, sadump is not activated even after expiry of the monitoring time. Do not specify 0 when time monitoring is being performed.
Action after exceeding Restart tries	Specify the action to be taken if the repeated restart attempts due to a watchdog timeout or other causes exceed the above number of retries. The action types are as follows: • Stop rebooting and Power Off • Stop rebooting • Diagnostic Interrupt assert The default setting is [Stop rebooting and Power Off].
Automatic Power On Delay	Specify the delay time before the power-on operation in an automatic restart. The setting range is 0 to 10 minutes. The default setting is 0 minutes.

Item	Description
Cancel Boot Watchdog	Select [Cancel Boot Watchdog] to disable OS boot monitoring. If the Boot Watchdog is canceled in this window, the system does not initiate OS boot monitoring until [Enable] is set again for the Boot Watchdog in the [Watchdog] window of PSA. For details about the [Watchdog] window of PSA, see Section 7.15.1, "[Watchdog] window," in Part IV, "PSA." The default is [No Check]. Remarks: OS boot monitoring is a PSA function. The monitoring starts when the Boot Watchdog timeout time is set in the PSA window. If the specified Boot Watchdog timeout time is too short, however, a timeout may occur before the system starts PSA, which can stop the Boot Watchdog timer. As a result, repeated reboots may occur. In such cases, PSA has not yet started, and the PSA page that provides the Boot Watchdog function cannot be displayed, so the Boot Watchdog cannot be displayed. Likewise, if any of the following operations is performed, PSA will not boot, resulting in any of the aforementioned problems: • Booting from a CD-ROM disk • Booting the system in single-user mode (Linux) • Booting the system in safe mode (Windows) • Backing up or restoring data by using SystemcastWizard Provided as a measure against this problem, this check box disables the Boot Watchdog without using PSA.

Table 5.41 Buttons in the [ASR (Automatic Server Restart) Control] window

Button	Description
Apply	Click the [Apply] button to: • Set the specified values in items such as [Number of Restart Tries] [Action after exceeding Restart tries]. • Disable the Boot Watchdog if the [Cancel Boot Watchdog] check box is checked.
Cancel	Click the [Cancel] button to revert to the original settings.

(1) Menu operation

[System] → [ASR Control]

(2) GUI operation

1 Specify values in items in the window and check the [Cancel Boot Watchdog] check box as required, and click the [Apply] button.
The specified values are then set. Furthermore, if the [Cancel Boot Watchdog] check box is checked, the Boot Watchdog is disabled.

5.3 User Administration Menu

The [User Administration] menu enables user administration on the PRIMEQUEST-series machine.

5.3.1 [User List] window

The [User List] window displays information on registered user accounts.

This window is displayed only for users with the administrator privilege.

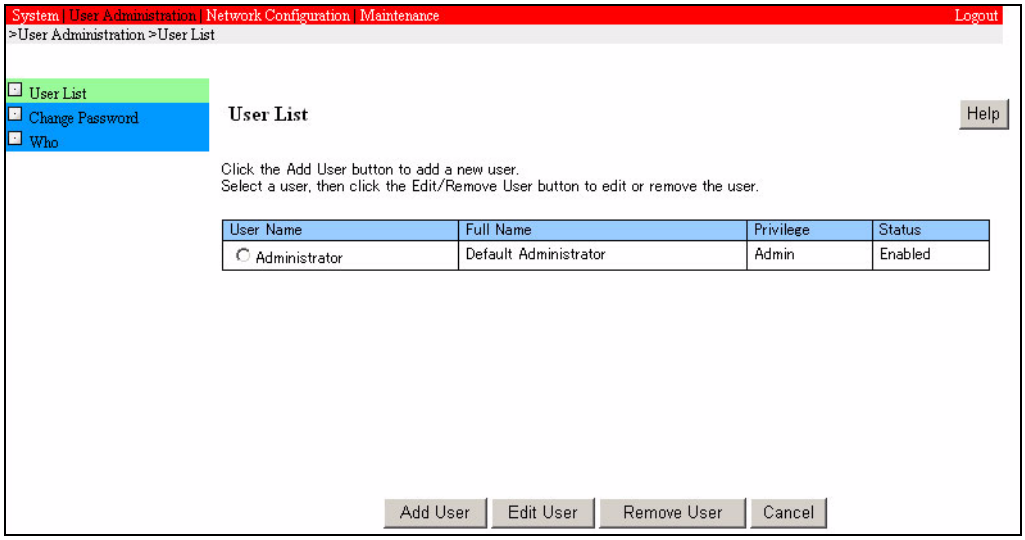


Figure 5.26 [User List] window

Users whose status is set to [Disable] are grayed out.

Table 5.42 Displayed and setting items in the [User List] window

Item	Description
User name	Indicates the user name.
Full Name	Indicates the actual name or other information associated with [User Name].
Privilege	User account privilege
Status	Current account status: • Enable: Available • Disabled: Not available

Table 5.43 Buttons in the [User List] window

Button	Description
Add User	Click the [Add User] button to display the [Add/Edit User] window. A new user can be registered in this window.
Edit User	Select a user from the list of users, and click the [Edit User] button to display the [Add/Edit User] window. Management information for the user can be changed in this window.
Remove User	Select a user from the list of users, click the [Remove User] button, and a confirmation dialog box opens. Click the [OK] button to remove the user.
Cancel	Click the [Cancel] button to revert to the original settings without any modifications.

(1) Menu operation

[User Administration] → [User List]

(2) GUI operation

- Registering a new user
  1. Click the [Add User] button.
     The [Add User] window is displayed.
  2. Register a new user in the [Add User] window.
- Changing management information for a user
  1. Select a user by clicking the radio button next to the user name, and click the [Edit User] button.
     The [Edit User] window is displayed.
  2. Edit management information for the user in the [Edit User] window.
- Removing a user
  1. Select a user by clicking the radio button next to the user name, and click the [Remove User] button.
     A [Confirm Removal] dialog box opens.
  2. Click the [OK] button in the [Confirm Removal] dialog box to remove the user.
     The user is removed.

5.3.1.1 [Add User] window

User management information can be changed in the [Add User] window.

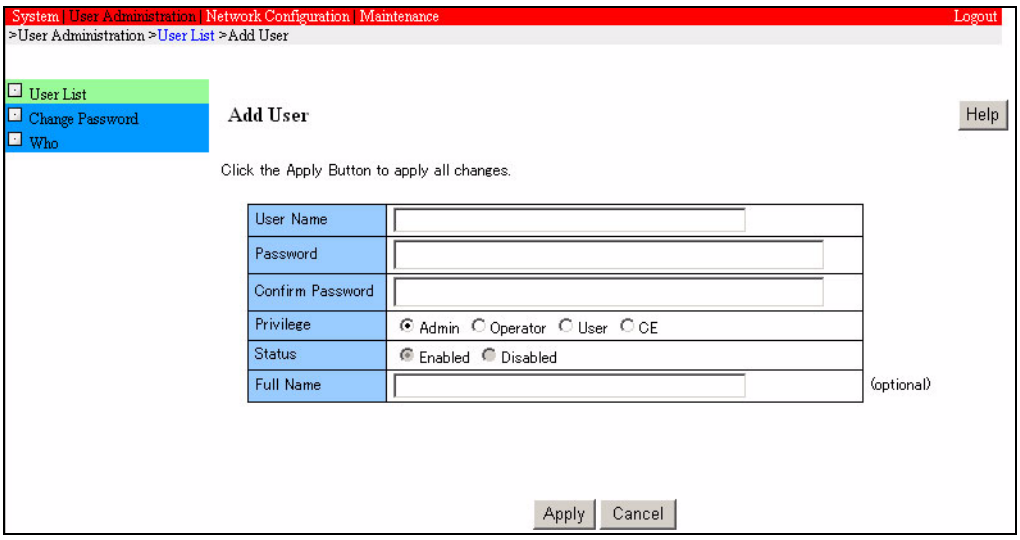


Figure 5.27 [Add User] window

Table 5.44 Displayed and setting items in the [Add User] window

Item	Description
User name	Specify a user name. The user name must be from 8 to 32 characters long. You can use the following characters for user names: 0-9, a-z, A-Z, - (hyphen), _ (underscore) The first character must be one of a-z or A-Z.
Password	Specify a password. The password must be from 8 to 32 characters long. You can use the following characters for passwords: 0-9, a-z, A-Z, special characters: ! " # $ % & ' ( ) = - ^ ~ \ @ ` [ ] { } : * ; + ? < . > , / _ |
Confirm Password	Enter the password again for confirmation.

Item	Description
Privilege	User account privilege • [User]: Permitted only to refer to the PRIMEQUEST-series machine status. • [CE]: Permitted to refer to the PRIMEQUEST-series machine status and operate maintenance. • [Operator]: Permitted to refer to the PRIMEQUEST-series machine status and configure system settings. • [Admin]: Permitted to perform every type of operation. Note: [Admin] means administrator privilege.
Status	Specify the current account status: • Enabled: Available • Disabled: Not available
Full Name	Enter a real name or other such name that is related to [User Name]. The full name must not be longer than 32 characters.

Since user privileges are set to restrict users' operation of the MMB, users who do not have the appropriate privileges cannot operate the MMB. For details on operation restrictions according to privileges, see Section 5.1, "List of Menus in the Web-UI Window."

Table 5.45 User privilege levels and operation restrictions

Privilege level	Operation	Description
User	P	Referring to the PRIMEQUEST system status
	NP	Setting system configuration information
	NP	Turning on or off power to the system
CE	P	Referring to the PRIMEQUEST system status
	NP	Changing user management and network settings
	NP	Turning on or off power to the system by using the normal power-on or power-off procedure
	P	Performing maintenance operations
Operator	P	Referring to and setting the system status
	NP	Changing user management settings and LAN configurations
Administrator	P	All operations

[Operation] P: Permitted NP: Not permitted

Table 5.46 Buttons in the [Add User] window

Button	Description
Apply	Sets the specified values and redisplays the [User List] window.
Cancel	Redisplays the [User List] window without setting the specified values.

(1) Menu operation

[User Administration] → [User List] → [Add User] button

(2) GUI operation

1 Specify user management information, and click the [Apply] button.
Then, the specified management information is set, and the [User List] window is displayed again.

5.3.1.2 [Edit User] window

User management information can be changed in the [Edit User] window.

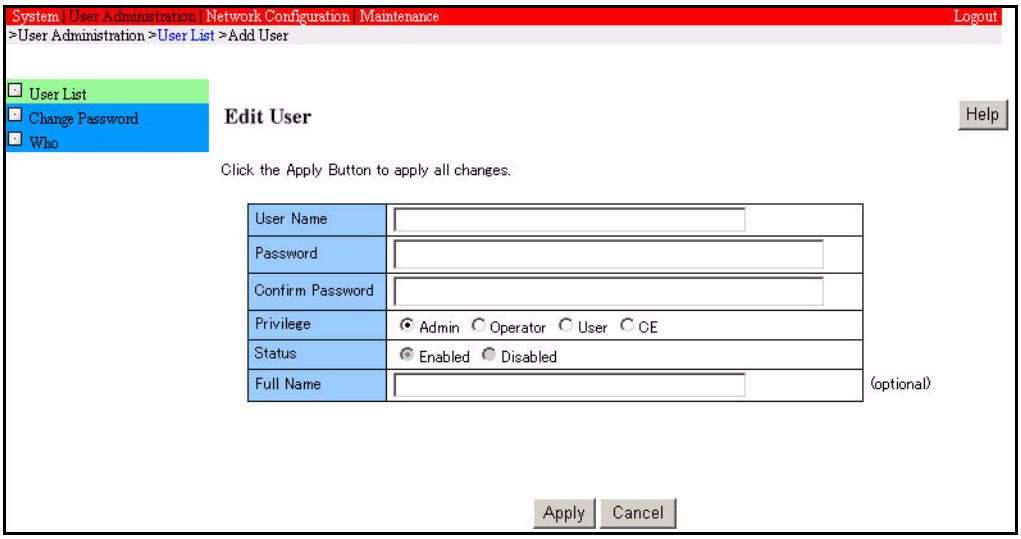


Figure 5.28 [Edit User] window

Table 5.47 Displayed and setting items in the [Edit User] window

Item	Description
User name	Specify a user name. The user name must be from 8 to 32 characters long. You can use the following characters for user names: 0-9, a-z, A-Z, - (hyphen), _ (underscore) The first character must be one of a-z or A-Z.
Password	Specify a password. The password must be from 8 to 32 characters long. You can use the following characters for passwords: 0-9, a-z, A-Z, special characters: ! " # $ % & ' ( ) = - ^ ~ \ @ ` [ ] { } : * ; + ? < . > , / _ |
Confirm Password	Enter the password again for confirmation.

Item	Description
Privilege	User account privilege • [User]: Permitted only to refer to the PRIMEQUEST-series machine status. • [CE]: Permitted to refer to the PRIMEQUEST-series machine status and operate maintenance. • [Operator]: Permitted to refer to the PRIMEQUEST-series machine status and configure system settings. • [Admin]: Permitted to perform every type of operation.
Status	Specify the current account status: • Enabled: Available • Disabled: Not available
Full Name	Enter a real name or other such name that is related to [User Name]. The full name must not be longer than 32 characters.

Since user privileges are set to restrict users' operation of the MMB, users who do not have the appropriate privileges cannot operate the MMB. For details on operation restrictions according to privileges, see Section 5.1, "List of Menus in the Web-UI Window."

Table 5.48 User privilege levels and operation restrictions

Privilege level	Operation	Description
User	P	Referring to the PRIMEQUEST system status
	NP	Setting system configuration information
	NP	Turning on or off power to the system
CE	P	Referring to the PRIMEQUEST system status
	NP	Changing user management and network settings
	NP	Turning on or off power to the system by using the normal power-on or power-off procedure
	P	Performing maintenance operations
Operator	P	Referring to and setting the system status
	NP	Changing user management settings and LAN configurations
Administrator	P	All operations

[Operation] P: Permitted NP: Not permitted

Table 5.49 Buttons in the [Edit User] window

Button	Description
Apply	Sets the specified values and redisplays the [User List] window.
Cancel	Redisplays the [User List] window without setting the specified values.

(1) Menu operation

[User Administration] → [User List] → [Edit User] button

(2) GUI operation

1 Specify user management information, and click the [Apply] button. Then, the specified management information is set, and the [User List] window is displayed again.

5.3.2 [Change Password] window

Users who are logged in can change their own passwords in the [Change Password] window.

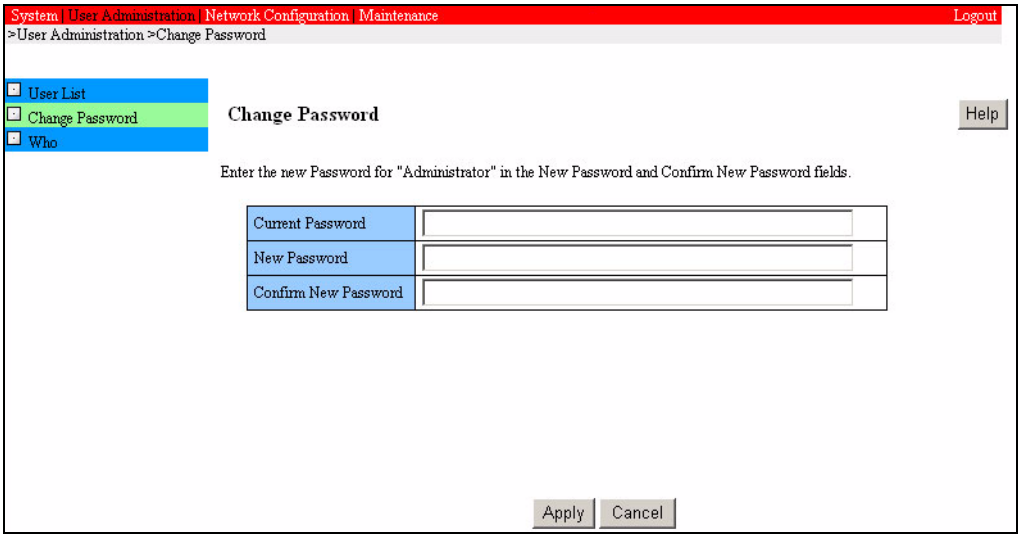


Figure 5.29 [Change Password] window

Table 5.50 Displayed and setting items in the [Change Password] window

Item	Description
Current Password	Enter the password of the user who is logged in.
New Password	Specify a new password. The password must be from 8 to 32 characters long. You can use the following characters for passwords: 0-9, a-z, A-Z, special characters: ! " # $ % & ' ( ) = - ^ ~ \ @ ` [ ] { } : * ; + ? < . > , / _ |
Confirm New Password	Enter the new password again for confirmation.

Table 5.51 Buttons in the [Change Password] window

Button	Description
Apply	Specify a new password, and click the [Apply] button to register the password.
Cancel	Click the [Cancel] button to revert to the original setting without registering the new password.

(1) Menu operation

[User Administration] → [Change Password]

(2) GUI operation

1 Enter the current password into [Current Password], enter the new password into both [New Password] and [Confirm New Password], and click the [Apply] button.
The new password is then set.

5.3.3 [Who] window

The [Who] window displays a list of the users currently accessing the MMB Web-UI.

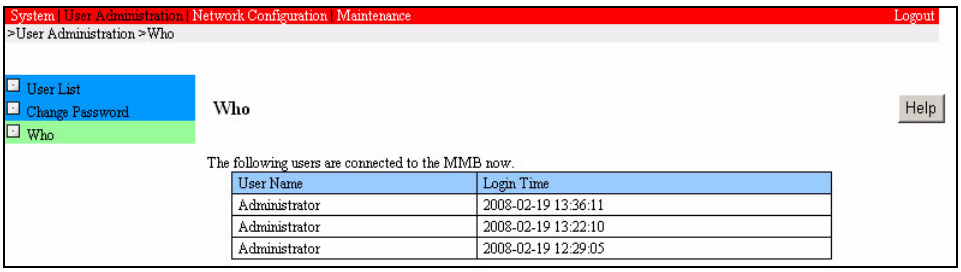


Figure 5.30 [Who] window

Table 5.52 Displayed items in the [Who] window

Item	Description
User Name	User name of the user logging in via a serial port, Telnet/SSH, or MMB Web-UI
Login Time	Login times of the accessing users
By	MMB Web-UI or Telnet/SSH used by the user for login Remarks: A hyphen (-) is displayed when the user logs in via a serial port of the MMB.
From	Host name or IP address of the remote host from which the user logs in remotely Remarks: A hyphen (-) is displayed when the user logs in via a serial port of the MMB.

(1) Menu operation

[User Administration] → [Who]

(2) GUI operation

None

5.4 Network Configuration Menu

The [Network Configuration] menu can be used to:

- Display and specify network interfaces
- Specify network protocols
- Configure security settings

Only users with the administrator privilege can access this menu.

Note:

MMB uses the following TCP/IP port numbers.

- 623/udp: RMCP communication
- 664/udp: RMCP communication
- 5000: event communication from PSA

5.4.1 [Date/Time] window

The MMB date and time can be set in the [Date/Time] window.

Remarks:

- When NTP is Enable, Date and Time cannot be set.
- If the MMB is set as an NTP server and the system is set as an NTP client, use the following setting:
  NTP: Enable
  NTP Server1: 0.0.0.0
  to NTP Server 3

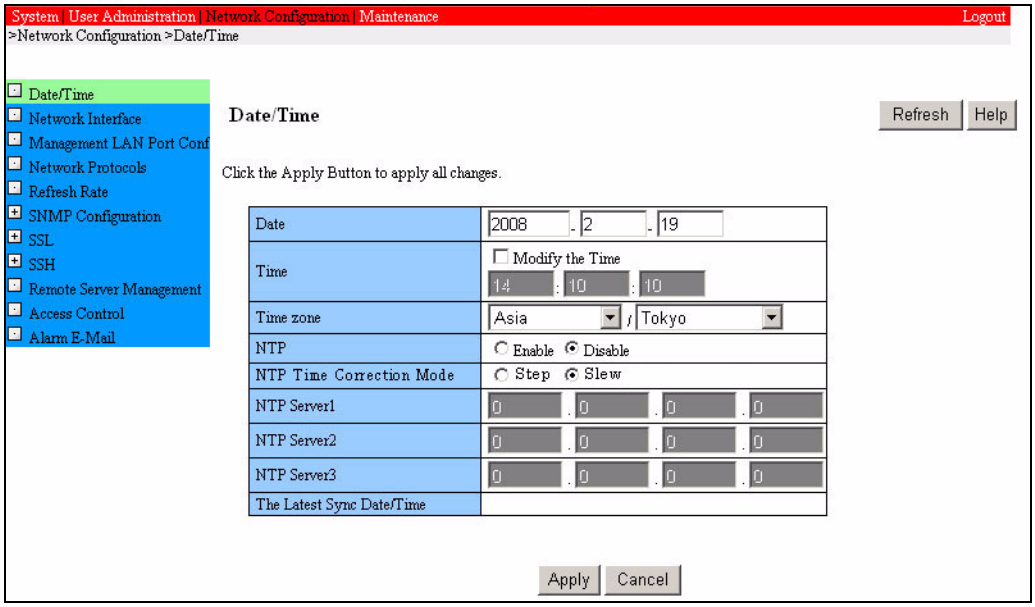


Figure 5.31 [Date/Time] window

Table 5.53 Displayed and setting items in the [Date/Time] window

Item	Description
Date	Specify a date.
Time	Specify hour:minute:second (24-hour format). To set the time, check the check box "Modify the Time" and entry in the hh:mm:ss time field. Because the MMB time when this window is opened is displayed, reloading is required to update the display. When the automatic update is set, the time when the window is updated is displayed.
Time zone	Select a time zone from the pulldown list.
NTP	Enable or disable the NTP function. If [Enable] is specified, the MMB synchronizes the NTP server time settings on NTP1 to NTP3, which are listed below. • Enable: Enable the NTP function. • Disable: Disable the NTP function. To use the MMB as an NTP server from another client, [Enable] must be set for the NTP function. The default setting is [Disable].

Item	Description
NTP Time Correction Mode	Set the NTP time correction mode. Remarks: This item is available if "enable" is set for the NTP function. If "disable" is set for the function, this setting is grayed out. • Step mode As long as the time difference with the NTP time server is within 128 ms, time correction is performed in slew mode. If the difference exceeds 128 ms, time is corrected in a single step. • Slew mode Regardless of the actual difference with the NTP time server, time is corrected gradually. However, since only a correction by 0.0005 seconds is possible per second, time can only be corrected by a maximum of 43 seconds in one day. The default setting is "Step mode."
NTP Server1	Specify the IP address of the primary NTP server. (This setting is valid only if [Enable] is set for the NTP function. If the setting is [Disable], this item is grayed out.)
NTP Server2	Specify the IP address of the secondary NTP server. (This setting is valid only if [Enable] is set for the NTP function. If the setting is [Disable], this item is grayed out.)
NTP Server3	Specify the IP address of the tertiary NTP server (This setting is valid only if [Enable] is set for the NTP function. If the setting is [Disable], this item is grayed out.)
The Latest Sync Data/Time	Date and time of the latest time synchronization between the specified NTP server and the MMB

Table 5.54 Buttons in the [Date/Time] window

Button	Description
Apply	Specify a date, time zone, etc., and click the [Apply] button to set the specified values.
Cancel	Click the [Cancel] button to revert to the original settings for the date, time zone, etc.

(1) Menu operation

[Network Configuration] → [Date/Time]

(2) GUI operation

1 Specify a date, time zone, etc., and click the [Apply] button.
The specified date, time zone, etc., are then set.

Note:

- If you change the time zone during an REMCS operation, notify the REMCS Center of the new time zone. Check the connection by referring to "Connection check" in Section 7.1.3, "REMCS service operation procedure" in the *PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/Operation Information* (C122-E074EN).

5.4.2 [Network Interface] window

The [Network Interface] window allows you to specify IP addresses and other information for MMB access.

The specified IP addresses are accessed by using the MMB Web-UI or by using SNMP from the management server.

Note: If you change the IP address, the system terminated its connection to the MMB Web-UI. To use the MMB Web-UI, log in again.

Remarks:

- After a setting for [MMB IP Address] is changed in this window, network operation is temporarily stopped to reflect the new setting, suppressing display of the Web-UI.
  In such cases, you can reconnect to and display the Web-UI by making a selection from the menu.
  The physical IP address and the virtual IP address of MMB#0 and MMB#1 set in the same subnet.

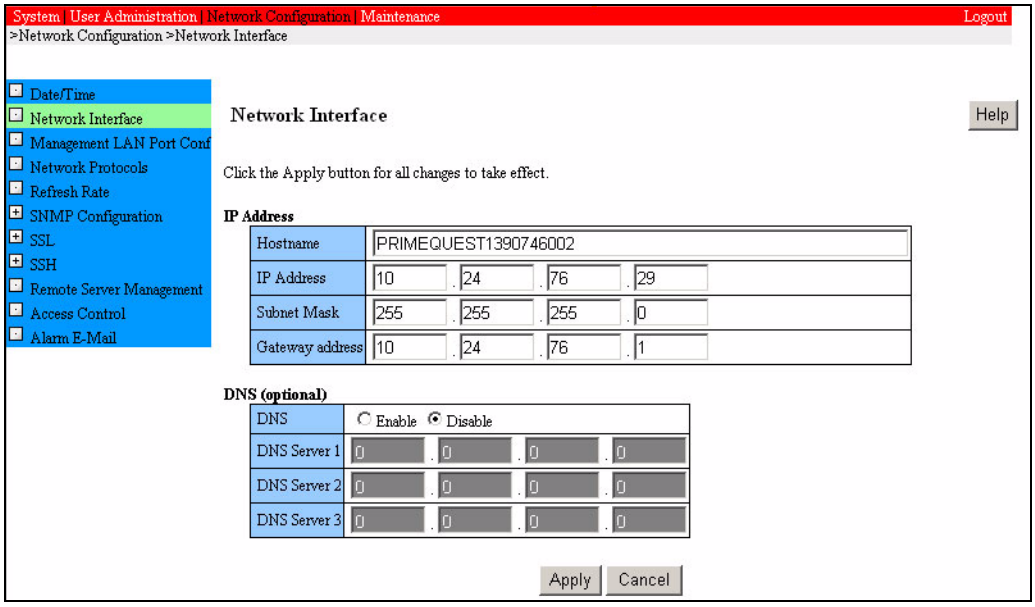


Figure 5.32 [Network Interface] window

Table 5.55 Displayed and setting items in the [Network Interface] window

Item	Description
IP Address	
Hostname	Specify a host name. Remarks: The characters that can be input are lowercase letters a to z, uppercase letters A to Z, numbers 0 to 9, a hyphen (-), and a dot (.). The following restrictions are imposed: • The host name must begin with an alphabetic character. • The host name must not begin with a hyphen (-) or dot (.). The default host name is "PRIMEQUEST" + the product serial number.
IP Address	Specify an IP address.
Subnet Mask	Specify the subnet mask.
Gateway address	Specify the gateway IP address.
DNS (optional)	
DNS	Specify whether to use DNS servers: Enable: Uses DNS servers Disable: Does not use DNS servers The default setting is [Disable].
DNS Server 1	Specify the IP address of the primary DNS server.
DNS Server 2	Specify the IP address of the secondary DNS server.
DNS Server 3	Specify the IP address of the tertiary DNS server.

Table 5.56 Buttons in the [Network Interface] window

Button	Description
Apply	Enter an IP address, subnet mask, etc., and click the [Apply] button to set the entered values.
Cancel	Click the [Cancel] button to revert to the original settings for the IP address, subnet mask, etc.

(1) Menu operation

[Network Configuration] → [Network Interface]

(2) GUI operation

1 Enter a subnet mask, IP address, etc. for network interface information, and click the [Apply] button to set the specified values.
The specified IP address, subnet mask, etc. are then set.

5.4.3 [Management LAN Port Configuration] window

The [Management LAN Port Configuration] window can be used to specify the speed and duplex mode of each MMB port.

Remarks: If the Speed/Duplex setting of an MMB LAN port is not "Auto," use a cross cable for the interconnection between the MMB LAN port and the switching hub.
However, when using an REMCS port of an MMB with a part number (*) that ends in 004AB or lower, the following notes apply.

* Confirm the part number of the MMB with the Part Number item in the [MMB] window (Click [System] → [MMB].).

- If the Speed/Duplex setting of the REMCS port is set to other than "AUTO," use a LAN cable.
- If the Speed/Duplex setting of the device to connect to the REMCS port is set to other than "AUTO," set the Speed/Duplex setting of the REMCS port of the MMB to the same setting as that of the device.

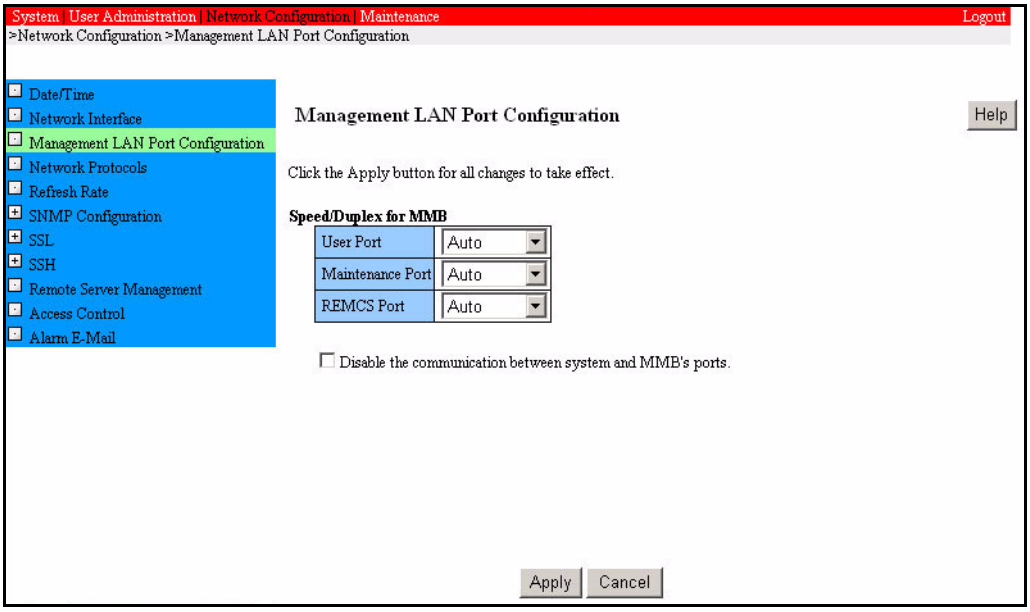


Figure 5.33 [Management LAN Port Configuration] window

Table 5.57 Displayed and setting items in the [Management LAN Port Configuration] window

Item	Description
Speed/Duplex for MMB	
User port	Specify the speed and duplex mode: • Auto • 100M/Full • 100M/Half • 10M/Full • 10M/Half The default setting is [Auto].
Maintenance port	Same as above
REMCS port	Same as above
Disable the communication between system and MMB's ports.	Define the disconnection between the system and each MMB port.

Table 5.58 Buttons in the [Management LAN Port Configuration] window

Button	Description
Apply	Specify speed and duplex mode, etc., and click the [Apply] button to set the specified values.
Cancel	Click the [Cancel] button to revert to the original settings for the speed and duplex mode, etc.

(1) Menu operation

[Network Configuration] → [Management LAN Port Configuration]

(2) GUI operation

1 Specify Speed and Duplex of each port, and the disconnection between the system and MMB port, and then click the [Apply] button.

5.4.3.1 Setting the connection of management LAN hub

This function makes the Speed/Duplex setting for each port on the MMB board. It also makes the VLAN setting for a LAN port on a BB that is connected to the MMB LAN port and to the administration LAN. Moreover, it sets the communication speed and communication method (Duplex) for each port on the MMB board. To make these settings, use administrator authority.

Remarks: When connecting the MMB LAN port to the switching hub unit, use a crossover cable when the Speed/Duplex setting of the MMB LAN port is set to other than "AUTO."

- If the Speed/Duplex setting of the REMCS port is set to other than "AUTO," use a LAN cable.
- If the Speed/Duplex setting of the device to connect to the REMCS port is set to other than "AUTO," set the Speed/Duplex setting of the REMCS port of the MMB to the same setting as that of the device.

Connection functions of management LAN

The management LAN hub on the MMB accommodates networks of the system on the BB, user ports, REMCS port, and Fujitsu certified service engineer ports. If this hub functions as a typical hub, the following problem occurs.

- The business system installed on the BB can be accessed, and this poses a security risk.

To solve this problem, make connection settings for the management LAN hub.
The connection functions of the PRIMEQUEST management LAN can be used in one of the three modes below, so that the user can select the mode that is suited to the operation method.

VLAN mode of management LAN

The following two modes are available. These modes can be selected by selecting or clearing the "Disable the communication between system and the MMB's ports" check box. The default is "unchecked."

- Connection mode (when the check box is cleared)

  Communication between systems on the BB is enabled. However, communication between REMCS ports, Fujitsu certified service engineer ports, and user ports, and communication between REMCS ports, Fujitsu certified service engineer ports, and system ports on the BB are disabled. Communication is enabled only between the ports indicated by [O] in Table 5.59.

Table 5.59 Connection mode (when the check box is cleared)

No VAN mode	User port	Certified service engineer port	REMCS port	MMB	System port on BB
User port	O	X	X	O	O
Certified service engineer port	X	O	X	O	X
REMCS port	X	X	O	O	X
MMB	O	O	O	O	O
System port on BB	O	X	X	O	O

O: Communication is possible.

X: Communication is impossible.

- Disconnection mode (when the check box is selected)

  Mode for upgraded security

  Management LAN communication of the system on a BB is disconnected. Intra-cabinet communication between the MMB and system port on the BB is disabled. Communication is possible only between the ports indicated by [O] in Table 5.60.

Table 5.60 Disconnection mode (when the check box is selected)

Port disable mode	User port	Certified service engineer port	REMCS port	MMB	System port on BB
User port	O	X	X	O	X
Certified service engineer port	X	O	X	O	X
REMCS port	X	X	O	O	X
MMB	O	O	O	O	X
System port on BB	X	X	X	X	O

O: Communication is possible.

X: Communication is impossible.

5.4.4 [Network Protocols] window

The network protocols of the MMB can be specified in the [Network Protocols] window.

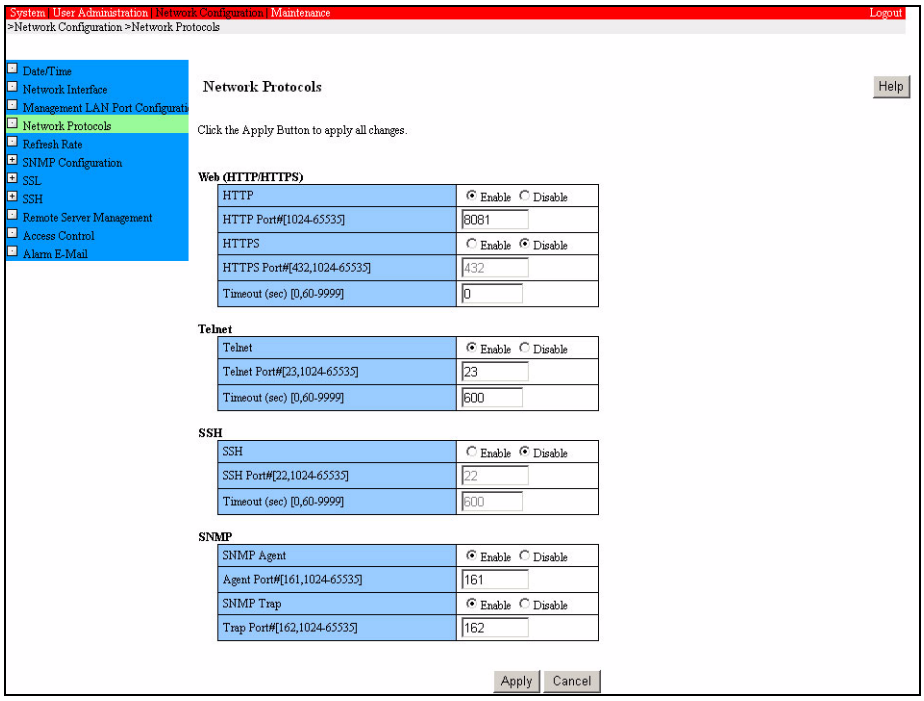


Figure 5.34 [Network Protocols] window

Table 5.61 Displayed and setting items in the [Network Protocols] window

Item	Description
Web (HTTP/HTTPS)	
HTTP	Specify whether to use HTTP: • Enable: Uses HTTP • Disable: Does not use HTTP The default setting is [Disable].
HTTP Port# [1024-65535]	Specify the port number used for HTTP communication. The default setting is 8081.
HTTPS	Specify whether to use HTTPS: • Enable: Uses HTTPS • Disable: Does not use HTTPS The default setting is [Disable]. Remarks: [Enable] can be set only if a valid SSL certificate is registered. If [Enable] is specified when no valid SSL certificate is registered, an error message is displayed.

Item	Description
HTTPS Port# [432, 1024-65535]	Specify the port number used for HTTPS communication. The default setting is 432.
Timeout (sec)	Specify in seconds the amount of time that elapses without input in an HTTP/HTTPS connection before a timeout occurs. The setting range is 0, 60 to 9999 seconds. If 0 is specified, no timeout occurs and the connection remains established. The default setting is 600 seconds.

Telnet

Telnet	Specify whether to use Telnet: • Enable: Uses Telnet • Disable: Does not use Telnet The default setting is [Disable].
Port# [23, 1024-65535]	Specify the port number used for Telnet communication. The default setting is 23.
Timeout (sec)	Specify in seconds the amount of time that elapses without input in a Telnet connection before a timeout occurs. The setting range is 0, 60 to 9999 seconds. If 0 is specified, no timeout occurs and the connection remains established. The default setting is 600 seconds.

SSH

SSH	Specify whether to use SSH: • Enable: Uses SSH • Disable: Does not use SSH The default setting is [Disable].
Port# [22, 1024-65535]	Specify the port number used for SSH communication. The default setting is 22.
Timeout (sec)	Specify in seconds the amount of time that elapses in an SSH connection before a timeout occurs. The setting range is 0, 60 to 9999 seconds. If 0 is specified, no timeout occurs and the connection remains established. The default setting is 600 seconds.

SNMP

SNMP Agent	Specify whether to use SNMP Agent: • Enable: Uses SNMP Agent • Disable: Does not use SNMP Agent The default setting is [Disable].
Agent Port#[161, 1024- 65535]	Specify the port number used for SNMP Agent. The setting range is 161,1024 to 65535. The default setting is 161.
SNMP Trap	Specify whether to use SNMP traps. • Enable: Uses SNMP traps • Disable: Does not use SNMP traps The default setting is [Disable].
Trap port#[162, 1024- 65535]	Specify the port number used for SNMP traps. The setting range is 162,1024 to 65535. The default setting is 162.

Table 5.62 Buttons in the [Network Protocols] window

Button	Description
Apply	Specify a port number, timeout time, etc., and click the [Apply] button to set the specified values.
Cancel	Click the [Cancel] button to revert to the original settings for the port number, timeout time, etc.

(1) Menu operation

[Network Configuration] → [Network Protocols]

(2) GUI operation

1 Specify a port number, timeout time, etc. for protocol information, and click the [Apply] button to set the specified values.
The specified port number, timeout time, etc. are then set.

5.4.5 [Refresh Rate] window

The [Refresh Rate] window can be used to specify automatic refresh for a Web-UI page whose contents change.

This automatic refresh mode can be set and managed for individual users.

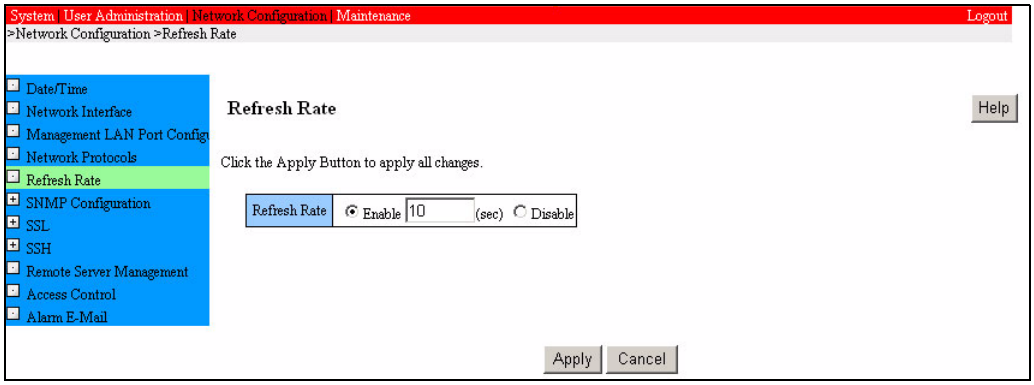


Figure 5.35 [Refresh Rate] window

Table 5.63 Displayed or setting item in the [Refresh Rate] window

Item	Description
Refresh Rate	Specify whether to periodically refresh a page whose displayed contents change. • Enable: It is possible to specify the refresh rate in seconds in a range from 5 to 999 seconds. The pages will be refreshed at the specified intervals. • Disable: Automatic irregular refreshes. The default setting is [Disable].

Table 5.64 Buttons in the [Refresh Rate] window

Button	Description
Apply	Specify whether to enable periodic refresh, click the [Apply] button, and the specified refresh information is set.
Cancel	Click the [Cancel] button to revert to the original settings in refresh information.

(1) Menu operation

[Network Configuration] → [Refresh Rate]

(2) GUI operation

1 Specify values in [Refresh Rate], and click the [Apply] button.
The specified refresh information is then set.

5.4.6 SNMP Configuration menu

The [SNMP Configuration] menu provides the following windows:

- [SNMP Community]
- [SNMP Trap]
- [SNMPv3 Configuration]

This section describes these windows and their operations.

Remarks: This configuration enables the system to obtain standard and extended MIB information and receive SNMP traps. The SNMP-based control manager software monitors the PRIMEQUEST hardware by obtaining MIB information and receiving SNMP traps. For details on the extended MIB information provided by the PRIMEQUEST control agent, see Chapter 9, "MIB Tree Provided by PRIMEQUEST" in the *PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/Operation Information* (C122-E074EN).

5.4.6.1 [SNMP Community] window

SNMP settings can be configured in the [SNMP Community] window.

Up to 16 communities can be set up in the MMB.

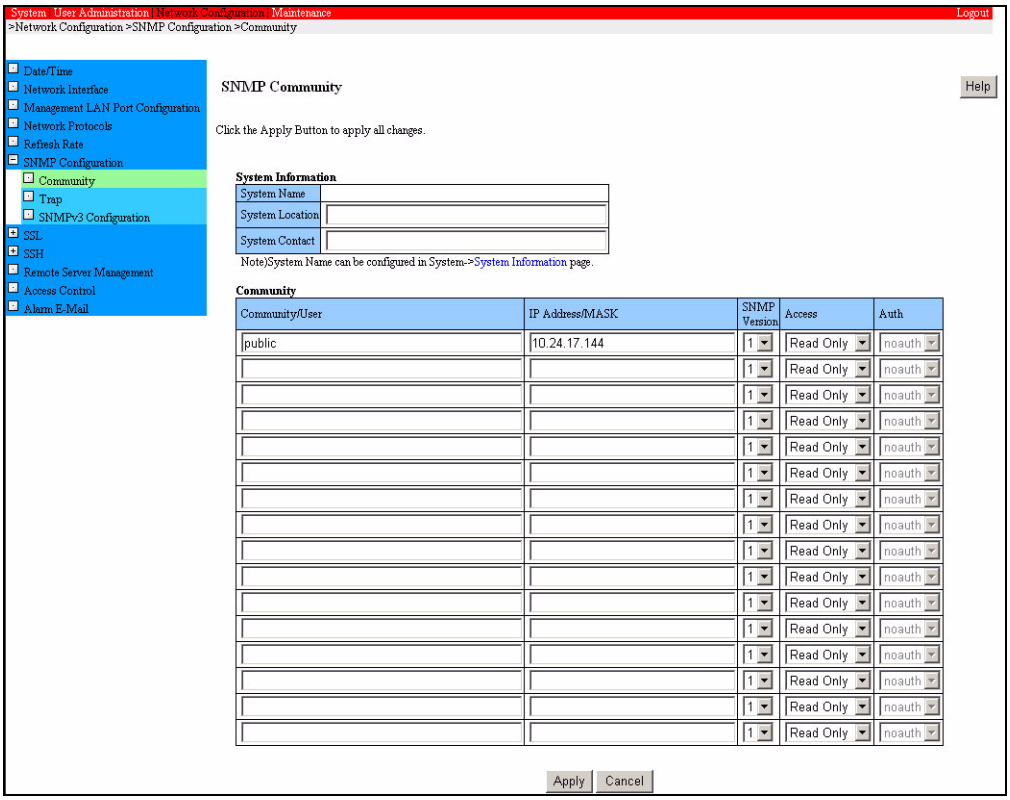


Figure 5.36 [SNMP Community] window

Table 5.65 Displayed and setting items in the [SNMP Community] window

Item	Description
System Information	
System Name	PRIMEQUEST system name specified in the [System Information] window
System Location	Specify a system location. Remarks: Any of the following characters can be used: [0-9], [a-z], [A-Z], " "(en-size space), !" (double quotation mark) # $ % & ' (single quotation mark) ( ) = - ^ ~ \ (or back slash) @ ` [ ] { } : * ; + ? < . > , / _ |. However, the following restrictions apply: - The following characters cannot be used at the beginning of a string: # (en-size space) - The following character cannot be used at the end of the string: (en-size space)
System Contact	Specify a system contact. Remarks: Any of the following characters can be used: [0-9], [a-z], [A-Z], " "(en-size space), !" (double quotation mark) # $ % & ' (single quotation mark) ( ) = - ^ ~ \ (or back slash) @ ` [ ] { } : * ; + ? < . > , / _ |. However, the following restrictions apply: - The following characters cannot be used at the beginning of a string: # (en-size space) - The following character cannot be used at the end of the string: (en-size space)
Community	
Community	Specify an SNMP community string. Remarks: Any of the following characters can be used: [0-9],[a-z],[A-Z], " "(en-size space), ! " (double quotation mark) # $ % & ' (single quotation mark) ( ) = - ^ ~ \ (or back slash) @ ` [ ] { } : * ; + ? < . > , / _ |. However, the following characters cannot be used at the beginning of a string: " ' ` #
IP Address/MASK	Specify an IP address or the subnet mask for IP addresses that have access permission.

