

FUJITSU Server

PRIMEQUEST 1000 Series

Installation Manual



Preface

This manual describes how to set up this product, including the steps for installation of the PRIMEQUEST 1000 series server, initialization, and software installation. The manual is intended for system administrators.

For details on the regulatory compliance statements and safety precautions, see the *PRIMEQUEST 1000 Series Safety and Regulatory Information* (C122-E115EN).

Errata and addenda for the manual

PRIMEQUEST 1000 Series Errata and Addenda (C122-E119EN) provides errata and addenda for the manual.

Read the *PRIMEQUEST 1000 Series Errata and Addenda* (C122-E119EN) thoroughly in reference to the manual.

For Safe Operation

How to use this manual

This manual contains important information about the safe use of this product. Read the manual thoroughly to understand the information in it before using this product. Be sure to keep this manual in a safe and convenient location for quick reference.

Fujitsu makes every effort to prevent users and bystanders from being injured and to prevent property damage. Be sure to use the product according to the instructions in the manual.

About this product

This product is designed and manufactured for standard applications. Such applications include, but are not limited to, general office work, personal and home use, and general industrial use. The product is not intended for applications that require extremely high levels of safety to be guaranteed (referred to below as "safety-critical" applications). Use of the product for a safety-critical application may present a significant risk of personal injury and/or death. Such applications include, but are not limited to, nuclear reactor control, aircraft flight control, air traffic control, mass transit control, medical life support, and missile launch control. Customers shall not use the product for a safety-critical application without guaranteeing the required level of safety. Customers who plan to use the product in a safety-critical system are requested to consult the Fujitsu sales representatives in charge.

Storage of accessories

Keep the accessories in a safe place because they are required for server operation.

Organization and Notation of This Manual

This section describes the following topics:

- [Organization of this manual](#)
- [Manuals for the PRIMEQUEST 1000 series](#)
- [Related manuals](#)
- [Abbreviations](#)
- [Notation](#)
- [Notation for the CLI \(command line interface\)](#)
- [Notes on notations](#)
- [Alert messages](#)
- [Product operating environment](#)
- [Trademarks](#)

Organization of this manual

This manual is organized as follows.

CHAPTER 1 Installation Overview

Chapter 1 describes the workflow up to actual operation of the PRIMEQUEST 1000 series server.

CHAPTER 2 Preparing for Main Unit Installation

Chapter 2 describes the preparation before main unit installation. This preparation includes work up to power cable connection.

CHAPTER 3 Work before Operating System Installation

Chapter 3 describes the work that must be done before you install an operating system on the PRIMEQUEST 1000 series server. The chapter also describes settings for actual operation and various setup work.

CHAPTER 4 Installing the Operating System and Bundled Software

Chapter 4 describes how to install the operating system and bundled software.

CHAPTER 5 Work after Operating System Installation (PRIMEQUEST 1800E2)

Chapter 5 describes how to make various necessary settings after operating system installation on the PRIMEQUEST 1800E2.

CHAPTER 6 Work after Operating System Installation (PRIMEQUEST 1800E)

Chapter 6 describes how to make PSA and various other necessary settings after operating system installation on the PRIMEQUEST 1800E.

CHAPTER 7 Work after Installation

Chapter 6 describes the work performed after PRIMEQUEST 1000 series installation. This work includes configuring NTP and security.

CHAPTER 8 Powering On and Off a Partition

Chapter 7 describes partition power control.

APPENDIX A Lists of Settings (Links)

Appendix A provides links to Appendix A List of Settings in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

APPENDIX B Manual PSA Installation and Uninstallation

Appendix B describes how to manually install and uninstall PSA for a specific operating system.

APPENDIX C Software (Links)

Appendix C provides a link to 3.3 Bundled Software in the *PRIMEQUEST 1000 Series General Description* (C122-B022EN).

APPENDIX D Configuring the SAN Boot Environment

Appendix D is a link to the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).

APPENDIX E Notes on VMware Installation

Appendix E describes the procedure for installing a built-in hard disk in a RAID environment in VMware vSphere and provides notes on installation.

APPENDIX F Setting up the NTP Server (Windows)

Appendix G describes how to specify and set of an NTP server for a specific Windows operating system.

Index

The index lists keywords and the pages that they refer to, helping readers quickly find the necessary information in the manual.

Manuals for the PRIMEQUEST 1000 series

The following manuals have been prepared to provide you with the information necessary to use the PRIMEQUEST 1000 series.