Item	Description
SNMP Version	Select an SNMP version: • 1 • 2 • 3
Access	Select an access privilege: • Read Only: Read-only permission • Read Write: Read/write permission
Auth	Select a security level: This item can be selected only if 3 is selected for [SNMP Version]. If 1 or 2 is selected for [SNMP Version], [noauth] is automatically set for the item. • noauth: The authentication function is not used. • auth: The authentication function is used. • priv: The authentication function and privacy function (data encryption) are used.

Table 5.66 Buttons in the [SNMP Community] window

Button	Description
Apply	Specify community settings and an IP address that has access permission, and click the [Apply] button to set the specified values.
Cancel	Click the [Cancel] button to revert to the original settings for a community and an IP address that has access permission.

(1) Menu operation

[Network Configuration] → [SNMP Configuration] → [Community]

(2) GUI operation

- Specifying community settings and other information

  1 Enter values for a community, an IP address that has access permission, an SNMP version, access privilege, authentication level, etc., and click the [Apply] button.
  The entered values are then set.

- Clearing community settings and other information

  1 Clear community settings and the specified IP address that has access permission, and click the [Apply] button.
  Values are cleared from the settings.

5.4.6.2 [SNMP Trap] window

SNMP trap destinations can be specified in the [SNMP Trap] window.

Up to 16 trap destinations can be set.

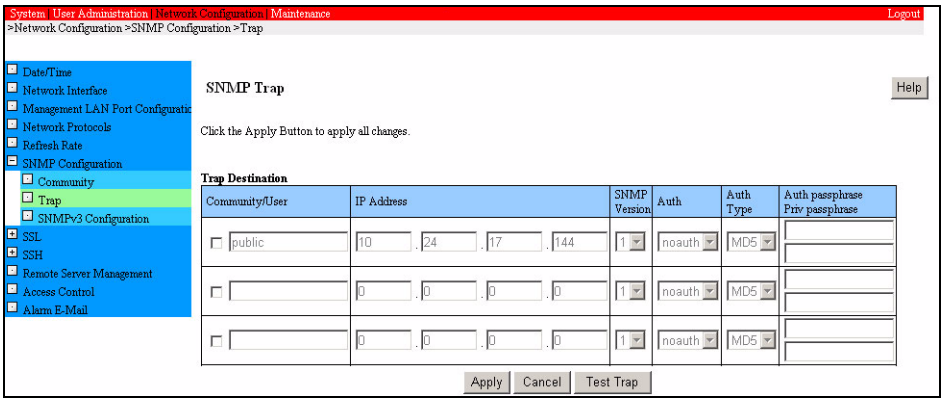


Figure 5.37 [SNMP Trap] window

Table 5.67 Displayed and setting items in the [SNMP Trap] window

Item	Description
Community/User	Specify a community or user name. Remarks: Any of the following characters can be used: [0-9], [a-z], [A-Z], " "(en-size space), !" (double quotation mark) # $ % & ' (single quotation mark) ( ) = - ^ ~ \ (or back slash) @ ` [ ] { } : * ; + ? < . > , / _ |. However, the following characters cannot be used at the beginning of a string: " ' ` #
IP Address	Specify an IP address as a trap destination.
SNMP Version	Select an SNMP version: • 1: A version-1 SNMP trap is sent. • 2: A version-2 SNMP trap is sent. • 3: A version-3 SNMP trap is sent.
Auth	Specify the authentication level. • noauth: Disables authentication and encryption based on a password (enables authentication based on a user name). • auth: Enables authentication based on a password but disables encryption based on a password. • priv: Enables authentication and encryption based on a password.

Item	Description
Auth Type	• md5: Selects MD5 as the hash function for password-based encryption. • sha: Selects SHA as the hash function for password-based encryption.
Auth passphrase	Displays the packet encryption keyword used at the time of password-based authentication (no password-based encryption).
Priv passphrase	Displays the packet encryption keyword used at the time of password-based authentication and encryption.

Table 5.68 Buttons in the [SNMP Trap] window

Button	Description
Apply	Specify a community or user name, trap destination, etc., and click the [Apply] button to set the specified values.
Cancel	Click the [Cancel] button to revert to the original settings for the community or user name, trap destination, etc.
Test Trap	Click the [Test Trap] button to send a test trap to the current trap destination.

(1) Menu operation

[Network Configuration] → [SNMP Configuration] → [Trap]

(2) GUI operation

- Specifying SNMP trap information

  1 Enter a community or user name, trap destination IP address, SNMP version, and authentication level, and click the [Apply] button.
  The entered values are then set.

- Sending a test trap

  1 Click the [Test Trap] button.
  Values are cleared from the settings.
  A test trap is sent.

5.4.6.3 [SNMP v3 Configuration] window

An engine ID unique to SNMP v3 as well as user information can be specified in the [SNMP v3 Configuration] window.

Up to 16 SNMP v3 users can be registered. Registered users are listed in this window.

Note: If the engine ID or IP address is changed, setup for users who have been registered for SNMP v3 access must be completed again, starting from the beginning. The SNMP daemon must be restarted to validate registered users. Therefore, when the [Apply] button in the window is clicked, the SNMP service stops temporarily.

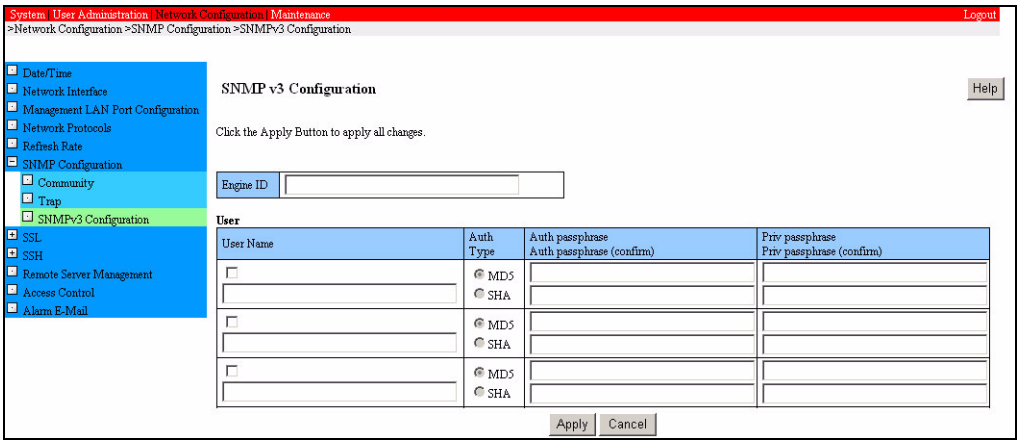


Figure 5.38 [SNMP v3 Configuration] window

Table 5.69 Displayed and setting items in the [SNMP v3 Configuration] window

Item	Description
Engine ID	Specify an engine ID. Remarks: Any of the following characters can be used: [0-9], [a-z], [A-Z], " "(en-size space), !" (double quotation mark) # $ % & ' (single quotation mark) ( ) = - ^ ~ \ (or back slash) @ ` [ ] { } : * ; + ? < . > , / _ |. However, the following restrictions apply: - The following characters cannot be used at the beginning of a string: # (en-size space) - The following character cannot be used at the end of the string: (en-size space)

Item	Description
User	
User Name	Specify a user name. Checking the check box of the target user enables input of a user name. Remarks: Any of the following characters can be used: [0-9],[a-z],[A-Z], ! " (double quotation mark) # $ % & ' (single quotation mark) ( ) = - ^ ~ \ (or back slash) @ ` [ ] { } : * ; + ? < . > , / _ |. However, the following characters cannot be used at the beginning of a string: " ' ` #
Auth Type	Select an authentication type: • MD5: Uses MD5 as a hash function for password encryption • SHA: Uses SHA as a hash function for password encryption
authpassphrase	Keyword used for packet encryption if password-based authentication (no encryption) is enabled.
privpassphrase	Keyword used for packet encryption if password-based authentication and encryption is enabled.

Table 5.70 Buttons in the [SNMP v3 Configuration] window

Button	Description
Apply	Select a user, and click the [Apply] button to restart the SNMP daemon to reflect the user's changes.
Cancel	Click the [Cancel] button to not change information.

(1) Menu operation

[Network Configuration] → [SNMP Configuration] → [SNMPv3 Configuration]

(2) GUI operation

- Reflecting a selected user's settings

  1 Check the check box of a user, enter necessary information, and click the [Apply] button.
  The selected user's settings are then reflected. The SNMP daemon is restarted in this procedure.

- Disabling a selected user

  1 To disable a user's access, check the check box of the user, enter nothing for the user name, and click the [Apply] button.
  The selected user's access is then disabled.

5.4.7 SSL menu

The [SSL] menu provides the following windows:

- [Create CSR]
- [Export Key/CSR]
- [Import Certificate]
- [Create Selfsigned Certificate]

This section describes these windows and their operations.

5.4.7.1 [Create CSR] window

The [Create CSR] window allows you to create a private key and a corresponding Certificate Signing Request (CSR).

The values entered in this window must comply with the guidelines of the certificate authority selected as the destination because each certificate authority has unique guidelines.

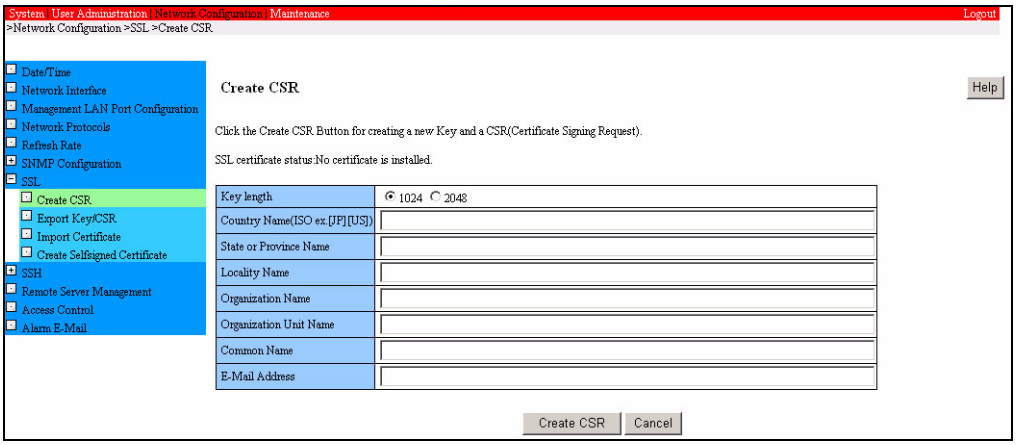


Figure 5.39 [Create CSR] window

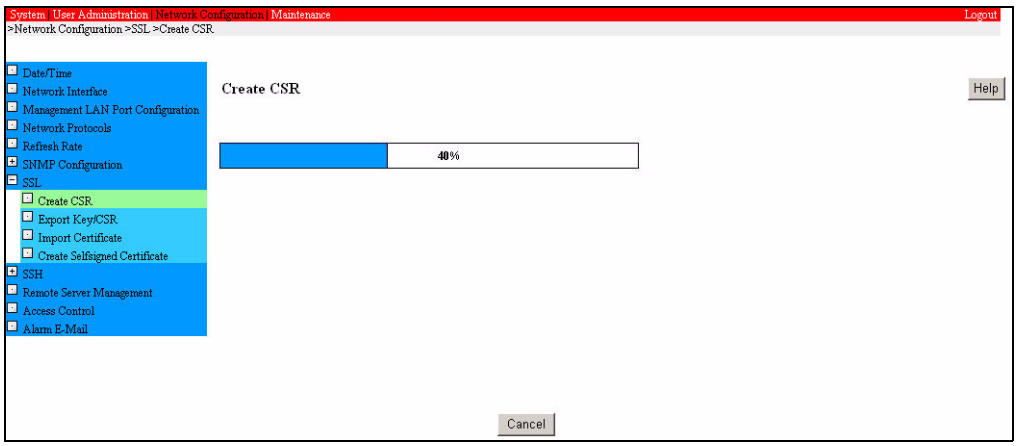


Figure 5.40 Create CSR (In Progress) indicator

Table 5.71 Displayed and setting items in the [Create CSR] window

Item	Description
SSL certificate status	Current installation status of an SSL certificate: • No certificate is installed. • CSR has been generated. • A self-signed certificate is installed. • A signed certificate is installed.
Key length	Select a key length (number of bits) for the created private key by clicking the corresponding radio button: • 1024 • 2048
Country Name	Specify two alphabetic characters as the ISO country code of the owner in the created CSR: • Japan: JP • USA: US
State or Province Name	Specify up to 56 valid characters as the state or province name of the owner in the created CSR.
Locality Name	Specify up to 56 valid characters as the city name of the owner in the created CSR.
Organization Name	Specify up to 56 valid characters as the organization name (company name) of the owner in the created CSR.
Organization Unit Name	Specify up to 56 valid characters as the organization unit name of the owner in the created CSR.

Item	Description
Common Name	Specify up to 56 valid characters as the server FQDN of the owner in the created CSR. Example: www.mycompany.com The browser uses this information to check the website. Some browsers refuse to establish a secure connection unless the same name is set for the server name and [Common Name] in the electronic certificate. The value in [Common Name] must not include a protocol specifier (http://), port number, or path name. Also, no wildcard, such as "*" and "?", or IP address can be used.
Email Address	Specify up to 40 valid characters as the e-mail address of the owner in the created CSR.

Table 5.72 Buttons in the [Create CSR] window

Button	Description
Create CSR	Specify the private key length, ISO country code of the owner, etc., click the [Create CSR] button, and a dialog box opens. Clicking the [OK] button in the dialog box creates the private key and CSR.
Cancel	Clicking the [Cancel] button cancels the creation of a private key and a CSR. The private key length and the owner's ISO country code are restored to the initial information.

(1) Menu operation

[Network Configuration] → [SSL] → [Create CSR]

(2) GUI operation

1 Specify the private key length, ISO country code of the owner, etc., and click the [Create CSR] button.
A dialog box opens to inform the user that the existing private key cannot be used once a new private key is created.

2 Click the [OK] button in the dialog box.
A new private key and a certificate signing request are created. This takes a few minutes. A confirmation dialog box opens when they have been created.

3 Click the [OK] button in the confirmation dialog box to register the new private key.
The new private key is registered, and the [Export Key/CSR] window is displayed.

5.4.7.2 [Export Key/CSR] window

The [Export Key/CSR] window allows you to export a private key or Certificate Signing Request (CSR) from the MMB.

Note: For security reasons, care must be taken in storage of a private key. It is preferable to back up the private key because it is required for using the certificate issued for it.

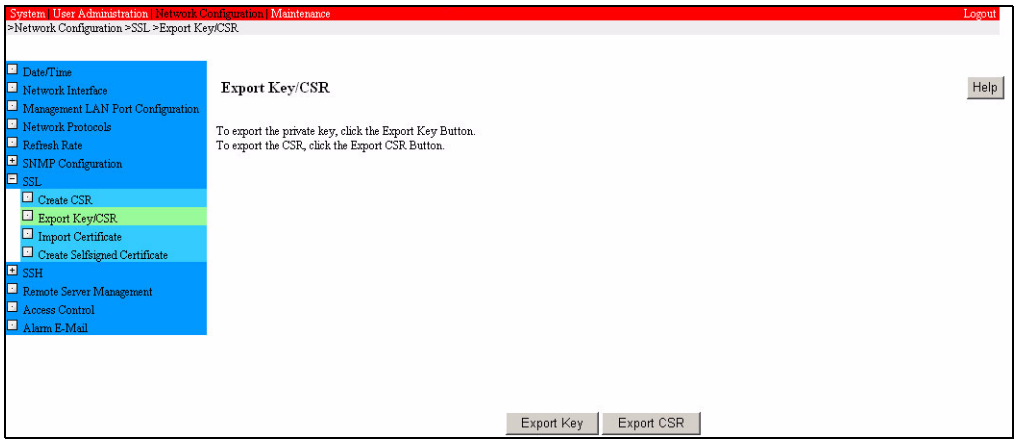


Figure 5.41 [Export Key/CSR] window

Table 5.73 Buttons in the [Export Key/CSR] window

Item	Description
Export Key	Exports a private key.
Export CSR	Exports a CSR.

(1) Menu operation

[Network Configuration] → [SSL] → [Export Key/CSR]

(2) GUI operation

- Exporting a private key
  1. Click the [Export Key] button.
     A dialog box opens.
  2. Specify a save path in the dialog box.
     The exported private key is saved with the specified path.
- Exporting a CSR

1 Click the [Export CSR] button.
A dialog box opens.
2 Specify a save path in the dialog box.
The exported CSR is saved with the specified path.

5.4.7.3 [Import Certificate] window

The [Import Certificate] window can be used to import a signed electronic certificate from the certifying to the MMB.

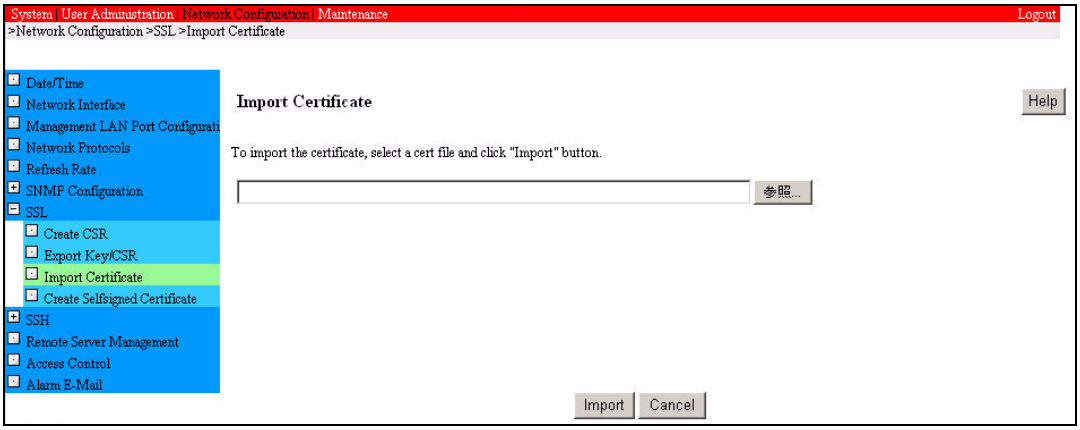


Figure 5.42 [Import Certificate] window

Table 5.74 Buttons in the [Import Certificate] window

Item	Description
Browse	Opens a file selection dialog box.
Import	Imports an electronic certificate.
Cancel	Cancels importing a file.

(1) Menu operation

[Network Configuration] → [SSL] → [Import Certificate]

(2) GUI operation

1 Click the [Browse] button, select the file to be imported, and click the [Import] button.
The file with the electronic certificate is imported.

5.4.7.4 [Create Selfsigned Certificate] window

A self-signed certificate can be created in the [Create Selfsigned Certificate] window.

Remarks: Before creating a self-signed certificate, make sure that [Disable] is set in [HTTPS] in the [Network Protocols] window. If [Enable] is set, set [Disable] before creating a self-signed certificate in this window.

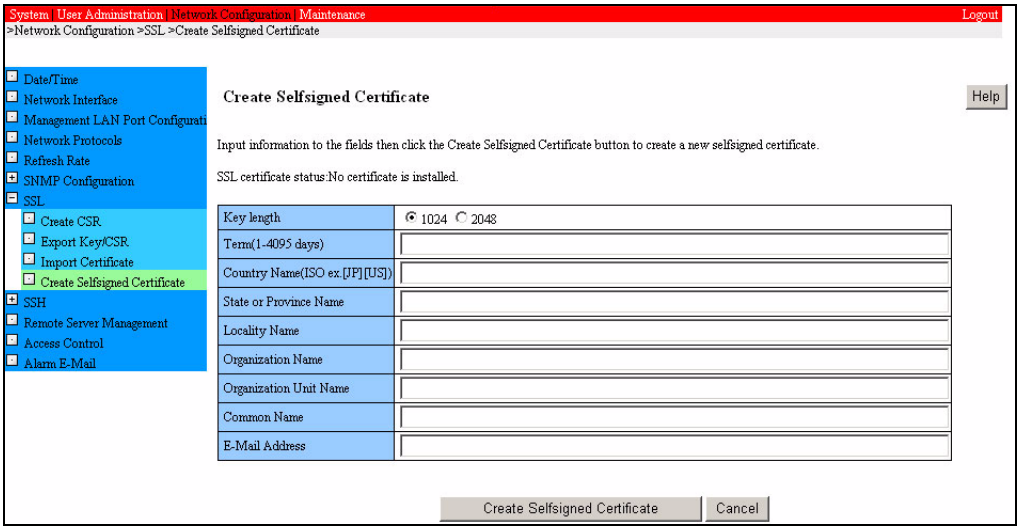


Figure 5.43 [Create Selfsigned Certificate] window

Table 5.75 Displayed and setting items in the [Create Selfsigned Certificate] window

Item	Description
SSL certificate status	Current installation status of an SSL certificate: • No certificate is installed. • CSR has been generated. • A self-signed certificate is installed. • A signed certificate is installed.
Key length	Select a key length (number of bits) for the created private key by clicking the corresponding radio button: • 1024 • 2048
Term (1-4095 days)	Specify the validity term in number of days for the created self-signed certificate.
Country Name	Specify two alphabetic characters as the ISO country code of the owner in the created self-signed certificate: • Japan: [JP] • USA: [US]

Item	Description
State or Province Name	Specify up to 56 valid characters as the state or province name of the owner in the created self-signed certificate.
Locality Name	Specify up to 56 valid characters as the city name of the owner in the created self-signed certificate.
Organization Name	Specify up to 56 valid characters as the organization name (company name) of the owner in the created self-signed certificate.
Organization Unit Name	Specify up to 56 valid characters as the organization unit name of the owner in the created self-signed certificate.
Common Name	Specify up to 56 valid characters as the server domain name of the owner in the created self-signed certificate.
Email Address	Specify up to 40 valid characters as the e-mail address of the owner in the created self-signed certificate.

Table 5.76 Buttons in the [Create Selfsigned Certificate] window

Button	Description
Create Self-signed Certificate	Specify the private key length, ISO country code of the owner, etc., click the [Create Self-signed Certificate] button, and a dialog box opens. Click the [OK] button in the dialog box to create a self-signed certificate.
Cancel	Click [Cancel] button to cancel creating a certificate.

(1) Menu operation

[Network Configuration] → [SSL] → [Create Selfsigned Certificate]

(2) GUI operation

1 Before creating a self-signed certificate, make sure that [Disable] is set in [HTTPS] in the [Network Protocols] window. If [Enable] is set, set [Disable] (see Section 5.4.4, "[Network Protocols] window").

2 Specify the private key length, ISO country code of the owner, etc., and click the [Create Self-signed Certificate] button.
A confirmation dialog box opens.

3 Click the [OK] button in the dialog box.
A self-signed certificate is created. This takes a few minutes. When it has been created, the window displays "SSL certificate status: A Self-signed certificate is installed.", indicating that the self-signed certificate has been installed.

5.4.8 SSH menu

The [SSH] menu provides the [Create SSH Server Key] window. This section explains the [Create SSH Server Key] window and its operations.

5.4.8.1 [Create SSH Server Key] window

A private key for the SSH server can be created in the [Create SSH Server Key] window.

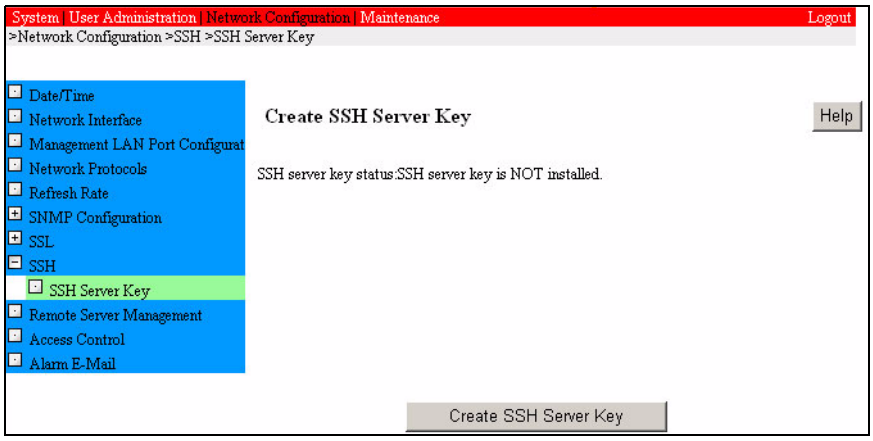


Figure 5.44 [Create SSH Server Key] window

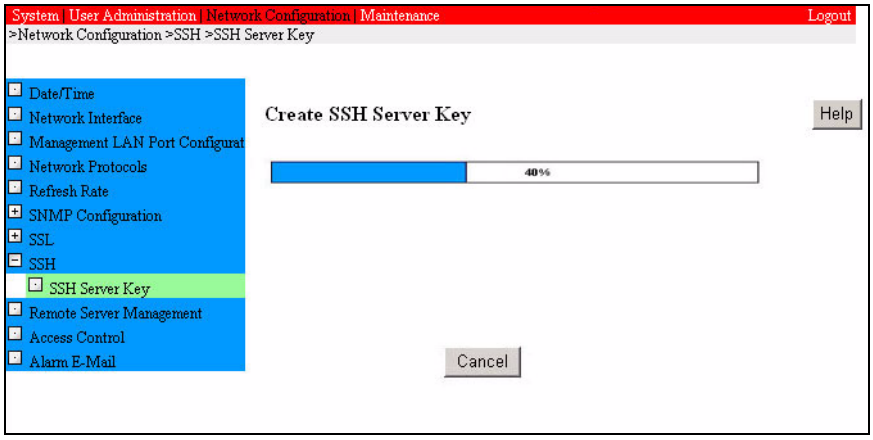


Figure 5.45 Create SSH Server Key (In Progress) indicator

Table 5.77 Displayed item in the [Create SSH Server Key] window

Item	Description
SSH Server Key status	Current installation status of an SSH server private key: • SSH server key is NOT installed.

Table 5.78 Button in the [Create SSH Server Key] window

Button	Description
Create SSH Server Key	Creates an SSH server private key.

(1) Menu operation

[Network Configuration] → [SSH] → [Create SSH Server Key]

(2) GUI operation

1 Before creating a private key, make sure that [Disable] is set in [SSH] in the [Network Protocols] window. If [Enable] is set, set [Disable] (see Section 5.4.4, "[Network Protocols] window").

2 Click the [Create SSH Server Key] button in this window.
A private key is created. This takes a few minutes. A confirmation dialog box opens when it has been created.

3 Click the [OK] button in the confirmation dialog box to register the new private key.
The new private key is registered. To not register the new private key, click the [Cancel] button in the confirmation dialog box.
The new private key would then be discarded.

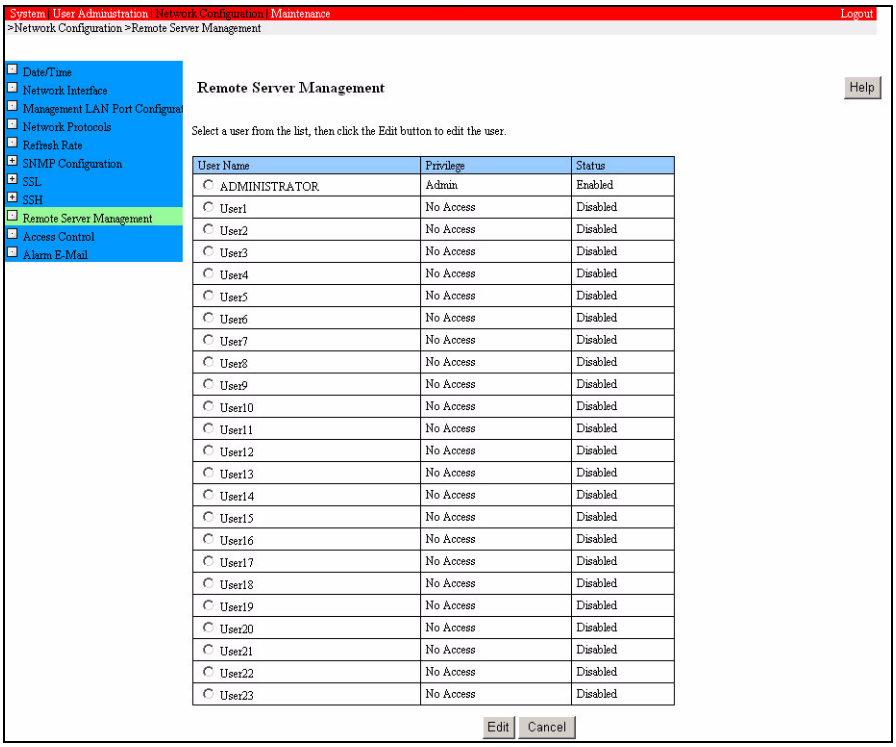
5.4.9 [Remote Server Management] window

User information required for MMB remote-control using RMCP can be specified in the [Remote Server Management] window.

Up to 24 users can be registered.

The default settings for all users are [Disabled] and [No Access]. Furthermore, the default user names are "User0" to "User23".

For MMB remote-control using RMCP, values must be specified in [User Name], [Password], and [Privilege], and [Enabled] must be set for the applicable user. Authentication for remote access uses the user names and passwords of users with [Enabled] set.



User Name	Privilege	Status
ADMINISTRATOR	Admin	Enabled
User1	No Access	Disabled
User2	No Access	Disabled
User3	No Access	Disabled
User4	No Access	Disabled
User5	No Access	Disabled
User6	No Access	Disabled
User7	No Access	Disabled
User8	No Access	Disabled
User9	No Access	Disabled
User10	No Access	Disabled
User11	No Access	Disabled
User12	No Access	Disabled
User13	No Access	Disabled
User14	No Access	Disabled
User15	No Access	Disabled
User16	No Access	Disabled
User17	No Access	Disabled
User18	No Access	Disabled
User19	No Access	Disabled
User20	No Access	Disabled
User21	No Access	Disabled
User22	No Access	Disabled
User23	No Access	Disabled

Figure 5.46 [Remote Server Management] window

Table 5.79 Displayed and setting items in the [Remote Server Management] window

Item	Description
User Name	User name. To specify user management information, click the radio button.
Privilege	User account privilege: • Admin: Permission for all operations • Operator: Permission to view the system and configure system settings • User: Permission only to view the system • CE: Permission to view the system and conduct system maintenance • No Access: No permission for any operation
Status	Current account status: • Enabled: Available • Disabled: Not available

Table 5.80 Buttons in the [Remote Server Management] window

Button	Description
Edit	Select a user name and click the [Edit] button to display the [Edit User] window.
Cancel	Click the [Cancel] button to revert to the original settings in management information.

(1) Menu operation

[Network Configuration] → [Remote Server Management]

(2) GUI operation

1 Select a user by clicking the radio button of the user, and click the [Edit] button.
The [Edit User] window is displayed.

2 Specify management information for the user in the [Edit User] window.

5.4.9.1 [Edit User] window

User management information can be changed in the [Edit User] window.

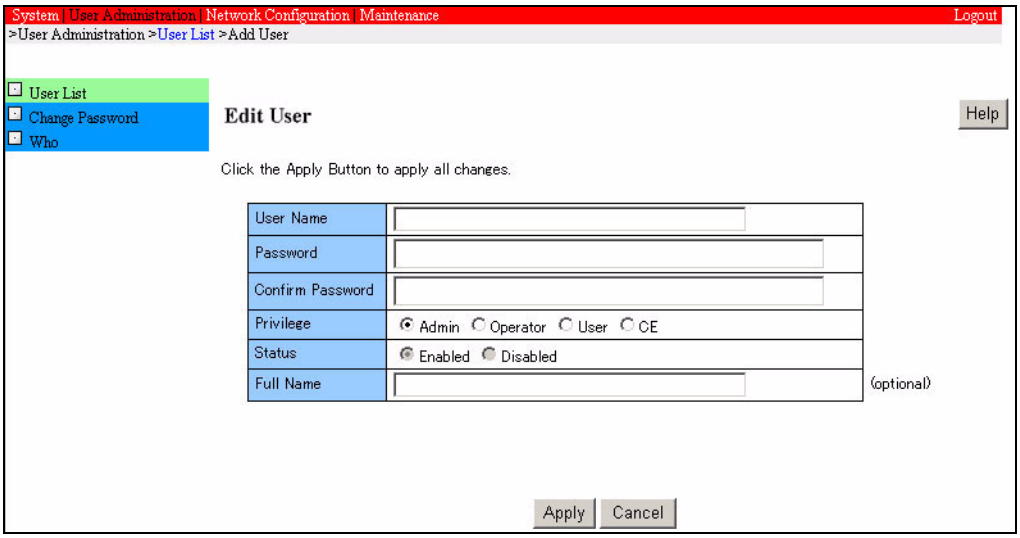


Figure 5.47 [Edit User] window

s

Table 5.81 Displayed and setting items in the [Edit User] window

Item	Description
User Name	Specify a user name. The user name must be from 8 to 16 characters long. The following types of characters can be used for a user name: En-sized alphabetic characters (uppercase and lowercase letters) and en-sized numeric characters
Password	Specify a password. The password must be from 8 to 16 characters long. The following types of characters can be used for a password: En-sized alphabetic characters (uppercase and lowercase letters) and en-sized numeric characters

Item	Description
Confirm Password	Enter the password again for confirmation.
Privilege	Specify the user account privilege. One of the following must be selected: • Admin: Permission for all operations • Operator: Permission to view the system and configure system settings • User: Permission only to view the system • CE: Permission to view the system and conduct system maintenance • No Access: No permission for any operation A user with [No Access] is not allowed to access remotely.
Status	Specify whether the account is available: • Enabled: Available • Disabled: Not available

Table 5.82 Buttons in the [Edit User] window

Button	Description
Apply	Specify a name, password, etc., as management information for the selected user, and click the [Apply] button to set this specified information.
Cancel	Click the [Cancel] button to revert to the original settings for the user name, password, etc.

(1) Menu operation

[Network Configuration] → [Remote Server Management] → [Edit] button

(2) GUI operation

1 Specify user management information such as a user name and a password, and click the [Apply] button.
The specified user management information is then set.

5.4.10 [Access Control] window

The [Access Control] window enables access control based on network protocols so that MMB security is maintained.

Up to 16 filters can be set for access control.

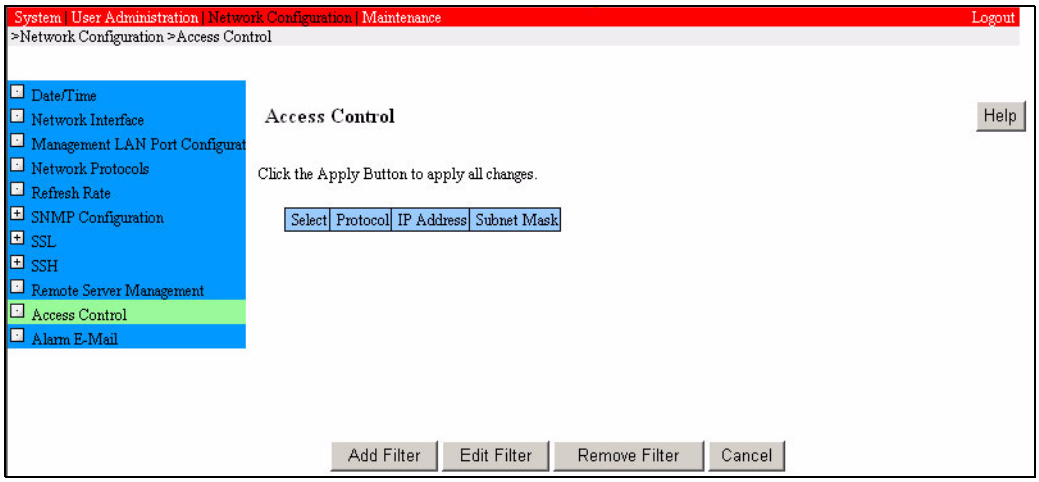


Figure 5.48 [Access Control] window

This window lists filters in alphabetic order by protocol name.

Table 5.83 Displayed and setting items in the [Access Control] window

Item	Description
Select	To edit or delete a filter, select the filter.
Protocol	Protocol subject to IP filtering: • HTTP • HTTPS • Telnet • SSH • SNMP
Access Control	Specifies whether to permit or deny access.
IP Address	IP address that has access permission
Subnet Mask	Subnet mask of IP addresses that have access permission

Table 5.84 Buttons in the [Access Control] window

Button	Description
Add Filter	Click the [Add Filter] button. A new filter can be added in the [Add Filter] window that is displayed.
Edit Filter	Select a filter from the list of filters, and click the [Edit Filter] button. The selected filter can be edited in the [Edit Filter] window that is displayed.
Remove Filter	Select a filter from the list of filters, and click the [Remove Filter] button. The selected filter is removed.
Cancel	Click the [Cancel] button to not change information.

(1) Menu operation

[Network Configuration] → [Access Control]

(2) GUI operation

- Adding a new filter
  1. Click the [Add Filter] button.
     The [Add Filter] window is displayed.
  2. Add a new filter in the [Add Filter] window.
- Editing a filter
  1. To edit a filter, select the filter by clicking its radio button, and click the [Edit Filter] button. The [Edit Filter] window is displayed.
  2. Edit the filter in the [Edit Filter] window.
- Removing a filter
  1. To remove a filter, select the filter by clicking its radio button, and click the [Remove Filter] button.
     A confirmation dialog box opens for confirmation of removal.
  2. Click the [OK] button to remove the filter.
     The filter is removed, and the [Access Control] window is displayed again.
  3. The list of filters in the [Access Control] window can be checked to confirm that the filter has been removed.

5.4.10.1 [Add Filter] window/[Edit Filter] window

Filters can be added and edited using the [Add Filter] and [Edit Filter] windows, respectively.

This section describes only the [Edit Filter] window, which can be used to edit a filter, and does not describe the [Add Filter] window, which can be used to add a filter. Except for the different window titles, these windows have the same window format and operating methods.

Note: When using the Web browser of the computer or workstation to set the proxy, specify an IP address that takes the proxy setting into consideration.

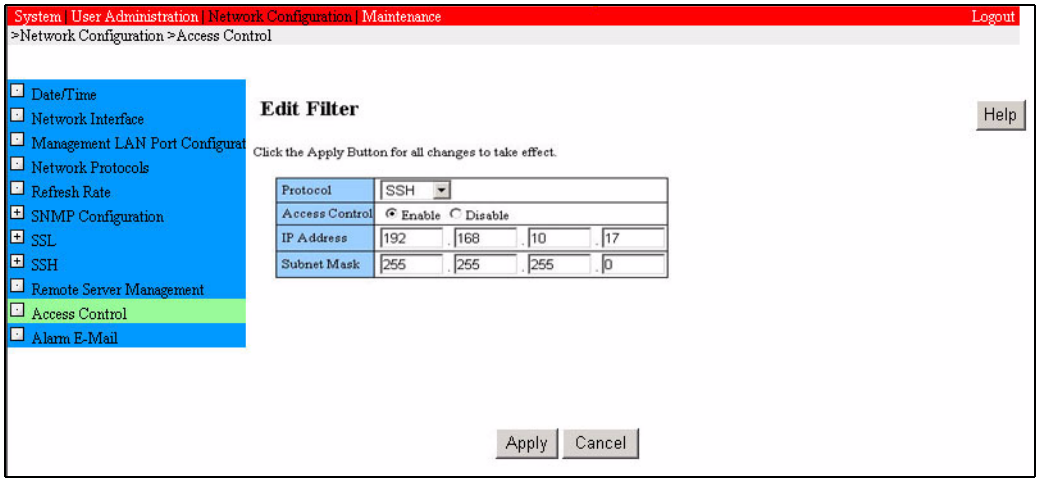


Figure 5.49 [Edit Filter] window

Table 5.85 Displayed and setting items in the [Edit Filter] window

Item	Description
Protocol	Select the target protocol for IP filtering from the pulldown list: • HTTP • HTTPS • Telnet • SSH • SNMP
Access Control	Select the [Enable] or [Disable] radio button to specify whether to use access control. Selecting [Disable] permits access from any IP address using the protocol selected above. Furthermore, the [IP Address] and [Subnet Mask] fields described below are grayed out, and input to them is not possible. Selecting [Enable] enables input in the [IP Address] and [Subnet Mask] fields and permits access from the specified IP address using the protocol selected in [Protocol].
IP Address	Enter an IP address that has access permission.
Subnet Mask	Enter the subnet mask of IP addresses that have access permission.

Table 5.86 Buttons in the [Edit Filter] window

Button	Description
Apply	After completing the [Protocol], [Access Control], and/or other settings, click the [Apply] button. The specified information takes effect on the system.
Cancel	Click the [Cancel] button to revert to the original settings for the protocol and access control.

(1) Menu operation

[Network Configuration] → [Access Control] → [Add Filter] button/[Edit Filter] button

(2) GUI operation

1 Make [Protocol], [Access Control], and/or other settings, enter an IP address and a subnet mask, and then click the [Apply] button.
Additions or changes are then made to management information accordingly.

5.4.11 [Alarm E-Mail] window

E-mail notification of events that occur in the PRIMEQUEST-series machine can be specified in the [Alarm E-Mail] window.

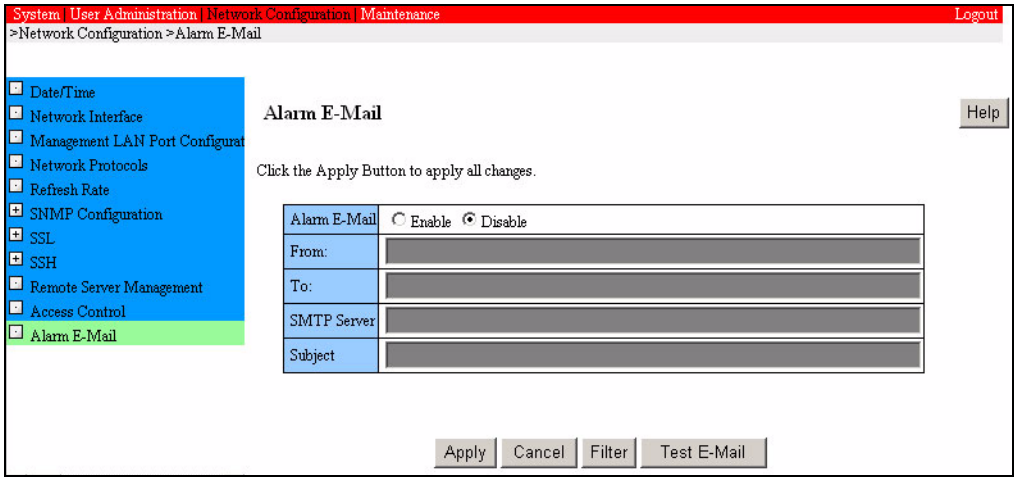


Figure 5.50 [Alarm E-Mail] window

Table 5.87 Displayed and setting items in the [Alarm E-Mail] window

Item	Description
Alarm E-Mail	Specify whether alarm e-mail is sent for an event that occurs: • Enable: Sends e-mail • Disable: Does not send e-mail
From:	Specify the e-mail address that sends the e-mail.
To:	Specify the e-mail address that receives the e-mail.
SMTP Server	Specify the IP address or FQDN of an SMTP server. The FQDN can be specified only if a DNS is set up.
Subject	Specify a subject line for the e-mail.

Table 5.88 Buttons in the [Alarm E-Mail] window

Button	Description
Apply	Specify whether alarm e-mail is sent, the e-mail address of the sender, etc., and click the [Apply] button to set the specified values.
Cancel	Click the [Cancel] button to revert to the original settings for whether alarm e-mail is sent, the e-mail address of the sender, etc.
Filter	Click the [Filter] button to display the [Alarm E-Mail Filtering Condition] window, which can be used to specify filtering conditions on the events that require sending of alarm e-mail.

Button	Description
Test E-Mail	Click the [Test E-Mail] button to send test alarm e-mail to the specified destination.

(1) Menu operation

[Network Configuration] → [Alarm E-Mail]

(2) GUI operation

1. Specify whether alarm e-mail is sent, the e-mail address of the sender, etc.
2. Click the [Filter] button to specify filtering conditions on the events that require sending of alarm e-mail.
   The [Alarm E-Mail Filtering Condition] window is displayed.
3. Specify filtering conditions in the [Alarm E-Mail Filtering Condition] window (see Section 5.4.11.1, "[Alarm E-Mail Filtering Condition] window").
4. Click the [Test E-Mail] button to send test alarm e-mail.
   Test alarm e-mail is sent to the specified destination.
5. Click the [Apply] button.
   The specified values in this window are then set.

Note: For specifying FQDN, the DNS server must be specified. The DNS server can be specified in [Network Configuration] → [Network Interface].

5.4.11.1 [Alarm E-Mail Filtering Condition] window

The [Alarm E-Mail Filtering Condition] window allows you to specify filtering conditions for events that trigger the transmission of alarm E-Mail messages.

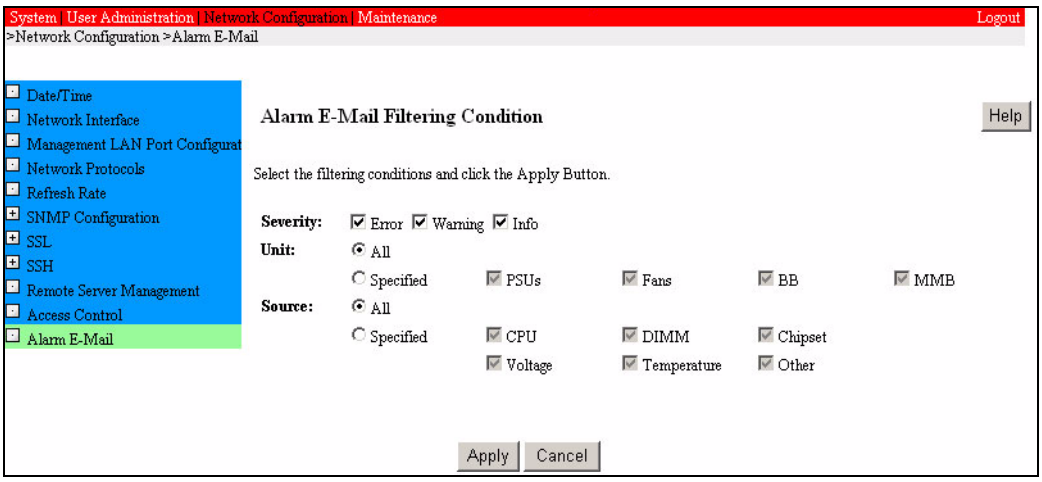


Figure 5.51 [Alarm E-Mail Filtering Condition] window

Table 5.89 Displayed and setting items in the [Alarm E-Mail Filtering Condition] window

Item	Description
Severity	Select the severity of events for event filtering by checking the corresponding check box. More than one severity options can be selected. • Error: Serious problem such as a hardware failure • Warning: Event that is not serious now but will possibly develop into a problem • Info: Normal event such as power-on By default, all of the options are selected.
Unit	Select a target unit for event filtering. Select either [All] or [Specified] by clicking its radio button. Selecting [All] disables event filtering based on units. Selecting [Specified] enables event filtering based on units and checking of check boxes, so a unit can be selected for event filtering. The default setting is [All].

Item	Description
Source	Select a target source for event filtering. Select either [All] or [Specified] by clicking its radio button. Selecting [All] disables event filtering based on sources. Selecting [Specified] enables event filtering based on sources and checking of check boxes, so a source can be selected for event filtering. The default setting is [All].

Table 5.90 Buttons in the [Alarm E-Mail Filtering Condition] window

Button	Description
Apply	Specify values in [Severity], [Unit], etc., and click the [Apply] button to set the specified filtering conditions.
Cancel	Click the [Cancel] button to revert to the original settings in filtering conditions such as [Severity] and [Unit].

(1) Menu operation

[Network Configuration] → [Alarm E-Mail] → [Filter] button

(2) GUI operation

1 Specify values in [Severity], [Unit], etc., and click the [Apply] button.
The specified filtering conditions are then set.

5.5 Maintenance Menu

Maintenance on the PRIMEQUEST-series machine can be conducted from the [Maintenance] menu.

5.5.1 Firmware Update menu

The [Firmware Update] menu provides the following windows:

- [MMB Firmware Update]
- [PAL/SAL Firmware Update]
- [EFI Firmware Update]
- [BMC Firmware Update]

The following description covers these windows and operations on them. However, certified service engineers are responsible for updating firmware.

5.5.1.1 [MMB Firmware Update] window

MMB firmware can be updated in the [MMB Firmware Update] window.

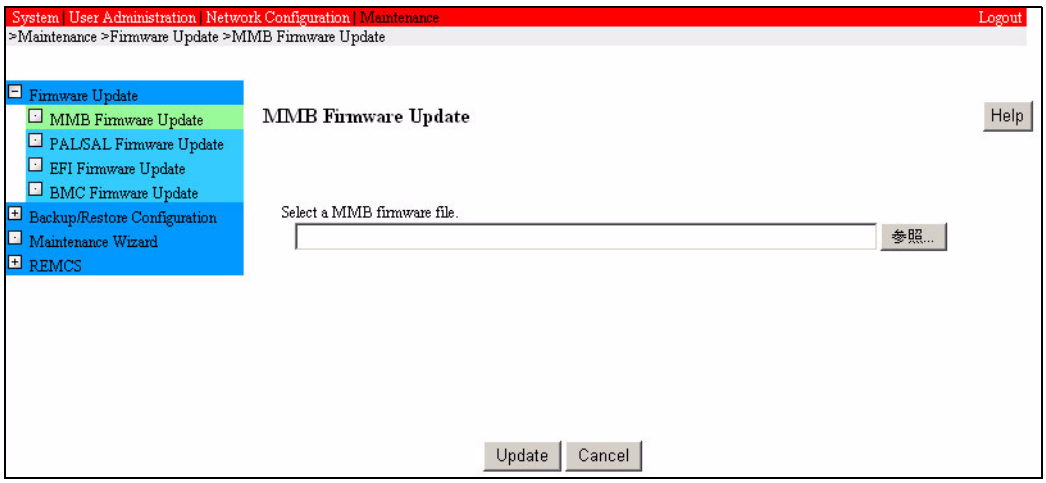


Figure 5.52 [MMB Firmware Update] window (selection)

Table 5.91 Displayed and setting items in the [MMB Firmware Update] window

Item	Description
Select a MMB firmware file.	Select an update file containing MMB firmware.

Table 5.92 Buttons in the [MMB Firmware Update] window

Button	Description
Browse	Opens a file selection dialog box.
Update	Opens a confirmation dialog box displaying current firmware version information and update firmware version information.
Cancel	Cancels the settings made in this window.

(1) Menu operation

[Maintenance] → [Firmware Update] → [MMB Firmware Update]

(2) GUI operation

- Procedure

1. Using the [Browse] button or [Select a firmware file] in the [MMB Firmware Update] window, select an update file containing MMB firmware, and click the [Update] button.
   A confirmation dialog box opens with current firmware version information and update firmware version information displayed.
   If the specified file does not contain MMB firmware, a warning dialog box opens with an error message displayed. Then, a consistency check is performed to check whether the version of MMB firmware in the specified file matches that in other firmware files. If the versions do not match, a confirmation dialog box opens to indicate that they do not match and ask whether to continue or cancel processing.
2. Click [OK] in the confirmation dialog box to continue the update.
   The MMB firmware is updated.

- Checking after an update
  - Updating firmware reboots the MMB. After the MMB is rebooted, connect to the MMB again and display the [MMB] window from the [System] menu to confirm that the MMB firmware version has been updated.
    If the firmware was not updated, the error status can be checked in the [System Event Log] window displayed from the [System] menu.
  - If the [(Standby)] MMB and not the [(Active)] MMB was selected in [Select MMB(s) to update] in the [MMB Firmware Update] window
    The firmware update completion window for the (Standby) MMB, not the (Active) MMB, is displayed. Confirm the completion of the firmware update in this window.

5.5.1.2 [PAL/SAL Firmware Update] window

The PAL/SAL firmware stored on a BB can be updated in the [PAL/SAL Firmware Update] window.

Note:

- The system must be powered off in advance of this update work.
- The OS must be shut down before updating PAL/SAL firmware.

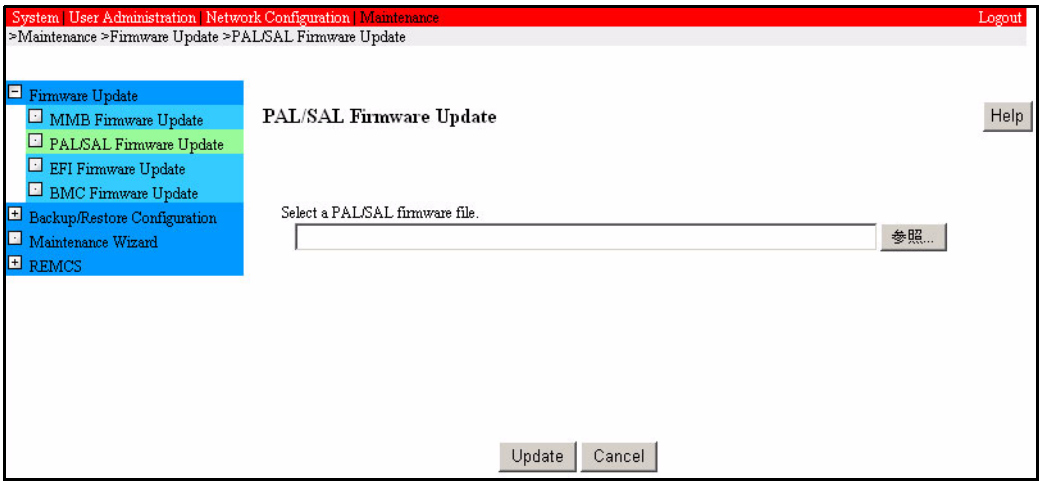


Figure 5.53 [PAL/SAL Firmware Update] window (selection)

Table 5.93 Displayed and setting items in the [PAL/SAL Firmware Update] window (selection)

Item	Description
Select PAL/SAL firmware file	Specify an update file containing PAL/SAL firmware.

Table 5.94 Buttons in the [PAL/SAL Firmware Update] window

Button	Description
Browse	Opens a file selection dialog box.
Upload	Opens a confirmation dialog box displaying current firmware version information and version information on the firmware to be uploaded.
Cancel	Cancels the settings made in this window.

(1) Menu operation

[PAL/SAL Firmware Update] window (selection)

[Maintenance] → [Firmware Update] → [PAL/SAL Firmware Update]

(2) GUI operation

1 Click the [Browse] button, specify an update file containing PAL/SAL firmware, and click the [Update] button.
The system must be powered off in advance of this update work.
If the specified file does not contain PAL/SAL firmware, a warning dialog box opens with an error message displayed. Then, a consistency check is performed to check whether the version of PAL/SAL firmware in the specified file matches that of other firmware files. If the versions do not match, a confirmation/warning dialog box opens for confirmation to continue processing.

2 If there is no problem, click the [OK] button in the confirmation dialog box.

Another confirmation dialog box appears with current firmware version information and update firmware version information displayed for confirmation.

3 Click the [OK] button in the [PAL/SAL Firmware Upload] window to continue the update.

To indicate the completion of the update, a confirmation dialog box opens when the update ends normally.

5.5.1.3 [EFI Firmware Update] window

EFI firmware stored on the BMM board can be updated in the [EFI Firmware Update] window.

Note:

- The system must be powered off in advance of this update work.
- The OS must be shut down before updating EFI firmware.

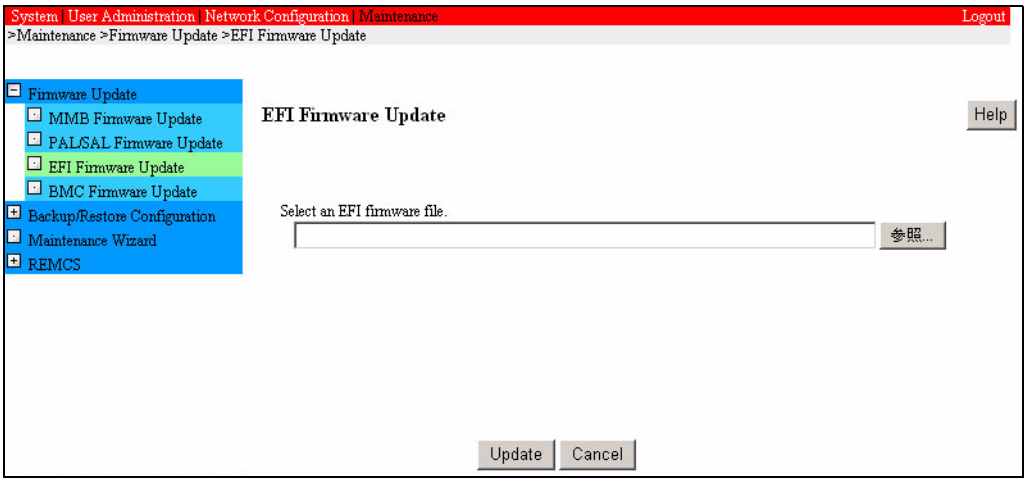


Figure 5.54 [EFI Firmware Update] window

Table 5.95 Displayed and setting items in the [EFI Firmware Update] window

Item	Description
Select EFI firmware file	Specify an update file containing EFI firmware.

Table 5.96 Buttons in the [EFI Firmware Update] window

Button	Description
Browse	Opens a file selection dialog box.
Update	Opens a confirmation dialog box displaying current firmware version information and update firmware version information.
Cancel	Cancels the settings made in this window.

(1) Menu operation

[Maintenance] → [Firmware Update] → [EFI Firmware Update]

(2) GUI operation

1 Click the [Browse] button, specify an update file containing EFI firmware, and click the [Update] button.
The system must be powered off in advance of this update work.
If the specified file does not contain EFI firmware, a warning dialog box opens with an error message displayed. Then, a consistency check is performed to check whether the version of EFI firmware in the specified file matches that of other firmware files. If the versions do not match, a dialog box opens to indicate that they do not match and ask whether to continue or cancel processing.

2 Click the [OK] button in the confirmation dialog box to continue the update.
Another confirmation dialog box opens with current firmware version information and update firmware version information displayed.

3 Click the [OK] button in the confirmation dialog box to continue the update.
To indicate the completion of the update, a confirmation dialog box opens when the update ends normally.

5.5.1.4 [BMC Firmware Update] window

BMC firmware can be updated in the [BMC Firmware Update] window.

Remarks:

- When the BMC is updated, the BMC reboots itself, causing a temporary interruption in service. To prevent possible problems, Fujitsu recommends that the system be powered off.

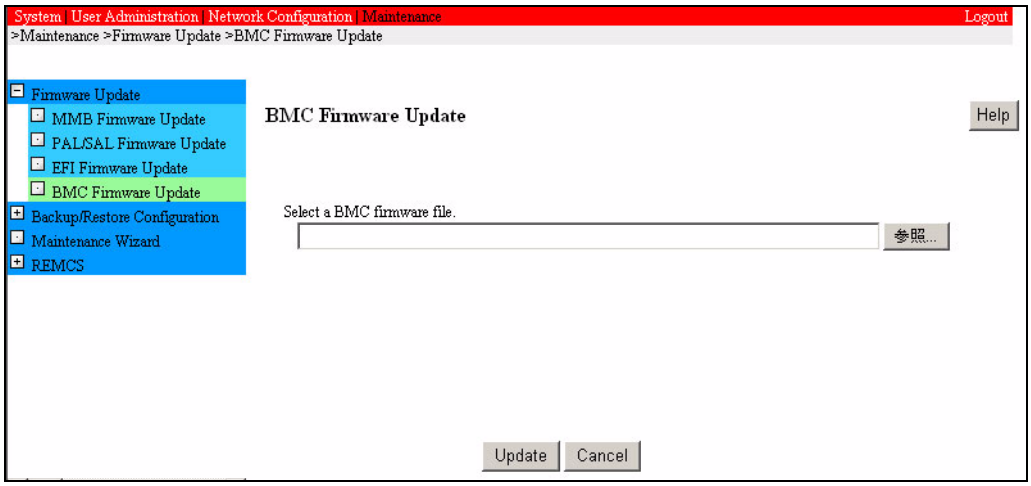


Figure 5.55 [BMC Firmware Update] window

Table 5.97 Displayed and setting items in the [BMC Firmware Update] window

Item	Description
Select a BMC firmware file	Specify an update file containing BMC firmware.

Table 5.98 Buttons in the [BMC Firmware Update] window

Button	Description
Browse	Opens a file selection dialog box..
Update	Opens a confirmation dialog box displaying current firmware version information and update firmware version information.
Cancel	Cancels the settings made in this window.

(1) Menu operation

[Maintenance] → [Firmware Update] → [BMC Firmware Update]

(2) GUI operation

1 Click the [Browse] button, specify an update file containing BMC firmware, and click the [Update] button.
A confirmation dialog box opens with current firmware version information and update firmware version information displayed.
If the specified file is not a BMC firmware file, an error message is displayed. Then, a consistency check is performed to check whether the version of BMC firmware in the specified file matches that of other firmware files. If the versions do not match, a dialog box opens to indicate that they do not match and ask whether to continue or cancel processing.

2 Click the [OK] button in the confirmation dialog box to continue the update. The update is executed. When the update ends normally, a confirmation dialog box opens to indicate that the update is completed.

5.5.2 Backup/Restore Configuration menu

[Backup/Restore Configuration] menu provides the following windows:

- [Backup/Restore MMB Configuration]
- [Backup/Restore EFI Configuration]

This section describes these windows and their operations.

Be sure to periodically save MMB configuration and EFI configuration information.

5.5.2.1 [Backup/Restore MMB Configuration] window

MMB configuration information can be backed up and restored using the [Backup/Restore MMB Configuration] window. The MMB configuration information is saved on the PC that runs the Web browser.

Remarks: To restore the MMB configuration information, the system must be powered off. For details on the procedure, see Section 5.2.14, "[Power Control] window."

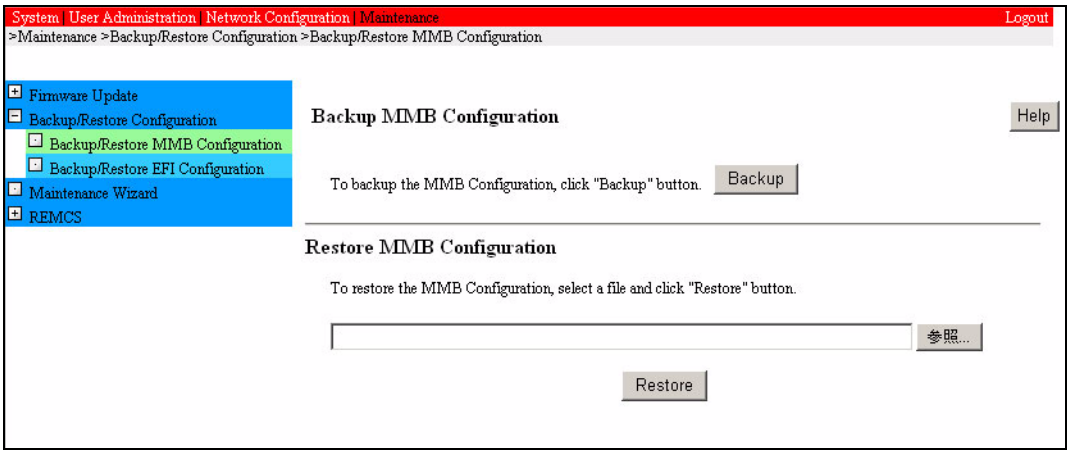


Figure 5.56 [Backup/Restore MMB Configuration] window

Table 5.99 Buttons in the [Backup/Restore MMB Configuration] window

Item	Description
Backup	Click the [Backup] button and a dialog box opens, and the save destination can be specified in the dialog box. Select the save path, and click the [OK] button to download the file. The default name of the backup MMB configuration file is: • MMB_(backup-date)_(MMB-version).dat
Browse	Opens a file selection dialog box.
Restore	Select an MMB configuration file saved on a remote PC, and click the [Restore] button to transfer the file to the MMB. When file transfer to the MMB is completed, the [Backup/Restore MMB Configuration] dialog box opens for confirmation to restore the MMB configuration. Click the [OK] button to restore the MMB configuration.

(1) Menu operation

[Maintenance] → [Backup/Restore Configuration] → [Backup/Restore MMB Configuration]

(2) GUI operation

- Backing up MMB configuration information
  1. Click the [Backup] button.
     The save destination dialog box opens in the browser.
  2. Select the save path in the save destination dialog box, and click the [OK] button.
     The MMB configuration information file is downloaded.
- Restoring MMB configuration information
  1. Click the [Browse] button, and select a backup MMB configuration file.
  2. Click the [Restore] button.
     The file is transferred to the MMB, and the [MMB Configuration File Information:] dialog box opens.
  3. Click the [OK] button in the [MMB Configuration File Information:] dialog box.
     The MMB configuration file is restored.
  4. The MMB is rebooted and the restored data is validated.

5.5.2.2 [Backup/Restore EFI Configuration] window

The [Backup/Restore EFI Configuration] window can be used to back up EFI configuration information to the PC whose browser displays this window.

The PAL/SAL/EFI setting must be made from the Boot Manager menu of EFI.

This section explains how to back up the EFI configuration information to a PC, where the browser is operating, and restore the backup information.

Figure 5.57 [Backup/Restore EFI Configuration] window

Table 5.100 Buttons in the [Backup/Restore EFI Configuration] window

Button	Description
Backup	Click the [Backup] button, and a dialog box opens in the browser. Select the save path, and click the [OK] button to download the file. The default name of the backup EFI configuration file is: • EFI_save-date_EFI-version.dat
Browse	Opens a file selection dialog box.
Restore	Select the EFI configuration file stored in the remote PC and click the [Restore] button to transfer the file to EFI. After the file transfer to EFI is complete, the [Backup/Restore EFI Configuration] dialog box opens to confirm whether to continue restore processing. Click the [OK] button to execute restoration.

(1) Menu operation

[Maintenance] → [Backup/Restore Configuration] → [Backup/Restore EFI Configuration]

(2) GUI operation

- Backup of the EFI configuration information

  1. Click the [Backup] button.
     The save destination dialog box opens.
  2. Select the save path in the save destination dialog box, and click the [OK] button.
     The EFI configuration information file is downloaded.

- Restoration of the EFI configuration information

  1. Click the [Browse] button, and select a backup EFI configuration information file stored on a remote PC.
  2. Click the [Restore] button.
     The EFI configuration information file is restored.

5.5.3 [Maintenance Wizard] window

The [Maintenance Wizard] window can be used for device maintenance with a wizard.

CAUTION

Guarantee of operation

Fujitsu certified service engineers use the [Maintenance Wizard] window for maintenance. Customers should not use this window. Doing so may cause a failure.

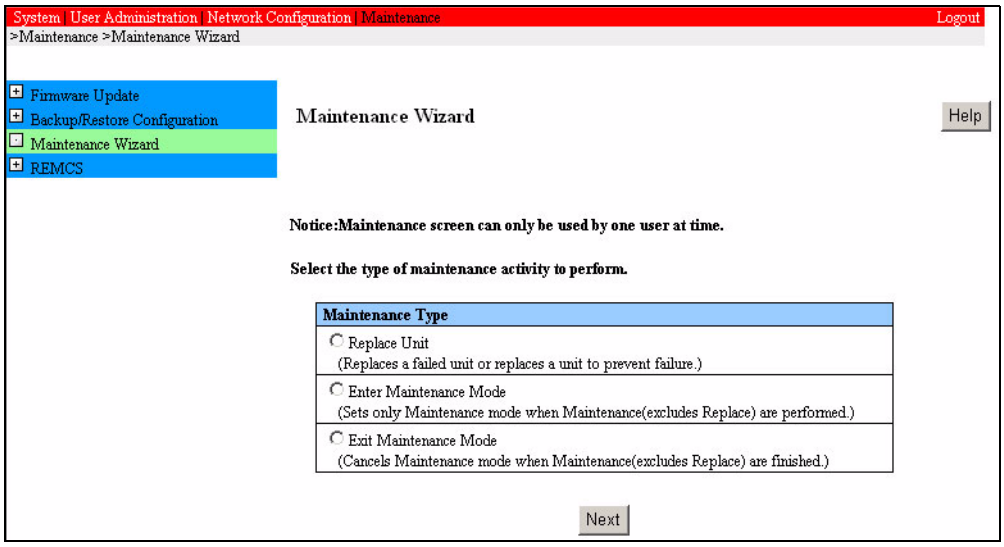


Figure 5.58 [Maintenance Wizard] window

Table 5.101 Buttons in the [Maintenance Wizard] window

Button	Description
Next	Displays the [Maintenance Wizard (Select Maintenance Mode)] window.

(1) Menu operation

[Maintenance] → [Maintenance Wizard]

5.5.4 REMCS menu

The REMCS menu can be used for REMCS-related operations and settings.

For details on REMCS, see Chapter 7, "REMCS" in the *PRIMEQUEST 500A/500/400 Series Reference Manual: Tools/Operation Information* (C122-E074EN).

CHAPTER 6 CLI Operations

This chapter describes operations performed to run and manage the PRIMEQUEST-series machine via the command line interface (CLI).

6.1 Basic CLI Operations

This section describes the command line interface (CLI) provided with the MMB.

The CLI can be accessed in either of the following two ways:

- Through the MMB serial port
- From a remote PC via the MMB management LAN

6.1.1 Access through the serial interface

1. Connect the MMB to the user terminal (e.g., notebook PC) with an RS-232C cross cable.
2. Launch the terminal software (e.g., Windows HyperTerminal) on the terminal, and set up the terminal software as follows.

Table 6.1 Setting items of terminal software

Setting item	Value
Bits per second	19200
Data bit	8
Parity	None
Stop bit	1
Flow control	None
Emulation	VT100

3. Enter a user name and password to log in when the login prompt is displayed.

6.1.2 Access via the management LAN interface

1. Connect the MMB to a remote PC with a straight LAN cable.
2. Launch a Telnet or SSH client on the remote PC, and specify the IP address of the MMB and the Telnet port number or the SSH port number to establish a connection.
3. Enter an account name and password to log in.

Additional note: The connection function provided by the MMB uses the SSH V2 protocol. Therefore, terminal software that supports SSH V2 must be prepared in order to establish an MMB connection using the SSH protocol.

6.1.3 List of CLI commands

The following table lists CLI commands. The letters in the Privilege column mean the following:

- Y: The command can be executed.
- N: The command cannot be executed.

Table 6.2 CLI commands

Command name	Privilege				Remarks
	Admin	Operator	User	CE	
factory_default	Y	N	N	Y	Restores information to its state at the time of shipment from the factory. Note: Do not use this command during system operation. Doing so restores all information to its state at the time of shipment from the factory.
clear access_control	Y	N	N	N	Clears the access control settings.
clear ssh_key	Y	Y	Y	Y	Deletes an SSH public key.
power off	Y	N	N	N	Powers off the entire system.
power on	Y	N	N	N	Powers on the entire system.
download ssh_key	N	N	Y	N	Downloads an SSH public key.
set date	Y	N	N	N	Sets a date and time.
set timezone	Y	N	N	N	Sets a time zone.
set gateway	Y	N	N	N	Sets a default gateway.
set http	Y	N	N	N	Enables or disables the HTTP server.

Command name	Privilege				Remarks
	Admin	Operator	User	CE	
set http_port	Y	N	N	N	Specifies the port used to accept an HTTP session.
set https	Y	N	N	N	Enables or disables the HTTPS server.
set https_port	Y	N	N	N	Specifies the port used to accept an HTTPS session.
set ssh	Y	N	N	N	Enables or disables SSH.
set ssh_port	Y	N	N	N	Specifies the port used to accept an SSH session.
set telnet	Y	N	N	N	Enables or disables Telnet.
set telnet_port	Y	N	N	N	Specifies the port used to accept a Telnet connection.
set ip	Y	N	N	N	Sets an IP address and a net mask for the management LAN interface.
set hostname	Y	N	N	N	Sets an MMB host name in the Fully Qualified Domain Name (FQDN) format.
set remcs	Y	N	N	Y	Sets routing for the REMCS port of the management LAN.
show access_control	Y	N	N	N	Displays the current access control settings.
show date	Y	Y	Y	Y	Displays the current date and time.
show timezone	Y	Y	Y	Y	Displays the time zone.
show gateway	Y	N	N	N	Displays the default gateway IP address that is set for the management LAN interface.
show http	Y	Y	Y	Y	Displays the current HTTP server status.
show http_port	Y	Y	Y	Y	Displays the port currently connected to an HTTP session.
show https	Y	Y	Y	Y	Displays the current HTTPS server status.
show https_port	Y	Y	Y	Y	Displays the port currently connected to an HTTPS session.
show ssh	Y	Y	Y	Y	Displays the current SSH server status.
show ssh_port	Y	Y	Y	Y	Displays the port currently connected to an SSH session.
show telnet	Y	Y	Y	Y	Displays the current Telnet server status.
show telnet_port	Y	Y	Y	Y	Displays the port currently connected to a Telnet session.
show ip	Y	Y	Y	Y	Displays the IP address and the net mask that are set for the management LAN interface.
show hostname	Y	Y	Y	Y	Displays the MMB host name.

Command name	Privilege				Remarks
	Admin	Operator	User	CE	
show network	Y	Y	Y	Y	Displays the network configuration that is set for the management LAN interface.
show remcs	Y	N	N	Y	Displays the routing configuration information for the REMCS port of the management LAN.
who	Y	Y	Y	Y	Displays the login names and times of users who are logged in to the MMB.
help	Y	Y	Y	Y	Displays help information on available commands.
update MMB	Y	N	N	Y	Updates MMB firmware.
update BMC	Y	N	N	Y	Updates BMC firmware.
update EFI	Y	N	N	Y	Updates EFI firmware.
update SAL	Y	N	N	Y	Updates PAL/SAL firmware.
exit	Y	Y	Y	Y	Logs out.
password	Y	Y	Y	Y	Changes the password.
ping	Y	Y	Y	Y	Sends an ICMP echo message to the destination specified in <IP address> or <server name>.

*1 Do not use this command during system operation. Doing so restores all information to its state at the time of shipment from the factory.

6.2 Setting Commands

The following commands are used to specify information:

- factory_default
- clear access_control
- clear ssh_key
- power off
- power on
- download ssh_key
- set date
- set timezone
- set gateway
- set http
- set http_port
- set https
- set https_port
- set ssh
- set ssh_port
- set telnet
- set telnet_port
- set ip
- set hostname
- set remcs

This section describes how to use these commands.

6.2.1 factory_default

This command resets MMB configuration information to the default values.

Executing this command restores all information to its state at the time of shipment from the factory.

Therefore, user and network configurations must be set up again after the command is executed.

- Privilege: Users with the Admin privilege or CE privilege

(1) Synopsis

```
factory_default [-f]
```

(2) Options

-f: Sets factory default values without prompting for confirmation.

(3) Examples

```
# factory_default
Reset to factory default [n]: y
```

6.2.2 clear access_control

Clears the IP filtering settings.

- Privilege: Users with the Admin privilege

(1) Synopsis

```
clear access_control
```

(2) Options

None

(3) Examples

None

6.2.3 clear ssh_key

This command deletes a public key that is registered for a logged-in user and used for SSH public key authentication.

- Privilege: Any user

(1) Synopsis

```
clear ssh_key
```

(2) Options

None

(3) Examples

None

6.2.4 power off

This command powers off the entire system.

- Privilege: Users with the Admin privilege

(1) Synopsis

```
power off [force]
```

(2) Options

- force: Forcibly powers off the system without shutting down the OS running.

(3) Examples

None

6.2.5 power on

This command powers on the entire system.

- Privilege: Users with the Admin privilege

(1) Synopsis

```
power on
```

(2) Options

None

(3) Examples

None

6.2.6 download ssh_key

This command downloads and registers a public key from a specified server so that a logged-in user can use the public key for SSH public key authentication.

The input format for the URL is as follows:

- http://host/path/file
- ftp://host/path/file

If no server is specified, the following message is displayed to prompt for URL input:

#download ssh_key

URL:

- Privilege: Users with the User privilege

(1) Synopsis

```
download ssh_key<URL>
```

(2) Options

None

(3) Examples

None

6.2.7 set date

This command sets a date and time. Specify a date and time in the following format:

- MM : Month (01 to 12)
- DD : Day (day of the month)
- hh : Hour (00 to 23)
- mm : Minute (00 to 59)
- CC : See Options.
- YY : See Options.
- ss : See Options.

● Privilege: Users with the Admin privilege

(1) Synopsis

```
set date MMDDhhmm {[CC] YY} [,ss]
```

(2) Options

- CC : Specify the first two digits of a year.
- YY : Specify the last two digits of a year.
- ss : Specify the seconds.

(3) Examples

None

6.2.8 set timezone

This command sets a time zone.

The date and time must be set again with the set date command after a time zone is set.

● Privilege: Users with the Admin privilege

(1) Synopsis

```
set timezone <timezone>
```

(2) Options

<timezone>: region/city name

Table 6.3 lists the time zone settings.

Table 6.3 Time zone settings

Region name	Specification format (region/city name)		
America	America/Anchorage	America/Adak	America/Indiana/ Indianapolis
	America/Indiana/Knox	America/Indiana/ Marengo	America/Indiana/ Petersburg
	America/Indiana/Vevay	America/Indiana/ Vincennes	America/Anguilla
	America/Araguaina	America/Aruba	America/Atka
	America/Bahia	America/Belem	America/Boa_Vista
	America/Boise	America/Buenos_Aires	America/Cambridge_Bay
	America/Campo_Grande	America/Catamarca	America/Cayman
	America/Chicago	America/Coral_Harbour	America/Cordoba
	America/Cuiaba	America/Curacao	America/Danmarkshavn
	America/Dawson	America/Dawson_Creek	America/Denver
	America/Detroit	America/Edmonton	America/Eirunepe
	America/Fort_Wayne	America/Fortaleza	America/Glace_Bay
	America/Godthab	America/Goose_Bay	America/Grand_Turk
	America/Guadeloupe	America/Halifax	America/Indianapolis
	America/Inuvik	America/Iqaluit	America/Jujuy
	America/Juneau	America/Knox_IN	America/Los_Angeles
	America/Louisville	America/Maceio	America/Manaus
	America/Martinique	America/Mendoza	America/Menominee
	America/Miquelon	America/Moncton	America/Montreal
	America/Montserrat	America/New_York	America/Nipigon
	America/Nome	America/Noronha	America/Pangnirtung
	America/Phoenix	America/Porto_Acre	America/Porto_Velho
	America/Puerto_Rico	America/Rainy_River	America/Rankin_Inlet
	America/Recife	America/Regina	America/Rio_Branco
	America/Rosario	America/Sao_Paulo	America/Scoresbysund
	America/Shiprock	America/St_Thomas	America/St_Vincent
	America/Swift_Current	America/Thule	America/Thunder_Bay
	America/Toronto	America/Vancouver	America/Virgin
	America/Whitehorse	America/Winnipeg	America/Yakutat
	America/Yellowknife	America/Argentina/ Buenos_Aires	America/Argentina/ Catamarca
	America/Argentina/ ComodRivadavia	America/Argentina/ Cordoba	America/Argentina/Jujuy
	America/Argentina/ La_Rioja	America/Argentina/ Mendoza	America/Argentina/ Rio_Gallegos
	America/Argentina/ San_Juan	America/Argentina/ Tucuman	America/Argentina/ Ushuaia
	America/Kentucky/ Louisville	America/Kentucky/ Monticello	America/North_Dakota/ Center

Region name	Specification format (region/city name)		
Asia	Asia/Seoul	Asia/Tokyo	
Atlantic	Atlantic/Azores	Atlantic/Bermuda	Atlantic/Canary
	Atlantic/Jan_Mayen	Atlantic/Faeroe	Atlantic/Reykjavik
	Atlantic/Madeira	Atlantic/South_Georgia	Atlantic/St_Helena
	Atlantic/Stanley		
Australia	Australia/Adelaide	Australia/ACT	Australia/Brisbane
	Australia/Broken_Hill	Australia/Canberra	Australia/Currie
	Australia/Darwin	Australia/Hobart	Australia/LHI
	Australia/Lindeman	Australia/Lord_Howe	Australia/Melbourne
	Australia/NSW	Australia/North	Australia/Perth
	Australia/Queensland	Australia/South	Australia/Sydney
	Australia/Tasmania	Australia/Victoria	Australia/West
	Australia/Yancowinna		
Brazil	Brazil/DeNoronha	Brazil/Acre	Brazil/East
	Brazil/West		
Canada	Canada/Atlantic	Canada/Central	Canada/East-Saskatchewan
	Canada/Eastern	Canada/Mountain	Canada/Newfoundland
	Canada/Pacific	Canada/Saskatchewan	Canada/Yukon
Europe	Europe/Amsterdam	Europe/Athens	Europe/Belfast
	Europe/Berlin	Europe/Brussels	Europe/Bucharest
	Europe/Budapest	Europe/Copenhagen	Europe/Dublin
	Europe/Gibraltar	Europe/Helsinki	Europe/Lisbon
	Europe/London	Europe/Luxembourg	Europe/Madrid
	Europe/Mariehamn	Europe/Oslo	Europe/Paris
	Europe/Prague	Europe/Rome	Europe/Stockholm
	Europe/Vatican	Europe/Vienna	Europe/Warsaw
	Europe/Zurich		
Pacific	Pacific/Auckland	Pacific/Chatham	Pacific/Fakaofo
	Pacific/Guam	Pacific/Honolulu	Pacific/Johnston
	Pacific/Marquesas	Pacific/Midway	Pacific/Niue
	Pacific/Norfolk	Pacific/Pago_Pago	Pacific/Pitcairn
	Pacific/Rarotonga	Pacific/Saipan	Pacific/Tahiti
	Pacific/Wallis		
America	US/Aleutian	US/Alaska	US/East-Indiana
	US/Arizona	US/Central	US/Michigan
	US/Eastern	US/Hawaii	US/Indiana-Starke
	US/Mountain	US/Pacific	US/Pacific-New
	US/Samoa		

(3) Examples

```
# set timezone Asia/Tokyo
```

6.2.9 set gateway

This command sets the default gateway.

- Privilege: Users with the Admin or CE privilege

(1) Synopsis

```
set gateway <ip address>
```

(2) Options

None

(3) Examples

None

6.2.10 set http

This command enables or disables the HTTP server.

- Privilege: Users with the Admin privilege

(1) Synopsis

```
set http {enable | disable}
```

(2) Options

None

(3) Examples

None

6.2.11 set http_port

This command sets the port number of the port used to accept an HTTP session.

The default setting is 8081. The setting range is 1024 to 65535.

- Privilege: Users with the Admin privilege

(1) Synopsis

```
set http_port <port>
```

(2) Options

None

(3) Examples

None

6.2.12 set https

This command enables or disables the HTTPS server.

- Privilege: Users with the Admin privilege

(1) Synopsis

```
set https {enable | disable}
```

(2) Options

None

(3) Examples

None

6.2.13 set https_port

This command sets the port number of the port used to accept an HTTPS session.

The default setting is 432. The setting range is 432,1024 to 65535.

- Privilege: Users with the Admin privilege

(1) Synopsis

```
set https_port <port>
```

(2) Options

None

(3) Examples

None

6.2.14 set ssh

This command enables or disables SSH.

- Privilege: Users with the Admin privilege

(1) Synopsis

```
set ssh {enable | disable}
```

(2) Options

None

(3) Examples

None

6.2.15 set ssh_port

This command sets the port number of the port used to accept an SSH session.

The default setting is 22. The setting range is 22,1024 to 65535.

- Privilege: Users with the Admin privilege

(1) Synopsis

```
set ssh_port <port>
```

(2) Options

None

(3) Examples

None

6.2.16 set telnet

This command enables or disables Telnet.

- Privilege: Users with the Admin privilege

(1) Synopsis

```
set telnet {enable | disable}
```

(2) Options

None

(3) Examples

None

6.2.17 set telnet_port

This command sets the port number of the port used to accept a Telnet connection.

The default setting is 23. The setting range is 23,1024 to 65535.

- Privilege: Users with the Admin privilege

(1) Synopsis

```
set telnet_port <port>
```

(2) Options

None

(3) Examples

None

6.2.18 set ip

This command sets an IP address and a net mask for the management LAN interface.

Specify the physical IP address of the MMB connected to a serial port.

- Privilege: Users with the Admin privilege

(1) Synopsis

```
set ip <ip address> <netmask>
```

(2) Options

None

(3) Examples

None

6.2.19 set hostname

This command sets an MMB host name in the Fully Qualified Domain Name (FQDN) format.

- Privilege: Users with the Admin privilege

(1) Synopsis

```
set hostname <host name>.<domain name>
```

(2) Options

None

(3) Examples

```
# set hostname XXXXX.fujitsu.com
```

6.2.20 set remcs

This command sets routing for the REMCS port of the management LAN.

Note:

- If this command is used to change the SMTP address, the SMTP server configuration must also be changed in the [REMCS Environment Setup] window. In addition, before REMCS initialization, the routing must be set with this command.
- When the REMCS connection is done with P-P, the < gateway address > and the <SMTP address> settings are unnecessary.
  In this case, specify 0.0.0.0 for <gateway address> and <SMTP address>.
- Specify "0.0.0.0" for "ip address" when you invalidate the setting with this command. Specify any value for other parameters. (Specifying 0.0.0.0 is recommended.)

- Privilege: Users with the Admin or CE privilege

(1) Synopsis

```
set remcs <ip address> <subnet mask> <gateway address> <smtp
address>
```

<ip address>: IP address assigned to the REMCS port

<subnet mask>: Subnet mask of the IP address

<gateway address>: gateway Address

<smtp address>: Mail server used for REMCS notification

(2) Options

None

(3) Examples

None

6.3 Display Commands

The following commands are used to display information:

- show access_control
- show date
- show timezone
- show gateway
- show https
- show https_port
- show ip
- show hostname
- show ssh
- show ssh_port
- show telnet
- show telnet_port
- show network
- show remcs
- who
- help

This section describes how to use these commands.

6.3.1 show access_control

This command displays the current access control settings.

- Privilege: Users with the Admin privilege

(1) Synopsis

```
show access_control
```

(2) Options

None

(3) Examples

None

6.3.2 show date

This command displays the current date and time.

- Privilege: Any user

(1) Synopsis

```
show date
```

(2) Options

None

(3) Examples

```
# show date
2004-08-31 20:40:17
```

6.3.3 show timezone

This command displays the time zone.

- Privilege: Any user

(1) Synopsis

```
show timezone
```

(2) Options

None

(3) Examples

```
# show timezone
Timezone is set to "Asia/Tokyo"
```

6.3.4 show gateway

This command displays the default gateway IP address that is set for the management LAN interface.

- Privilege: Any user

(1) Synopsis

```
show gateway
```

(2) Options

None

(3) Examples

```
# show gateway
Gateway Address: 10.1.2.1
```

6.3.5 show http

This command displays the current HTTP server status (enabled or disabled).

- Privilege: Any user

(1) Synopsis

```
show http
```

(2) Options

None

(3) Examples

```
# show http
HTTP: disabled
```

6.3.6 show http_port

This command displays the port number of the port currently connected to an HTTP session.

- Privilege: Any user

(1) Synopsis

```
show http_port
```

(2) Options

None

(3) Examples

```
# show http_port
HTTP Port Number:8081
```

6.3.7 show https

This command displays the current HTTP server status (enabled or disabled).

- Privilege: Any user

(1) Synopsis

```
show https
```

(2) Options

None

(3) Examples

```
# show https
HTTPS: disabled
```

6.3.8 show https_port

This command displays the current HTTPS server status (enabled on disabled).

- Privilege: Any user

(1) Synopsis

```
show https_port
```

(2) Options

None

(3) Examples

```
# show https_port
HTTPS Port Number:432
```

6.3.9 show ip

This command displays the IP address and the net mask that are set for the management LAN interface.

- Privilege: Any user

(1) Synopsis

```
show ip
```

(2) Options

None

(3) Examples

```
# show ip
IP Address    : 10.1.2.124
Netmask       : 255.255.255.0
```

6.3.10 show hostname

This command displays the MMB host name.

- Privilege: Any user

(1) Synopsis

```
show hostname
```

(2) Options

None

(3) Examples

```
 # show hostname
   xxxxx.fujitsu.com
```

6.3.11 show ssh

This command displays the current SSH server status (enabled or disabled).

- Privilege: Any user

(1) Synopsis

```
show ssh
```

(2) Options

None

(3) Examples

```
# show ssh
SSH: disabled
```

6.3.12 show ssh_port

This command displays the port number of the port currently connected to an SSH session.

- Privilege: Any user

(1) Synopsis

```
show ssh_port
```

(2) Options

None

(3) Examples

```
# show ssh_port
SSH Port Number:22
```

6.3.13 show telnet

This command displays the current Telnet server status (enabled or disabled).

- Privilege: Any user

(1) Synopsis

```
show telnet
```

(2) Options

None

(3) Examples

```
# show telnet
Telnet: disabled
```

6.3.14 show telnet_port

This command displays the port number of the port currently connected to a Telnet session.

- Privilege: Any user

(1) Synopsis

```
show telnet_port
```

(2) Options

None

(3) Examples

```
# show telnet_port
Telnet Port Number:23
```

6.3.15 show network

This command displays the following items in the network configuration information that is set for the management LAN interface:

- HOST name
- IP Address
- Netmask
- Gateway Address
- MAC Address
- HTTP status
- HTTP Port Number
- HTTPS status
- HTTPS Port Number
- Telnet status
- Telnet Port Number
- SSH status
- SSH Port Number

● Privilege: Any user

(1) Synopsis

```
show network
```

(2) Options

None

(3) Examples

```
# show network
XXXXX.fujitsu.com
IP Address:          10.1.2.124
Netmask:             255.255.255.0
Gateway Address:     10.1.2.1
MAC Address:00:AA:   00:12:34:55
HTTP:                disabled
HTTP Port Number:    8081
HTTPS:               disabled
HTTPS Port Number:   432
SSH:                 enabled
SSH Port Number:     22
Telnet:              disabled
Telnet Port Number:  23
```

6.3.16 show remcs

This command displays routing configuration information for the REMCS port of the management LAN.

- Privilege: Users with the Admin or CE privilege

(1) Synopsis

```
show remcs
```

(2) Options

None

(3) Examples

```
#show remcs
IP Address 192.162.1.10
Net Mask   255.255.255.0
Gateway    192.162.1.1
SMTP       10.19.128.90
```

6.3.17 who

This command displays the following information about users who are logged in to the MMB:

- Login name
- Login time of a user
- Remote host name (or IP address of remote host)
  A hyphen (-) is displayed when the user logs in via a serial port.
- Connection method (login via Telnet/SSH, MMB Web-UI, or serial port)
  - "Telnet/SSH" is displayed when the user logs in via Telnet/SSH.
  - "WebUI" is displayed when the user logs in via MMB Web-UI.
  - A hyphen (-) is displayed when the user logs in via a serial port.

● Privilege: Any user

(1) Synopsis

```
who
```

(2) Options

None

(3) Examples

None

6.3.18 help

This command displays help information on the available commands.

● Privilege: Any user

(1) Synopsis

```
help
```

(2) Options

None

(3) Examples

None

6.4 Update Commands

The following commands are used to update firmware:

- update MMB
- update BMC
- update EFI
- update SAL

This section describes how to use these commands.

6.4.1 update MMB

This command downloads an MMB firmware file from the specified URL and updates MMB firmware.

The input format for the URL is as follows:

http://host/path/file
ftp://host/path/file

A URL cannot be accessed through a proxy server.

Remarks: The MMB must be rebooted when MMB firmware is updated.

- Privilege: Users with the Admin privilege or CE privilege

(1) Synopsis

```
update MMB <url> [noverify] [quiet]
```

(2) Options

noverify: Disables the verify check.

quiet: Updates the firmware without interactive operation involving the user.