You can access HTML versions of these manuals at the following sites:

Japanese-language site: <http://jp.fujitsu.com/platform/server/primequest/manual/>

Global site: <http://jp.fujitsu.com/platform/server/primequest/manual-e/>

Title	Description	Manual code
<i>PRIMEQUEST 1000 Series Getting Started Guide</i>	Describes what manuals you should read and how to access important information after unpacking the PRIMEQUEST 1000 series server. (This manual comes with the product.)	C122-E114XA
<i>PRIMEQUEST 1000 Series Safety and Regulatory Information</i>	Contains important information required for using the PRIMEQUEST 1000 series safely.	C122-E115XA
<i>PRIMEQUEST 1000 Series Errata and Addenda</i>	Provides errata and addenda for the PRIMEQUEST 1000 series manuals. This manual will be updated as needed.	C122-E119EN
<i>PRIMEQUEST 1000 Series General Description</i>	Describes the functions and features of the PRIMEQUEST 1000 series.	C122-B022EN
<i>SPARC Enterprise/PRIMEQUEST Common Installation Planning Manual</i>	Provides the necessary information and concepts you should understand for installation and facility planning for SPARC Enterprise and PRIMEQUEST installations.	C120-H007EN
<i>PRIMEQUEST 1000 Series Hardware Installation Manual</i>	Includes the specifications of and the installation location requirements for the PRIMEQUEST 1000 series.	C122-H004EN
<i>PRIMEQUEST 1000 Series Installation Manual</i>	Describes how to set up the PRIMEQUEST 1000 series server, including the steps for installation preparation, initialization, and software installation.	C122-E107EN
<i>PRIMEQUEST 1000 Series User Interface Operating Instructions</i>	Describes how to use the Web-UI and UEFI to assure proper operation of the PRIMEQUEST 1000 series server.	C122-E109EN
<i>PRIMEQUEST 1000 Series Administration Manual</i>	Describes how to use tools and software for system administration and how to maintain the system (component replacement and error notification).	C122-E108EN

Title	Description	Manual code
<i>PRIMEQUEST 1000 Series Tool Reference</i>	Provides information on operation methods and settings, including details on the MMB, PSA, and UEFI functions.	C122-E110EN
<i>PRIMEQUEST 1000 Series Message Reference</i>	Lists the messages that may be displayed when a problem occurs during operation and describes how to respond to them.	C122-E111EN
<i>PRIMEQUEST 1000 Series REMCS Installation Manual</i>	Describes REMCS service installation and operation.	C122-E120EN
<i>PRIMEQUEST 1000 Series Glossary</i>	Defines the PRIMEQUEST 1000 series related terms and abbreviations.	C122-E116EN
<i>PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual</i>	Gives a revised version of APPENDIX D Configuring the SAN Boot Environment in the <i>PRIMEQUEST 1000 Series Installation Manual</i> (C122-E107EN). This manual describes procedures for installing the SAN boot environment and provides the latest information including notes on design.	C122-E155EN

Related manuals

The following manuals relate to the PRIMEQUEST 1000 series.

You can access these manuals at the following site:

<http://jp.fujitsu.com/platform/server/primequest/manual-e/>

Contact your sales representative for inquiries about the ServerView manuals.

Title	Description	Manual code
<i>ServerView Suite ServerView Operations Manager Quick Installation (Windows)</i>	Describes how to install and start ServerView Operations Manager in a Windows environment.	None
<i>ServerView Suite ServerView Operations Manager Quick Installation (Linux)</i>	Describes how to install and start ServerView Operations Manager in a Linux environment.	None
<i>ServerView Suite ServerView Installation Manager</i>	Describes the installation procedure using ServerView Installation Manager.	None
<i>ServerView Suite ServerView Operations Manager Server Management</i>	Provides an overview of server monitoring using ServerView Operations Manager, and describes the user interface of ServerView Operations Manager.	None

Title	Description	Manual code
<i>ServerView Suite ServerView RAID Management User Manual</i>	Describes RAID management using ServerView RAID Manager.	None
<i>ServerView Suite Basic Concepts</i>	Describes the basic concepts of ServerView Suite.	None
<i>ServerView Operations Manager Installation ServerView Agents for Linux</i>	Describes installation and update installation of ServerView Linux Agent.	None
<i>ServerView Operations Manager Installation ServerView Agents for Windows</i>	Describes installation and update installation of ServerView Windows Agent.	None
<i>ServerView Mission Critical Option User Manual</i>	Describes the necessary functions unique to PRIMEQUEST (notification via the MMB, hot replacement command) and ServerView Mission Critical Option (SVMco), which is required for supporting these functions. Also includes explanation of ServerView Mission Critical Option for VM (SVMcovm) required for VMware vSphere 5 server monitor.	None
<i>ServerView RAID Manager VMware vSphere ESXi 5 Installation Guide</i>	ServerView Describes the installation and settings required to use ServerView RAID Manager on the VMware vSphere ESXi 5 server.	None
<i>MegaRAID SAS Software</i>	Provides technical information on using array controllers. Refer to the manual from the SVS-DVD2 supplied with the product or from the following URL: The Fujitsu Technology Solutions manuals server http://manuals.ts.fujitsu.com/	None
<i>MegaRAID SAS Device Driver Installation</i>	Provides technical information on using array controllers. Refer to the manual from the SVS-DVD2 supplied with the product or from the following URL: The Fujitsu Technology Solutions manuals server http://manuals.ts.fujitsu.com/	None
<i>Modular RAID Controller Installation Guide</i>	Provides technical information on using array controllers.	None