(3) Examples

```
# update MMB http://host/path/mmbfirm001
Downloading an MMB firmware file...........

Current Firmware Version of MMB#0:XXXXX
New Firmware Version:             YYYYY

Are you sure to continue MMB Firmware Update? [Y|N]: Y

Updating MMB Firmware...............

The Firmware update of MMB#0 is successfully completed.

#
```

6.4.2 update BMC

This command downloads a BMC firmware file from the specified URL and updates BMC firmware.

The input format for the URL is as follows:

http://host/path/file
ftp://host/path/file

A URL cannot be accessed through a proxy server.

Additional note: The BMC must be rebooted when BMC firmware is updated. BMC service is interrupted when the BMC is rebooted. Therefore, Fujitsu recommends shutting down the OS before updating BMC firmware.

- Privilege: Users with the Admin privilege or CE privilege

(1) Synopsis

```
update BMC <url> [noverify] [quiet]
```

(2) Options

noverify: Disables the verify check.

quiet: Updates the firmware without interactive operation involving the user.

(3) Examples

```
# update BMC http://host/path/bmcfirm001
Downloading a BMC firmware file...........

Current Firmware Version                  : XXXXX
New Firmware Version:                       YYYYY

Are you sure to continue BMC Firmware Update? [Y|N]: Y

Updating BMC Firmware...............

The Firmware update is successfully completed.

#
```

6.4.3 update EFI

This command downloads an EFI firmware file from the specified URL and updates EFI firmware.

The input format for the URL is as follows:

http://host/path/file
ftp://host/path/file

A URL cannot be accessed through a proxy server.

Additional note: The system must be rebooted when EFI firmware is updated. Therefore, shut down the OS before updating EFI firmware.

- Privilege: Users with the Admin privilege or CE privilege

(1) Synopsis

```
update EFI <url> [noverify] [quiet]
```

(2) Options

noverify: Disables the verify check.

quiet: Updates the firmware without interactive operation involving the user.

(3) Examples

```
# update EFI http://host/path/bmcfirm001
Downloading a EFI firmware file...........

Current Firmware Version of                : XXXXX
New Firmware Version:                        YYYYY

Are you sure to continue EFI Firmware Update? [Y|N]: Y

Updating EFI Firmware...............

The Firmware update is successfully completed.

#
```

6.4.4 update SAL

This command downloads a PAL/SAL firmware file from the specified URL and updates PAL/SAL firmware.

The input format for the URL is as follows:

http://host/path/file
ftp://host/path/file

A URL cannot be accessed through a proxy server.

Note:

- The system must be rebooted when PAL/SAL firmware is updated. Therefore, shut down the OS before updating PAL/SAL firmware.

● Privilege: Users with the Admin privilege or CE privilege

(1) Synopsis

```
update SAL <url> [noverify] [quiet]
```

(2) Options

noverify: Disables the verify check.

quiet: Updates the firmware without interactive operation involving the user.

(3) Examples

```
# update SAL http://host/path/bmcfirm001
Downloading a PAL/SAL firmware file...........

Current Firmware Version          : XXXXX
New Firmware Version:               YYYYY

Are you sure to continue PAL/SAL Firmware Update? [Y|N]: Y

Updating PAL/SAL Firmware...............

The Firmware update is successfully completed.

#
```

6.5 Other Commands

In addition to the commands for specifying, displaying, and updating information, the following commands are available:

- exit
- passwd
- ping

This section describes how to use these commands.

6.5.1 exit

This command logs you out of the system.

- Privilege: Any user

(1) Synopsis

```
exit
```

(2) Options

None

(3) Examples

None

6.5.2 passwd

This command changes the password of a specified user.

Users granted the Admin privilege can change the passwords of all users, whereas users without the Admin privilege can only change their own passwords.

If USER is not specified, the command changes the password of the currently logged-in user.

The password change procedure is as follows:

1. Enter the current password when prompted.
   If the entered password is correct, processing continues. If not, the command rejects the password change requests and exits.
2. Enter the new password when prompted.
   The entered new password is checked to ensure that it is sufficiently complex. If no problem is found, processing continues. If this check fails, the command rejects the password change request.
3. Reenter the new password for confirmation when prompted. If the password entered now matches the password entered previously, the new password becomes effective. If not, the command rejects the password change request.

- Privilege: Any user

(1) Synopsis

```
passwd [USER]
```

(2) Options

USER: Specifies the user name of the user whose password is to be changed.

(3) Examples

```
# passwd
Current password: *************
New password: *****************
Re-enter new password: *****************
Password changed.
```

6.5.3 ping

This command sends an ICMP echo message to the destination specified in <IP address> or <server name>.

- Privilege: Any user

(1) Synopsis

```
ping [-c <count>] {<IP address>|<server name>}
```

(2) Options

-c count: Ends the processing after sending a specified number of packets.

(3) Examples

None

Part IV PSA

CHAPTER 7 Web-UI Operations

The PSA is a system management application that runs on the OS on PRIMEQUEST series machines. This chapter describes use of MMB Web-UI for PSA operations by providing a list of menus and describing screens and the operations.

Clicking [Partition] → [PSA] menu from the MMB Web-UI navigation bar displays the initial screen of the [OS Information] window.

Under any of the following conditions, however, the [OS Information] window is not displayed and the content area displays a message indicating that the OS or PSA is not operating:

- PSA is not installed in the system.
- The OS is not running.
- PSA is not running.
- A management LAN setting is not correct.

● Component status display and background color

The PSA window displays the status of components. The component status is indicated by text and displayed against a specific background color for easy identification, as shown in the following table.

Table 7.1 Component status and background colors

Status	Background color	Status	Background color
OK	White	Warning	Yellow
Not-present	Gray	Degraded	Yellow
Error	Red	Unknown	White

● Display for items whose values cannot be obtained

The PSA window displays "n.a." for any item whose value is unknown.

Note:

- If the load of the system is high, the following message may be displayed.
  - [n.a.] when the item value could not be acquired.
  - E_33005 Communication Error. (01:XXXX*1)
    *1 XXXX: 3301, 3399, or 3400

- [Refresh] button

In operation under PSA, the [Refresh] button is displayed in windows with changes. Click this button to reflect the new setting values to the window. When you select [Enable] in the [Refresh Rate] window for the MMB, no automatic refresh will become effective. New information is collected at regular intervals (30 minutes) to ensure that up-to-date values can be displayed. Therefore, the latest information may not be displayed depending on the time the button is clicked. Items on which up-to-date information is retrieved when they are displayed are noted in each description of the window.

Note: If you change the time zone when PSA is starting, PSA's internal local time is not updated. To update the local time, you need to restart PSA.

CAUTION

Mis-operation

If the browser update button and the frame update function in the contextual menu are used in the PSA setting window that is displayed when settings are completed, settings may be made by simply confirming the previously made settings.
Note that, in this case, the settings are made without displaying the corresponding confirmation dialog box.
Note also that a window with the new settings is displayed when the settings have been made. However, to confirm that all settings are correct, Fujitsu recommends displaying the window again using the Refresh button. If no Refresh button is available, the window should be opened again by selecting the corresponding menu once again.

7.1 List of Menus in the Web-UI Window

This section provides a list of PSA menus (the section enclosed by double lines in the following table) for Web-UI. The meanings of the symbols used in the Supported OS column are as follows:

- Supported OS
  - Y: Supported
  - N: Not supported
- Privilege
  - RW: The user can read and write in the window concerned (called a setting privilege user, in this document).
  - RO: The user can only read in the window concerned (called a read privilege user, in this document).
  - N/A: The window and submenu concerned are not displayed.

Table 7.2 Menus

Navigation bar		PSA submenus		Supported OS		Privilege				Remarks
Level 1	Level 2	Level 1	Level 2	Linux	Windows	Administrator	Operator	User	CE	
System										
	:									
	PSA									
		OS Information		Y	Y	RO	RO	RO	RO	Displays a unit outline and OS information. * The displayed items vary from one OS to another.
		CPUs		Y	Y	RO	RO	RO	RO	Displays CPU information in a list.
		DIMMs		Y	Y	RO	RO	RO	RO	Displays DIMM information in a list.
		PCI Devices		Y	Y	RW	RW	RO	RW	Displays PCI device information.
		Network								
			Network Interfaces	Y	Y	RO	RO	RO	RO	Displays the network status.
			Network Routing	Y	N	RO	RO	RO	RO	Displays the routing status.
		Disk Partitions		Y	N	RO	RO	RO	RO	Displays disk partition information.
		Hard Disks		Y	Y	RO	RO	RO	RO	Displays hard disk information in a list.
		Process List		Y	N	RW	RW	RO	N/A	Displays process information in a list and sends a signal to the specified process.
		System File		Y	N	RO	RO	RO	N/A	Displays system files.
		Inventory								
			Hardware Inventory	Y	Y	RO	RO	RO	RO	Displays a hardware inventory list.

Navigation bar		PSA submenus		Supported OS		Privilege				Remarks
Level 1	Level 2	Level 1	Level 2	Linux	Windows	Administrator	Operator	User	CE	
			Software Inventory	Y	N	RO	RO	RO	RO	Displays the OS version, and displays and downloads the RPM package information.
		Agent Log		Y	Y	RO	RO	RO	RO	Displays an agent log list.
		SEL		Y	Y	RO	RO	RO	RO	Downloads a system event log (binary format).
		Export List		Y	Y	RO	RO	RO	RO	Saves the information stored by PSA, in CSV format.
		Setup								
			Watchdog	Y	Y	RW	RW	RO	RO	Sets up Watchdog monitoring.
			S.M.A.R.T.	Y	Y	RW	RW	RO	RO	Sets up S.M.A.R.T. monitoring.
		Expansion File Unit		Y	Y	RW	RW	RO	RW	Displays information on the expansion file unit(s). This menu is displayed when one or more expansion file units are connected.

7.2 [OS Information] Window

The [OS Information] window displays a unit outline and OS information.

Remarks: This window displays items that vary depending on the installed OS.

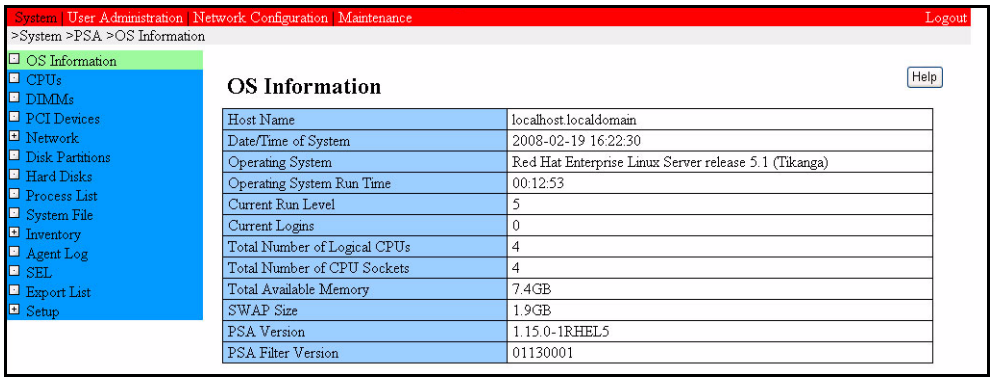


Figure 7.1 [OS Information] window (Linux)

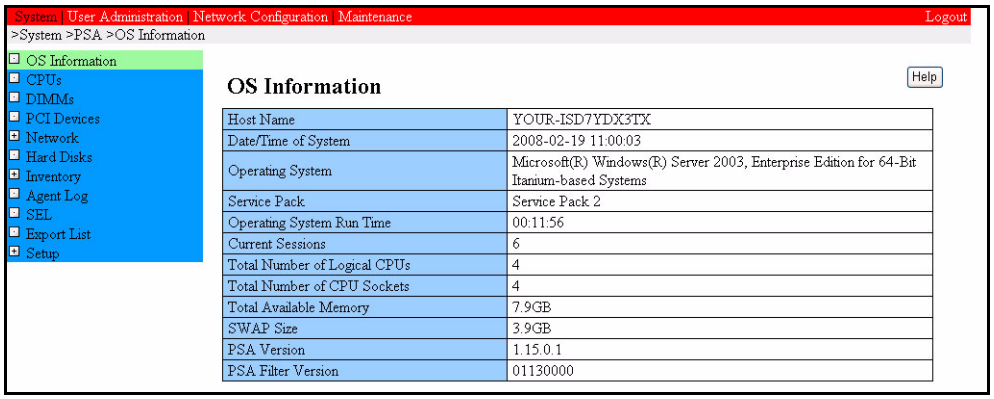


Figure 7.2 [OS Information] window (Windows)

Table 7.3 Displayed items in the [OS Information] window

Item	Description
Host Name	Host name that is set by the OS
Date/Time of System	System time (local time), as follows: yyyy-MM-dd HH:mm:ss * The latest information is retrieved when this window is displayed.
Operating System	OS name and version
Service Pack * Windows version only	Displays the OS service pack.
Operating System Run Time	OS operating time * The latest information is retrieved when this window is displayed.
Current Run Level * Only Linux supported	OS run level, ranging from Run Level 1 to 5 * The latest information is retrieved when this window is displayed.
Current Logins * Only Linux supported	Number of currently logged-in users * The latest information is retrieved when this window is displayed.
Current Sessions * Only Windows supported	Displays the number of current sessions. * The latest information is retrieved when this window is displayed.
Total Number of Logical CPUs	Number of logical CPUs recognized by the OS
Total Number of CPU Sockets	Number of physical CPU sockets
Total Available Memory	If the DIMM size is up to 1023 MB, it is displayed in MB units. If it is at least 1024 MB, it is displayed in GB units (rounded down to one decimal place).
SWAP Size	If the SWAP size is up to 1023 MB, it is displayed in MB units. If it is at least 1024 MB, it is displayed in GB units (rounded down to one decimal place). * In Windows Server 2008, if the virtual memory size is managed automatically, a hyphen (-) is displayed.
PSA Version	PSA version
PSA Filter Version	Version of the filter definition for the PSA hardware error monitoring function

(1) Menu operation

[System] → [PSA] → [OS Information]

(2) GUI operation

None

7.3 [CPUs] Window

The [CPUs] window displays in list form information on the CPUs.

Remarks: Uninstalled CPUs are displayed dimmed.

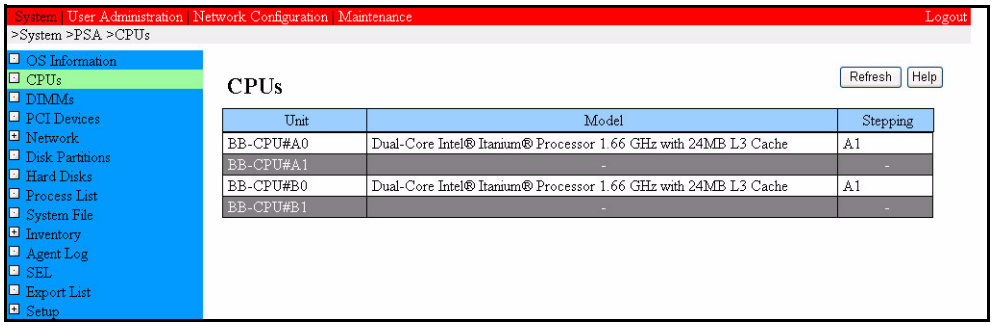


Figure 7.3 [CPUs] window

Table 7.4 Displayed items in the [CPUs] window

Item	Description
Unit	CPU identification names.
Model	CPU model. If CPU is not installed, a hyphen (-) is displayed.
Stepping	Displays CPU stepping. If CPU is not installed, a hyphen (-) is displayed.

(1) Menu operation

[System] → [PSA] → [CPUs]

(2) GUI operation

None

7.4 [DIMMs] Window

The [DIMMs] window displays in list form information on the DIMMs.

Remarks: Uninstalled DIMMs are displayed dimmed.

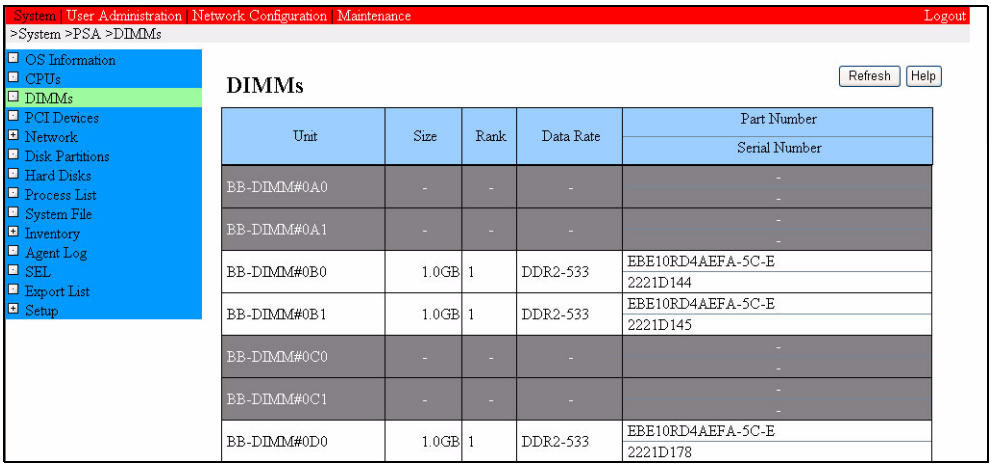


Figure 7.4 [DIMMs] window

Table 7.5 Displayed items in the [DIMMs] window

Item	Description
Unit	DIMM identification names.
Size	DIMM size If DIMM is not installed, a hyphen (-) is displayed.
Rank	DIMM rank number If DIMM is not installed, a hyphen (-) is displayed.
Data Rate	DIMM data rate. If DIMM is not installed, a hyphen (-) is displayed.
Part Number	DIMM part number. If DIMM is not installed, a hyphen (-) is displayed.
Serial Number	DIMM serial number. If DIMM is not installed, a hyphen (-) is displayed.

(1) Menu operation

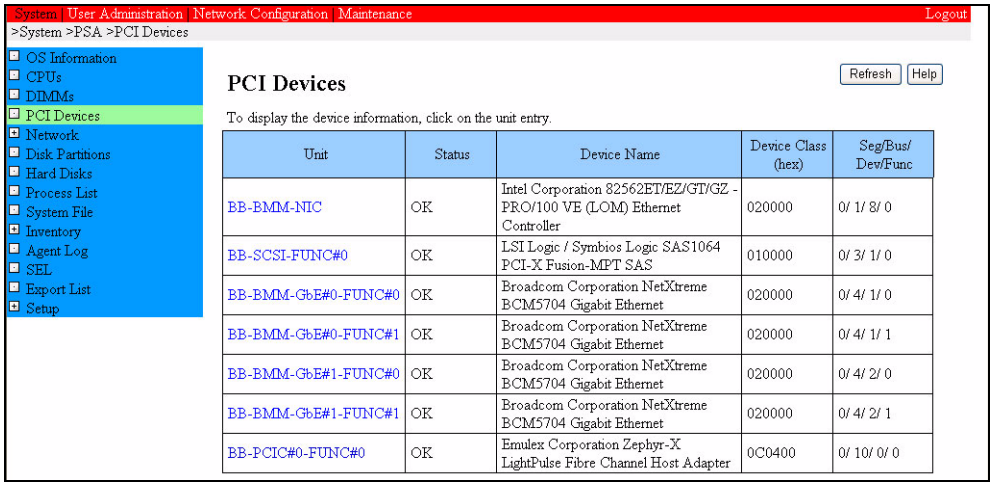
[System] → [PSA] → [DIMMs]

(2) GUI operation

None

7.5 [PCI Devices] Window

The [PCI Devices] window displays information about connected PCI devices.



Unit	Status	Device Name	Device Class (hex)	Seg/Bus/ Dev/Func
BB-BMM-NIC	OK	Intel Corporation 82562ET/EZ/GT/GZ - PRO/100 VE (LOM) Ethernet Controller	020000	0/ 1/ 8/ 0
BB-SCSI-FUNC#0	OK	LSI Logic / Symbios Logic SAS1064 PCI-X Fusion-MPT SAS	010000	0/ 3/ 1/ 0
BB-BMM-GbE#0-FUNC#0	OK	Broadcom Corporation NetXtreme BCM5704 Gigabit Ethernet	020000	0/ 4/ 1/ 0
BB-BMM-GbE#0-FUNC#1	OK	Broadcom Corporation NetXtreme BCM5704 Gigabit Ethernet	020000	0/ 4/ 1/ 1
BB-BMM-GbE#1-FUNC#0	OK	Broadcom Corporation NetXtreme BCM5704 Gigabit Ethernet	020000	0/ 4/ 2/ 0
BB-BMM-GbE#1-FUNC#1	OK	Broadcom Corporation NetXtreme BCM5704 Gigabit Ethernet	020000	0/ 4/ 2/ 1
BB-PCIC#0-FUNC#0	OK	Emulex Corporation Zephyr-X LightPulse Fibre Channel Host Adapter	0C0400	0/ 10/ 0/ 0

Figure 7.5 [PCI Devices] window

The [PCI Devices] window displays a list of PCI devices. Clicking a [Unit] item displays details about the corresponding device. Information is displayed for each PCI card function. If the PCI card is a multi-function PCI card, multiple lines of device information are displayed for a single unit.

When PCI cards are added or removed, it takes about 3 minutes for the information to be reflected on the window.

Table 7.6 Displayed items in the [PCI Devices] window

Item	Description
Unit	PCI device identification names.
Status	Integrated status of the hardware status of the PCI device and status of individual subordinate devices connected to it (and this includes the predicted fault status): • OK: Normally operating. • Error: Serious problem such as a hardware failure • Warning: Warning status (A problem may occur.) • Unknown: Unknown
Device Name	Device name that combines a vendor name and device name In Windows: "SCSI Controllers" and other such names are displayed for newly added devices after a hardware configuration change. After thirty minutes or so, however, these names are changed to device names recognized by the OS.
Device Class	Device class ID (in hexadecimal)
Seg/Bus/Dev/Func	The following numbers: • Segment number • Bus number • Device number • Function number

Table 7.7 Buttons in the [PCI Devices] window

Button	Description
Each box containing a [Unit] item	Click the box containing a [Unit] item to display the details window.

(1) Menu operation

[System] → [PSA] → [PCI Devices]

(2) GUI operation

1 Click a [Unit] item.
- If DeviceClass=020000, the [Ethernet controller] window is displayed.
- If DeviceClass=010000, the [Storage Controller] window is displayed.
- If DeviceClass=0C0400, the [Fibre Channel] window is displayed.
- For DeviceClass other than 020000, 010000, and 0C0400, the [PCI Device] window is displayed.

2 Click the [Return] button in the displayed window.
The [PCI Devices] window is displayed again.

7.5.1 [Ethernet Controller] window

If a [Device Class] item in the [PCI Devices] window is "020000" (Ethernet controller), the [Ethernet Controller] window displays Ethernet controller information.

A setting privilege user can clear the status by clicking the [Status Clear] button.

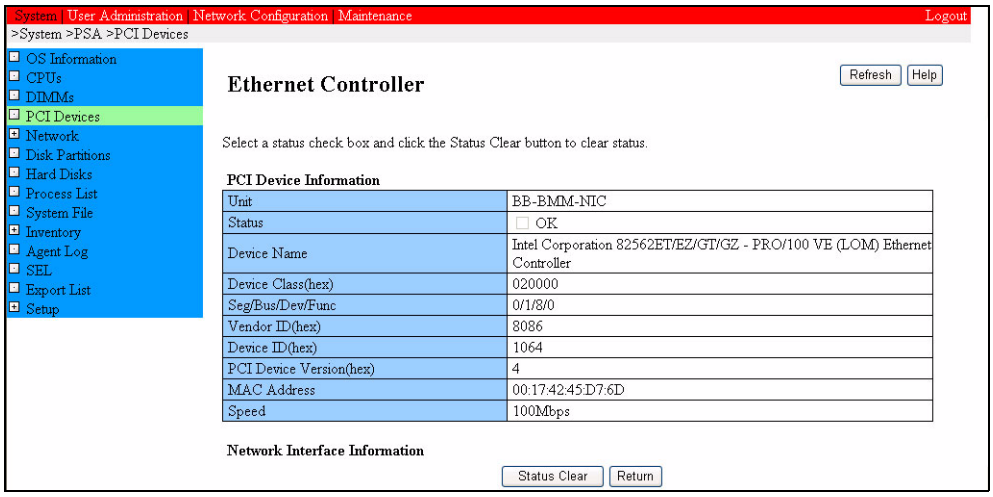


Figure 7.6 [Ethernet Controller] window

Table 7.8 Displayed and setting items in the [Ethernet Controller] window

Item	Description
PCI Device Information	
Unit	Ethernet controller identification name
Status	Ethernet controller status: • OK: Operating normally • Error: Serious problem such as a hardware failure • Warning: Warning status (A problem may occur.) • Unknown: Unknown Check the [Error] or [Warning] status check box to clear the status. Additional note: When the check box is checked, the status is not cleared until the [Status Clear] button is clicked.
Device Name	Device name that combines a vendor name and device name In Windows: "Ethernet Controller" and other such names are displayed for newly added devices after a hardware configuration change. After thirty minutes or so, however, these names are changed to device names recognized by the OS.
Device Class	Device class ID (in hexadecimal)
Seg/Bus/Dev/Func	The following numbers: • Segment number • Bus number • Device number • Function number
Vendor ID	Vendor ID (in hexadecimal)
Device ID	Device ID (in hexadecimal)
PCI Device Version	PCI device version number
MAC Address	MAC address • The window may display "n.a." if it is opened while PSA's internal information is being updated. The use of the Refresh button refreshes the window to display the correct information. • The window displays "n.a." if the driver is not loaded when PSA starts.
Speed	Network speed • The window may display "n.a." if it is opened while PSA's internal information is being updated. The use of the Refresh button refreshes the window to display the correct information. • The window displays "n.a." if the driver is not loaded. * The latest information is retrieved when this window is displayed when PSA starts.

Network Interface Information

Remarks: Network-related information may not be supplied depending on the type or status of the OS or a driver. A hyphen "-" is displayed for any of this information that is not supplied.

Item	Description
Interface Name	Names of al l interfaces allocated to the NIC (and this includes virtual IPs)
IP Address	The IP address of each interface is displayed.
IP Subnet Mask	The subnet mask of each interface is displayed.

MAC Statistics (Transmit Statistics)

* The latest information is retrieved when this window is displayed.

Notes:

- If the network connection is disabled by the Windows system, MAC Statistics information cannot be retrieved and zeros are displayed for all items.
- If the driver is not loaded when PSA starts, zeros are displayed for all items.

Item	Description
Total Packets	Number of packets passed using IP for transmission with a transport layer protocol (e.g., TCP or UDP). This does not include packets that were only transferred.
Total Bytes	Number of transmitted bytes
Defferred Xmite	Number of packets that waited in the first transmission attempt because the line was busy. Network congestion causes transmission delays. Currently, 0 is displayed for this item as a fixed setting.
Single Collisions	Number of packets that were successfully transmitted after exactly one collision. [Single Collisions] indicates network congestion. Currently, 0 is displayed for this item as a fixed setting.
Multiple Collisions	Number of packets that were successfully transmitted after several collisions. This does not include the packets already recorded in [Single Collisions]. [Multiple Collisions] indicates network congestion. Currently, 0 is displayed for this item as a fixed setting.
Excessive Collisions	Number of packets whose transmission failed because the maximum number of collisions was exceeded. The cause is extremely serious network congestion.
Carrier Sense Errors	Number of times that the carrier sense conditions were violated
Late Collision Errors	Number of packets for which no collision was detected until data exceeding 512 bits was transmitted. This indicates that the transmission route is too long and that the subsequent signal propagation time is too long, resulting in an overlap. Currently, 0 is displayed for this item as a fixed setting.
SQE Test Errors	Number of times that an SQE test error occurs

Item	Description
MAC Xmit Errors	Number of packets that could not be properly transmitted because of an internal error in the MAC layer. This does not include the packets already recorded in [Late Collision Errors], [Excessive Collisions], and [Carrier Sense Errors].

MAC Statistics (Receive Statistics)

* The latest information is retrieved when this window is displayed.

Notes:

- If the network connection is disabled by the Windows system, MAC Statistics information cannot be retrieved and zeros are displayed for all items.
- If the driver is not loaded when PSA starts, MAC Statistics information cannot be retrieved and zeros are displayed for all items.

Item	Description
Total Packets	Total number of IP datagrams received from all other stations. This includes the number of error datagrams.
Total Bytes	Number of bytes received
FCS Errors	Number of packets in which an FCS test detected an error. The cause is low transmission quality.
Alignment Errors	Number of packets received by the selected interface and found to have an incorrect length because the number of bytes is not an integer. The cause is low transmission quality. Currently, 0 is displayed for this item as a fixed setting.
Frame Too Long	Number of packets received by the selected interface and found to be longer than the maximum packet length (1,518 bytes)
MAC Receive Errors	Number of packets that could not be properly received because of an internal error in the MAC layer

Table 7.9 Buttons in the [Ethernet Controller] window

Button	Description
Status Clear	The [Status Clear] button is displayed only for a setting privilege user. Check the [Status] check box in [PCI Device Information], click the [Status Clear] button, and the [Confirm Settings] dialog box opens. Click the [OK] button in the [Confirm Settings] dialog box to clear the status of the Ethernet controller. If the notification suppression function is active to suppress mail/REMCS/SNMPtrap notification, this button deactivates the notification suppression function.
Return	Click the [Return] button to return to the previous window.

(1) Menu operation

[System] → [PSA] → [PCI Devices] → [Unit]

[System] → [PSA] → [Network] → [Network Interfaces] → [Unit]

(2) GUI operation

- Clearing the status of the Ethernet controller
  1. Check the [Status] check box, and click the [Status Clear] button.
     The [Confirm Settings] dialog box opens.
  2. Click the [OK] button in the [Confirm Settings] dialog box.
     The status of the Ethernet controller is cleared.
  3. Click the [Return] button.
     Return to the previous window.
- Leaving the status of the Ethernet controller as is
  1. Click the [Return] button.
     Return to the previous window.

(3) Error messages

If the system ends abnormally, any of the following messages is displayed in a dialog box.

Message	Meaning	Response
Error: Status Clear Error : ErrorCode=****	Status clearing failed. [ErrorCode] 3309: PCI Status Clear	If using Refresh and then repeating the operation in the window results in the same problem, contact the system administrator or a Fujitsu certified service engineer.

7.5.2 [Storage Controller] window

If a [Device Class] item in the [PCI Devices] window is "010000" (SCSI storage controller), the [Storage Controller] window displays storage controller information.

A setting privilege user can clear the status by clicking the [Status Clear] button.

If devices are added to or removed from the group of devices connected to the storage controller, a maximum of three minutes will be required to refresh the display to reflect the change.

Note:

- If a disk under GDS/PSDM control is added or removed during OS operation, the values displayed for [Device Type] and [Disk Capacity] in the [Storage Controller] window are not updated. To update them, PSA must be restarted or the following PSA command must be executed (the following command is supported only in the Linux version of PSA):

```
/opt/FJSVpsa/sh/force_search.sh -a
```

- If no device is connected to the storage controller, only the title row is displayed.

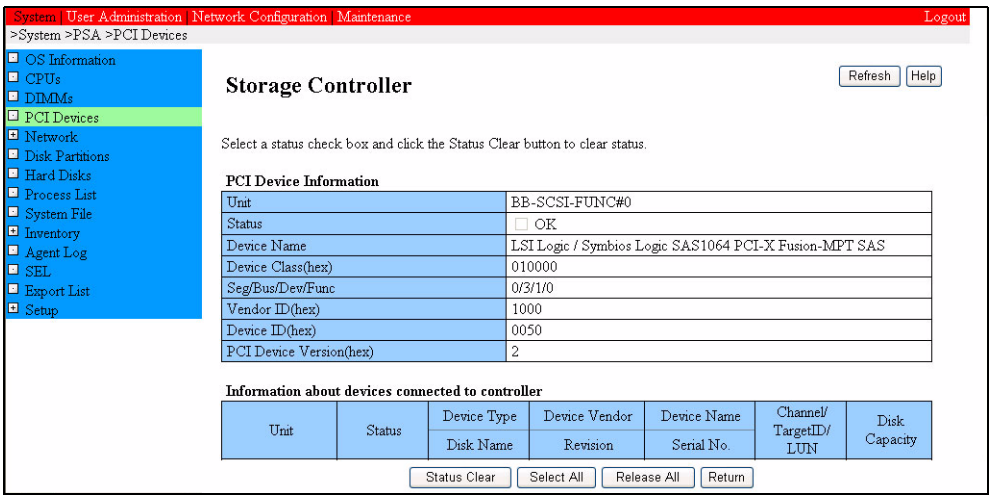


Figure 7.7 [Storage controller] window

Table 7.10 Displayed and setting items in the [Storage Controller] window

Item	Description
PCI Device Information	
Unit	SCSI storage controller identification name
Status	Hardware status of the storage controller (but not including the status of any subordinate device connected to it). • OK: Operating normally • Error: Serious problem such as a hardware failure • Warning: Warning status (A problem may occur.) • Unknown: Unknown Check the [Error] or [Warning] status check box to clear the status. Additional note: Check the check box and then click the [Status Clear] button to clear the status.
Device Name	Device name that combines a vendor name and device name In Windows: "SCSI Controllers" and other such names are displayed for newly added devices after a hardware configuration change. After thirty minutes or so, however, these names are changed to device names recognized by the OS.
Device Class	Device class ID (in hexadecimal)
Seg/Bus/Dev/Func	The following numbers: • Segment number • Bus number • Device number • Function number
Vendor ID	Vendor ID (in hexadecimal)
Device ID	Device ID (in hexadecimal)
PCI Device Version	PCI device version number (in hexadecimal)
Expansion File Unit * This item is displayed when one or more expansion file units are connected.	
Unit	Displays the identification name of the controller of an expansion file unit at the connection destination.
Information about devices connected to controller	
Unit	Displays the identification name of a device connected to the storage controller.
Status	Integrated status of the hardware status and predicted fault status of individual devices connected to the storage controller: • OK: Operating normally • Error: Serious problem such as a hardware failure • Warning: Warning status (A problem may occur. This includes S.M.A.R.T.) • Unknown: Unknown Check the check box to clear the status. Additional note: Check the check box and then click the [Status Clear] button to clear the status.

Item	Description
Device Type	Device type: • Direct Access • Sequential Access • Printer • Processor • WORM • CD-ROM • Scanner • Optical Device • Medium Changer • Communications • Unknown • Enclosure Linux: • Direct Access (GDS) Windows: • Direct Access (PSDM) * Linux The device type is displayed as "n.a." for any device other than the above. * Windows The device type is displayed as "Unknown" for any device other than the above (such as RBC/CardReader/Bridge/Other).
Disk Name	Disk device name. If the device is not a disk (including GDS or PSDM), a hyphen (-) is displayed.
Device Vendor	Device vendor
Revision	Device revision number
Device Name	Device model name
Serial No	Device serial number. If the device is not a disk (including GDS), a hyphen (-) is displayed.
Channel/TargetID/LUN	SCSI channel, SCSI target ID, and SCSI logical unit number of the device
Disk Capacity	If the device is a disk, its capacity is displayed in MB units if the capacity is up to 1023 MB, or in GB units (rounded down to one decimal place) if the capacity is at least 1024 MB. If the device is not a disk or it is a GDS or PSDM, a hyphen (-) is displayed. Since disk capacities are displayed on the assumption that 1 GB = 1024 MB = 1024 x 1024 KB, they are slightly smaller than on catalogs.

Table 7.11 Buttons in the [Storage Controller] window

Button	Description
Status Clear	The [Status Clear] button is displayed only for a setting privilege user. Check the [Status] check box in [PCI Device Information] or [Information about devices connected to controller], click the [Status Clear] button, and the [Confirm Settings] dialog box opens. Click the [OK] button in the [Confirm Settings] dialog box to clear the hardware status of the storage controller or a device connected to the storage controller. If the notification suppression function is active to suppress mail/REMCS/SNMPtrap notification, this button deactivates the notification suppression function.
Select All	The [Select All] button is displayed only for a setting privilege user. Click the [All Select] button to check all check boxes.
Release All	The [Release All] button is displayed only for a setting privilege user. Click the [Release All] button to uncheck all check boxes.
Return	Click the [Return] button to return to the previous window.

(1) Menu operation

[System] → [PSA] → [PCI Devices] → [Unit]

[System] → [PSA] → [Expansion File Unit] → [Unit] → [SDU#x] → [CTRL#x]

(2) GUI operation

- Clearing the hardware status of the storage controller

  1. Check the [Status] check box in [PCI Device Information] (see the Remark 1 below), and click the [Status Clear] button.
     The [Confirm Settings] dialog box opens.
  2. Click the [OK] button in the [Confirm Settings] dialog box.
     The hardware status of the storage controller is cleared.
  3. Click the [Return] button.
     Return to the previous window.

- Clearing the hardware status of a device connected to the storage controller

  1. Check the [Status] check box in [Information about devices connected to controller] (see the Remark 1 below), and click the [Status Clear] button.
     The [Confirm Settings] dialog box opens.

2 Click the [OK] button in the [Confirm Settings] dialog box.
The hardware status of the device connected to the storage controller is cleared.

3 Click the [Return] button.
Return to the previous window.

- Not clearing the storage controller status

1 Click the [Return] button.
Return to the previous window.

Remarks:

1 Clicking the [Select All] button selects all check boxes, and clicking the [Release All] button clears all check boxes.

2 Up to 500 status items can be cleared at a time. If the [Status Clear] button is clicked when more than 500 status items are selected, a dialog box opens to ask for confirmation to clear the first 500 status items.

(3) Error messages

If the system ends abnormally, any of the following messages is displayed in a dialog box.

Message	Meaning	Response
Error: Status Clear Error : ErrorCode=****	Status clearing failed. [ErrorCode] 3309: PCI Status Clear 3310: SMART Status Clear 3311: SCSI Status Clear	If using Refresh and then repeating the operation in the window results in the same problem, contact the system administrator or a Fujitsu certified service engineer.

7.5.3 [Fibre Channel] window

The [Fibre Channel] window displays fibre channel information when the [Device Class] item in the [PCI Devices] window is [0C0400] (Fibre Channel).

A user with setting privilege can clear the status by using the [Status Clear] button.

When the number of devices connected to the fibre channel is increased or decreased, it takes up to three minutes until the change is reflected in the screen display.

Notes:

- Information on a DISK in the ETERNUS multi-path driver environment is displayed under a PCI device with a multi-path specified. In Linux, [Serial No.], [Disk Capacity], and [Disk Name] are displayed using accurate values only under a PCI device (normally the device with the smallest bus number) with a multi-path specified. In Windows, [Serial No.], [Disk Capacity], and [Disk Name] are displayed as "n.a."
- When the number of DISKs under GDS control is increased or decreased while running the OS, the [Device Type] and [Disk Capacity] items in the [Fibre Channel] window are not updated. To update these items, it is necessary to reboot the PSA or manually execute the following PSA command.

```
/opt/FJSVpsa/sh/force_search.sh -a
```

- When the Power Path of an EMC is used, [Disk Name], [Serial No.], and [Disk Capacity] may be displayed as "n.a."
- When a device is not connected to the fibre channel, only the title row is displayed.

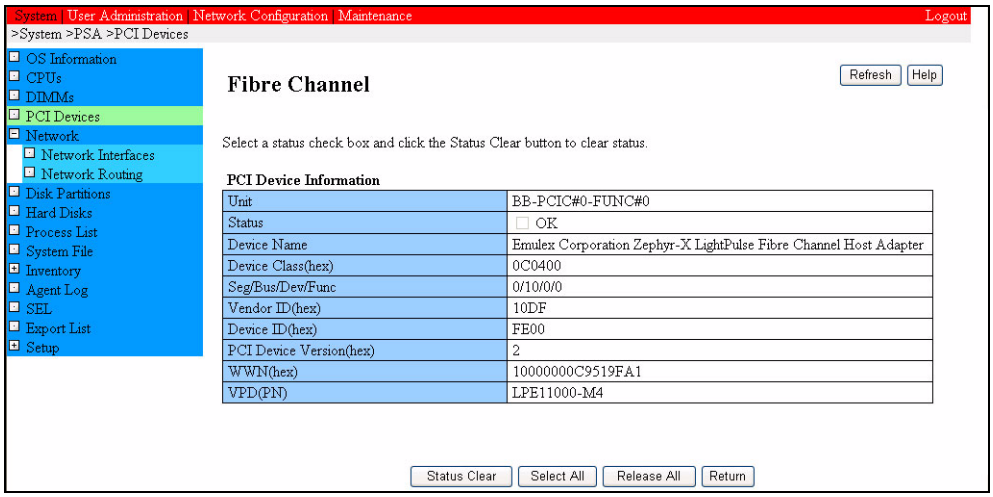


Figure 7.8 Fibre Channel window

Table 7.12 Display and setting items of [Fibre Channel] window

Item	Explanation
PCI Device Information	
Unit	Displays the identification name of a fibre channel.
Status	Displays the hardware status of the fibre channel (excluding the status of a device connected under the hardware). • OK: Normal • Error: An important problem such as a hardware error is detected. • Warning: Warning status (A problem may occur in the future.) • Unknown: Uncertain If [Error] or [Warning] is displayed, clear it by selecting the check box. Remarks: To clear the status, select the check box and click the [Status Clear] button.
Device Name	Displays a device name including a vendor name. Windows: A device, newly added after changing the hardware configuration, is displayed as "Fibre Channel," but is updated about 30 minutes later using a device name recognized by the OS.
Device Class	Displays a device class ID (hexadecimal).
Seg/Bus/Dev/Func	Displays the following numbers: • Segment No. • Path No. • Device No. • Function No.
Vendor ID	Displays a vendor ID (hexadecimal).
Device ID	Displays a device ID (hexadecimal).
PCI Device Version	Displays the version of a PCI device (hexadecimal).
WWN	Acronym of World Wide Name 64-bit address specifically assigned to a fibre channel switch and HBA (hexadecimal)
VPD(PN)	Acronym of Vital Product Data Displays the option information of PCI functions.
Information about devices connected to controller	
Unit	Displays the identification name of a device connected to the fibre channel.

Item	Explanation
Status	Displays a combination of the hardware status of a device connected to the fibre channel and the predictive monitoring status of the device. • OK: Normal • Warning: Warning status (A problem such as S.M.A.R.T. may occur in the future.) • Unknown: Uncertain • To clear the status, select the check box. Remarks: To clear the status, select the check box and click the [Status Clear] button.
Device Type	Displays a device type. • Direct Access • Sequential Access • Printer • Processor • WORM • CD-ROM • Scanner • Optical Device • Medium Changer • Communications • Unknown • Enclosure • Direct Access (GDS) * In Linux, a device other than indicated above is displayed as "n.a." * In Windows, a device other than indicated above (such as RBC/CardReader/Bridge/Other) is displayed as "Unknown".
Disk Name	Displays the name of a disk. For a non-disk device (such as a GDS), a hyphen [-] is displayed.
Device Vendor	Displays the vendor of a device.
Revision	Displays the version of a device.
Device Name	Displays the model name of a device.

Item	Explanation
Serial No	Displays the serial number of a device. For a non-disk device (such as GDS), a hyphen [-] is displayed.
Channel/TargetID/ LUN	Displays the SCSI channel, SCSI target ID, and SCSI logical unit number of a device.
Disk Capacity	When the device is a disk, the disk capacity is displayed. Up to 1,023 MB is displayed in MBs, and 1,024 MB and more are displayed in GBs (down to the first decimal place; the second and later decimal places are ignored.) For a non-disk device and GDS, a hyphen [-] is displayed. Because the disk capacity is displayed, assuming that 1 GB = 1,024 MB = 1,024 x 1,024 KB, its value is slightly smaller than the catalog value.

Table 7.13 Buttons in [Fibre Channel] window

Item	Explanation
Status Clear	The [Status Clear] button is displayed only for setting privilege users. To display the [Confirm Settings] dialog box, select the check box of the [Status] item of [PCI Device Information] or [Information about devices connected to controller], and click the [Status Clear] button. To clear the hardware status of a fibre channel or that of a device connected to the fibre channel, click the [OK] button in the [Confirm Settings] dialog box. When mail/REMCS/SNMPtrap notification is suppressed by a notification suppression function, notification suppression is also canceled.
Select All	The [Select All] button is displayed only for setting privilege users. Click the [Select All] button to select all check boxes.
Release All	The [Release All] button is displayed only for setting privilege users. Click the [Release All] button to release all check boxes.
Return	Click the [Return] button to return to the [PCI Devices] window.

(1) Menu operation

[System] → [PSA] → [PCI Devices] → [Unit]

(2) Window operation

- Clearing the hardware status of fibre channel

  1 Select the check box of the [Status] item of [PCI Device Information] (see Remark 1 below) and click the [Status Clear] button.
  The [Confirm Settings] dialog box is then displayed.

  2 Click the [OK] button in the [Confirm Settings] dialog box.
  The hardware status of the fibre channel is then cleared.

  3 Click the [Return] button.
  The [PCI Devices] window is then displayed.

- Clearing the hardware status of a device connected to fibre channel

  1 Select the check box of the [Status] item of [Information about devices connected to controller] (see Remark 1 below) and click the [Status Clear] button.
  The [Confirm Settings] dialog box is then displayed.

  2 Click the [OK] button in the [Confirm Settings] dialog box.
  The hardware status of the device connected to the fibre channel is then cleared.

  3 Click the [Return] button.
  The [PCI Devices] window is then displayed.

- Not clearing the status of fibre channel

  1 Click the [Return] button.
  The [PCI Devices] window is then displayed.

Remarks:

- Click the [Select All] button to select all check boxes. Click the [Release All] button to release all check boxes.
- Up to 500 statuses can be cleared at a time. If the [Status Clear] button is clicked with more than 500 statuses selected, only the first 500 statuses are cleared, along with a dialog box displayed to that effect.

(3) Error messages

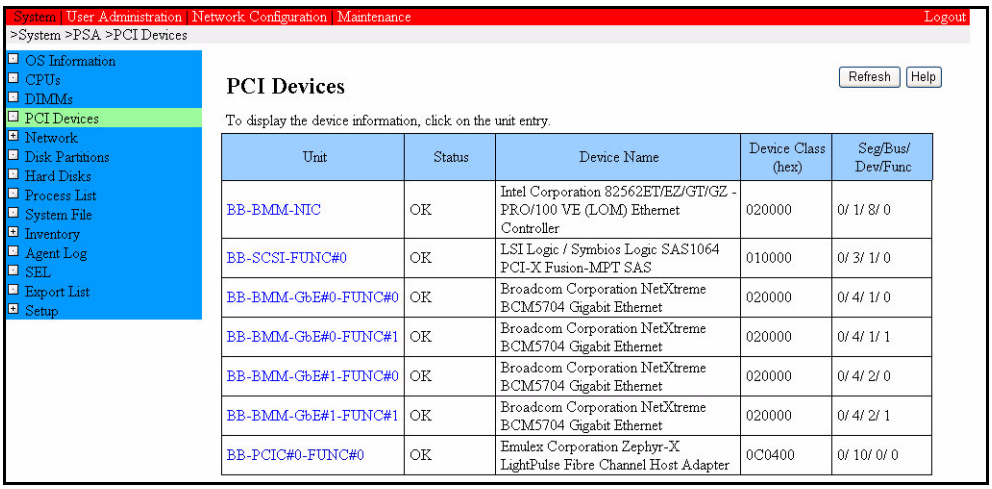
If an ABEND occurs, the following message is displayed in a dialog box:

Message	Meaning	Response
Error: Status Clear Error : ErrorCode=****	Status Clear failed. [ErrorCode] 3309: PCI Status Clear error 3310: SMART Status Clear error 3311: SCSI Status Clear error	If the problem cannot be resolved by refreshing the window and operating it again, contact the system administrator or a Fujitsu-certified service engineer.

7.5.4 [PCI Device] window

For a [Device Class] item in the [PCI Devices] window other than "020000" (Ethernet controller), "010000" (SCSI storage controller), and "0C0400" (Fibre Channel), the [PCI Device] window displays PCI device information.

A setting privilege user can clear the status by clicking the [Status Clear] button.



Unit	Status	Device Name	Device Class (hex)	Seg/Bus/ Dev/Func
BB-BMM-NIC	OK	Intel Corporation 82562ET/EZ/GT/GZ - PRO/100 VE (LOM) Ethernet Controller	020000	0/ 1/ 8/ 0
BB-SCSI-FUNC#0	OK	LSI Logic / Symbios Logic SAS1064 PCI-X Fusion-MPT SAS	010000	0/ 3/ 1/ 0
BB-BMM-GbE#0-FUNC#0	OK	Broadcom Corporation NetXtreme BCM5704 Gigabit Ethernet	020000	0/ 4/ 1/ 0
BB-BMM-GbE#0-FUNC#1	OK	Broadcom Corporation NetXtreme BCM5704 Gigabit Ethernet	020000	0/ 4/ 1/ 1
BB-BMM-GbE#1-FUNC#0	OK	Broadcom Corporation NetXtreme BCM5704 Gigabit Ethernet	020000	0/ 4/ 2/ 0
BB-BMM-GbE#1-FUNC#1	OK	Broadcom Corporation NetXtreme BCM5704 Gigabit Ethernet	020000	0/ 4/ 2/ 1
BB-PCIC#0-FUNC#0	OK	Emulex Corporation Zephyr-X LightPulse Fibre Channel Host Adapter	0C0400	0/ 10/ 0/ 0

Figure 7.9 [PCI Device] window

Table 7.14 Displayed and setting items in the [PCI Device] window

Item	Description
PCI Device Information	
Unit	PCI device identification name
Status	PCI device status • OK: Operating normally • Error: Serious problem such as a hardware failure • Warning: Warning status (A problem may occur.) • Unknown: Unknown Check the [Error] or [Warning] status check box to clear the status. Additional note: Check the check box and click the [Status Clear] button to clear the status.
Device Name	Device name that combines a vendor name and device name
Device Class	Device class ID (in hexadecimal)
Seg/Bus/Dev/Func	The following numbers: • Segment number • Bus number • Device number • Function number
Vendor ID	Vendor ID (in hexadecimal)

Item	Description
Device ID	Device ID (in hexadecimal)
PCI Device Version	PCI device version number (in hexadecimal)

Table 7.15 Buttons in the [PCI Device] window

Button	Description
Status Clear	The [Status Clear] button is displayed only for the setting privilege user. Check the [Status] check box in [PCI Device Information] and click the [Status Clear] button. The [Confirm Settings] dialog box opens. Click the [OK] button in the [Confirm Settings] dialog box to clear the PCI device status. If the notification suppression function is active to suppress mail/REMCS/SNMPtrap notification, this button deactivates the notification suppression function.
Return	Click the [Return] button to return to the [PCI Devices] window.

(1) Menu operation

[System] → [PSA] → [PCI Devices] → [Unit]

(2) GUI operation

- Clearing the PCI device status
  1. Check the [Status] check box and click the [Status Clear] button.
     The [Confirm Settings] dialog box opens.
  2. Click the [OK] button in the [Confirm Settings] dialog box.
     The PCI device status is cleared.
  3. Click the [Return] button.
     The [PCI Devices] window is displayed again.
- Not clearing the PCI device status
  1. Click the [Return] button.
     The [PCI Devices] window is displayed again.

(3) Error message

If the system ends abnormally, the following message is displayed in a dialog box.

Message	Meaning	Response
Error: Status Clear Error : ErrorCode=****	Status clearing failed. [ErrorCode] 3309: PCI Status Clear	If using Refresh and then repeating the operation in the window results in the same problem, contact the system administrator or a Fujitsu certified service engineer.

7.6 Network Menu

The [Network] menu displays the network status and routing status.

This menu has the following windows:

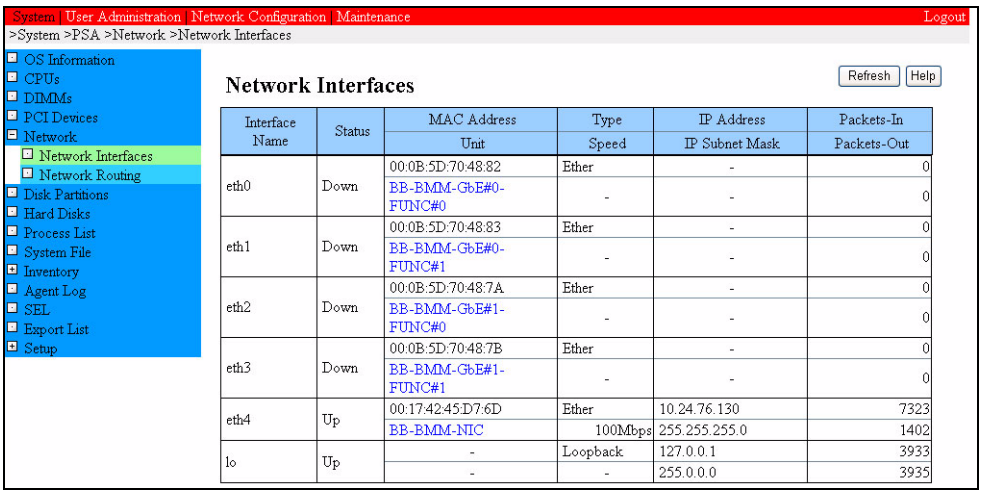
- [Network Interfaces] window
- [Network Routings] window

This section describes these windows and operations in them.

7.6.1 [Network Interfaces] window

The [Network Interfaces] window displays the network status.

Network-related information may not be supplied depending on the type or status of the OS or a driver. A hyphen "-" is displayed for any of this information that is not supplied.



Interface Name	Status	MAC Address / Unit	Type / Speed	IP Address / IP Subnet Mask	Packets-In / Packets-Out
eth0	Down	00:0B:5D:70:48:82	Ether	-	0
		BB-BMM-GbE#0-FUNC#0	-	-	0
eth1	Down	00:0B:5D:70:48:83	Ether	-	0
		BB-BMM-GbE#0-FUNC#1	-	-	0
eth2	Down	00:0B:5D:70:48:7A	Ether	-	0
		BB-BMM-GbE#1-FUNC#0	-	-	0
eth3	Down	00:0B:5D:70:48:7B	Ether	-	0
		BB-BMM-GbE#1-FUNC#1	-	-	0
eth4	Up	00:17:42:45:D7:6D	Ether	10.24.76.130	7323
		BB-BMM-NIC	100Mbps	255.255.255.0	1402
lo	Up	-	Loopback	127.0.0.1	3933
		-	-	255.0.0.0	3935

Figure 7.10 [Network Interfaces] window

The [Unit] item displays PCI device identification names for interfaces. Click the [Unit] item to display a detail window.

When the number of PCI cards is increased or decreased, it takes up to three minutes until the change is reflected in the window display.

Table 7.16 Displayed items in the [Network Interfaces] window

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Interface Name</td><td>Interface name</td></tr>
<tr><td>Status</td><td>LAN card and link status
<table>
<tr><th>Card status</th><th>Link status</th><th>Display</th></tr>
<tr><td>Up</td><td>Up</td><td>Up</td></tr>
<tr><td>Up</td><td>Down</td><td>Link Down</td></tr>
<tr><td>Up</td><td>Unknown</td><td>-</td></tr>
<tr><td>Down</td><td>Up</td><td>Down</td></tr>
<tr><td>Down</td><td>Down</td><td>Down</td></tr>
<tr><td>Down</td><td>Unknown</td><td>Down</td></tr>
</table>
• Up: Active
• Down: Not active
• Link Down: Link failure state
* The latest information is retrieved when this window is displayed.</td></tr>
<tr><td>Speed</td><td>Preset value of the transmission speed in megabits per second.
* The latest information is retrieved when this window is displayed.</td></tr>
<tr><td>Unit</td><td>Displays PCI device identification names for interfaces.</td></tr>
<tr><td>Type</td><td>Network type (high-level protocol type handled by the ARP protocol):
• Ether: Ethernet
• Loopback: Loopback (loopback interface)
• Unknown: Unknown</td></tr>
<tr><td>MAC Address</td><td>Physical address.</td></tr>
<tr><td>IP Address</td><td>IP address</td></tr>
<tr><td>IP Subnet Mask</td><td>Subnet mask</td></tr>
<tr><td>Packets-In</td><td>Number of IP packets received by an interface.
* The latest information is retrieved when this window is displayed.</td></tr>
<tr><td>Packets-Out</td><td>Number of IP packets transmitted by an interface.
* The latest information is retrieved when this window is displayed.</td></tr>
</table>

(1) Menu operation

[System] → [PSA] → [Network] → [Network Interfaces]

(2) GUI operation

None

7.6.2 [Network Routing] window

The [Network Routing] window displays the routing status.

Note: This window is only supported when the OS is Linux.

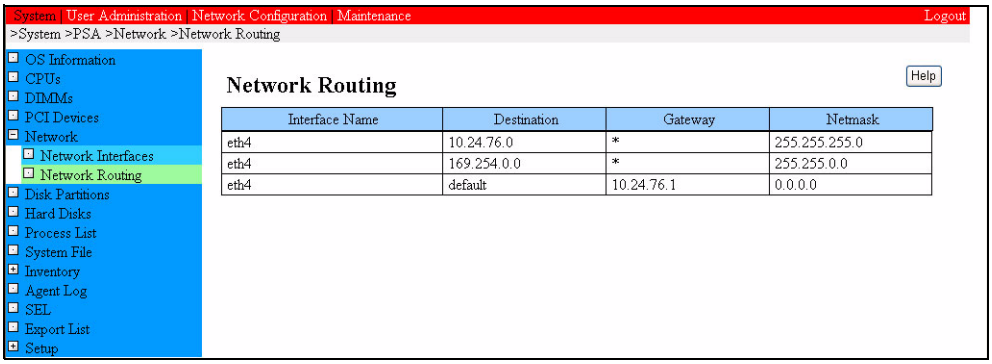


Figure 7.11 [Network Routing] window

Table 7.17 Displayed items in the [Network Routing] window

Item	Description
Interface Name	Interface name
Destination	Transmission destination
Gateway	Gateway. If there is no gateway, an asterisk [*] is displayed.
Netmask	Net mask

(1) Menu operation

[System] → [PSA] → [Network] → [Network Routing]

(2) GUI operation

None

7.7 [Disk Partitions] Window

The [Disk Partitions] window displays disk partition information.

Note:

- This window is only supported when the OS is Linux.
- These fields display the information collected at the time of PSA boot.

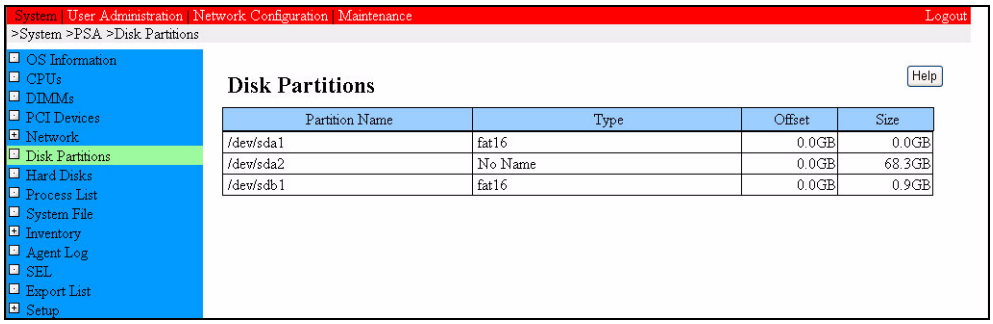


Figure 7.12 [Disk Partitions] window

Table 7.18 Displayed items in the [Disk Partitions] window

Item	Description
Partition Name	Disk partition name
Type	Disk partition type If no type is set, "No Name" is displayed. Example: The disk has been partitioned, but the partitions have not been formatted.
Offset	Disk partition offset value
Size	Disk partition size

(1) Menu operation

[System] → [PSA] → [Disk Partitions]

(2) GUI operation

None

7.8 [Hard Disks] Window

The [Hard Disks] window lists the DISK information.

When the number of DISKs is increased or decreased, it takes up to three minutes until the change is reflected in the window display.

Notes:

- In the ETERNUS multi-path environment in Linux, only the DISK (with the smallest bus number if there are two or more DISKs,) on one side with a multi-path specified is displayed. In Windows, a DISK with a multi-path specified is not displayed.
- If a disk under GDS/PSDM control is added or removed during OS operation, the values displayed for [Disk Capacity] are not updated. To update them, PSA must be restarted or the following PSA command must be executed (the following command is supported only in the Linux version of PSA):

```
/opt/FJSVpsa/sh/force_search.sh -a
```

- When the Power Path of an EMC is used, a DISK may not be displayed.

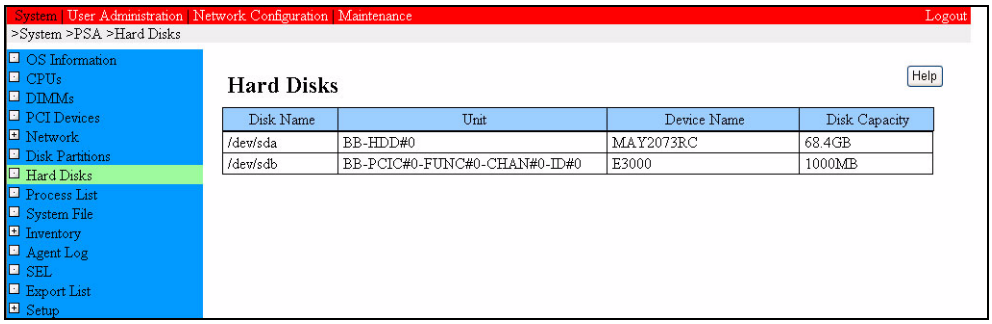


Figure 7.13 [Hard Disks] window

Table 7.19 Display items of [Hard Disks] window

Item	Description
Disk Name	Displays the name of a disk.
Unit	Displays a disk identification name.
Device Name	Displays the model name of a DISK.
Disk Capacity	Displays disk capacity. Up to 1,023 MB is displayed in MBs, and 1,024 MB and more are displayed in GBs (down to the first decimal place; the second and later decimal places are ignored.) For a GDS or PSDM, a hyphen [-] is displayed. Because the disk capacity is displayed, assuming that 1 GB = 1,024 MB = 1,024 x 1,024 KB, its value is slightly smaller than the catalog value.

(1) Menu operation

[System] → [PSA] → [Hard Disks]

(2) Window operation

None

7.9 [Process List] Window

The user can use the [Process List] window to monitor the current process information. For example, the user can watch the CPU usage time by process and thus easily check whether application processes are operating normally. If an unnecessary process is detected, a specific signal to the process can be sent.

Note: This window is only supported when the OS is Linux.

The [Process List] window has the following functions, required for process monitoring:

1 Displaying process list
2 Manual/Automatic updating of process list
3 Sorting process list
4 Transmitting a signal to the specified process

Remarks: The Administrator/Operator/User privilege can select these functions. However, the signal transmission function is not available to users with the User privilege. These functions are hidden on the menu and not available to users with the CE privilege.

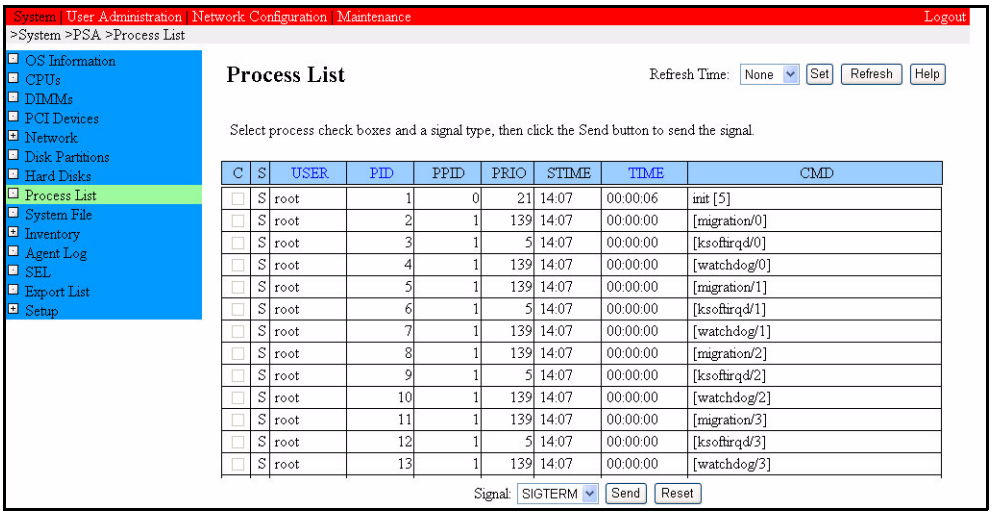


Figure 7.14 [Process List] window

Table 7.20 Displayed and setting items in the [Process List] window

Item	Description
Refresh Time	Screen update time. The user can select one of the following options: • None: No updating • 5sec: 5 seconds • 10sec: 10 seconds • 30sec: 30 seconds • 60sec: 60 seconds The default setting is [None].
C	Check boxes for the signal transmission function (more than one can be checked). The init process and [ ] process cannot be selected. Users with the User privilege can not select any of the check boxes.
S	Process status: • D: Sleep status where no interrupt is permitted • R: Executable • S: Sleep status • T: Trace in progress or stopped • Z: Zombie process (no longer exists)
USER	Process user name
PID	Process ID
PPID	Parent process ID
PRIO	Priority
STIME	Process start time: • Less than 24 hours: Process start time (Example: 14:20) • 24 hours or more: Process start date (Example: Mar04)
TIME	Cumulative CPU usage time
CMD	Command name
Signal	Signals that can be transmitted. The user can select one of the following values: • SIGTERM • SIGHUP • SIGKILL • SIGINT • SIGQUIT The default setting is [SIGTERM]. The [Signal] pulldown list is available only to the Administrator/ Operator privilege.

Table 7.21 Buttons in the [Process List] window

Button	Description
Set	Click the [set] button to set the automatic screen update time to the value selected from the [Refresh Time] pulldown list.
Refresh	Click the [Refresh] button to manually reload process list.
USER	Click [USER] to sort the process list in ascending order by user name.
PID	Click [PID] to sort the process list in ascending order by process ID.
TIME	Click [TIME] to sort the process list in descending order of cumulative CPU usage time.
Send	Check the check box of a process, select the signal, click the [Send] button, and the confirmation dialog box opens. Click the [OK] button in the confirmation dialog box, and the selected signal is transmitted to the specified process. The [Send] button is available only to the Administrator/Operator privilege.
Reset	Click the [Reset] button, and the checked check boxes are reset to the unchecked state. The [Reset] button is available only to users with the Administrator/Operator privilege.

(1) Menu operation

[System] → [PSA] → [Process List]

(2) GUI operation

- Updating process list
  - Select the update time from the [Refresh Time] pulldown list, and click the [Set] button.
    The selected update time is set, and the process list is automatically updated and redisplayed.
  - Click the [Refresh] button.
    The process list is manually updated and redisplayed.
- Sorting process list

  1 Click one of the [USER]/[PID]/[TIME] buttons in the process list information.
    The process list has been sorted with one of [User], [PID], or [TIME] used as the keyword.

- Transmitting a signal to the specified process

  1. To transmit a signal to a process, check the check box of the process, select the signal from the [Signal] pulldown list, and click the [Send] button.
     The confirmation dialog box opens.
  2. Click [OK] in the confirmation dialog box.
     The specified signal is transmitted to the specified process, and the process list after transmission is displayed.

7.10 [System File] (Selection) Window

The [System File] (selection) window displays the names of specific system files. The system administrator can use this function to select necessary system files and display them to facilitate the administration work.

Note: This window is only supported when the OS is Linux.

The [System File] window has the following functions:

1 Selecting system files
2 Displaying system files (the following system files can be displayed):
- /etc/hosts
- /etc/nsswitch.conf
- /etc/inittab
- /etc/fstab
- /etc/exports

These functions are available on the menu to the Administrator/Operator/User privilege.

The functions are hidden and not available on the menu to the CE privilege.

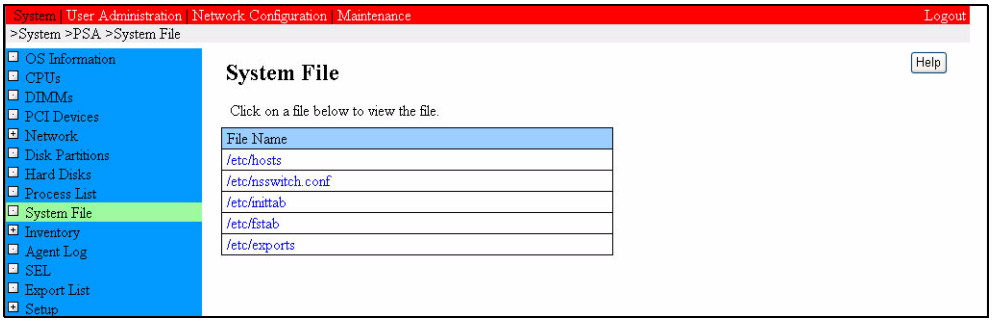


Figure 7.15 [System File] (selection) window

Table 7.22 Displayed item in the [System File] (selection) window

Item	Description
File Name	Names of system files, as follows: • /etc/hosts • /etc/nsswitch.conf • /etc/inittab • /etc/fstab • /etc/exports

Table 7.23 Buttons in the [System File] (selection) window

Button	Description
System file name	Click the box containing a file name to display the contents of the file.

(1) Menu operation

[System] → [PSA] → [System File]

(2) GUI operation

1 Click a system file.
The contents of the system file are displayed in the [System File] (display) window.

Additional note: If the selected system file cannot be displayed, an error message is displayed in the following format:

Table 7.24 Error messages

Error message	Cause
No such file	The specified file does not exist.
No absolute path	The file is specified with a relative path.
Read permission denied	When a user with User privilege uses this function, read permission to the system files listed in Table 7.26 is not given to "other users."
File size over	The specified file is larger than 2 MB.

An error message is displayed in the window as shown below.

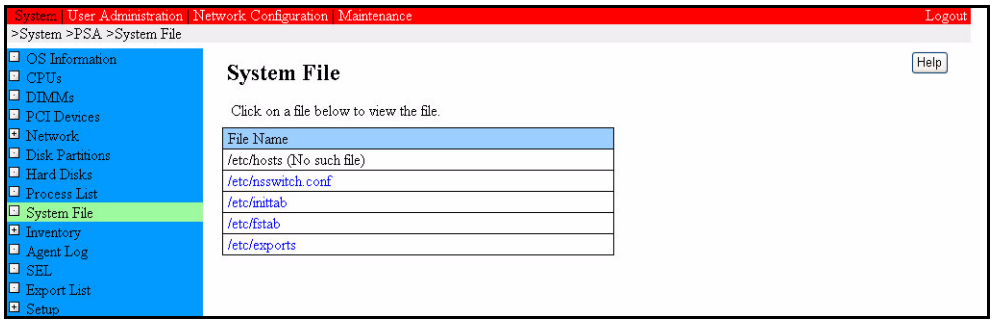


Figure 7.16 [System File] (selection) Error window

7.10.1 [System File] (display) window

The [System File] (display) window displays the contents of the system file selected in the [System File] (selection) window.

This function is available on the menu to the Administrator/Operator/User privilege.

The function is hidden and not available on the menu to the CE privilege.

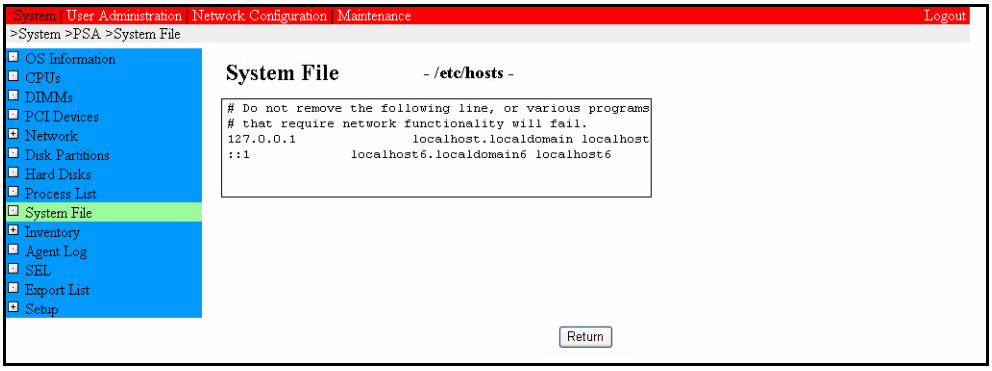


Figure 7.17 [System File] (display) window

This window is displayed when the system file [/etc/hosts] is selected in the [System File] (selection) window.

Table 7.25 Button in the [System File] (display) window

Item	Description
Return	Click the [Return] button to return to the [System File] (selection) window.

(1) Menu operation

[System] → [PSA] → [System File] → [file_name]

(2) GUI operation

1 Click the [Return] button.
The [System File] (selection) window is displayed again.

7.11 Inventory Menu

The [Inventory] menu displays inventories of the hardware and software.

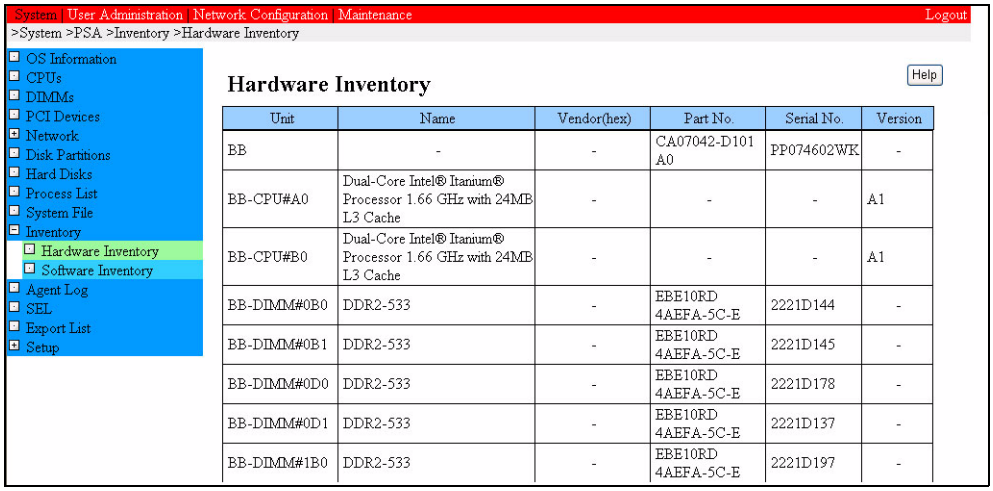
This menu has the following windows:

- [Hardware Inventory] window
- [Software Inventory] window

This section describes these windows and operations in them.

7.11.1 [Hardware Inventory] window

The [Hardware Inventory] window displays an inventory of hardware (BB, CPU, DIMM, PCI devices, and expansion file unit (SDU)).



Unit	Name	Vendor(hex)	Part No.	Serial No.	Version
BB	-	-	CA07042-D101 A0	PP074602WK	-
BB-CPU#A0	Dual-Core Intel® Itanium® Processor 1.66 GHz with 24MB L3 Cache	-	-	-	A1
BB-CPU#B0	Dual-Core Intel® Itanium® Processor 1.66 GHz with 24MB L3 Cache	-	-	-	A1
BB-DIMM#0B0	DDR2-533	-	EBE10RD 4AEFA-5C-E	2221D144	-
BB-DIMM#0B1	DDR2-533	-	EBE10RD 4AEFA-5C-E	2221D145	-
BB-DIMM#0D0	DDR2-533	-	EBE10RD 4AEFA-5C-E	2221D178	-
BB-DIMM#0D1	DDR2-533	-	EBE10RD 4AEFA-5C-E	2221D137	-
BB-DIMM#1B0	DDR2-533	-	EBE10RD 4AEFA-5C-E	2221D197	-

Figure 7.18 [Hardware Inventory] window

Table 7.26 Displayed items in the [Hardware Inventory] window

Item	Description
Unit	Identification name.
Name	Name
Vendor	Vendor ID or vendor name
PartNo.	Part number
SerialNo.	Serial number
Version	Version number

The following table describes what is displayed for devices in the columns of the above items. "-" indicates a column that is always displayed for the device.

	BB	CPU	DIMM	PCI device	SDU
Unit	Identification name	Identification name	Identification name	Identification name	Identification name
Name	–	CPU model	Type	Device name	–
Vendor	–	–	–	Vendor ID	–
PartNo.	Part number	–	Part number	–	–
SerialNo.	Serial number	–	Serial number	–	–
Version	–	Stepping	–	Version number	Unit version

(1) Menu operation

[System] → [PSA] → [Inventory] → [Hardware Inventory]

(2) GUI operation

None

7.11.2 [Software Inventory] window

The user can use the [Software Inventory] window, at the time of a failure, to obtain installation package information, which can be used as troubleshooting data.

Note: This window is only supported when the OS is Linux.

The [Software Inventory] window provides the following functions.

1 Displaying RPM packages list and the OS version
2 Displaying details on an RPM package
3 Downloading RPM package list information

A file that stores RPM package list information is named [rpmlist.csv] by default.

The downloaded information is saved in the format shown below. For details on these items, see Table 7.34, "Buttons in the [Agent Log Filtering Condition] window."

```
[Name], [Version], [Release], [Architecture], [Vendor],
[Build Date], [Install Date], [Group], [Source RPM], [Size],
[License], [Packager], [URL], [Summary], [Description]
```

These functions are available to users with any user privilege.

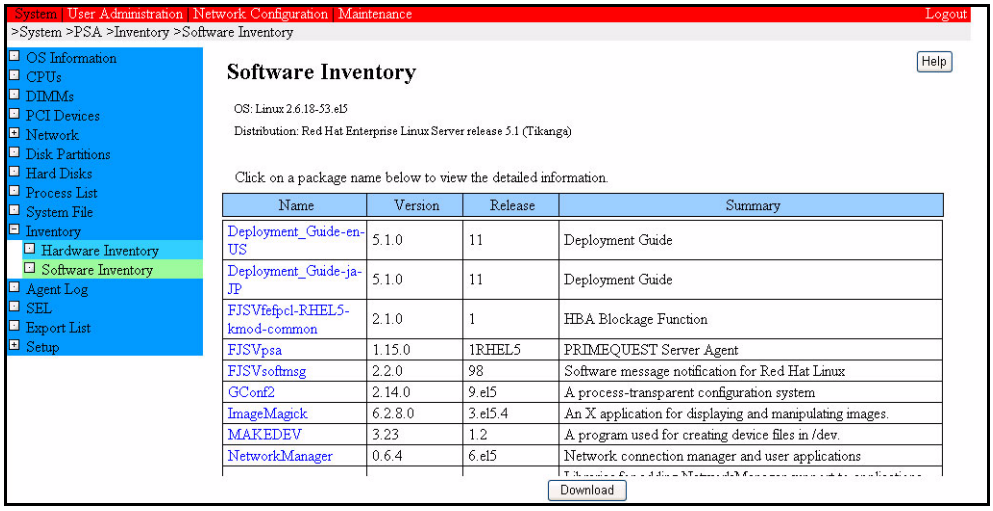


Figure 7.19 [Software Inventory] window

Remarks: If packages having the same RPM package name, but different CPU architectures are installed, the same RPM package name will be displayed multiple times in the name column.

Table 7.27 Displayed items in the [Software Inventory] window

- OS information

Item	Description
OS	OS name and kernel version
Distribution	Distribution name

- RPM package lists

Item	Description
Name	RPM package name
Version	RPM package version
Release	Release information
Summary	Summary information

Table 7.28 Buttons in the [Software Inventory] window

Button	Description
RPM package name	Click an RPM package name to display the [Software Inventory -Detail-] window.
Download	Click the [Download] button to download RPM package list information in CSV format.

(1) Menu operation

[System] → [PSA] → [Inventory] → [Software Inventory]

(2) GUI operation

- Displaying detailed package

1. Click an RPM package name.
   The [Software Inventory -Detail-] window is displayed.
2. Click the [Return] button in the [Software Inventory -Detail-] window.
   The [Software Inventory] window is displayed again.

- Downloading package list information

1. Click the [Download] button.
   The [Download File] dialog box opens.
2. Click the [Save] button in the [Download File] dialog box.
   The [Save As] dialog box opens.
3. In the [Save As] dialog box, specify a file and click the [Save] button.
   The package list is saved in the specified file in CSV format.

7.11.2.1 [Software Inventory -Detail-] window

The [Software Inventory -Detail-] window displays details on an RPM package.

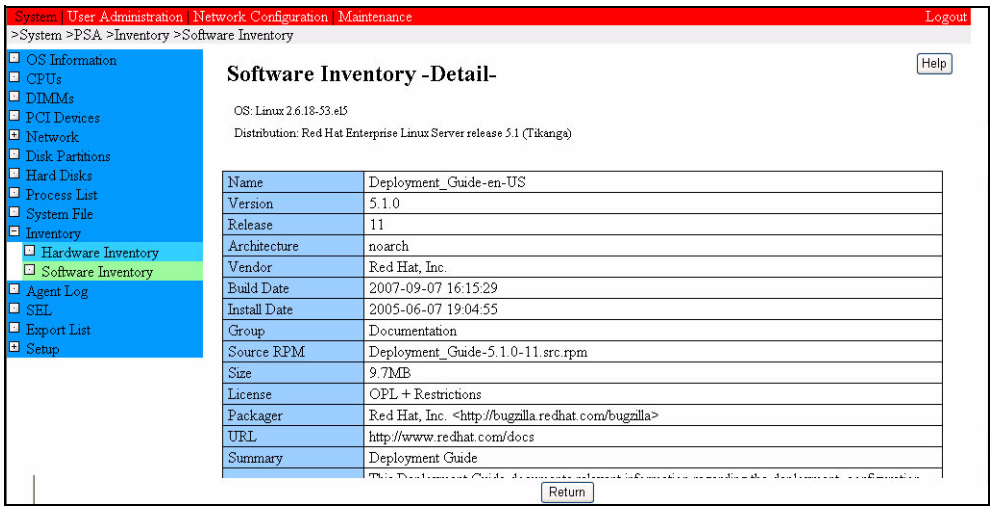


Figure 7.20 [Software Inventory -Detail-] window

Remarks: If the system includes RPM packages that correspond to multiple CPU architectures, the window displays detailed information on each of the CPU architectures.

Table 7.29 Displayed items in the [Software Inventory -Detail-] window

- OS information

Item	Description
OS	OS name and kernel version number
Distribution	Distribution name

- RPM package detail

Item	Description
Name	RPM package name
Version	RPM package version number
Release	Release information
Architecture	Indicates the CPU architecture.
Vendor	Vendor information
Build Date	Build date and time, as follows: yyyy-MM-dd HH:mm:ss
Install Date	Installation date and time, as follows: yyyy-MM-dd HH:mm:ss
Group	Group
Source RPM	Source RPM information
Size	Size in bytes, kilobytes, megabytes, or gigabytes (calculated to the first decimal place with the digits in subsequent decimal places omitted).
License	License
Packager	Package creator
URL	URL information
Summary	Summary information
Description	Detailed information

Table 7.30 Button in [Software Inventory -Detail-] window

Button	Description
Return	Click the [Return] button to return to the [Software Inventory] window.

(1) Menu operation

[System] → [PSA] → [Inventory] → [Software Inventory] → RPM package name

(2) GUI operation

1 Click the [Return] button.
The [Software Inventory] window is displayed again.

7.12 [Agent Log] Window

The [Agent Log] window displays an agent log list.

An agent log is a recorded history of PSA actions (Events detected within PSA with IDs from 00000 to 09999 are excluded.) Up to 5,000 agent logs are stored in binary format. When the maximum number of logs is reached, the logs are overwritten, starting from the oldest ones.

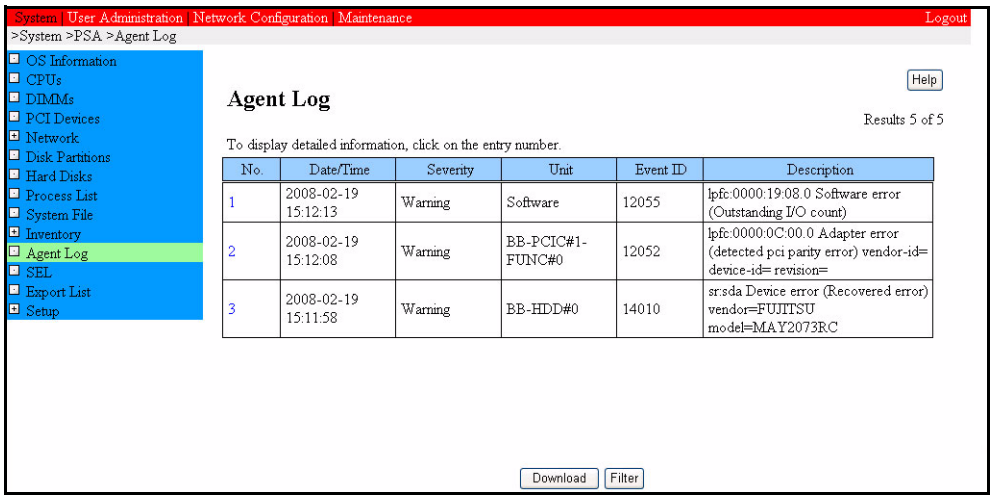


Figure 7.21 [Agent Log] window

On the initial screen, the latest 1,000 messages are displayed in descending order by time. Specify conditions in the [Agent Log Filtering Condition] window, and the messages that match the specified conditions are displayed.

The [Agent Log] window is horizontally split into two frames: the top frame displays a list of messages, and the bottom frame displays details related to the selected message. The bottom frame is blank when the list is initially displayed.

If there is no agent log or none matches the specified conditions, the [Agent Log] window displays the displayed item titles together with a message indicating that no log to be displayed exists.

Additional note: Up to 5000 agent log items can be stored, but one window can display up to 1000. To view the hidden agent log, specify filter conditions.

Note: The window supports ISO-8859-1 for displaying PSA action information. If the displayed window includes any character that is not supported, the [Agent Log] window contents may not be normally displayed. In such cases, specify an appropriate character code for the browser displaying the window.

Table 7.31 Displayed and setting items in the [Agent Log] window

Item	Description
Number of agent log items displayed	Number of displayed agent log items and number of stored agent log items for PSA actions Example: The latest 1,000 items out of 5,000 items are displayed: Results 1000 of 5000
No	Log number. If detailed information is available, this is underlined (linked).
Date/Time	Log time, as follows: yyyy-MM-dd HH:mm:ss
Severity	Severity level: • Error: Serious problem such as a hardware failure • Warning: Warning status (An event that is not serious but will possibly develop into a problem.) • Information: Information (Normal event)
Unit	Identification name of the location. If the unit name is unknown, "Unknown" is displayed. Unknown is displayed when any of the following conditions apply. • There is no information about the fault location in the driver's message. • An error has occurred with a device not being been managed by PSA. • During hot plugging, an abnormality occurred while the OS was recognizing the device, leading to PSA failing to recognize the device, which in turn caused an error occurrence. • During hot plugging, an error occurred during the interval after the OS recognized the device but before PSA could recognize it.
EventID	Event ID
Description	Message
Detailed information area (displayed in the bottom frame)	Details related to the message. Details on the selected log are displayed. If messages contain Japanese character codes, they may be corrupted.

Table 7.32 Buttons in the [Agent Log] window

Button	Description
Each box containing a log number under [No]	If detailed information is available, the number in the [No] column is underlined (linked). Clicking the link displays detailed agent log information in the bottom frame.
Download	Click the [Download] button to download all stored agent logs in CSV file format, regardless of the display conditions.
Filter	Click the [Filter] button to display the [Agent Log Filtering Condition] window, which allows the user to specify message filtering conditions.

(1) Menu operation

[System] → [PSA] → [Agent Log]

(2) GUI operation

- Downloading all agent logs stored by PSA in CSV file format

  1. Click the [Download] button.
     The [Download File] dialog box opens.
  2. Click the [Save] button in the [Download File] dialog box.
     The [Save As] dialog box opens.
  3. In the [Save As] dialog box, specify a file name, specify CSV files (with the extension .csv) as the file type, and click the [Save] button.
     A CSV file is downloaded to the specified location, and the [Download Completed] message box is displayed.
  4. Click the [Close] button in the [Download Completed] message box.
     The [Agent Log] window is displayed again.

- Specifying filtering conditions

  1. Click the [Filter] button.
     The [Agent Log Filtering Condition] window is displayed.
  2. Specify conditions in the [Agent Log Filtering Condition] window, and click the [Apply] button.
     The conditions are set, and the [Agent Log] window is displayed again.

Remarks:

- If at least one Agent Log item has been created, filtering conditions can be specified.

- The specified filtering conditions remain in effect as long as the [Agent Log] window is the active window. However, the conditions are reset when another window becomes the active window or the window is redisplayed from the menu.

7.12.1 [Agent Log Filtering Condition] window

The user can use the [Agent Log Filtering Condition] to specify filtering conditions for displaying a log list in the [Agent Log] window. Each filtering condition item is processed as an AND operand for displaying the list.

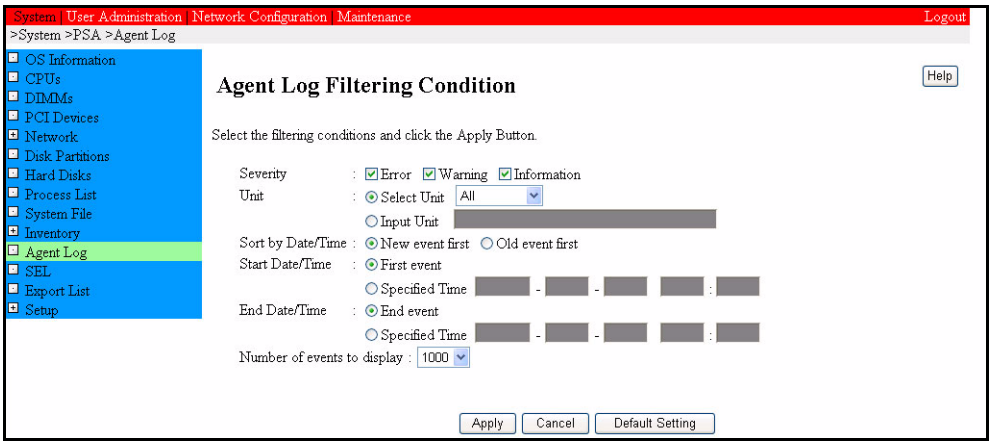


Figure 7.22 [Agent Log Filtering Condition] window

Table 7.33 Displayed and setting items in the [Agent Log Filtering Condition] window

Item	Description
Severity	The user can select an alert level by checking a check box (more than one can be checked): • Error: Serious problem such as a hardware failure • Warning: Event that is not serious but will possibly develop into a problem • Information: Normal event All levels are checked by default.

Item	Description
Unit	The user can click the corresponding radio button to either select a event location from the pulldown list or directly enter a unit name: Select Unit: To select a unit type Input Unit Name: To directly enter a unit name When selecting a event location from the pulldown list (only one item can be selected): • All • BB • CPU • DIMM • PCI_Card • Disk • Software • MMB/BMC * Selects events of MMB and BMC units as well as events that occurred in an MMB or BMC unit. • Network • SDU * This item is displayed when one or more expansion file units are connected. When directly entering a unit name: Characters that can be entered: En-size alphanumeric characters, en-size space, en-size symbols (up to 64 characters). However, this does not include the following symbols: <>%&"\ If only en-size spaces are entered or nothing is entered, the entered string is not valid. Strings are compared in right truncation mode. Example: If BB is specified, all units, including the CPU and DIMM, under control of BB are displayed. The default setting is [All].
Sort by Date/Time	The user can specify the order for displaying events, from new events to old events or vice versa, by clicking a radio button: • New event first • Old event first The default setting is [New event first].
Start Date/Time	The user can select the start time: • First event: Start from the first event • Specified Time: Start from the specified time The year, month, day, hour, and minute of the start time must also be entered when Specified Time is selected. The default setting is [First event].

Item	Description
End Date/Time	The user can select the end time: • End event: End at the last event • Specified Time: End at the specified time The year, month, day, hour, and minute of the end time must also be entered when Specified Time is selected. The default setting is [End event].
Number of events to display	The user can select the maximum number of events displayed in the window from the pulldown list: 100/200/300/400/500/1000 The default setting is 1000.