Title	Description	Manual code
	Refer to the manual from the SVS-DVD2 supplied with the product or from the following URL: The Fujitsu Technology Solutions manuals server http://manuals.ts.fujitsu.com/	

Abbreviations

This manual uses the following product name abbreviations.

Formal product name	Abbreviation
Red Hat® Enterprise Linux® 5 (for Intel 64)	Linux RHEL5, RHEL
Red Hat® Enterprise Linux® 5 (for x86)	
Red Hat® Enterprise Linux® 6 (for Intel64)	Linux RHEL6, RHEL
Red Hat® Enterprise Linux® 6 (for x86)	
Microsoft® Windows Server® 2003, Standard Edition	Windows Windows Server 2003
Microsoft® Windows Server® 2003, Enterprise Edition	
Microsoft® Windows Server® 2003, Datacenter Edition	
Microsoft® Windows Server® 2003, Standard x64 Edition	
Microsoft® Windows Server® 2003, Enterprise x64 Edition	
Microsoft® Windows Server® 2003, Datacenter x64 Edition	
Microsoft® Windows Server® 2003 R2, Standard Edition	
Microsoft® Windows Server® 2003 R2, Enterprise Edition	
Microsoft® Windows Server® 2003 R2, Datacenter Edition	
Microsoft® Windows Server® 2003 R2, Standard x64 Edition	
Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition	
Microsoft® Windows Server® 2003 R2, Datacenter x64 Edition	
Microsoft® Windows Server® 2008 Standard	Windows Windows Server 2008
Microsoft® Windows Server® 2008 Enterprise	
Microsoft® Windows Server® 2008 Datacenter	
Microsoft® Windows Server® 2008 R2 Standard	
Microsoft® Windows Server® 2008 R2 Enterprise	
Microsoft® Windows Server® 2008 R2 Datacenter	
Microsoft(R) Windows Server(R) 2012 Datacenter	Windows Windows Server 2012
Microsoft(R) Windows Server(R) 2012 Standard	

Formal product name	Abbreviation
Microsoft® Windows Server(R) 2012 R2 Datacenter	Windows
Microsoft® Windows Server(R) 2012 R2 Standard	Windows Server 2012
VMware vSphere(R) 4	VMware, vSphere 4.x, VMware 4.x
VMware vSphere(R) 5	VMware, vSphere 5.x, VMware 5.x
VMware(R) ESX(R) 4	ESX, ESX 4.x
VMware(R) ESXi(TM) 5	ESXi, ESXi 5.x
Novell(R) SUSE(R) LINUX Enterprise Server 11 Service Pack 2	SLES11 SP2

Notation

This manual uses the following fonts and symbols to express specific types of information.

Font or symbol	Meaning	Example
<i>italics</i>	Title of a manual that you should refer to	See the <i>PRIMEQUEST 1000 Series Installation Manual (C122-E107EN)</i> .
[]	Window names as well as the names of buttons, tabs, and drop-down menus in windows are enclosed in brackets.	Click the [OK] button.

Notation for the CLI (command line interface)

The following notation is used for commands.

Command syntax

Command syntax is represented as follows.

- Variables requiring the entry of a value are enclosed in angle brackets < >.
- Optional elements are enclosed in brackets [].
- Options for optional keywords are grouped in | (stroke) separated lists enclosed in brackets [].
- Options for required keywords are grouped in | (stroke) separated lists enclosed in braces { }.

Command syntax is written in a box.

Remarks

The command output shown in the PDF manuals may include line feeds at places where there is no line feed symbol (\ at the end of the line).

Notes on notations

- In this manual, the Management Board and MMB firmware are abbreviated as "MMB."
- In this manual, IOBs and GSPBs (LIOBs and LGSPBs within partitions) are collectively referred to as IO Units.
- Screenshots contained in this manual may differ from the actual product screen displays.

- The IP addresses, configuration information, and other such information appearing in this manual are display examples and differ from that displayed during actual operation.

Alert messages

This manual uses the following alert messages to prevent users and bystanders from being injured and to prevent property damage.

 WARNING	This indicates a hazardous (potentially dangerous) situation that is likely to result in death or 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 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 use the product more efficiently.