Table 7.34 Buttons in the [Agent Log Filtering Condition] window

Button	Description
Apply	Click the [Apply] button to display a list of only the messages that match the specified conditions in the [Agent Log] window. If no matching message exists, a message with a title is displayed, stating that there is no log to be displayed.
Cancel	Click the [Cancel] button to return to the previous window with an agent log list.
Default Setting	Click the [Default Setting] button to return the selected values to the default values.

(1) Menu operation

[System] → [PSA] → [Agent Log] → [Filter]

(2) GUI operation

- To display the [Agent Log] window in specified filtering conditions:
  1. Specify conditions, and click the [Apply] button.
     The [Agent Log] window is displayed again. The [Agent Log] window displays a list of only the messages that match the specified conditions. If no matching message exists, a message with a title is displayed, stating that there is no log to be displayed.
- To redisplay the [Agent Log] window
  1. Click the [Cancel] button. The specified selections are canceled and the [Agent Log] window reappears.
- To return the selected values to the default values:
  1. Click the [Default Setting] button. The conditions selected for all parameters are cleared and the parameters revert to their default values.

7.13 [SEL] Window

The [SEL] window allows you to download SEL files (binary format).

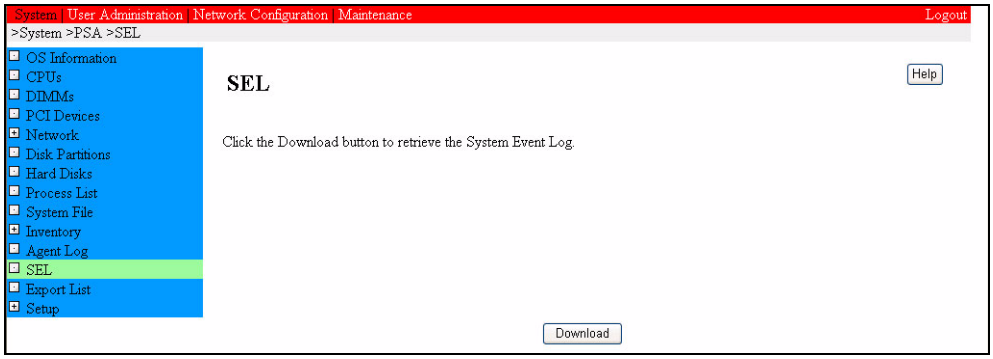


Figure 7.23 [SEL] window

Table 7.35 Buttons in the [SEL] window

Item	Description
Download	Click the [Download] button, and a download confirmation dialog box and a dialog box used to specify the destination file name open in turn. Click the [Save] button in each of these two dialog boxes to download the current SEL log files.

(1) Menu operation

[System] → [PSA] → [SEL]

(2) GUI operation

1 Click the [Download] button.
The [Download File] dialog box opens.

2 Click the [Save] button in the [Download File] dialog box.
The [Save As] dialog box opens.

3 In the [Save As] dialog box, specify a file name (without selecting a file type nor specifying an extension) and click the [Save] button.
The file is downloaded and the [Download Completed] message box is displayed.

4 Click the [Close] button in the [Download Completed] message box.
The [SEL] window is displayed again.

7.14 [Export List] Window

The [Export List] window provides the export function, which allows the user to save snapshots of information stored by PSA to files in CSV format .

Exporting is performed from the [Export] window.

Up to 100 files of export data can be saved. When the number of saved files exceeds 100, the oldest file is deleted and a new file is saved. As long as the number of saved files is less than the maximum number, export data is not deleted unless the user deletes it intentionally. Export data can be downloaded as many times as desired.

Downloaded export data is stored in CSV format, allowing it to be read using an application such as EXCEL.

Be sure to back up the PSA setting information after changing the PSA settings.

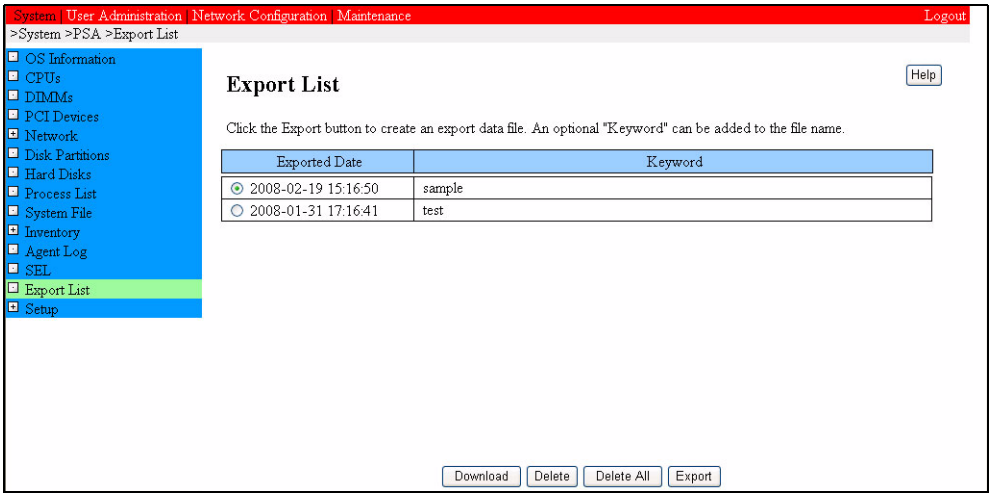


Figure 7.24 [Export List] window

On the initial screen of the [Export List] window, a list of files that have been exported is displayed, starting from the newest one.

Table 7.36 Displayed and setting items in the [Export List] window

Item	Description
Exported Date (Radio Button)	Select the file to be downloaded or deleted, using the appropriate radio button.
Exported Date	The export date and time is displayed. Example: 2004-05-06 08:45:00 * The local time in the system is used.
Keyword	The keyword entered at the export time is displayed.

Table 7.37 Buttons in the [Export List] window

Button	Description
Download	Click the [Download] button to download the selected export file to your terminal, using the download function.
Delete	Click the [Delete] button to delete the selected export file from the management domain.
Delete All	Click the [Delete All] button, and a confirmation dialog box opens. Click the [OK] button in the confirmation dialog box to delete all export files from the management domain.
Export	Click the [Export] button, and the export setting window opens.

(1) Menu operation

[System] → [PSA] → [Export List]

(2) GUI operation

- Saving a snapshot of information stored by PSA to a file in CSV format

  1 Click the [Export] button.
  The [Export] window opens.

  2 In the [Export] window, enter a keyword and click the [Export] button.
  When export is successful, a CSV file is created in the specified directory, and the [Export List] window is displayed again. The [Export List] window displays the latest information.
  If export fails, the [Export Failed Message] dialog box opens.

  3 Click the [OK] button in the [Export Failed Message] dialog box.
  The [Export List] window is displayed again.

- Downloading an export file to your terminal

  1 Select the radio button of the file to be exported (only one can be selected), and click the [Download] button.
  The [Download File] dialog box opens.

2 Click the [Save] button in the [Download File] dialog box.
The [Save As] dialog box opens.

3 In the [Save As] dialog box, specify a file name (with csv as the file type) and click the [Save] button.
A CSV file is downloaded to the specified location, and the [Download Completed] message box is displayed.

4 Click the button in the [Download Completed] message box to close the message box.
The [Export List] window is displayed again. The [Export List] window displays the latest information.

- Deleting export files from the management domain

1 Either click the [Delete All] button or select the radio button of the file to be deleted (only one can be selected), and click the [Delete] button.
The [Confirm Deletion] dialog box opens.

2 Click the [OK] button in the [Confirm Deletion] dialog box.
When the file or all files are successfully deleted, the [Export List] window is displayed again. The [Export List] window displays the latest information.
If deletion fails, the [Deletion Failed] dialog box opens.

3 Click the [OK] button in the [Deletion Failed] dialog box.
The [Export List] window is displayed again.

Note: When an attempt is made to download an export file to the terminal, the following message will be displayed if the file has already been deleted.
E_33005 Communication Error. (01:3378)
In this event, choose [Export List] from the menu again to redisplay the list.

(3) Error messages

If the system ends abnormally, any of the following messages is displayed in a dialog box.

Table 7.38 Error messages

Message	Meaning	Response
Error: Delete File Error : ErrorCode=****	Deleting an exported file failed. 3306: SISP recovery error (one deleted) 3307: SISP recovery error (all deleted)	If repeating the operation in the window results in the same problem, contact the system administrator or a Fujitsu certified service engineer.

7.14.1 [Export] window

The user can use the [Export] window to export files. The user can assign a keyword to the export data. A keyword is optional although it is useful in distinguishing data.

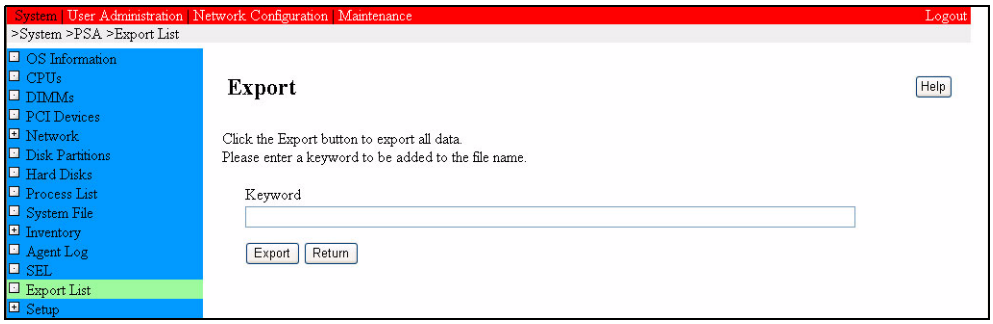


Figure 7.25 [Export] window

Table 7.39 Displayed and setting items in the [Export] window

Item	Description
Keyword	The user can enter a keyword (optional) in the text input field to add the keyword to export data. Up to 50 characters can be entered, including en-size alphanumeric characters, the en-size space character, and en-size symbols. However, this does not include the following symbols: <>%&”,\ This field is left blank to omit a keyword.

Table 7.40 Buttons in the [Export] window

Button	Description
Export	Click the [Export] button to verify the entered keyword, collect information that has been stored by PSA, and create a CSV file in the specified directory. When the file is successfully created, the [Export List] window displays the latest information, with the created file at the top of the list. If export fails, the [Export Failed] dialog box opens. Click the [OK] button, and the [Export List] window displays the latest list.
Return	Click the [Return] button to cancel export processing. The [Export List] window displays the latest list.

(1) Menu operation

[System] → [PSA] → [Export List] → [Export]

(2) GUI operation

1 Enter a keyword, and click the [Export] button.
When a CSV file is successfully created, the [Export List] window is displayed again. The [Export List] window displays the latest list, with the created file at the top of the list.
If export fails, the [Export Failed Message] dialog box opens.

2 If the export operation fails, click the [OK] button in the [Export Failed Message] dialog box.
The [Export List] window is displayed again, and the window displays the latest list.

(3) Error messages

If the system ends abnormally, any of the following messages is displayed in a dialog box.

Table 7.41 Error messages

Message	Meaning	Response
Error: Export Error : ErrorCode=****	Export failed. [ErrorCode] 3308: SISP recovery error	If repeating the operation in the window results in the same problem, contact the system administrator or a Fujitsu certified service engineer.

7.15 Setup Menu

The [Setup] menu has the following windows:

- [Watchdog] window
- [S.M.A.R.T.] window

This section describes these windows and operations in them.

7.15.1 [Watchdog] window

Monitoring with Software Watchdog and monitoring with Boot Watchdog can be set up in the [Watchdog] window.

Only a setting privilege user can change the settings.

The Software Watchdog directs the PSA to restart periodically the Watchdog timer. However, if the PSA cannot restart the Watchdog timer within the specified time due to such system errors as a high OS load and an unreturned response, the MMB executes the specified action.

The Boot Watchdog is a function that executes the specified action unless OS boot is completed within a specified length of time. For the Boot Watchdog, specify options other than the timeout value in the [ASR Control] window of the MMB. The [ASR Control] window also provides a function that disables the Boot Watchdog settings in an emergency. For details about the [ASR Control] window, see Section 5.2.17, "[ASR (Automatic Server Restart) Control] window" in Part III, "MMB."

CAUTION

Malfunction

Before any of the following operations is performed, [Disable] must be set for the Boot Watchdog.

- Booting from a CD-ROM disk
- Booting the system in single-user mode (Linux)
- Booting the system in safe mode (Windows)
- Backing up or restoring data by using SystemcastWizard

If any of the above operations is performed with [Enable] set for the Boot Watchdog, OS restart is attempted repeatedly for the specified number of times. The system then takes the specified action (Stop rebooting and Power Off, Stop rebooting, or Diagnostic interrupt assert). The number of retries of the OS restart and the actions to be taken can be set in the [ASR Control] window for the MMB-UI.

In the [ASR Control] window, check [Cancel Boot Watchdog], and click the [Apply] button. [Disable] can thus be forcibly set for the Boot Watchdog.

For details about the [ASR (Automatic Server Restart) Control] window of MMB, see Section 5.2.17, "[ASR (Automatic Server Restart) Control] window," in Part III, "MMB."

- If 0 is specified for the value of Number-of-Restart-Tries in the [ASR (Automatic Server Restart) Control] window of the MMB, the specified action is not executed even after a lapse of the time at which a timeout should occur. Do not specify 0 for the value when you enable watchdog monitoring.

  For details of the [ASR (Automatic Server Restart) Control] window of the MMB, see Section 5.2.17, "[ASR (Automatic Server Restart) Control] window" in Part III, "MMB."

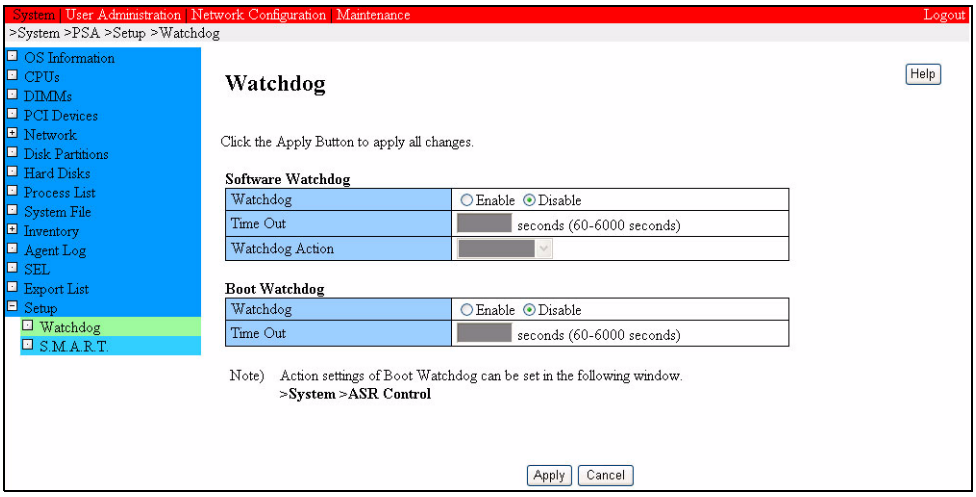


Figure 7.26 [Watchdog] window

Table 7.42 Displayed and settings items in the [Watchdog] window

Item	Description
Software Watchdog	
Watchdog	The user can enable or disable SoftWare Watchdog monitoring: • Disable: Disable monitoring • Enable: Enable monitoring The default setting is [Disable].
TimeOut	The user can specify a timeout value in seconds, which is used while the SoftWare Watchdog monitoring is enabled: Range: 60 to 6000 seconds This item can be specified only if [Enable] is selected. The default setting is 3600 seconds.
Watchdog Action	The user can select from a pulldown list the action to be executed after a timeout: • No Action: Execute no action. Except SEL output. • Reset: Reset the system • Power Off: Power off the system forcibly without the normal OS termination process (shutdown) • Power Cycle: Forcibly power off the system and power it on again • INIT: Issue an INIT interrupt to the system You can only specify this item when you select [Enable]. The default is [No Action].
Boot Watchdog	
Watchdog	The user can enable or disable Boot Watchdog monitoring: • Disable: Disable monitoring • Enable: Enable monitoring The default setting is [Disable]. Note: Before any of the following operations is performed, [Disable] must be set for the Boot Watchdog. • Booting from a CD-ROM disk • Booting the system in single-user mode (Linux) • Booting the system in safe mode (Windows) • Backing up or restoring data by using SystemcastWizard

Item	Description
TimeOut	The user can specify a timeout value in seconds, which is used while Boot Watchdog monitoring is enabled: Range: 60 to 6000 seconds Note: Determine the value based on the duration from when the system power is turned on and [System Progress] in the [Power Control] window of the MMB changes to [Boot] to when it changes to [OS Running]. Fujitsu recommends setting a value that is at least twice this elapsed time in order to prevent mistaken detection. Also, consider the time taken to save a dump in the event of an OS panic. You can only specify this item if you select [Enable]. The default value is 0 seconds. Note that you always need to change the default value.

Table 7.43 Buttons in the [Watchdog] window

Button	Description
Apply	Click the [Apply] button to set the values entered for Watchdog monitoring. Clicking this button validates the settings for both Software Watchdog and Boot Watchdog.
Cancel	Click the [Cancel] button to clear the entered values and revert to the original settings.

(1) Menu operation

[System] → [PSA] → [Setup] → [Watchdog]

(2) GUI operation

- Setting up Watchdog monitoring (when correct values are entered)

1. Select and enter values for the Watchdog monitoring settings, and click the [Apply] button.
   If the entered values are correct, the [Confirm Settings] dialog box opens.
2. Click the [OK] button in the [Confirm Settings] dialog box.
   The Watchdog monitoring settings are set.
   When setup is successfully completed, the [Watchdog] window is displayed again.
   If setup terminates abnormally, the [Abnormal Settings Report] dialog box opens.
3. Click the [OK] button in the [Abnormal Settings Report] dialog box.
   The [Watchdog] window is displayed again.

- Setting up Watchdog monitoring (when incorrect values are entered)

  1 Select and enter values for the Watchdog monitoring settings, and click the [Apply] button.
  If the entered values are incorrect, the [Input Value Error] dialog box opens.

  2 Click the [OK] button in the [Input Value Error] dialog box.
  The [Watchdog] window is displayed again.

(3) Error messages

If the system ends abnormally, any of the following messages is displayed in a dialog box.

Table 7.44 Error messages

Message	Meaning	Response
Error: Software WatchDog Set Error : ErrorCode=****	Making a setting for the Software Watchdog failed. [ErrorCode] 3300: Resource shortage 3301: SNMPSET error	If repeating the operation in the window results in the same problem, contact the system administrator or a Fujitsu certified service engineer.
Error: Boot WatchDog Set Error : ErrorCode=****	Making a setting for the Software Watchdog was successful but making a setting for the Boot Watchdog failed. [ErrorCode] 3300: Resource shortage 3301: SNMPSET error	If repeating the operation in the window results in the same problem, contact the system administrator or a Fujitsu certified service engineer.

7.15.2 [S.M.A.R.T.] window

The hard disk has a S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) function for predictive monitoring.

The [S.M.A.R.T.] windows allows you to specify whether to perform S.M.A.R.T. monitoring for HDDs in order to detect warning signs of impending failures. This setting can only be changed by users who have been granted the setting privilege.

The setting is implemented for all disks at the same time.

The target disks are as follows:

- Internal disks (except disks that do not support S.M.A.R.T. monitoring)
- External disks (except RAID units and disks that do not support S.M.A.R.T. monitoring)

Information to be monitored and processing to be performed by S.M.A.R.T

- Information to be monitored
  S.M.A.R.T. performs predictive monitoring for the information types below and reports when the threshold defined for each of them in S.M.A.R.T. is exceeded. The threshold for each item depends on the type of disk of each vendor.
  - Temperature
  - Read error rate
  - Write error rate
  - Seek error rate
  - Spin-up time
  - Number of remaining alternate sectors

  Setting monitoring polls S.M.A.R.T. on each disk periodically (about every six hours) to check whether a predictive signs of failure have been detected.

- Processing performed at detection of a predictive sign of error
  - Blinks the Fault LED on the relevant disk by repeating a cycle of "four quick blinks + pause"
  - Outputs information posted from S.M.A.R.T. to SYSLOG and reports it (REMCS/e-mail)

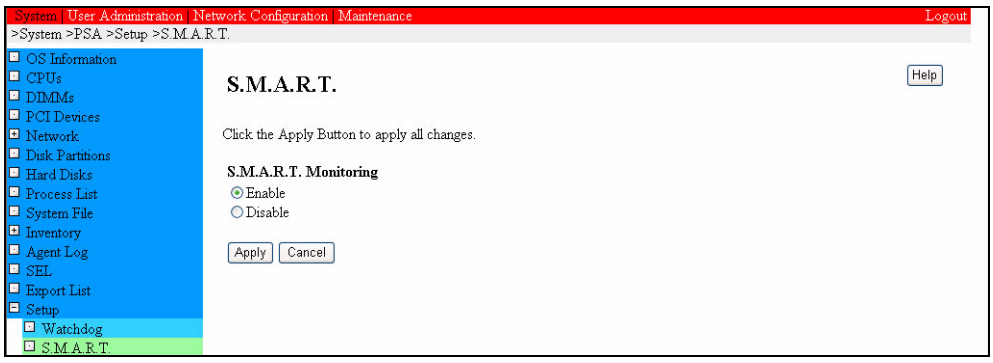


Figure 7.27 [S.M.A.R.T.] window

Table 7.45 Displayed and settings items in the [S.M.A.R.T.] window

Item	Description
S.M.A.R.T. Monitoring	Specify whether to perform S.M.A.R.T. monitoring. • Enable: Enable monitoring • Disable: Disable monitoring The default setting at the time of shipment is [Enable]. Only a setting privilege user can specify this setting. A read privilege user can view the selected setting but cannot specify the setting.

Table 7.46 Buttons in the [S.M.A.R.T.] window

Button	Description
Apply	Click the [Apply] button to set the selected S.M.A.R.T. monitoring setting. If either of the radio buttons is selected, the [Confirm Settings] dialog box opens. When the [OK] button in the [Confirm Settings] dialog box is clicked, the selected S.M.A.R.T. monitoring setting is actually set, and the [S.M.A.R.T.] window is displayed with the setting reflected.
Cancel	Click the [Cancel] button to revert to the original setting.

(1) Menu operation

[System] → [PSA] → [Setup] → [S.M.A.R.T.]

(2) GUI operation

1 Select a S.M.A.R.T. monitoring setting by selecting a radio button, and click the [Apply] button.
If input is correct, the [Confirm Settings] dialog box opens.

2 Click the [OK] button in the [Confirm Settings] dialog box.
The S.M.A.R.T. monitoring setting is set.
When setup is successfully completed, the [S.M.A.R.T.] window is displayed again.
If setup terminates abnormally, the [Abnormal Settings Report] dialog box opens.

3 Click the [OK] button in the [Abnormal Settings Report] dialog box.

(3) Error messages

If the system ends abnormally, any of the following messages is displayed in a dialog box.

Table 7.47 Error messages

Message	Meaning	Response
Error: S.M.A.R.T. Set Error :ErrorCode=****	Making a setting for S.M.A.R.T failed. [ErrorCode] 3300: Resource shortage 3301: SNMPSET error	If repeating the operation in the window results in the same problem, contact the system administrator or a Fujitsu certified service engineer.

7.16 [Expansion File Unit] Window

The [Expansion File Unit] window displays information on the expansion file units that are included.

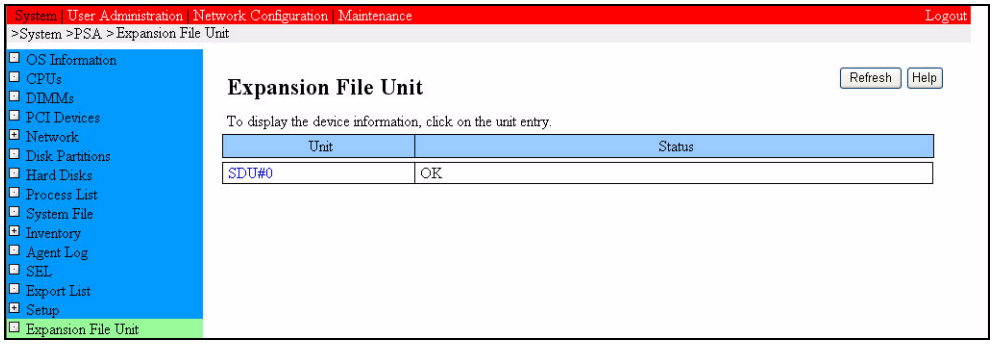


Figure 7.28 [Expansion File Unit] window

The [Expansion File Unit] window lists the connected expansion file units. Click the [Unit] item to display a detail window.

Note: The window is displayed when at least one expansion file unit is connected.

Table 7.48 Display items of [Expansion File Unit] window

Item	Explanation
Unit	Displays the identification name of an expansion file unit.
Status	Displays the hardware status (unified status of the fan, power supply, and controller of an expansion file unit) of an expansion file unit as follows: • OK: Normal • Error: An important problem such as a hardware error is detected. • Warning: Warning status (A problem may occur in the future.) • Unknown: Uncertain It takes up to five minutes until a status change is reflected in the window display.

Table 7.49 Buttons of [Expansion File Unit] window

Button	Explanation
Display frame of each [Unit]	Click the display frame of each [Unit] to display a detail window.

(1) Menu operation

[System] → [PSA] → [Expansion File Unit]

(2) Window operation

1 Click the item [Unit].
The [SDU#x] window is then displayed.

2 Click the [Return] button in the displayed [SDU#x] window.
The [Expansion File Unit] window is then displayed.

7.16.1 [SDU#x] window

The [SDU#x] window displays information on an expansion file unit.

Setting privilege users can clear the status with the [Status Clear] button.

Note: The window is displayed when at least one expansion file unit is connected.

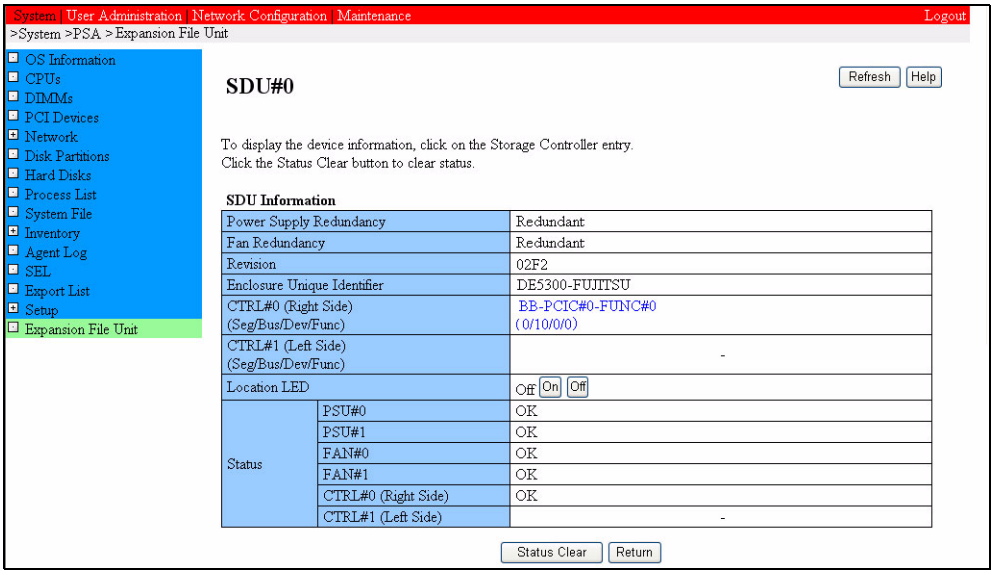


Figure 7.29 [SDU#x] window

Table 7.50 Display and setting items of [SDU#x] window

Item	Explanation
SDU Information	
Power Supply Redundancy	Displays the redundant status of a power supply unit as follows: • Redundant: The PSU is redundant. • [Non-redundant:Sufficient Resource]: Although PSU redundancy is lost, there is a PSU necessary for system operation. • [Non-redundant:Insufficient Resource]: The redundancy is lost and a PSU necessary for system operation is not enough. • Unknown: Uncertain It takes up to five minutes until a status change is reflected in the window display. Remarks: Click the [Status Clear] button to clear the status.
Fan Redundancy	Displays the redundant status of a fan as follows: • Redundant: The fan is redundant. • [Non-redundant:Sufficient Resource]: Although fan redundancy is lost, there is a fan necessary for system operation. • [Non-redundant:Insufficient Resource]: The redundancy is lost and there is no fan necessary for system operation. • Unknown: Uncertain It takes up to five minutes until a status change is reflected in the window display. Remarks: Click the [Status Clear] button to clear the status.
Revision	Displays a device version.
Enclosure Unique Identifier	Displays a device type
CTRL#0(Right Side) (Seg/Bus/Dev/Func)	Displays the identification name of the storage controller on the connection route (right side) and the following numbers: • Segment No. • Path No. • Device No. • Function No. If there is no connection to the storage controller, a hyphen [-] is displayed.
CTRL#1(Left Side) (Seg/Bus/Dev/Func)	Displays the identification name of the storage controller on the connection route (left side) and the following numbers: • Segment No. • Path No. • Device No. • Function No. If there is no connection to the storage controller, a hyphen [-] is displayed.

Item	Explanation
Location LED	Displays the status of a location LED. The display status includes the following: • On: ON • Off: OFF • Unknown: Uncertain Click the [On] and [Off] buttons to turn the LED on and off.
Status - PSU#0 Status - PSU#1	Displays the status of each PSU as follows: • OK: Normal • Warning: Warning status (A problem may occur in the future.) • Not-present: Not installed • Unknown: Uncertain It takes up to five minutes until a status change is reflected in the window display.
Status - FAN#0 Status - FAN#1	Displays the status of each fan as follows: • OK: Normal • Warning: Warning status (A problem may occur in the future.) • Not-present: Not installed • Unknown: Uncertain It takes up to five minutes until a status change is reflected in the window display.
Status - CTRL#0 (Right Side) Status - CTRL#1 (Left Side)	Displays the status of each controller as follows: • OK: Normal • Warning: Warning status (A problem may occur in the future.) If there is no connection to the storage controller, a hyphen [-] is displayed. It takes up to five minutes until a status change is reflected in the window display.

Table 7.51 Buttons of [SDU#x] window

Button	Explanation
Status Clear	The [Status Clear] button is displayed only for setting privilege users. Click the [Status Clear] button to display the [Confirm Settings] dialog box. Click the [OK] button in the [Confirm Settings] dialog box to clear the hardware status (fan, power supply, and controller status) of an expansion file unit. When mail/REMCS/SNMPtrap notification is suppressed within a specified time by a notification suppression function, notification suppression is also canceled.
Return	Click the [Return] button to return to the [Expansion File Unit] window.

(1) Menu operation

[System] → [PSA] → [Expansion File Unit] → [Unit]

(2) Window operation

- Clearing the hardware status of an expansion file unit
  1. Click the [Status Clear] button.
     The [Confirm Settings] dialog box is then displayed.
  2. Click the [OK] button in the [Confirm Settings] dialog box.
     The hardware status of the expansion file unit is then cleared.
  3. Click the [Return] button.
     The [Expansion File Unit] window is then displayed.
- Not clearing the hardware status of an expansion file unit
  1. Click the [Return] button.
     The [Expansion File Unit] window is then displayed.

(3) Error messages

If an ABEND occurs, the following messages are displayed in a dialog box:

Message	Meaning	Response
Error: Status Clear Error : ErrorCode=****	Status Clear failed. [ErrorCode] 3470: SDU Status Clear error	If the problem cannot be resolved by operating the window again in the menu operation in (1), contact the system administrator or a Fujitsu-certified service engineer.
Error: LED Set Error : ErrorCode=****	LED setting failed. [ErrorCode] 3471: LED control error	Check the status of the expansion file unit. Then reboot the PSA and operate the window again in the menu operation in (1). If the problem cannot be resolved, contact the system administrator or a Fujitsu-certified service engineer.

CHAPTER 8 CLI Operations

PSA is a system management application that runs on PRIMEQUEST series machines.

8.1 Basic CLI Operations

This section describes the CLI provided for OS commands.

Login to the OS is required for use of the CLI.

For details on the commands available to users depending on their user privileges, see Table 8.1, "Commands."

8.1.1 List of CLI commands

A list of PSA CLI commands is provided below. The letters in the Privilege column have the following meanings:

- Y: Requires the root privilege (Linux) or Administrator privilege (Windows).
- N: The command can be executed by general users.

Table 8.1 Commands

No	Command name	Privilege	Remarks	Linux	Windows
1	SAF-TE operation command	Y	Operates an SAF-TE unit and HDDs under its control.	Y	N
2	PSA start/stop command	Y	Starts and stops PSA.	Y	N (*1)
3	PSA troubleshooting data collection command	Y	Collects troubleshooting data for PSA.	Y	Y
4	Filter definition update commands	Y	Copies filter definitions to a PSA work directory or updates them.	Y	Y
5	Get local partition number command	N	Outputs the local partition number to the standard output.	Y	Y
6	Get serial number command	N	Outputs the serial number to the standard output.	Y	Y
7	SNMP security setting command	Y	Sets the host that is to accept SNMP packets.	N	Y
8	SAL/EFI firmware update command	Y	Reserves or cancels the SAL/EFI firmware update command.	Y	Y
9	Firmware update setup command	Y	Preparing for online firmware updating. This command must execute before SAL/EFI Firmware Update Command.	N	Y
10	Get firmware information command	Y	Collects firmware information.	Y	Y

*1 Start: Click [Control Panel], [Management Tools], and [Services] in that order to start PSA Environment Control Service. Start PRIMEQUEST Server Agent and PRIMEQUEST PEMCommand Service.

Stop: Click [Control Panel], [Management Tools], and [Services] in that order to select PSA Environment Control Service, PRIMEQUEST Server Agent, and PRIMEQUEST PEMCommand Service.

8.2 SAF-TE Operation Command (diskctrl)

The diskctrl command displays SAF-TE units and HDDs under its control in a list, powers on and off HDDs, and turns on and off location LEDs, which indicate the HDD locations, according to the specified options.

Remarks:

- This command can be used only with Linux.
- The execution of this command requires the root privilege.
- Turning off an HDD for preventive replacement requires the following operation:
  - If the HDD has been mirrored by GDS, disconnect the HDD first.
  - If the HDD has not been mirrored by GDS, unmount the HDD.

Note:

- When hot-swapping or hot-adding an internal hard disk for a PRIMEQUEST, simply inserting the hard disk will not allow power to be supplied to the hard disk. You always need to execute the pertinent SAF-TE operation command for power-on.
- RAID devices are excluded here. For information on how to replace RAID hard disks, refer to the pertinent manual for the RAID device.
- When you are executing this command for hard disk replacement, the following message may be output during power-on operation. For operation, you do not need to be concerned about this message.

```
kernel: mptscsih: ioc0: >> Attempting bus reset!
(sc=e000004082adc480)
kernel: mptbase: ioc0: IOCStatus(0x0048): SCSI Task
Terminated
```

- If you insert a hard disk, turn on the power to the disk, realize that you have inserted the disk with the disk orientation incorrect, turn off the power, and re-insert the disk correctly, you must be careful so that you execute power-off at least 60 seconds or so after power-on. If the interval between the power-on and power-off is too short, the OS's HotPlug process, which is activated at power-on, may cause the following error message to be output:

```
kernel: Device sdb not ready.
kernel: end_request: I/O error, dev sdb, sector 204706
kernel: Buffer I/O error on device sdb1, logical block
6396
```

- If you start PSA during SAF-TE operation command execution, PSA will not work normally. Start PSA after the command ends its processing.
  For information on the operating procedure of this command, see Section 1.3, "Support of Hot Swapping" in the *PRIMEQUEST 500A/ 500/400 Series Reference Manual: Tools/Operation Information* (C122-E074EN).
- Using the SAF-TE operator command to execute multiple operations at the same time may cause the system to terminate abnormally. Retry executing this command after verifying that it is not being used to execute multiple operations at the same time.
- Manually execute the command below for PSA in the following cases:
  - Hot maintenance of a hard disk is performed when using SUSE.
  - Hot maintenance of a hard disk of GDS is performed when using RHEL.

```
/opt/FJSVpsa/sh/force_search.sh -a
```

(1) Synopsis

```
/opt/FJSVpsa/bin/diskctrl {-l|-e|-i|-o|-c} {Devicename|/dev/sgx/slotno}
```

(2) Options

{-l|-e|-i|-o|-c}

-l: Status display
Displays each SAF-TE unit and its subordinate HDDs recognized by the OS in a list.

-e: Power-off instruction
Turns off power to the HDD specified in [Devicename] or the slot of the SAF-TE unit specified in [/dev/sgx/slotno], and turns on the fault LED.

-i: Location display
Initiates blinking of the fault LED for the HDD specified in [Devicename] or the slot of the SAF-TE unit specified in [/dev/sgx/slotno].

-o: Location turnoff
Turns off the fault LED for the HDD specified in [Devicename] or the slot of the SAF-TE unit specified in [/dev/sgx/slotno].

-c: Power-on command
Turns on power to the slot of the SAF-TE unit specified in [/dev/sgx/slotno].

[/dev/sgx/slotno]
Specifies the logical device name of the HDD subject to operation or the slot number of an SAF-TE unit:

Devicename: Specify the logical device name of the OS.
(Example: /dev/sda if it is the first SCSI disk unit)

Note: The logical device name is deleted when the power-off instruction (-e) is executed. Therefore, before specifying a logical device name, use the state indication option (-l) to check for that logical device in the operating system.

/dev/sgx/slotno: Specify the slot number of sgx (SAF-TE device).
(Example: /dev/sg0/1 if it is the slot 1 of the sg0).

(3) Example

The following example displays all SAF-TE units in the OS and the status of their individual slots in a list:

```
# /opt/FJSVpsa/bin/diskctrl -l
```

Display example	Description of status
`/dev/sg0`	
`  0 /dev/sda Power-On Fault LED-Off`	<- Normal operation
`  1 /dev/sdb Power-On Fault LED-Predicted Fault`	<- Predicted fault
`/dev/sg1`	
`  0 --mount  Not Activated  Fault LED-Off`	<- No HDD is inserted or powered on.
`  1 --mount  Power-Off Fault LED-On`	<- Power-off
`/dev/sg2`	
`  0 /dev/sdd Power-on Fault LED-Identify`	<- Location display on
`  1 none`	<- Empty slot
`/dev/sg3`	
`  0 none`	* The number displayed under /
`  1 none`	dev/sgx indicates the slot number.

The following example powers off an HDD before the unit is replaced or removed:

```
# /opt/FJSVpsa/bin/diskctrl -e /dev/sda
```

The following example verifies the HDD mounting location before an additional HDD is installed:

```
# /opt/FJSVpsa/bin/diskctrl -i /dev/sg0/3
```

The following example turns off a fault LED that the user kept blinking to indicate the location for HDD replacement or addition:

```
# /opt/FJSVpsa/bin/diskctl -o /dev/sg0/3
```

The following example powers on an HDD that the user installed for HDD replacement or addition:

```
# /opt/FJSVpsa/bin/diskctrl -c /dev/sg0/3
```

(4) Output messages

The following messages will be output at the time of abnormal termination.

Table 8.2 SAF-TE operation command (diskctrl) massages

Message	Meaning	Response
FJSVpsa: E 02150 diskctrl GDS access failed	GDS access failed.	Verify that the installed GDS is correctly configured.
FJSVpsa: E 02151 diskctrl Device access failed	Access to the specified device failed.	Retry. If an error recurs, check if the device is already offline because of failure. If sg does not exist under /dev, load the sg driver using modprobe and then retry.
FJSVpsa: E 02152 diskctrl no memory available	Insufficient memory	Check for free memory space availability. Terminate unnecessary processes and then retry.
FJSVpsa: E 02157 diskctrl Power-off failed	HDD power-off failed.	Retry. If an error recurs, delete or replace the HDD when the power to the system is off.
FJSVpsa: E 02158 diskctrl Cannot blinking location-LED	LED blinking failed.	Retry. If an error recurs, the SAF-TE device may be faulty. Check for an sg error. Perform replacement or other action.

Message	Meaning	Response
FJSVpsa: E 02159 diskctrl Cannot clear location-LED	LED extinguishing failed.	Retry. If an error recurs, the SAF-TE device may be faulty. Check for an sg error. Perform replacement or other action.
FJSVpsa: E 02160 diskctrl Power-on failed	HDD power-on failed.	Check the slot number of the specified SAF-TE device and retry. If an error recurs, the SAF-TE device may be faulty. Check for an sg error. Perform replacement or other action.
FJSVpsa: E 02165 diskctrl Operation not permitted	No execution privilege.	Log in as the superuser and retry.
FJSVpsa: E 02166 diskctrl Stopped	The command being executed was canceled by Ctrl+C.	None
FJSVpsa: E 02167 diskctrl Invalid option	An invalid option was specified.	Specify correct options.
FJSVpsa: E 02169 diskctrl too few or more option	Incorrect number of command options.	Specify correct options.
FJSVpsa: E 02170 diskctrl Cannot stop HDD	HDD rotation stop failed.	Retry. If an error recurs, check whether the device is already offline because of failure.
FJSVpsa: E 02171 diskctrl Cannot get device information	Device information acquisition failed.	Check the HDD information that is recognized by the OS. If there is no sg under /dev, load the sg driver by using modprobe, and then retry the command.
FJSVpsa: E 02173 diskctrl sg device not found	sg (SAF-TE device) cannot be found.	If the sg driver has not been loaded, load it with the modprobe command before retrying the operation. If the sg driver has been loaded, simply retry the operation.
FJSVpsa: E 02174 diskctrl Device not found	The specified device is not found.	Check for devices and specify the correct device names. If there is no sg under /dev, load the sg driver by using modprobe, and then retry the command.
FJSVpsa: E 02175 diskctrl SAF-TE access failed (Read Enclosure Configuration)	A command on the SAF-TE device encountered an error.	Retry. If an error recurs, the SAF-TE device may be faulty. Check for an sg error. Perform replacement or other action.

Message	Meaning	Response
FJSVpsa: E 02176 diskctrl SAF-TE access failed (Read Enclosure Status)	A command on the SAF-TE device encountered an error.	Retry. If an error recurs, the SAF-TE device may be faulty. Check for an sg error. Perform replacement or other action.
FJSVpsa: E 02177 diskctrl SAF-TE access failed (Read Device Slot Status)	A command on the SAF-TE device encountered an error.	Retry. If an error recurs, the SAF-TE device may be faulty. Check for an sg error. Perform replacement or other action.
FJSVpsa: E 02186 %s is busy. Please retry after a few minutes.	A power-off instruction was issued to a busy device.	Issue the power-off instruction later.
FJSVpsa: E 02187 internal error	An internal error occurred.	Contact a certified service engineer.
FJSVpsa: W 2188 diskctrl Can not power off GDS control disk.	An HDD configured in the GDS was specified. Power cannot be turned off.	Release the relevant HDD from GDS control and then turn off the power.

8.3 PSA Start/Stop Command (y30FJSVpsa)

The [y30FJSVpsa] command starts or stops the PSA.

Remarks:

- This command can be used only with Linux.
- The execution of this command requires the root privilege.
- Since PSA is a daemon program, it usually is automatically started at the time of boot.
- When PSA is stopped and restarted, all statuses contained in PSA are cleared.

Note: If you start PSA during SAF-TE operation command execution, PSA will not work normally. Start PSA after the command ends its processing.

(1) Synopsis

- RedHat

```
/sbin/service y30FJSVpsa {start | stop}
```

- SUSE

```
/etc/init.d/y30FJSVpsa {start | stop}
```

(2) Options

start | stop

start: Starts PSA.
stop: Stops PSA.

(3) Examples

The following example starts PSA:

- RedHat

```
# /sbin/service y30FJSVpsa start
```

- SUSE

```
# /etc/init.d/y30FJSVpsa start
```

The following example stops PSA:

- RedHat

```
# /sbin/service y30FJSVpsa stop
```

- SUSE

```
# /etc/init.d/y30FJSVpsa stop
```

(4) Exit status

0: Normal exit

>0: Abnormal exit

(5) Notes

If PSA is booted by the v30FJSVpsa command, the message shown below may be displayed. However, this message does not indicate any operational problem.

/bin/mknod: `/dev/watchdog': File exists

8.4 PSA Troubleshooting Data Collection Command (getopsa)

The getopsa command collects troubleshooting data for PSA. Specifically, it outputs the installation status of individual application packages, a list of files and modules, configuration files, internal logs, traces files, etc., to one compressed file.

Remarks: Execution of this command requires the root or Administrator privilege.

Linux

(1) Synopsis

```
/opt/FJSVpsa/sh/getopsa output_filename
```

Specify the output destination file for the troubleshooting data after it is compressed, by using a full pathname in [output_filename].

(2) Options

None

(3) Example

The following example outputs the troubleshooting data to a file in [/tmp/dump/psa_dump]:

```
# /opt/FJSVpsa/sh/getopsa /tmp/dump/psa_dump
```

(4) Exit status

0: Normal exit

>0: Abnormal exit

Windows

(1) Synopsis

```
getopsa output_filename
```

Specify the output destination file for the troubleshooting data after it is compressed, by using a full pathname in [output_filename].

(2) Options

None

(3) Example

The following example outputs the troubleshooting data to a file in [\tmp\dump\psa_dump]:

```
> getopsa C:\temp\dump\psa_dump
```

(4) Exit status

None

8.5 Filter Definition Update Commands (fltcpy, fltupdate)

There are two filter definition update commands: fltcpy and fltupdates.

The fltcpy command copies the definitions from any directory containing filter definitions expanded from an archive file, etc., to the PSA work directory for updating filter definitions.

The fltupdate command copies the definitions from the PSA work directory for updating filter definitions to the operation directory to update the current filter definitions.

Remarks

- Execution of this command requires the root or Administrator privilege.
- Filter definitions cannot be updated while PSA is running.

(1) Synopsis

- Linux

```
/opt/FJSVpsa/sh/fltcpy [-f] [-d directory_name]
/opt/FJSVpsa/sh/fltupdate [-f]
```

- Windows

```
fltcpy [-f] [-d directory_name]
fltupdate [-f]
```

(2) Options

- fltcpy

[-f]

Forcibly updates the filter definitions in the work directory. This option is required for reverting to older filter definitions.
Without this option specified, the system does not update the filter definitions in the work directory if they are newer than those that would replace them in an update.

[-d directory_name]

Allows the user to specify a directory containing expanded filter definitions for an update.
If this option is omitted, the current directory will be used.

- fltupdate

[-f]

Forcibly updates the filter definitions in the operation directory. This option is required for reverting to older filter definitions.
Without this option specified, the system does not update the filter definitions in the operation directory if they are newer than those that would replace in an update.

(3) Examples

- Linux

● Ordinary update procedure
The following example stops PSA, executes the command for copying update files in the [/tmp/filter] directory containing an expanded file definition for an update, and restarts PSA after the fltcpy command is completed:

```
# /sbin/service y30FJSVpsa stop
# /opt/FJSVpsa/sh/fltcpy -d /tmp/filter
# /sbin/service y30FJSVpsa start *
```

* If the OS is restarted after execution of the fltcpy command, this procedure is not required because PSA is automatically started.

● Forced update procedure
The following example reverts to the older filter definition (a filter definition in the [/tmp/filter] directory):

```
# /sbin/service y30FJSVpsa stop
# /opt/FJSVpsa/sh/fltcpy -f -d /tmp/filter
# /opt/FJSVpsa/sh/fltupdate -f
# /sbin/service y30FJSVpsa start
```

- Windows

  - Ordinary update procedure
    The following example stops PSA, executes the command for copying update files in the [\tmp\filter] directory containing an expanded file definition for an update, and restarts PSA after the fltcpy command is completed:

```
> net stop "PRIMEQUEST Server Agent"
> fltcpy  -d  C:\temp\filter
> net start "PRIMEQUEST Server Agent"
```

  * If the OS is restarted after execution of the fltcpy command, this procedure is not required because PSA is automatically started.

  - Forced update procedure
    The following example reverts to the older filter definition (a filter definition in the [\tmp\filter] directory):

```
> net stop "PRIMEQUEST Server Agent"
> fltcpy  -f  -d  /tmp/filter
> fltupdate -f
> net start "PRIMEQUEST Server Agent"
```

(4) Output messages

Filter definition update commands display the following messages:

Table 8.3 Filter definition update command (fltcpy, fltupdate) messages

Message	Meaning	Response
FJSVpsa: E 02700 fltupdate initialization failed	Initialization failed.	Verify that the login user is the superuser and that the PSA is correctly installed.
FJSVpsa: E 02701 fltupdate version file read error	Version read failed.	Verify that the login user is the superuser and that the PSA is correctly installed.
FJSVpsa: E 02702 fltupdate version file format error	A format error was detected in the version information.	Verify that the PSA is correctly installed.
FJSVpsa: E 02703 fltupdate internal error	An internal conflict occurred.	Contact a certified service engineer.
FJSVpsa: I 02704 fltupdate updating filter file	The filter version is to be updated.	None
FJSVpsa: I 02705 fltupdate unnecessary to update filter file	The filter version does not need to be updated.	None
FJSVpsa: E 02707 fltupdate failed to update filter file	Filter updating was not completed normally.	Verify that the login user is the superuser and that the PSA is correctly installed.
FJSVpsa: I 02708 fltupdate normally end	The filter was not updated normally.	None
FJSVpsa: E 02709 fltupdate failed to update filter file	Filter updating was not completed normally.	Verify that the login user is the superuser and that the PSA is correctly installed.
FJSVpsa: E 02710 fltout version file format error	An invalid value was specified for the version information.	An error possibly exists in the provided filter definition. Contact a certified service engineer.
FJSVpsa: E 02711 fltupdate fltout filter file open error	The filter file cannot be opened.	Verify that the login user is the superuser and that the PSA is correctly installed.
FJSVpsa: E 02712 fltout filter file read error	Filter information read failed.	Verify that the login user is the superuser and that the PSA is correctly installed.
FJSVpsa: E 02713 fltout filter file format error	An error was detected in the filter file.	An error possibly exists in the provided filter definition. Contact a certified service engineer.
FJSVpsa: E 02714 fltout initialization failed	Initialization failed.	Verify that the login user is the superuser and that the PSA is correctly installed.

Message	Meaning	Response
FJSVpsa: E 02716 fltupdate illegal version	The specified version value is outside the range.	An error possibly exists in the provided filter definition. Contact a certified service engineer.
FJSVpsa: E 02717 fltupdate illegal version	The specified version value is invalid.	An error possibly exists in the provided filter definition. Contact a certified service engineer.
FJSVpsa: E 02718 fltupdate cannot update filter file	The filter cannot be updated because PSA is active.	Stop PSA and then retry.

8.6 Get Local Partition Number Command (getpartid)

The getpartid command outputs a local partition number to the standard output.

Remarks: This command always returns 0 in PRIMEQUEST 510A Series.

Linux

(1) Synopsis

```
/opt/FJSVpsa/sh/getpartid
```

(2) Options

None

(3) Example

```
$ /opt/FJSVpsa/sh/getpartid
0
```

(4) Exit status

0: Normal exit

>0: Abnormal exit

Windows

(1) Synopsis

```
getpartid
```

(2) Options

None

(3) Example

```
> getpartid
  0
```

(4) Exit status

0: Normal exit

>0: Abnormal exit

8.7 Get Serial Number Command (getserialno)

The getserialno command outputs a serial number to the standard output. The second line is the serial number for use in Europe.

Linux

(1) Synopsis

```
/opt/FJSVpsa/sh/getserialno
```

(2) Options

None

(3) Example

```
$ /opt/FJSVpsa/sh/getserialno
xxxxxxxxxxxx
yyyyyyyyyyyy
```

(4) Exit status

0: Normal exit

>0: Abnormal exit

Windows

(1) Synopsis

```
getserialno
```

(2) Options

None

(3) Example

```
> getserialno
  xxxxxxxxxx
  yyyyyyyyyy
```

(4) Exit status

0: Normal exit

>0: Abnormal exit

8.8 SNMP Security Setting Command (setsnmpsec)

The setsnmpsec command sets SNMP service security (sets the host that accepts SNMP packets). If the SNMP service security setting is "Accept SNMP packets from any host." you do not need to execute this command.

If the MMB IP address is changed after PSA installation in an environment where the SNMP service security setting is "Accept SNMP packets from any host," execute this command when the SNMP service security setting is changed from "Accept SNMP packets from any host" to "Accept SNMP packets from these hosts."

Remarks:

- This command can be used only with Windows.
- The execution of this command requires the Admin privilege.

(1) Synopsis

```
setsnmpsec
```

(2) Options

None

(3) Example

```
> setsnmpsec
```

(4) Output messages

- Normal termination

  FJSVpsa : I 04200 Security setting for SNMP Service was completed.

- Abnormal termination

  FJSVpsa : E 04201 Anerror occurred at the time of security setting for SNMP Service.

(5) Notes

After you execute this command, you need to restart the SNMP Service.

8.9 SAL/EFI Firmware Update Command (fjfwupdate)

The fjfwupdate command reserves and cancels firmware updating, and displays an updating list. This command displays a log that is output during firmware updating.

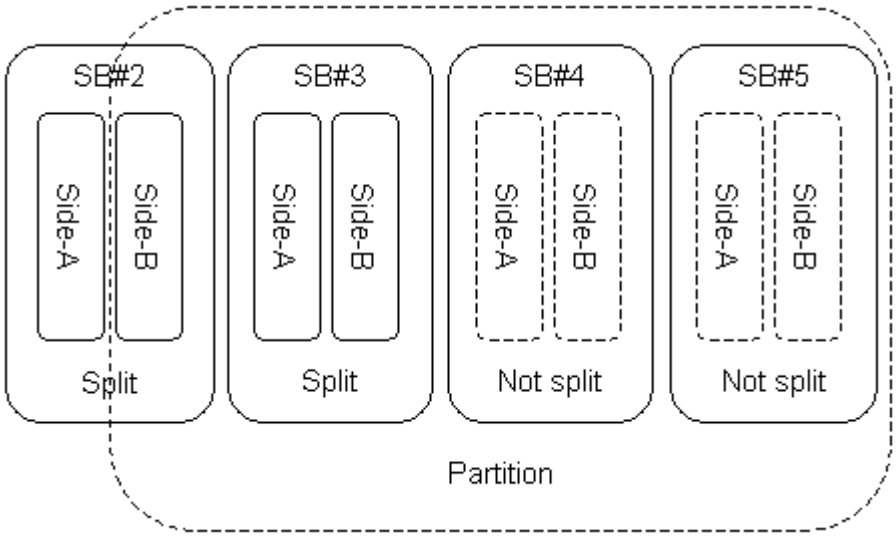
When the OS is rebooted after reserving firmware updating, firmware updating automatically starts.

The environment needs to be set up before this command can be used.

Notes:

- Be careful when using the fjfwupdate command in an environment where the system disk is mirrored by PRIMEQUEST System Disk Mirror (PSDM) on Windows 2003 Server. In such cases, follow the procedure described in "Using the fjfwupdate command in an environment where the system volume is mirrored by PSDM (on Windows 2003 Server) " to temporarily disable mirroring by PSDM before executing the fjfwupdate command. Otherwise, the system disk will not be mirrored normally by PSDM.
- The execution of this command requires root privilege (or Administrator privilege for Windows).
- The targets of online firmware updating are

  SAL firmware: All SB in the partition.
  PQ 400 series: A-side only.
  Other series: Both sides.
  EFI firmware: Only Home IOU in the partition
  Example) PRIMEQUEST 580



If the partition is configured as shown in the above figure, SAL firmware updating targets are SB#2 (Side-B), SB#3 (Side-A, Side-B), SB#4 (Side-A, Side-B), and SB#5 (Side-A, Side-B).

- The exit status is not the result of firmware updating. Refer to the result of firmware updating with the -l option.
- Only the last reservation for the same kind of firmware (SAL or EFI) prior to rebooting the OS becomes effective.
- The reservation is accepted only after the validity of the firmware binary file and the update tool is verified.
- Firmware updating is executed after the shutdown process is completed.
- At least 20MByte (to use for firmware binary file, update tool, log file and so on) of free space is required for the EFI partition.
- Do not operate the power control during updating firmware.
- Do not operate all on the directory for firmware update.
- When replacing the System Volume Disk [or Disk for firmware update] or uninstalling FJSVpsa, delete the EFI boot option for this command by following the procedure below. If you deleted the boot option once, the Setup sequence needs to be followed again.
  - For deletion from the EFI Boot Manager

    Select the following items
    Boot Option Maintenance Menu → Delete Boot Option(s) → PRIMEQUEST Online Firmware Update (don't select)
  - For deletion from the OS

    [Linux]
    Confirm the boot option Number of "PRIMEQUEST Online Firmware Update (don't select)" with the "efibootmgr" command. Then delete this boot option.

```
#efibootmgr
BootCurrent: 0000
Timeout: 10 seconds
BootOrder: 0000,fffe,fff0,fff2,0008,0009
Boot0000* RHEL4 U2
Boot0008* PRIMEQUEST Online Firmware Update (don't select) <- target
bootoption
Boot0009* sadump (DON'T SELECT!)

#efibootmgr -b 0008 -B , <- specify the target bootoption’s four digit
hexadecimal character string
BootCurrent: 0000
Timeout: 10 seconds
BootOrder: 0000,fffe,fff0,fff2,0009
Boot0000* RHEL4 U2
Boot0009* sadump (DON'T SELECT!)

#
```

[Windows]
Confirm the boot option Number of "PRIMEQUEST Online Firmware Update (don't select)" with the "bootcfg" command. Then delete this boot option.

```
C:\>bootcfg

Boot Options
------------
Timeout:             30
Default:             \Device\HarddiskVolume3\WINDOWS
CurrentBootEntryID:  1

Boot Entries
------------

Boot entry ID:    1
OS Friendly Name: Windows Server 2003, Datacenter
OsLoadOptions:    /noexecute=optout /redirect
BootFilePath:     \Device\HarddiskVolume1\EFI\Microsoft\WINNT50.1\
ia64ldr.efi
OsFilePath:       \Device\HarddiskVolume3\WINDOWS

Boot entry ID:    2
OS Friendly Name: RHEL4 GA

Boot entry ID:    3
OS Friendly Name: RedHat U2 GA

Boot entry ID:    4
OS Friendly Name: DVD/Acpi(PNP0A03,0)/Pci(1D|1)/Usb(0, 0)/Usb(1, 0)

Boot entry ID:    5
OS Friendly Name: Network/Acpi(PNP0A03,0)/Pci(1E|0)/Pci(8|0)/
Mac(000B5D6E015E)

Boot entry ID:    6
OS Friendly Name: EFI Shell [Built-in]

Boot entry ID:    7
OS Friendly Name: PRIMEQUEST Online Firmware Update (don't select)

C:\>bootcfg /Delete /ID 7 <- specify the target bootoption’s decimal
character string
SUCCESS: Specified boot entry has been deleted.
```

- [Windows]
  - Firmware updating cannot be reserved when there is no remainder in the drive letter.
  - The firmware updating process is executed following the occurrence of reset by Panic, etc.

Using the fjfwupdate command in an environment where the system volume is mirrored by PSDM (on Windows 2003 Server)

Be careful when using the fjfwupdate command in the environment described below. In such cases, follow the procedure below to temporarily disable mirroring by PSDM before executing the fjfwupdate command. Otherwise, the system disk will not be mirrored normally by PSDM.

- Applicable environment

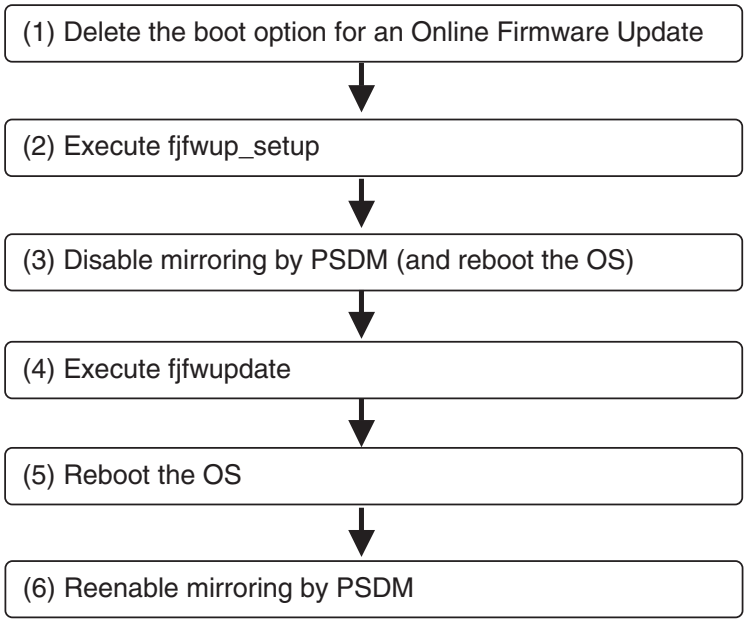
  Cabinet: Every PRIMEQUEST model

  OS: Windows 2003 Server

  Other: Environment where the system disk is mirrored by PSDM

- Procedure

  To update SAL/EFI firmware in an environment that satisfies the above conditions, follow the procedure below.



1. Delete the boot option "PRIMEQUEST Online Firmware Update (don't select)" as instructed in "For deletion from the OS" under "Note" in Section 8.9.
2. Execute the PSA command "fjfwup_setup" to prepare for the firmware update.

```
> fjfwup_setup
```

3 Execute the PSDM commands "sdxinfo" and "sdxsysdisk" to temporarily system disk mirroring. To temporarily disable disk mirroring, start Disk Administrator, and confirm the disk number of the disk containing the EFI system partition. Execute the sdxinfo -D command. Find the line on which the value in the DEVNAME column is equal to the confirmed disk number. Then, record the group name displayed in the GROUP column on that line. The group name indicates the group whose mirroring is to be removed.
Also, record the DEVNAME value on all lines on which the GROUP value is the same as the recorded group name. The DEVNAME values indicate the disks belonging to the group whose mirroring is to be disabled.

Example: The system disk number confirmed with Disk Administrator is 0.

```
>sdxinfo -D
OBJ  NAME   TYPE   GROUP   DEVNAM DEVBLKS  STATUS
---- ------ ------ ------- ------ -------- -------
disk Disk0  mirror Group1  0      35291136 VALID
disk Disk1  mirror Group1  3      35291136 VALID
disk Disk2  mirror Group1  4      35291136 VALID
disk Disk3  mirror Group2  5      35291136 VALID
disk Disk4  mirror Group2  7      35291136 VALID
```

In the above example, the group whose mirroring is disabled is Group1, and the disks belonging to the group are disks 0, 3, and 4.
The sdxsysdisk -R command with the recorded group name specified is executed to disable mirroring of the group.

Example: Disabling mirroring of Group1

```
>sdxsysdisk -R -g Group1
```

The OS is automatically rebooted after the command is executed. If the OS is not rebooted automatically, reboot the OS manually.

4 After the OS is rebooted, execute the PSA command "fjfwupdate" to prepare for the firmware update.

```
>fjfwupdate [-sal|-efi] updatetool firmwarefile
 firmware updating (firmwarefile) is reserved.
 Reboot is needed for updating firmware.
```

5 Reboot the OS, and update the firmware.
Start the firmware update after the OS shutdown. The original OS is booted after the firmware update is completed.
After the OS is booted, execute the fjfwupdate command to check the firmware update results.

```
> fjfwupdate -l
```

6 Reenable the disk mirroring disabled in step 3 in the system disk mirror system by executing the sdxsysdisk command to restore the state confirmed in step 3.
Use Disk Administrator to find the disk number of the current system disk. The disk number of the current system disk is displayed by Disk Administrator. The current system disk is the disk that has the C drive.
Among the disk numbers recorded in step 3, format each disk whose disk number is not the disk number of the current system disk .

Example: Disk numbers 0, 3, and 4 were recorded in step 3 and the current system disk is disk 0. (Format disks 3 and 4.)

```
> diskpart
diskpart> select disk 3
diskpart> clean
diskpart> convert gpt
diskpart> select disk 4
diskpart> clean
diskpart> convert gpt
diskpart> exit
```

Reenable mirroring by PSDM with the current system disk (disk 0) as the copy source.

Example: Disk numbers 0, 3, and 4 were recorded in step 3, and the current system disk is disk 0.

```
> sdxsysdisk -M -p 0:keep,3,4
```

(1) Synopsis

```
# /opt/FJSVpsa/sh/fjfwupdate [ -sal | -efi ] <tool>
<firmbinfile>
# /opt/FJSVpsa/sh/fjfwupdate -c <listnum>
# /opt/FJSVpsa/sh/fjfwupdate -p
# /opt/FJSVpsa/sh/fjfwupdate -l
```

(2) Options

[-sal | -efi] <tool> <firmbinfile>:Reserve firmware updating

This option reserves firmware updating. When you use this option, you should specify the update tool (<tool>) and firmware binary file (<firmbinfile>). You can use both the absolute path and the relative path, when you specify the filename. This option verifies the validity of the specified update tool and the firmware binary file.

-p: Display reserving list

This option displays the reservation list reserved with the [-sal | -efi] options.

-c <listnum>: Cancel the reservation

This option cancels the reservation set with the [-sal | -efi] options. When you use this option, you should specify the reservation number (<listnum>) displayed by the -p option.

-l: Display the latest execution log
This option displays the latest execution log.
This log is a firmware update log or a firmware application status log.

(3) Exit status

This is not the result of firmware updating but the result of command execution.

0: Normal exit

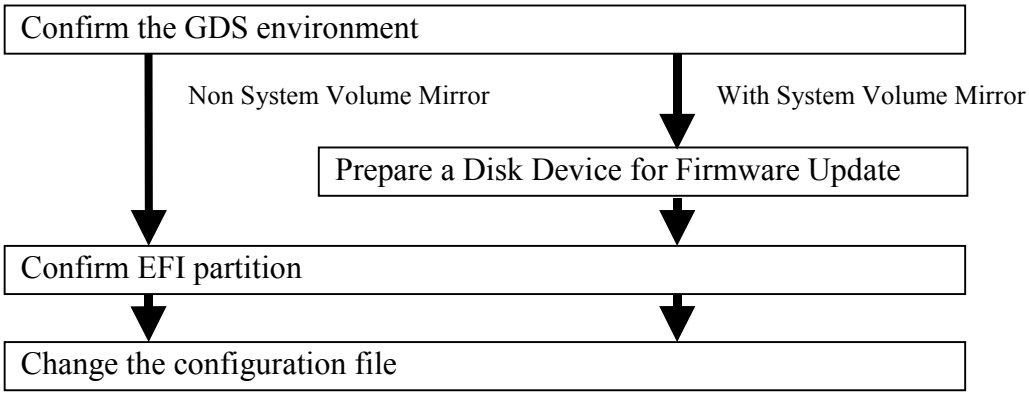
>0: Abnormal exit The fjfwupdate command displays an error message.

(4) Setup

This command is included in FJSVpsa package.

After installing FJSVpsa, set up the environment in accordance with the instructions below.

1 Linux



7 Confirm the GDS environment
If the system has the System Volume Mirror configuration set with PRIMECLUSTER GDS, the setup operation in step 2 needs to be executed.
In other cases, confirm the EFI Partition and follow the instructions in step 3.

8 Prepare the disk partition for Firmware Update
If the system has the System Volume Mirror configuration set with PRIMECLUSTER GDS, mount the disk partition that is not included with GDS Mirroring.
The disk partition must meet the following conditions.
Disk label: gpt
type: vfat
size: 20 M byte or more
Create the new partition with the "parted" command and execute formatting with the "mkfs.vfat" command.
After creating the disk partition, add the following information on "/etc/fstab".

```
# This file is edited by fstab-sync - see 'man fstab-sync' for details
/dev/sfdsk/RootClass/dsk/rootVolume /          ext3    defaults        1 1
/dev/sfdsk/RootClass/dsk/efiVolume  /boot/efi  vfat    defaults        0 0
none                                /dev/pts   devpts  gid=5,mode=620  0 0
none                                /dev/shm   tmpfs   defaults        0 0
/dev/sfdsk/RootClass/dsk/homeVolume /home      ext3    defaults        1 2
none                                /proc      proc    defaults        0 0
none                                /sys       sysfs   defaults        0 0
/dev/sfdsk/RootClass/dsk/usrVolume  /usr       ext3    defaults        1 2
/dev/sfdsk/RootClass/dsk/varVolume  /var       ext3    defaults        1 2
/dev/sfdsk/RootClass/dsk/swapVolume swap       swap    defaults        0 0
# add information
/dev/sdc1                           /mnt/OLFU  vfat    defaults        0 0
```

Mount the disk partition with the following command.
mount -a

9 Confirm the EFI partition

Confirm the device special file name of the EFI partition with the following command.

```
# df –t vfat
Filesystem          1K-blocks     Used Available Use% Mounted on
/dev/sda1             102182     10916     91266  11% /boot/efi
```

If the mounted device on /boot/efi is /dev/sda1, the other procedure is not required for Setup.

If the device special file name is not formatted as

/dev/sd<x><n>

<x>: one or more lowercase alphabetic characters

<n>: one or more decimal numeric characters

Prepare a disk partition following the instructions in step 2.

10 Change the configuration file

If you prepare a disk partition in accordance with the instructions in step 2 or if the device special name of the EFI partition is not the equivalent of /dev/sda1, change the configuration file as follows.

Configuration file: /etc/opt/FJSVpsa/local/lofu.conf

Change item: DEVICE.

```
DEVICE=/dev/sdd1      ->delete # comment and assign the EFI partition
#PATH=/boot/efi/efi/fujitsu/fjfwupdate
```

The "PATH" Item written in the configuration file does not need to be assigned. If you want to use the subdirectory of the EFI partition, you have to set the absolute path name.

Note: The configuration file is read only once when you first execute this command. After that, this command, when executed, does not read the configuration file. If you want to change the setting, check [REMARKS].

2 Windows

The "fjfwup_setup" command needs to be executed before using this command.

For details see "Firmware Update Setup Command (Windows Only)."

(5) Examples

- Examples of LINUX

● Initial setting (when no changes are made to the Configuration file).

```
#df -t vfat
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda1               102182     10916     91266  11% /boot/efi
#
```

● Initial setting (when changes are made to the Configuration file)

```
#df -t vfat
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda7               102182     10916     91266  11% /boot/efi

#vi /etc/opt/FJSVpsa/local/olfu.conf

DEVICE=/dev/sda7
#PATH=/boot/efi/efi/fujitsu/fjfwupdate

#
```

● Initial setting (In case of System Volume Mirror by GDS).

```
(/dev/sdc is the new disk)
#parted /dev/sdc
(parted) mkpartfs primary fat32 0 200
(parted) p
Disk geometry for /dev/sdc: 0.000-70092.996 megabytes
Disk label type: gpt
Minor   Start     End      Filesystem  Name    Flags
1       0.017     256.473  fat16

#mkfs.vfar
mkfs.vfat 2.8 (28 Feb 2001)

#vi /etc/fstab

/dev/sdc1 /mnt/OLFU  vfat    defaults        0 0

#
#mount -a
#df -t vfat
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sfdsk/RootClass/dsk/efiVolume
                        102182     13008     89174  13% /boot/efi
/dev/sdc1               262464         0    262464   0% /mnt/OLFU

#vi /etc/opt/FJSVpsa/local/olfu.conf

DEVICE=/dev/sdc1
#PATH=/boot/efi/efi/fujitsu/fjfwupdate

#
```

The following are examples of execution results after downloading the firmware binary file and update tool.

- Normal operation.

```
# ls
EFI0109+head.bin  SAL0113+head.bin  salupdate.efi

# /opt/FJSVpsa/sh/fjfwupdate -sal salupdate.efi SAL0113+head.bin
firmware updating (SAL0113+head.bin) is reserved
reboot is needed for updating firmware

# /opt/FJSVpsa/sh /fjfwupdate -p
No.       tool                 bin
1         salupdate.efi        SAL0113+head.bin

# /opt/FJSVpsa/sh/fjfwupdate -efi salupdate.efi EFI0109+head.bin
firmware updating (EFI0109+head.bin) is reserved
reboot is needed for updating firmware

# /opt/FJSVpsa/sh/fjfwupdate -p
No.       tool                bin
1         salupdate.efi       SAL0113+head.bin
2         salupdate.efi       EFI0109+head.bin

# /opt/FJSVpsa/sh/fjfwupdate -c 1
firmware updating (SAL0113+head.bin) is canceled

# /opt/FJSVpsa/sh/fjfwupdate -p
No.       tool                bin
1         efiupdate.efi       EFI0109+head.bin

# /opt/FJSVpsa/sh/fjfwupdate -sal salupdate.efi SAL0113+head.bin
firmware updating (SAL0113+head.bin) is reserved
reboot is needed for updating firmware

# /opt/FJSVpsa/sh/fjfwupdate -p
No.       tool                bin
1         efiupdate.efi       EFI0109+head.bin
2         salupdate.efi       SAL0113+head.bin

# /optFJSVpsa/sh/fjfwupdate -l
New firmware is applicable now
# reboot
.......
# /optFJSVpsa/sh/fjfwupdate -l
03/31/2006
13:59:04
Online Firmware Update Script Start
03/31/2006
13:59:04
SAL firmware update start


<SAL Version>
Current SAL Version = 1.12
New SAL Version = 1.13
  *snip*
SAL firmware update end
03/31/2006
14:05:07
EFI firmware update start

<EFI Version>
Current EFI Version = 1.8
New EFI Version = 1.9
  *snip*
EFI firmware update end
03/31/2006
14:08:32
Online Firmware Update Script End
```

- Illegal operation (Specifying the SAL firmware binary file in the -efi option).

```
# /opt/FJSVpsa/sh/fjfwupdate -efi efiupdate.efi SAL0113+head.bin
E xxx firmware header error (firmtype):SAL0113+head.bin
```

- Overlapping Reservation (EFI firmware updating).

```
# /opt/FJSVpsa/sh/fjfwupdate -sal salupdate.efi SAL0113+head.bin
# /opt/FJSVpsa/sh/fjfwupdate -p
No.       tool              bin
1         alupdate.efi      SAL0113+head.bin

# /opt/FJSVpsa/sh/fjfwupdate -sal salupdate.efi SAL0114+head.bin
$ /opt/FJSVpsa/sh/fjfwupdate -p
No.       tool              bin
1         salupdate.efi     SAL0114+head.bin
```

- Examples of WINDOWS

  - Execution of fjfwup_setup.

```
C:\update> fjfwup_setup
Reservation for adding bootoption was completed

#reboot

.......

#on EFI Shell reset automatically
startup.nsh> echo -off
resetting...

#on OS
C:\update> fjfwup_setup
I) already added bootoption
```

The following are examples of execution results after downloading the firmware binary file and update tool.

- Normal operation

```
C:\update>dir
 Volume in drive C has no label.
 Volume Serial Number is 0CB9-1257

 Directory of C:\update

04/04/2006  11:54 AM    <DIR>          .
04/04/2006  11:54 AM    <DIR>          ..
01/12/2006  05:24 PM         4,194,368 EFI0109+head.bin
03/11/2006  11:26 AM         4,194,368 SAL0114+head.bin
03/23/2006  10:27 PM           395,776 salupdate.efi
               3 File(s)      8,784,512 bytes
               2 Dir(s)  40,019,918,848 bytes free

C:\update>fjfwupdate -sal salupdate.efi SAL0114+head.bin
firmware updating (SAL0114+head.bin) is reserved
reboot is needed for updating firmware

C:\update> fjfwupdate -p
No.      tool              bin
1        salupdate.efi     SAL0114+head.bin

C:\update>fjfwupdate -efi salupdate.efi EFI0109+head.bin
firmware updating (EFI0109+head.bin) is reserved
reboot is needed for updating firmware

C:\update> fjfwupdate -p
No.      tool              bin
1        salupdate.efi     SAL0114+head.bin
2        salupdate.efi     EFI0109+head.bin

C:\update> fjfwupdate -c 1
firmware updating (SAL0114+head.bin) is canceled

C:\update> fjfwupdate -p
No.      tool              bin
1        efiupdate.efi     EFI0109+head.bin

C:\update>fjfwupdate -sal salupdate.efi SAL0114+head.bin
firmware updating (SAL0114+head.bin) is reserved
reboot is needed for updating firmware

C:\update> fjfwupdate -p
No.      tool              bin
1        efiupdate.efi     EFI0109+head.bin
2        salupdate.efi     SAL0114+head.bin
```

- Normal operation (continued)

```
C:\update> fjfwupdate -p
No.        tool            bin
1          efiupdate.efi   EFI0109+head.bin
2          salupdate.efi   SAL0114+head.bin

C:\update> fjfwupdate -l
New firmware is applicable now

#execute reboot

.......

C:\update> fjfwupdate -l
03/31/2006
13:59:04
Online Firmware Update Script Start
03/31/2006
13:59:04
SAL firmware update start

<SAL Version>
same as LINUX
```

- Illegal operation (Specifying the SAL firmware binary file in the -efi option)

```
C:\update> fjfwupdate -efi efiupdate.efi SAL0114+head.bin
firmware header error (firmtype): C:\update\SAL0114+head.bin
```

- Overlapping Reservation (EFI firmware updating)

```
C:\update> fjfwupdate -sal salupdate.efi SAL0113+head.bin
Firmware updating (SAL0114+head.bin) is reserved
Reboot is needed for updating firmware

C:\update> fjfwupdate -p
No.      tool               bin
1        salupdate.efi      SAL0113+head.bin

C:\update> fjfwupdate -sal salupdate.efi SAL0114+head.bin
firmware updating (SAL0113+head.bin) is canceled
firmware updating (SAL0114+head.bin) is reserved
reboot is needed for updating firmware

C:\update> fjfwupdate -p
No.      tool               bin
1        salupdate.efi      SAL0114+head.bin
```

(6) Output messages

[The fjfwupdate command displays the following messages:]

Message	Meaning	Response
E) firmware header error (%s1):%s2	%s1:signature or firmtype or checksum or chassis type %s2:firmbinfile A format error was detected in a firmware binary file.	%s1: signature or checksum or crc16 Check the validity of the firmware binary file. %s1: firmtype Check the type of firmware. %s1: chassystype Check the acceptable model of the firmware binary file. %s1: Not listed above Contact a certified service engineer.
E) tool header error (%s1):%s2	%s1:signature or format %s: tool A format error was detected in the update tool.	Check the adaptability to the online firmware updating of the tool.
E) operation is not permitted	No execution privilege.	Log in as the superuser and retry.
E) no space left on %s	%s : directory name No space left on %s.	Check for free disk space availability.
E) invalid option :%s	%s : Invalid option An invalid option was specified.	Specify correct option.
E) too few or more argument	Incorrect number of command options.	Specify correct option.
E) can’t find reservation No. :%d	An invalid reservation No. was specified.	Check the reservation No. with –p option. And specify correct reservation No.

Message	Meaning	Response
E) internal error :%s	%s : Detail of error An internal error has occurred.	%s: machine.conf Check the status of FJSVpsa service. %s: /etc/opt/FJSVpsa/local/olfu.conf Check for the existence of the file. %s: olfu_set.conf An Illegal boot option exists. Delete the boot option for the online firmware update according to the procedure in remarks. %s: no psa env path Check the "FJSVpsa_INSTALLPATH" environment variable. %s: Not listed above Contact a certified service engineer.
E) no such file or directory:%s	%s:File or directory name Can't find the file or directory.	Specify the correct filename or directory name.
I) firmware updating (%s) is reserved	%s:Firmware binary file name Reservation was completed.	None
I) firmware updating (%s) is canceled	%s:Firmware binary file name Reservation was canceled.	None
E) %s is not a vfat device or not mounted	%s:DEVICE setting value A device specified in the configuration file is not of vfat format or cannot mount. Linux only	Check the format(vfat) of the specified device in the setting file, and mount the device.
E) %s1 is not a vfat filesystem or not on %s2	%s1:PATH setting value %s2:DEVICE setting value A device specified in the configuration file is not of vfat format or does not exist. Linux only	Check the format (vfat) of the specified path in the setting file, or Check for the existence of the path on the device.

Message	Meaning	Response
E) illegal setting (/etc/opt/FJSVpsa/local/olfu.conf)	Setting of configuration file is invalid. Linux only	Check the validity of the setting file.
E) %s is not a block device	%s:DEVICE setting value A device specified in the configuration file is not a block device. Linux only	Check the type (block device) of the specified device.
E) fjfwup_setup command is needed before execute this command	Windows only	Execute the "fjfwup_setup" command.
E) no empty drive. Please make empty drive to mount EFI partition	Windows only	Check for free drive letter availability.

[fjfwupdate -p option message]

Message	Meaning	Response
there is no reservation	-	None

[fjfwupdate -l option message]

Message	Meaning	Response
New firmware is applicable now	A new firmware version has become available in between normal firmware update periods and can be applied immediately. Execute the firmware update after a OS reboot.	None
Internal error (%s)	%s:detail of error Unable to execute firmware update.	Contact a certified service engineer

[Other Problems]

Problem	Recovery
The message "Paused - press any key to continue" was output before the firmware updating started. (Linux Only)	1. Press any key and display the EFI boot option list. 2. Select the OS Boot Option 3. Execute the "efibootmgr" command and check the item of "BootNext" #efibootmgr BootNext: 0008 <- check the number BootCurrent: 0000 Timeout: 10 seconds BootOrder: 0000,fffe,fff0,fff2,0008,0009 Boot0000* RHEL4 U2 Boot0008* PRIMEQUEST Online Firmware Update (don't select) Boot0009* sadump (DON'T SELECT!) 4. Delete the BootNext flag with "efibootmgr -N" #efibootmgr -N 0008 <- specify the target number BootCurrent: 0000 Timeout: 10 seconds BootOrder: 0000,fffe,fff0,fff2,0008,0009 Boot0000* RHEL4 U2 Boot0008* PRIMEQUEST Online Firmware Update (don't select) Boot0009* sadump (DON'T SELECT!) 5. Delete the Boot Option for online firmware updating. See [Remarks]. 6. Retry setup sequence. See (4), "Setup."
OS was rebooted after the firmware updating was reserved, but the firmware update was not executed and the OS started. (Windows Only)	1. Delete the Boot Option for online firmware updating. See [Remarks]. 2. Retry "fjfwup_setup" command ,and reboot OS.

8.10 Firmware Update Setup Command (fjfwup_setup)

Preparing for online firmware updating.

This command must be executed once after OS installation.

After this command is executed, reboot is required to add the boot option on the EFI.

Note:

- Operation with 14 vfat disk partitions or more is not guaranteed.
- This command can be used only with Windows.
- The execution of this command requires the Administrator privilege.
- At least 20MByte (to use for update script, log file and so on) of free space is required for the EFI partition.
- The firmware updating can't be reserved when there is no remainder in the drive letter.
- This command cannot be canceled.

(1) Synopsis

```
#fjfwup_setup
```

(2) Options

None

(3) Exit Status

This is not the result of adding the boot option on the EFI but the result of command execution.

0: Normal exit

>0: Abnormal exit. The fjfwup_setup command displays an error message.

(4) Examples

This command adds the boot option on the EFI for the Firmware update command. Follow the procedure below.

1 Execute fjfwup_setup command(on the Command Prompt in OS)

→ following message is displayed

I) reboot is required to add the boot option

2 Rebooting the OS

→ Adding the boot option on the EFI Shell and reset, and then rebooting the OS.

3 Execute fjfwup_setup to confirm the result of adding the boot option.

following message is displayed.

I) already added boot option

(5) Output messages

Message	Meaning	Response
E) no empty drive please make empty drive to mount EFI partition	-	Check for free drive letter availability.
E) no space left on %s	%s: EFI Partition or %FJSVpsaInstallPass%	Check for free disk space availability.
E) internal error :%s	%s :detail of error	%s: no psa env path Check the "FJSVpsa_INSTALLPATH" environment variable. %s: no EFI option Check the normal EFI Shell boot option. %s: Not listed above Contact a certified service engineer.
I) reservation for adding bootoption was completed	-	None
I) reboot is needed for adding bootoption	-	None
I) already added bootoption %s	%s setup operation executed result. It is displayed only once after setup operation.	None

[Other Problems]

Problem	Recovery
Paused at the EFI Shell during reboot.	1. Change the boot order of "EFI Shell [Built-in]" from top to bottom with the "Boot Option Maintenance Menu" on the EFI Menu. 2. Select OS Boot Option to boot the OS. See [NOTE] to isolate the cause.

8.11 Get Firmware Information Command (getfwinfo)

The getfwinfo command collects the model name and serial number of the cabinet, and the firmware version numbers, and then outputs the information collected to a text-format file. Firmware information is collected from all BB MMBs mounted in the cabinet.

Remarks: Executing this command requires root or Administrator privilege.

(1) Synopsis

- Linux

```
/opt/FJSVpsa/sh/getfwinfo  {output_filename}
```

{output_filename} specifies the name of the output file.

- Windows

```
> getfwinfo  {output_filename}
```

{output_filename} specifies the name of the output file.

(2) Options

None

(3) Examples

- Linux

The command below outputs firmware information to the /tmp/fwinfo.txt file.

```
#/opt/FJSVpsa/sh/getfwinfo  /tmp/fwinfo.txt
```

- Windows

The command below outputs firmware information to the C:\tmp\fwinfo.txt file.

```
> getfwinfo  C:\tmp\fwinfo.txt
```

(4) Output file format

The firmware information on mounted BB and MMBs is output in the following format:

```
- Date -
2007/11/13 10:54:38

- Machine Info -
Part Number  =MC2B0R211
Serial Number=xxxxxxxxxxxx
                yyyyyyyyyyyy

- Firmware Version Info -
PAL_A/B = 1.27/2.20
SAL_A/B = 2.13/2.13
BMC     = 1.27
EFI     = 1.10.1.13
MMB     = 1.33
```

Date of command execution

Model name

Serial number
("yyyyyyyyyyyy" is output only when a serial number for the European market is set.)

PAL/SAL firmware version number

BMC firmware version number

EFI version number

MMB firmware version number

(5) Exit status

0: Normal end

1: Abnormal end

One of the following messages is displayed if the command ends abnormally:

Table 8.4 Get firmware information command (getfwinfo) messages

Message	Meaning	Response
No filename	Output file is not specified.	Specify an output file.
Open failed : *filename*	Creation of specified output file failed.	The full path name of the output file is invalid or a file with the same name as the specified file name is found. Change the full path name of the output file and retry the command.
firmver internal error	An internal processing error occurred.	Retry the command. If this message is displayed again, contact a Fujitsu certified service engineer.
IPMI driver open error	Access to the IPMI driver failed.	
IPMI access failed	Information collection by IPMI failed.	
Machine type is unknown	Machine type identification failed.	Contact a Fujitsu certified service engineer.

(6) Notes

- If PSA and SNMP are stopped when this command is executed, the command displays the message below without the model name and serial number output. However, the command continues processing to collect firmware version numbers.
  Message displayed: SNMP access failed

Part V EFI

CHAPTER 9 EFI Overview

Figure 9.1 outlines the PRIMEQUEST extensible firmware interface (EFI) of firmware that boots the operating system (OS).

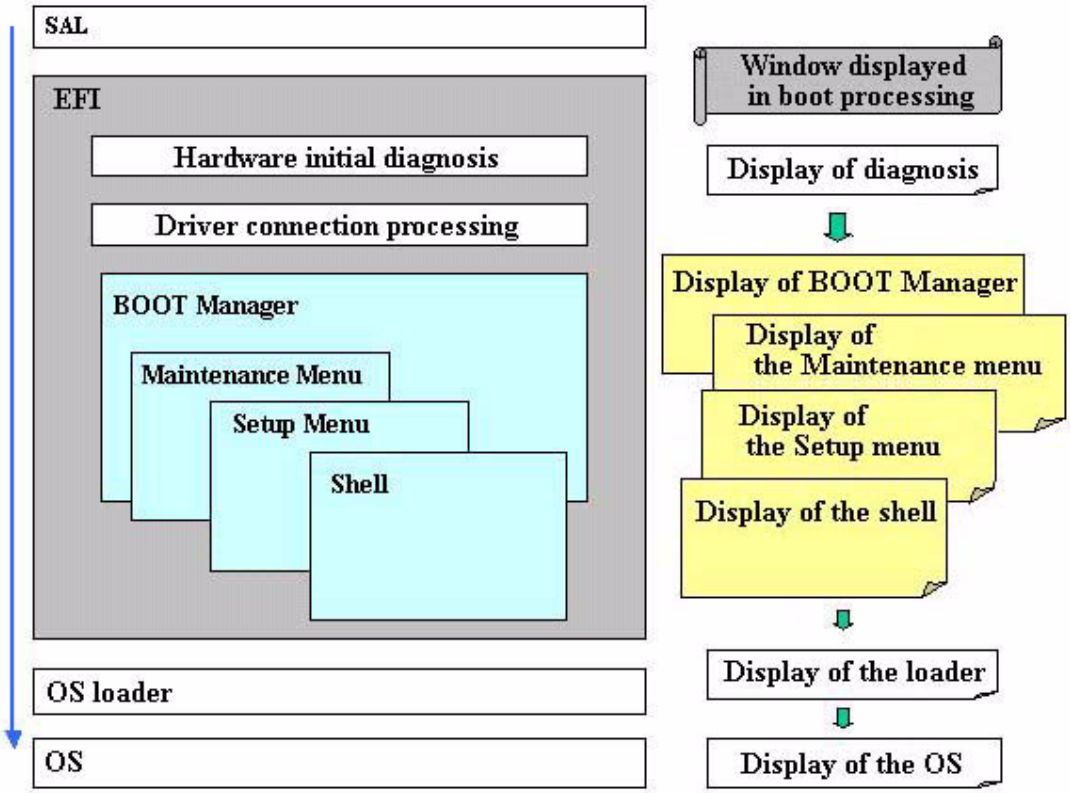


Figure 9.1 EFI outline

The main PRIMEQUEST EFI (hereafter called EFI) functions include the following:

- Supports boot processing of the OS loader
- Supports control of booted devices
- Supports console functions
- Supports EFI application execution prior to the OS boot

SAL expands EFI in memory for operation.

9.1 Boot Function

The EFI loads the different types of EFI drivers required for boot processing and, initialize those drivers.

EFI Boot Manager (hereafter called "Boot Manager") automatically executes boot processing according to preset boot information.

This boot information is set in advance by the installer and stored in the NVRAM variables of the EFI.

9.1.1 NVRAM variables for boot control

This section describes the NVRAM variables that control boot processing.

(1) Boot#### variable

Information about the OS loader booted by Boot Manager is stored in this variable.

The information is stored in the EFI_LOAD_OPTION format as shown below. The #### part of the variable represents a displayable string of hexadecimal numbers ranging from 0000 to FFFF.

```
EFI_LOAD_OPTION Descriptor
    UINT32            Attributes ;
    UINT16            FilePathListLength ;
    CHAR16            Description[] ;
    EFI_DEVICE_PATH   FilePathList[] ;
    UINT8             OptionalData [] ;
```

(2) Driver#### variable

Information about the drivers loaded immediately before booting by Boot Manager is stored in this variable. The information is stored in the EFI_LOAD_OPTION format as shown above. The #### part of the variable represents a displayable string of hexadecimal numbers ranging from 0000 to FFFF.

(3) BootOrder variable

This variable specifies the actual boot sequence of the target programs specified by the Boot#### variable.

(4) DriverOrder variable

This variable specifies the actual loading sequence of the target drivers specified by the Driver#### variable.

(5) BootNext variable

This variable specifies the Boot#### variable used for booting by Boot Manager in the next boot processing. Boot Manager clears the BootNext variable before control is passed to the boot target specified by the variable. If Boot Manager fails to boot the specified target boot program, boot processing continues according to the BootOrder variable.

9.1.2 Boot processing order

If the BootNext variable is not found, Boot Manager selects Boot#### variables in the order specified by the BootOrder variable to execute boot processing.

If boot processing fails for any of the following reasons, Boot Manager continues processing with the next Boot#### variable specified in the BootOrder variable:

1. The device or file specified by the Boot#### variable does not exist.
2. A CD-ROM/DVD device is specified as the boot target, but it contains no media.
3. PXE boot is specified, but a cable is disconnected.
4. PXE boot is specified, but the PXE server is not configured.
5. A hard disk device is specified, but it contains no EFI partition.
6. A CD-ROM/DVD device is specified, but it contains no EFI partition.
7. A virtual floppy disk device is specified, but it contains no EFI partition.
8. The file specified as the boot target fails during read processing.
9. The file specified as the boot target is not in the EFI executable format.
10. The Linux kernel does not exist.
11. elilo is forcibly terminated during startup, such as because of [ESC] key input.

Remarks: If an error occurs after control is passed to the OS loader, the boot target is not switched and reset processing is executed using timer monitoring.

9.1.3 Controlling auto-boot processing

By default, Boot Manager executes OS boot processing immediately during power-on boot processing. If no OS is installed, the EFI shell is started.

However, you can interrupt the boot processing and display the Boot Manager menu as follows:

(1) Displaying the Boot Manager menu by making a setting from the MMB Web-UI

Auto-boot can be temporarily cancelled with an MMB Web-UI operation. For details, see Section 10.1, "Starting Boot Manager."

(2) Displaying the Boot Manager menu by changing the Timeout value in an NVRAM variable.

You can use the Timeout value in an NVRAM variable to specify the wait time for boot processing. Specify a period ranging from 1 and 65534 seconds for Timeout. Boot processing is suspended and the Boot Manager menu is displayed during the specified period. The default value is 0.

If a value other than 0 is specified for Timeout and a key is pressed for input during the wait time, auto-boot processing resumes.

For details, see Section 10.3.5, "[Set Auto Boot Timeout] window."

CHAPTER 10 Boot Manager

Boot Manager allows you to configure selected OS automatic booting, start the EFI shell, specify or modify the automatic boot sequence, and display or modify the SCSI driver configuration.

10.1 Starting Boot Manager

By default, the PRIMEQUEST machine immediately starts its OS without displaying the Boot Manager menu.

To display the Boot Manager menu for making various settings, follow the procedure below.

1. From the MMB Web-UI menu, click [System] → [Boot Control]. [Boot Control] window appears.
2. Select [Force boot into EFI Boot Manager] from [Boot Selector], and click the [Apply] button.
3. Turn on the power to the system. Boot Manager starts after EFI starts. The Boot Manager menu window shown in Figure 10.1 appears on the console.

10.2 Boot Manager Menu

The Boot Manager menu displays the boot options specified in Boot#### variables in the order specified by the BootOrder variable. Auto-boot processing is executed in the order of priority specified with this variable.

Also, you can use key input with the Boot Manager menu to select and start any boot option regardless of the BootOrder values.

When installing an OS, the installer adds the OS boot options, which can also be selected from the Boot Manager menu.

```
EFI Boot Manager ver 1.10 [x.x]

Please select a boot option

    EFI Shell [Built-in]
    DVD/Acpi(PNP0A03,0)/Pci(1D|1)/Usb(0, 0)/Usb(1,0)
    Network/Acpi(PNP0A03,0)/Pci(1E|0)/Pci(8|0)/Mac(000B56E004F)
    Boot Option Maintenance Menu
    Setup Menu





    Use ↑ and ↓ to change option(s). Use Enter to select an option
```

Figure 10.1 Example of the displayed [Boot Manager Menu] window

The table below describes the items displayed in the window shown in Figure 10.1.

Table 10.1 Display items in the [Boot Manager Menu] window

Item	Description
EFI Shell [Built-in]	Starts the EFI shell.
DVD/Acpi (PNP0A03,0)/	Performs booting from a DVD-ROM or CD-ROM.
Floppy/Acpi (PNP0A03,0)/	Performs booting from a floppy disk.

Item	Description
Network/Acpi (PNP0A03,0)/	Performs network booting.
Boot Option Maintenance Menu	Displays the [Boot Option Maintenance Menu], which can be used to add and delete Boot#### variables and change boot priorities with the BootOrder variable.
Setup Menu	Displays the [EFI Setup Menu], which can be used to display and change the SCSI driver configuration.

(1) Menu operation

[System] → [Boot Control] → [Force boot into EFI Boot Manager]

(2) Window operation

Boot Manager allows you to use the keys listed in the table below, for example, to select items.

Table 10.2 Keys used for Boot Manager operation

Key	Description
↑ ↓	Moves the cursor up or down. The [^] key can also be used as the up arrow key and the [v] or [V] key can also be used as the down arrow key.
← →	Moves the cursor to the left or right. The [←] key can also be used as the left arrow key and the [→] key can also be used as the right arrow key.
PageUp / PageDown	Displays the previous or next screen.
Home / End	Moves the cursor to the top or bottom item on the screen.
Enter	Makes the current item selection effective.

Remarks: Note that this table does not apply to the SCSI Configuration Utility, which is invoked from the [Setup] menu. For details, see the key operation descriptions displayed in the window or Help.

10.3 Boot Option Maintenance Menu

The Boot Option Maintenance menu allows you to directly perform a boot from a specified boot file, add or delete boot options (Boot#### variable of NVRAM variables), or change the boot sequence (BootOrder variable).

```
Boot Option Maintenance Menu

Main Menu. Select an Operation


        Boot From a File
        Add a Boot Option
        Delete Boot Option(s)
        Change Boot Order
        Set Auto Boot Timeout

        Reset System
        Exit
```

Figure 10.2 Example of the displayed [Boot Option Maintenance Menu (Main Menu)] window

Table 10.3 Outline of functions available in the [Boot Option Maintenance Menu (Main Menu)] window

Function	Description
Boot From a File	Performs a boot from a specified file.
Add a Boot Option	Adds a new boot option.
Delete Boot Option(s)	Deletes the specified boot option(s).
Change Boot Order	Changes boot priorities and reflect the changes to the BootOrder variable.
Set Auto Boot Timeout	Specifies the input wait time in seconds that may elapse after Boot Manager displays its menu during auto-boot processing.
Reset System	Resets the system.
Exit	Used to return to the [Boot Manager Menu] window.

(1) Menu operation

Select [Boot Manager] → [Boot Option Maintenance Menu].

(2) Window operation

1 Select the item to execute by moving the cursor up or down.
2 Press the [Enter] key.

10.3.1 [Boot From a File] window

This window allows you to perform a boot by directly specifying the boot file contained in a device.

```
Boot Option Maintenance Menu

Boot From a File.  Select a Volume


   NO_VOLUME_LABEL [Acpi(PNP0A03,0)/Pci(1|1)/Pci(0|2)/Pci(1|0)/Scsi
   Removable Media Boot [Acpi(PNP0A03,0)/Pci(1D|1)/Usb(0, 0)/Usb(1,
   Load File [Acpi(PNP0A03,0)/Pci(1E|0)/Pci(8|0)/Mac(000B5D6E004F)]
   Load File [EFI Shell [Built-in]]
   Exit
```

Figure 10.3 Example of the displayed [Boot From a File] window

(1) Menu operation

Select [Boot Manager] → [Boot Option Maintenance Menu] → [Boot From a File].

(2) Window operation

1 Select a device from the displayed device list, and then select a boot file. Selecting [Exit] closes the [Boot From a File] window.
2 Press the [Enter] key.

10.3.2 [Add a Boot Option] window

This window allows you to add new boot options. Boot options comprise information stored in Boot#### variables, including the device path and OS loader information and the boot information to be passed to the OS loader.

```
Boot Option Maintenance Menu

Add a Boot Option. Select a Volume


   NO_VOLUME_LABEL[Acpi(PNP0A03,0)/Pci(1|1)/Pci(0|2)/Pci(1|0)/Scsi
   RemovableMediaBoot[Acpi(PNP0A03,0)/Pci(1D|1)/Usb(0,0)/Usb(1,
   LoadFile[Acpi(PNP0A03,0)/Pci(1E|0)/Pci(8|0)/Mac(00B5D6E004F)]
   LoadFile[EFI Shell[Built-in]]
   Exit
```

Figure 10.4 Example of the displayed [Add a Boot Option] window

(1) Menu operation

Select [Boot Manager] → [Boot Option Maintenance Menu] → [Add a Boot Option].

(2) Window operation

1. Select a device from the displayed device list, and then select a boot file.
2. Specify the following items:

   [Enter New Description:]

   Enter a boot option description that will be displayed in the Boot Manager menu.

   [Enter BootOption Data Type:]

   If an optional parameter needs to be passed to the OS loader, press the [a] (Ascii) or [u] (Unicode) key. If no optional parameter is required, press the [n] key.
3. If necessary, specify optional parameters after [Enter BootOption Data:].
4. For Save [Y-Yes N-No]:, press the [y] key.

(3) Example

An example is provided below.

Enter New Description: Linux Boot

Enter BootOption Data Type: Unicode

Enter BootOption Data: elilo mylinux 3

Save [Y-Yes N-No]: y

This example shows the booting of OS (Linux) in run level 3 with mylinux specified in the label in elilo.conf.

Figure 10.5 shows a sample boot file and Figure 10.6 shows a boot option setting example.

```
prompt
timeout=20
default=linux
relocatable

image=vmlinuz-2.6.9-1.648_EL
        label=linux
        initrd=initrd-2.6.9-1.648_EL.img
        read-only
        root=/dev/VolGroup00/LogVol00

image=vmlinuz-2.6.9-1.648_EL-test
        label=mylinux
        initrd=initrd-2.6.9-1.648_EL.img
        read-only
        root=/dev/VolGroup00/LogVol00
```

Figure 10.5 Sample boot file (elilo.conf)

```
   Filename: \EFI\redhat\elilo.efi
 DevicePath:[Acpi(PNP0A03,1)/Pci(1F|0)/Pci(2|0)/Scsi(Pun1,Lun0)/HD
(Part1,SigA478626A-9672-449A-A86B-2BC3F4CAD9E2)/\EFI\redhat\elilo.efi]
   IA-64 EFI Application 06/16/04  12:05a    345,564 bytes


   Enter New Description:  Linux Boot
   New BootOption Data. ASCII/Unicode strings only, with max of 240 characters

   Enter BootOption Data Type [A-Ascii U-Unicode N-No BootOption] :  Unicode

   Enter BootOption Data [Data will be stored as Unicode string]:
 elilo mylinux 3



   Save [Y-Yes N-No]:
```

Figure 10.6 Boot option setting example

When, in this example, you select [Exit] from the [Boot Option Maintenance Menu] after setting boot options, an item named "Linux Boot" is added to the [Boot Manager Menu] window, as shown in Figure 10.7.

If this [Linux Boot] is selected, Linux is started in run level 3.

```
EFI Boot Manager ver 1.10 [x.x]

Please select a boot option

    EFI Shell [Built-in]
    DVD/Acpi(PNP0A03,0)/Pci(1D|1)/Usb(0,0)/Usb(1,0)
    Network/Acpi(PNP0A03,0)/Pci(1E|0)/Pci(8|0)/Mac(000B56E004F)
    Linux Boot
    Boot Option Maintenance Menu
    Setup Menu





    Use ↑ and ↓ to change option(s). Use Enter to select an option
```

Figure 10.7 Boot Manager menu as it is displayed after a boot option is added

10.3.3 [Delete Boot Option(s)] window

This window allows you to delete one or more specified boot options.

```
Boot Option Maintenance Menu

Delete Boot Option(s).  Select an Option


    EFI Shell [Built-in]
    DVD/Acpi(PNP0A03,0)/Pci(1D|0)/Usb(0, 0)
    Floppy/Acpi(PNP0A03,0)/Pci(1F|0)/Acpi(PNP0604,0)
    Network/Acpi(PNP0A03,0)/Pci(1|1)/Pci(0|0)/Pci(1|0)/Mac(0007E9246
Delete All Boot Options
    Save
    Help
    Exit

    VenHw(D65A6B8C-71E5-4DF0-A909-F0D2992B5AA9)
    BootFFFE
```

Figure 10.8 Example of the displayed [Delete Boot Option(s)] window

Table 10.4 Functions of submenus available in the Delete Boot Option(s) window

Submenu	Description
Delete All Boot Options	Displays the message shown below. Delete ALL of above Boot Options [Y-Yes N-No]: Pressing the [y] or [Y] key deletes all boot options. Pressing the [n] or [N] key cancels the deletion operation.
Save	Saves the configuration after the deletion.
Help	Displays help information on the [Delete Boot Option(s)] window.
Exit	Closes the [Delete Boot Option(s)] window. If you deleted one or more boot options, but did not execute [Save], the following confirmation message appears: Save? [Y to save, N to ignore] If you press the [y] or [Y] key, the settings are saved and then the window closes. If you press the [n] or [N] key, the new settings are discarded and the window closes.

Not only the basic keys listed in Table 10.2, "Keys used for Boot Manager operation," but also the keys listed in Table 10.5 below can be used in the [Change Boot Order] window.

Table 10.5 Keys used for operation on the [Delete Boot Option(s)] window

Key	Description
d	When the [d] or [D] key is pressed for input, the following message is displayed: Delete selected Boot Option [Y-Yes N-No]: Pressing the [y] or [Y] key deletes the selected boot options. Pressing the [n] or [N] key cancels deletion.
a	When the [a] or [A] key is pressed for input, the following message is displayed: Delete ALL of above Boot Options [Y-Yes N-No]: Pressing the [y] or [Y] key deletes all boot options. Pressing the [n] or [N] key cancels deletion.

(1) Menu operation

Select [Boot Manager] → [Boot Option Maintenance Menu] → [Delete Boot Option(s)].

(2) Window operation

1. Select the boot option(s) you want to delete.
   The question "Delete selected Boot Option [Y-Yes N-No]:" appears.
2. When you press the [y] key, the selected boot option(s) are deleted.
3. Select [Save] and press the [Enter] key.
4. Select [Exit] and press the [Enter] key to close the [Delete Boot Option(s)] window.

Remarks: To delete all options at the same time, press the [a] key.
Press the [y] key as input for "Delete All of above Boot Options[Y-Yes N-No]." All the boot options are then deleted.

10.3.4 [Change Boot Order] window

The [Change Boot Order] window lists boot options, with the highest-priority options displayed first. The window is used to change the displayed order of the options.

```
Boot Option Maintenance Menu

Change Boot Order.  Select an Operation

    EFI Shell [Built-in]
    DVD/Acpi(PNP0A03,0)/Pci(1D|0)/Usb(0, 0)
    Floppy/Acpi(PNP0A03,0)/Pci(1F|0)/Acpi(PNP0604,0)
    Network/Acpi(PNP0A03,0)/Pci(1|1)/Pci(0|0)/Pci(1|0)/Mac(0007E9246
    Save
    Help
    Exit

    VenHw(D65A6B8C-71E5-4DF0-A909-F0D2992B5AA9)
    BootFFFE
```

Figure 10.9 Example of the displayed [Change Boot Order] window

Table 10.6 Functions of submenus available in the [Change Boot Order] window

Submenu	Description
Save	Saves the settings.
Help	Displays help information on the [Change Boot Order] window.
Exit	Closes the [Change Boot Order] window. If you deleted one or more boot options, but did not execute [Save], the following confirmation message appears: Save? [Y to save, N to ignore] If you press the [y] or [Y] key, the settings are saved and then the window closes. If you press the [n] or [N] key, the new settings are discarded and the window closes.

Not only the basic keys listed in Table 10.2, "Keys used for Boot Manager operation," but also the keys listed in Table 10.7 below can be used in the [Change Boot Order] window.

Table 10.7 Keys used for operation on the [Change Boot Order] window

Key	Description
u	Raises the priority of the boot option one level.
d	Lowers the priority of the boot option one level.

(1) Menu operation

Select [Boot Manager] → [Boot Option Maintenance Menu] → [Change Boot Order].

A window like Figure 10.9 appears. This window displays boot options based on the boot sequence.

(2) Window operation

1. Select one or more boot options whose priority in the boot sequence should be changed.
2. Press the [u] or [d] keys to change the boot sequence of the boot options.
3. Select [Save] and press the [Enter] key to save the settings.
4. Select [Exit] to close the [Change Boot Order] window.

10.3.5 [Set Auto Boot Timeout] window

If you want the system to display the Boot Manager menu and wait for input instead of immediately booting the OS, use this menu to specify the wait time.

```
Boot Option Maintenance Menu

Set Auto Boot Timeout. Select an Option


    Set Timeout Value
    Disable Timeout
    Help
    Exit
```

Figure 10.10 Example of the displayed [Set Auto Boot Timeout] window

Table 10.8 Functions of submenus available in the [Set Auto Boot Timeout] window

Submenu	Description
Set Timeout Value	Specifies the input wait time that may elapse after Boot Manager displays its menu.
Disable Timeout	Displays the [Boot Manager Menu] window instead of performing automatic boot processing.
Help	Displays help information on the [Set Auto Boot Timeout] window.
Exit	Closes the [Set Auto Boot Timeout] window.

(1) Menu operation

Select [Boot Manager] → [Boot Option Maintenance Menu] → [Set Auto Boot Timeout].

A window like Figure 10.10 appears.

(2) Window operation

1 Use the following submenu to specify a timeout value.
Set Timeout Value: Specify a value of time in seconds that may elapse before booting starts (0 <= N <= 65534). The default is 0.
Disable Timeout: Select this item if you want the system to display the [Boot Manager] menu and wait for input instead of performing automatic boot processing.

2 Select [Exit] and press the [Enter] key to close the [Set Auto Boot Timeout] window.

10.3.6 Reset System

This window allows you to reset the system.

(1) Menu operation

Select [Boot Manager] → [Boot Option Maintenance Menu] → [Reset System].

The [Boot Option Maintenance Menu] closes and the system is reset.

10.3.7 Exit

This window allows you to return to the [Boot Manager] menu.

(1) Menu operation

Select [Boot Manager] → [Boot Option Maintenance Menu] → [Exit].

The [Boot Option Maintenance] menu closes and the [Boot Manager] menu returns.

10.4 EFI Setup Menu

The EFI Setup Menu allows you to start an EFI driver configuration tool and set up the USB keyboard.

```
                              EFI Setup Menu
    *[EFI Configuration Utility]  [Keyboard]  [Exit]

    Invokes the driver configuration tool.
```

Figure 10.11 EFI Setup Menu as it is displayed immediately after startup

Table 10.9 Functions of the EFI Setup Menu

Item	Description
EFI Configuration Utility	Starts the EFI driver configuration tool. You can choose the SCSI configuration tool in on-board mode.
Keyboard	Specifies the USB keyboard to be used in the preboot environment.
Exit	Used to return to the Boot Manager menu window.

(1) Menu operation

Select [Boot Manager] → [Setup Menu].

A window like Figure 10.11 appears.

(2) Window operation

1 Select the desired item by moving the cursor to the left or right.
2 Press the [Enter] key.

10.4.1 [EFI Configuration Utility] window

This window allows you to start the EFI driver configuration tool.

Remarks: The controllers listed in the [EFI Configuration Utility] window are limited to those whose configuration utilities are implemented by the corresponding EFI drivers. An EFI driver configuration utility can be invoked by selecting the corresponding controller in this window.
Some EFI drivers do not have a configuration utility, and the operation of a configuration utility varies depending on the specifications of the EFI driver. For details, see the driver specifications.
If a configuration utility is provided separately as an EFI application, use it to configure the controller.

```
                              EFI Setup Menu
 [EFI Configuration Utility]  [Keyboard]  [Exit]

                        EFI Configuration Utility

    *[S#00:B#83: D#01:F#0]  Acpi(PNP0A03,0)/Pci(9|1)/Pci(0|0)/Pci(1|0)
     [S#00:B#83: D#01:F#1]  Acpi(PNP0A03,0)/Pci(9|1)/Pci(0|0)/Pci(1|1)
     [S#00:B#84:D#01:F#0]  LSI Logic Ultra320 SCSI Controller
     [S#00:B#84:D#01:F#1]  LSI Logic Ultra320 SCSI Controller
     [S#00:B#86:D#01:F#0]  Acpi(PNP0A03,0)/Pci(A|1)/Pci(0|0)/Pci(1|0)
     [S#00:B#86:D#01:F#1]  Acpi(PNP0A03,0)/Pci(A|1)/Pci(0|0)/Pci(1|1)
     [S#00:B#87:D#01:F#0]  LSI Logic Ultra320 SCSI Controller
     [S#00:B#87:D#01:F#1]  LSI Logic Ultra320 SCSI Controller

Esc=Exit
S=PCI Segment  B=PCI Bus  D=PCI Device  F=PCI Function
```

Figure 10.12 Example of the displayed [EFI Configuration Utility] window

Table 10.10 Symbols displayed for the [EFI Configuration Utility] window

Symbol	Description
S#n	PCI segment number.
B#n	PCI bus number
D#n	PCI device number
F#n	PCI function number

(1) Menu operation

[Boot Manager] → [Setup Menu] → [EFI Configuration Utility].

(2) Window operation

1 Select the item you want to reconfigure.
The configuration tool corresponding to the selected item starts.

2 Make the necessary configuration changes, and then press the [Esc] key to exit from the [EFI Configuration Utility] window.

10.4.2 [Keyboard] window

This window allows you to specify the USB keyboard type to be used in the preboot environment.

```
                              EFI Setup Menu
   [EFI Configuration Utility]  [Keyboard]  [Exit]

                                 Keyboard

       * Auto setting                <*>
         Specific setting JP         < >
                          US         < >

 S=Save  Esc=Exit
```

Figure 10.13 Example of the displayed [Keyboard] window

Table 10.11 Items displayed in the [Keyboard] window

Item	Description
Auto setting	Automatically determines the keyboard type by obtaining the country information for the connected keyboard. Use this item only when you are sure that the keyboard can transmit appropriate country information to the system.
Specific setting	Explicitly specifies a keyboard type. Use this item when the keyboard cannot transmit appropriate country information to the system.

(1) Menu operation

[Boot Manager] → [Setup Menu] → [Keyboard].

(2) Window operation

1 Select the item to change the keyboard configuration. For information on the meaning of each item, see Table 10.11.
2 Press the [s] or [S] key to save the settings.
3 Press the [Esc] key to close the [Keyboard] window.

CHAPTER 11 EFI Shell and EFI Commands

The PRIMEQUEST EFI supports the EFI shell function, which enables commands to be executed from a console.

11.1 Auto-startup File

After being started, the EFI shell first checks for the startup.nsh file in the specified execution path.

If the file is found, the commands written in the file are executed before a wait for input from the console. The startup.nsh file is optional.

Remarks: The execution path is the directory path specified in the path variable of a shell environment variable.
The directory path can be displayed and changed by the set command.

11.2 EFI Shell Command Syntax

Shell environment variables can be specified and referenced with the set command.

As shown below, the environment variable name must be enclosed between the % characters for access when it is used as an argument to a shell command:

%myvariable%

The shell has a special variable called lasterror. This variable retains the return value of the shell command executed last.

The "*", "?", "[", and "]" characters are handled as wildcard characters in a file name used as an argument to a shell command.

Table 11.1 Wildcards

String	Explanation
"*"	Represents zero or more characters in a file name.
"?"	Represents exactly one character in a file name.
"[" string "]"	Represents any one character between [and]. Example: [a-zA-Z]

11.3 Output Redirection

Output of an EFI shell command can be redirected to a file. The syntax of the redirection is as follows:

Command > unicode_output_file_pathname
Command >a ascii_output_file_pathname
Command 1> unicode_output_file_pathname
Command 1>a ascii_output_file_pathname
Command 2> unicode_output_file_pathname
Command 2>a ascii_output_file_pathname
Command >> unicode_output_file_pathname
Command >>a ascii_output_file_pathname
Command 1>> unicode_output_file_pathname
Command 1>>a ascii_output_file_pathname

Table 11.2 lists the character strings used to indicate a redirect or append operation.

Table 11.2 Special strings

String	Explanation
">"	Redirects the standard output to a Unicode file.
">a"	Redirects the standard output to an ASCII file.
"1>"	Redirects the standard output to a Unicode file.
"1>a"	Redirects the standard output to an ASCII file.
"2>"	Redirects the standard error output to a Unicode file.
"2>a"	Redirects the standard error output to an ASCII file.
">>"	Appends the standard output to a Unicode file.
">>a"	Appends the standard output to an ASCII file.
"1>>"	Appends the standard output to a Unicode file.
"1>>a"	Appends the standard output to an ASCII file.

The shell can redirect the standard output or standard error output to a single file.

Remarks: The standard output and the standard error output cannot both be redirected to the same file. Redirection to multiple files at the same time is not possible.

11.4 Batch Script

The EFI shell can execute commands from batch script files as follows:

- The batch script files use the ".nsh" extension.
- The batch script files are created as Unicode files or ASCII files.
- The batch scripts support the positional argument, which can be used to reference each argument by a number, as in %n (n=0 to 9).
  %0 indicates the script file currently being executed.
- The display during execution of a command from a batch script is echoed on the console.
- The echo –off command is used to disable display of a command read from a batch file.
- The shell does not save information on execution of a command from a batch script.
- The history save function used with cursor keys is not supported.
- If a command error occurs in a batch script, processing is continued by default.
- A batch script can test the results from the last command executed by using the if command with the lasterror shell variable specified.
- A line in a batch script can be commented out by inserting the "#" character.

Glossary

ACS (AC Section)

AC power input section

ASIC (Application Specific Integrated Circuit)

Integrated circuit (IC) designed and manufactured for specific applications

API (Application Program Interface)

A set of instructions and functions used for developing operating systems and middleware

BB (Baseboard)

Unit on which CPUs, memories, and various chipsets are mounted

BIOS (Basic Input Output System)

Part of the operating system (OS) function. The BIOS is the system that controls input/output to devices. For the PRIMEQUEST-series machine, BIOS is a general term for PAL, SAL, and EFI.

BMC (Baseboard Management Controller)

The BMC is a system management controller that continuously monitors the system for serious hardware errors and notifies the OS of such errors.

BMM (BMC Module)

Board on which legacy I/O ports such as BMC, VGA, USB, and COM ports are mounted

BP (Backplane)

The backplane is connected to SBs, IO Units, and other devices. It constitutes the memory and I/O interconnect (crossbar).

Business LAN

LAN used to configure a user business system

CLI (Command Line Interface)

This interface with UNIX or DOS allows the user to enter commands and optional arguments to communicate with the OS.

CoA

Abbreviation for Certificate of Authenticity. This is a visual identifier that helps identify genuine Microsoft software and components.

COM Port (Communication Port)

RS-232C serial port for PC/AT compatible machines. A COM port is also called an "RS-232C port." Most PC/AT compatible machines each have two COM ports, which are often used to connect a modem, terminal adapter, or scanner. Most of these ports use D-Sub 25-pin or D-Sub 9-pin connectors.

DDR2 (Double Data Rate 2)

Standards for the next generation of memory that operates at higher speeds and consumes less power than conventional DDR memory

DIMM (Dual Inline Memory Module)

This compact memory module has pins on both sides and is mainly used in notebook PCs.

DVD-ROM (Digital Versatile Disc-Read-Only Memory)

Digital format for high-volume storage of data on optical disks

ECC (Error Checking Correction)

Error correction code or a method of using the error correction code to check for and correct errors

EFI (Extensible Firmware Interface)

Specifications for an interface between an OS and firmware. Instead of the BIOS, EFI is used for hardware control.

FC (Fibre Channel)

One of the serial interface standards. The Fibre Channel standard uses fiber cables as the transmission medium.

Firmware

Built-in software for basic hardware control

FWH (Firmware Hub)

LSI device from Intel Corporation. FWH is flash memory that stores SAL (BIOS). The PRIMEQUEST-series machine uses two types of FWH: one type is mounted on an SB and the other is mounted in an IO Unit.

GAC (Global Address Controller)

One of the ASICs developed by Fujitsu for the PRIMEQUEST-series machine

GbE (Gigabit Ethernet)

Ethernet standards for high-speed communication of up to 1 Gbps

GDS

Abbreviation for PRIMECLUSTER GDS

GDX (Global Data Xbar)

One of the ASICs developed by Fujitsu for the PRIMEQUEST-series machine

GLS

Abbreviation for PRIMECLUSTER GLS

HBA

Abbreviation for a host bus adapter

HDD (Hard Disk Drive)

Device that reads a hard disk. HDD may also be an abbreviation for the hard disk itself.

Hot Plug

Method of replacing components while power is on

HTTP (Hypertext Transfer Protocol)

Protocol used by Web servers and clients for data transmission

I2C (Inter Integrated Circuit)

Protocol used for high-speed communication between integrated circuits (ICs)

IA (Intel Architecture)

Generic term for the basic design (architecture) of Intel's microprocessors

IFT (Instruction Fetch)

Mechanism for reading instructions stored in memory

IHV (Independent Hardware Vendor)

This hardware provider has no special relationship with a particular hardware or OS maker.

IP address (Internet Protocol Address)

Identification number assigned to each computer connected to an IP network, such as the Internet and intranets

IPMI (Intelligent Platform Management Interface)

Standardized interface specifications established so that SNMP and server management software can monitor server hardware independently of specific hardware systems and OSs

ISV (Independent Software Vendor)

This application software provider has no special relationship with a particular hardware or OS maker.

LAN (Local Area Network)

Using optical fiber, for example, this network allows data to be transferred among computers and printers connected in a facility.

LDAP (Lightweight Directory Access Protocol)

Protocol used to access directory databases in a TCP/IP network, such as the Internet and intranets

LDX (Local Data Xbar)

One of the ASICs developed by Fujitsu for the PRIMEQUEST-series machine

LED

Abbreviation for a light emitting diode

MAC address (Media Access Control Address)

Unique address assigned to each network interface device, switch, or router mounted on a network interface card (NIC) or motherboard

Management LAN

This LAN connects the MMB to the system on the BB and to LANs outside the cabinet so that the PRIMEQUEST system can be managed.

MIB (Management Information Base)

Information released by a network device managed by SNMP in order to post the device status to an external destination

Middleware

Software that runs under an OS and provides application software with more advanced and detailed functions than the OS. It is positioned between the OS and application software in terms of its characteristics.

MMB (Management Board)

This server management board is a system control unit whose tasks include control and monitoring of cabinet hardware, and system initialization.

NIC (Network Interface Controller)

Hardware that supports network functions

NTP (Network Time Protocol)

Standard time information protocol used on the Internet. Highly precise time information with consideration of line speeds and load changes in paths can be obtained with this protocol.

PAL (Physical Abstract Layer)

Firmware that provides platform initialization and operating system boot functions

PCI Hot Plug

Technology that enables PCI cards to be mounted and removed while the system is operating

PCI (Peripheral Component Interconnect)

Bus architecture established by PCI SIG for connecting PC components

Platform

OS type or environment that is the basis for operation of application software

POST (Power-On Self Test)

Hardware test that is automatically run when the computer is powered on

Private LAN

LAN used for internal control, under which firmware programs installed on hardware components communicate with one another. MMB firmware, and BMC firmware installed on IO Units can use a private LAN for communication with one another. OSs and applications cannot use a private LAN.

PSA (PRIMEQUEST Server Agent)

Software that performs hardware error monitoring and configuration management over PRIMEQUEST

PSU (Power Supply Unit)

Component that converts AC voltage to DC voltage as a DC power supply

PXE

PXE (Preboot eXecution Environment) Network boot standard based on BIOS technology that enables remote operation of management tasks such as system start and OS installation/update

RAID (Redundant Array of Independent Disks)

Technology that increases reliability and processing speeds by using multiple hard disks as a single disk

REMCS (Remote Customer Support System)

Fujitsu's remote customer support service

RHEL (Red Hat Enterprise Linux)

Linux distribution released by Red Hat, Inc.

SAF-TE

Abbreviation for a SCSI accessed fault-tolerant enclosure

SAL (System Abstraction Layer)

Firmware that supports processor initialization and error recovery functions

SAN (Storage Area Network)

Dedicated network for connections between a server and storage devices

SAS (Serial Attached SCSI)

One of SCSI standards. SAS is a serial transmission interface for connecting devices such as hard disks to a computer.

SASBP (SAS Back Plane)

SASBP is used for HDD monitoring and LED on/off control.

SCSI (Small Computer System Interface)

Standards for connections between PCs and peripherals. SCSI was established by the American Standards Association.

SDRAM (Synchronous DRAM)

Memory standard for access speeds that are higher than those of DRAM

SEL (System Event Log)

Information on the processing parameters, processing, and processing results logged during hardware and software operations

SIRMS (Software Product Information Collection for Remote Maintenance Support)

Software that collects configuration information on software installed in PRIMEQUEST

S.M.A.R.T. (Self-Monitoring Analysis Reporting Technology)

Function that enables a hard disk to monitor its own conditions and notify the BIOS of any error detected

SMP (Symmetric Multiple Processor)

Parallel processing system in which all processors work together through common memory resources

SNMP (Simple Network Management Protocol)

TCP/IP-compliant protocol for managing devices in a network

SSL (Secure Sockets Layer)

Protocol under which information is encrypted for transmission. SSL was developed by Netscape Communications Corp.

Systemwalker

One of Fujitsu's middleware products. Systemwalker is integrated operation management software.

Telnet

Protocol or standard method for remote control of computers connected to a TCP/IP network, such as the Internet and intranets

UPS (Uninterruptible Power Supply)

Power supply unit that stores power and protects against possible damage and loss of computer data from a momentary voltage drop or unexpected power failure

USB (Universal Serial Bus)

One of the standards on connecting peripheral devices such as keyboards and mice

VLAN (Virtual LAN)

Function that logically groups the ports of one switching hub so each group works as an independent LAN

Web UI (Web User Interface)

Index

A

access control 4-8, 5-114
Access Control window 5-114
access procedure. 2-9
Add a Boot Option window. 10-6
Add Filter window. 5-116
Add Schedule window 5-56
Add User window. 5-70
Administrator 2-13
agent log 4-28
Agent Log Filtering Condition window 7-50
Agent Log window 7-47
Alarm E-mail Filtering Condition window 5-120
Alarm E-Mail window 5-118
alert message . . . . . v, vii
Apply button. 2-10
ASR Control window 3-12, 3-13, 5-64
automatic partition restart. 3-12
automatic server restart 5-64
auto-startup file 11-1

B

Backup EFI Configuration window 5-133
Backup/Restore Configuration menu 5-131
Backup/Restore MMB Configuration window. 5-131
batch script. 11-4
BMC Firmware Update window 5-129
boot control 9-2
boot control of partition. 3-10
Boot Control window 3-10, 3-11
boot firmware 9-1
Boot From a File window 10-5
boot function 9-2
Boot Manager menu 10-2
Boot Manager, starting. 10-1
Boot Option Maintenance menu 10-4
Bootcfg.exe 3-28
button area. 2-8

C

Cancel button 2-11
CE 2-13
certificate signing request. 5-101, 5-103, 5-104
Change Boot Order window 10-11
Change Password window 5-75
character string input field 2-10
clear access_control 6-2, 6-6
clear ssh_key 6-2, 6-7
CLI. 2-1
CLI command list
  MMB 6-2
  PSA 8-1
CLI operation. 6-1, 8-1
  access through serial interface. 6-1
  access via management LAN interface 6-2
CLI operation, switching with. 2-15
COM port connection 3-19, 3-27
command description format. 1-3
command line interface 2-1
component name and function 3-1
console operation 4-18
console redirection 4-7, 4-18
  buffering of 4-21
console redirection switch 4-19
Console Redirection Switch window. 4-19, 4-20, 5-60
console redirection to Web-UI 4-22
Console Redirection window. 5-62
content display frame 2-3, 2-7
contents of manual i
CPUs window 7-7
Create CSR window 5-101
Create Selfsigned Certificate window 5-106
Create SSH Server Key window 5-108
CSR. 5-103, 5-104
CSR exporting. 5-104

D

Date/Time window. 5-78
Delete Boot Option(s) window. 10-9
DIMMs window 7-8

Disk Partitions window 7-31
diskctrl 8-3
display command 6-19
displaying and using window 2-10
download ssh_key 6-2, 6-8

E

Edit Filter window 5-116
Edit Schedule window 5-58
Edit User window 5-73, 5-112
EFI 9-1
EFI command 11-1
EFI Configuration Utility window 10-16
EFI Firmware Update window 5-127
EFI function 9-1
EFI Setup menu 10-15
EFI shell 11-1
EFI shell command syntax 11-2
electronic certificate 5-105
E-mail 5-118
EMS connection 3-27
environmental requirement for
using product vi
error log 4-28
error message 7-39
error status 2-2
Ethernet Controller window 7-11
event. 5-7, 5-8, 5-9, 5-10
event detail, displaying 4-16
event log, checking. 4-11
event to be displayed, selecting 4-14
Exit 10-14
exit 6-4, 6-35
Expansion File Unit window 7-67, 7-68
Export Key/CSR window 5-104
Export List window 7-54
Export window 7-57

F

factory_default 6-2, 6-6
Fans Status Clear window 5-27
Fans window. 5-25
Fibre Channel window 7-21, 7-22, 7-24
filter definition update
command 8-2, 8-13
filter definition update command
(fltcpy, fltupdate) message 8-16
filtering condition
Agent Log 7-49, 7-50
Alarm Email. 5-120
System Event Log. 5-8
Firmware Information window 5-18
firmware maintenance 4-8
Firmware Update menu 5-122
frame configuration 2-3

G

get firmware information
command 8-43
get firmware information command
(getfwinfo) message. 8-44
get local partition number
command 8-2, 8-18
get serial number command 8-2, 8-20
GUI 4-25

H

Hard Disks window 7-32, 7-33
hardware configuration display 4-6
hardware configuration
management 4-26
hardware error monitoring 4-27
Hardware Inventory window 7-41
hardware monitoring 4-7
help 6-4, 6-29

I

Import Certificate window. 5-105
information frame. 2-3, 2-4
information managed by partition. 4-30
Inventory menu 7-41
IOU#x window 5-45
IP address input field 2-11

K

Keyboard window 10-17

L

LAN connection 3-19
LED 3-31
LEDs window. 5-22
linkage with upper-level operation
management software 4-30
log collection 4-27
log information 4-10

Logout 2-5

M

MAC address input field 2-12
Maintenance menu 5-122
maintenance operation 4-29
maintenance status 2-5
Maintenance Wizard window 5-135
management LAN interface
CLI operation 6-2
Management LAN Port
Configuration window 5-84
menu list
MMB 5-1
PSA 7-3
MMB Firmware Update window 5-122
MMB user environment 4-7
MMB Web-UI (maintenance)
function 4-5
MMB Web-UI (network/security)
function 4-4
MMB Web-UI (system) function 4-1
MMB Web-UI (user) function 4-3
MMB window 5-46

N

navigation bar 2-5
Network Configuration menu 5-78
network environment setting
and change 4-8
Network Interface window 5-81
Network Interfaces window 7-28
Network menu 7-28
Network Protocols window 5-89
Network Routing window 7-30
normal status 2-1
note on safety vii
NVRAM variable 9-2

O

operation management GUI 4-25
Operator 2-13
organization of manual i
OS information display 4-26
other command 6-35
output redirection 11-3

P

PAL/SAL Firmware Update window . . . 5-125
Partition Information window 7-5
passwd 6-36
password 5-70, 5-73, 5-75, 6-4
PCI Devices window 7-9
ping 6-4, 6-37
power control 4-8
Power Control window 3-8, 3-9
partition 5-48
power off 6-2, 6-7
power on 6-2, 6-8
power status 3-17
Power Supply window 3-17, 3-18, 5-23
power-off operation
using CLI 3-16
power-off procedure 3-4
using MMB Web-UI 3-6
power-on operation
using CLI 3-16
power-on procedure 3-3
using MMB Web-UI 3-5
predictive sign 7-64
PRIMECLUSTER linkage 4-29
PRIMEQUEST 510A 3-2
private key 5-101, 5-102, 5-103,
5-104, 5-106, 5-107
private key exporting 5-104
privilege level 2-13
Process List window 7-34
product handling xi
PSA function 4-25
PSA start/stop command 8-2, 8-9
PSA troubleshooting data
collection command 8-2, 8-11
pulldown list 2-10

R

read privilege user 7-3, 7-65
reference manual iii
Refresh 7-2
Refresh Rate window 5-92
REMCS linkage 4-29
remote desktop connection 3-21
remote PC connection 2-1
Remote Server Management
window 5-110
remote shutdown of Windows 3-19

via COM port connection 3-27
via LAN connection 3-20
Reset System 10-14

S

S.M.A.R.T. window 7-64
SAF-TE operation command 8-2, 8-3
SAF-TE operation command (diskctrl) massage 8-6
SAL/EFI firmware update command (fjfwupdate) 8-23
SB#x Status Clear window 5-38
SB#x window 5-30
schedule 5-52
adding 5-55
changing 5-55
deleting 5-55
Schedule Control window 5-52
Schedule List window 5-53
Schedule menu. 5-52
scheduled operation 4-8
SDU#x window 7-68, 7-69, 7-71
SEL
clearing event saved in 4-10, 4-13
downloading event data saved in 4-13
SEL window 7-53
selection field 2-10
self-signed certificate 5-106, 5-107
serial interface
CLI operation 6-1
Set Auto Boot Timeout window. 10-13
set date. 6-2, 6-9
set gateway 6-2, 6-12
set hostname 6-3, 6-17
set http 6-2, 6-12
set http_port 6-3, 6-13
set https 6-3, 6-13
set https_port 6-3, 6-14
set ip. 6-3, 6-16
set remcs 6-3, 6-17
set ssh 6-3, 6-14
set ssh_port 6-3, 6-15
set telnet. 6-3, 6-15
set telnet_port. 6-3, 6-16
set timezone 6-2, 6-9
setting area. 2-8
setting button 2-10
setting command 6-5
setting information
saving and restoring 4-9
setting privilege user 7-3, 7-11, 7-14, 7-16, 7-19, 7-59, 7-64, 7-65
Setup menu 7-59
show access_control 6-3, 6-20
show date 6-3, 6-20
show gateway 6-3, 6-21
show hostname 6-3, 6-24
show http 6-3, 6-22
show http_port 6-3, 6-22
show https 6-3, 6-23
show https_port 6-3, 6-23
show ip. 6-3, 6-24
show network. 6-4, 6-27
show remcs 6-4, 6-28
show ssh 6-3, 6-25
show ssh_port 6-3, 6-25
show telnet. 6-3, 6-26
show telnet_port 6-3, 6-26
show timezone. 6-3, 6-21
shutdown
through remote desktop connection. 3-21
via EMS connection 3-27
with Shutdown.exe command 3-20
with Telnet 3-24
shutdown method 3-20
Shutdown.exe 3-20
SNMP Community window 5-94
SNMP Configuration menu 5-93
SNMP security setting command. 8-22
SNMP Trap window 5-97
SNMP v3 Configuration window 5-99
Software Inventory -Detail- window 7-45
Software Inventory window 7-43
special string 11-3
SSH 4-21
SSH menu 5-108
SSL certificate 5-106
SSL menu 5-101
SSL support. 4-8
Status. 2-4
status display 2-8
Storage Controller window. 7-16
submenu frame 2-3, 2-6
submenu hierarchy display bar 2-5

switching 2-14
with CLI operation 2-15
with Web-UI operation 2-14
system account
unification of 4-7
system event log 4-28
System Event Log (Detail)
window 4-16, 4-17, 5-13
System Event Log Filtering
Condition window 4-14, 4-15, 5-10
System Event Log
window 2-4, 4-11, 4-12, 5-7
System File (display) window 7-40
System File (Selection) window 7-38
System Information window 5-15
System menu 5-5
System Power Control
window 3-5, 3-6
System Setup window 3-34, 3-35, 5-19
system status 2-1
System Status window 5-5

T

Telnet 3-24, 4-21
Temperature window 5-29
terminal software setting 3-15
text convention iv
text field 2-10
time synchronization 4-8
time zone setting 6-10
title area 2-7
troubleshooting information 4-31

U

update BMC 6-4, 6-31
update command 6-30
update EFI 6-4, 6-32
update MMB 6-4, 6-30
update SAL 6-4, 6-33
upper-level operation management software
linkage with 4-30
UPS 3-32
UPS connection 3-32
User 2-13
user administration 5-68
User Administration menu 5-68
user authority management 4-6
User List window 5-68
user management 4-8, 5-70, 5-73
user privilege level 2-13, 5-71, 5-74

V

VLAN function of management LAN 5-86
VLAN mode of management LAN 5-87

W

warning status 2-1
Watchdog window 7-59
Web-UI 2-1
Web-UI operation 5-1, 7-1
switching with Web-UI operation 2-14
Web-UI window 2-1, 5-1
basic operation 2-9
list of menu 5-1, 7-3
Web-UI, overview 2-1
who 6-4, 6-29
Who window 5-77
wildcard 11-2
window and part of manual,
correspondence between 1-4
window description format 1-2
Windows, remote shutdown 3-19

Reader's Comment Form

We would appreciate your comments and suggestions for improving this publication.

Date:_____
Your Name:_____
Company: _____
Address: _____
City/State/Zip:_____
Phone/Email address: _____

Publication No.: C122-E096-01EN
Publication Name: PRIMEQUEST 510A REFERENCE MANUAL: BASIC OPERATION/ GUI/COMMANDS

Your Comments:

Page	Line	Comments
Reply requested: ❑ Yes ❑ No		

Please evaluate the overall quality of this manual by checking (✓)the appropriate boxes

	Good	Fair	Poor		Good	Fair	Poor		Good	Fair	Poor
Organization:	❑	❑	❑	Use of examples:	❑	❑	❑	Legibility:	❑	❑	❑
Accuracy:	❑	❑	❑	Index coverage:	❑	❑	❑	Binding:	❑	❑	❑
Clarity:	❑	❑	❑	Cross referencing:	❑	❑	❑	Figures and tables:	❑	❑	❑
Overall rating of this publication:	❑	❑	❑					General appearance:	❑	❑	❑

Technical level: ❑ Too detailed ❑ Appropriate ❑ Not enough detail

All comments and suggestions become the property of Fujitsu Limited.

For Users in U.S.A., Canada, and Mexico

Fold and fasten as shown on back
No postage necessary if mailed in U.S.A.

Fujitsu Computer Systems
Attention: Engineering Ops M/S 249
1250 East Arques Avenue
Sunnyvale, CA 94085-5401
FAX: (408) 746-6676

For Users in Other Countries

Fax this form to the number below or send this form to the address below.

Fujitsu Learning Media Limited
FAX: 81-3-3730-3702
37-10 Nishi-Kamata 7-chome
Oota-Ku
Tokyo 144-0051
JAPAN

FUJITSU LIMITED

FOLD AND TAPE

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO 741 SUNNYVALE CA

POSTAGE WILL BE PAID BY ADDRESSEE

FUJITSU

FUJITSU COMPUTER SYSTEMS
ATTENTION ENGINEERING OPS M/S 249
1250 EAST ARQUES AVENUE
SUNNYVALE CA 94085-5401

FOLD AND TAPE

FUJITSU