Alert messages in the text

An alert statement follows an alert symbol. An alert statement is indented on both ends to distinguish it from regular text. Similarly, one space line is inserted before and after the alert statement.



Only Fujitsu certified service engineers should perform the following tasks on this product and the options provided by Fujitsu. Customers must not perform these tasks under any circumstances. Otherwise, electric shock, injury, or fire may result.

- Newly installing or moving equipment
- Removing the front, rear, and side covers
- Installing and removing built-in options
- Connecting and disconnecting external interface cables
- Maintenance (repair and periodic diagnosis and maintenance)

The [List of important alert items](#) tables list important alert items.

Product operating environment

This product is a computer intended for use in a computer room environment. For details on the product operating environment, see the following manual:

PRIMEQUEST 1000 Series Hardware Installation Manual (C122-H004EN)

Notes

- If you have a comment or request regarding this manual, or if you find any part of this manual unclear, please take a moment to share it with us by filling in the form at the following webpage, stating your points specifically, and sending the form to us:
https://www-s.fujitsu.com/global/contact/computing/PRMQST_feedback.html
- The contents of this manual may be revised without prior notice.
- The PDF file of this manual is intended for display using Adobe® Reader® in single page viewing mode at 100% zoom.
- The PRIMEQUEST 1800E2/1800E model supports only 200 V power supply.

Trademarks

- Microsoft, Windows, and Windows Server are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.
- Linux is a registered trademark of Linus Torvalds.
- Red Hat, the Shadowman logo and JBoss are registered trademarks of Red Hat, Inc. in the U.S. and other countries.
- Intel and Xeon are trademarks or registered trademarks of Intel Corporation.
- Ethernet is a registered trademark of Fuji Xerox Co., Ltd. in Japan and is a registered trademark of Xerox Corp. in the United States and other countries.
- VMware is a trademark or registered trademark of VMware, Inc. in the United States and other countries.
- Novell and SUSE Linux Enterprise Server are trademarks of Novell, Inc.
- Xen is a trademark or registered trademark of Citrix Systems, Inc. or its subsidiaries in the United States and other countries.
- Other company names and product names are the trademarks or registered trademarks of their respective owners.
- Trademark indications are omitted for some system and product names in this manual.

Safety Precautions

List of important alert items

The following tables list the important alert items contained in this manual.



This indicates a hazardous (potentially dangerous) situation that is likely to result in death or serious personal injury if the user does not perform the procedure correctly.

Work category	Warning	Location
Setup	Field engineers perform the following tasks on this product. Customers must not perform these tasks under any circumstances. Otherwise, electric shock, injury, or fire may result. - Newly installing or moving equipment - Removing the front, rear, and side covers - Installing and removing built-in options - Connecting and disconnecting external interface cables - Maintenance (repair and periodic diagnosis and maintenance)	1.1 Setup Workflow



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

Work category	Warning	Location
Normal operation	The unit may be damaged or operating abnormally. - Follow the precautions, warnings, and instructions shown on the main unit. - Do not block the vent holes. - Do not install the main unit in a location exposed to direct sunlight or close to a device that may generate large amounts of heat. - Do not install the main unit in a location exposed to large amounts of dust, corrosive gas, or salt spray. - Do not install the main unit in a location subject to strong vibration. Install the main unit on a flat surface. - Use grounded Category 3 wiring or better. Using another type of grounded wiring may cause abnormal operation. - Do not route cables under the main unit. Do not allow cables to become taut. - Do not disconnect the power cables while the main unit power is on. - If it is hard to push the connector latch of a LAN cable or other cable when attempting to disconnect the cable, push it with a flathead screwdriver. Forcibly inserting a finger may cause personal injury or damage the unit. - Do not place anything on top of the main unit. Do not work above or on top of the main unit. - Prevent rapid rises in the ambient temperature during winter. Such an abrupt temperature change may cause condensation to form in the main unit. Allow sufficient warm-up time before starting operation. - Do not install the main unit close to a photocopier, air-conditioning unit, welder, or other device that generates electromagnetic noise. - Do not install the main unit close to a device that generates large amounts of electrical noise. - Do not connect the main unit to the same power supply line as an elevator in the facility or other equipment that would expose it to sudden voltage drops. - Implement antistatic measures at the installation site. - Confirm that the power supply voltage and frequency are adequate according to the respective ratings shown on the main unit. - Do not insert or drop foreign matter into the openings of the main unit. The main unit contains high-voltage components. If any metallic matter or other electro-conductive object enters the main unit through an opening, it may cause a short circuit. This may lead to fire, electric shock, or damage to the main unit. - For details on maintenance of the main unit, contact the distributor where you purchased your product, or your sales representative.	2.1 Safety Precautions

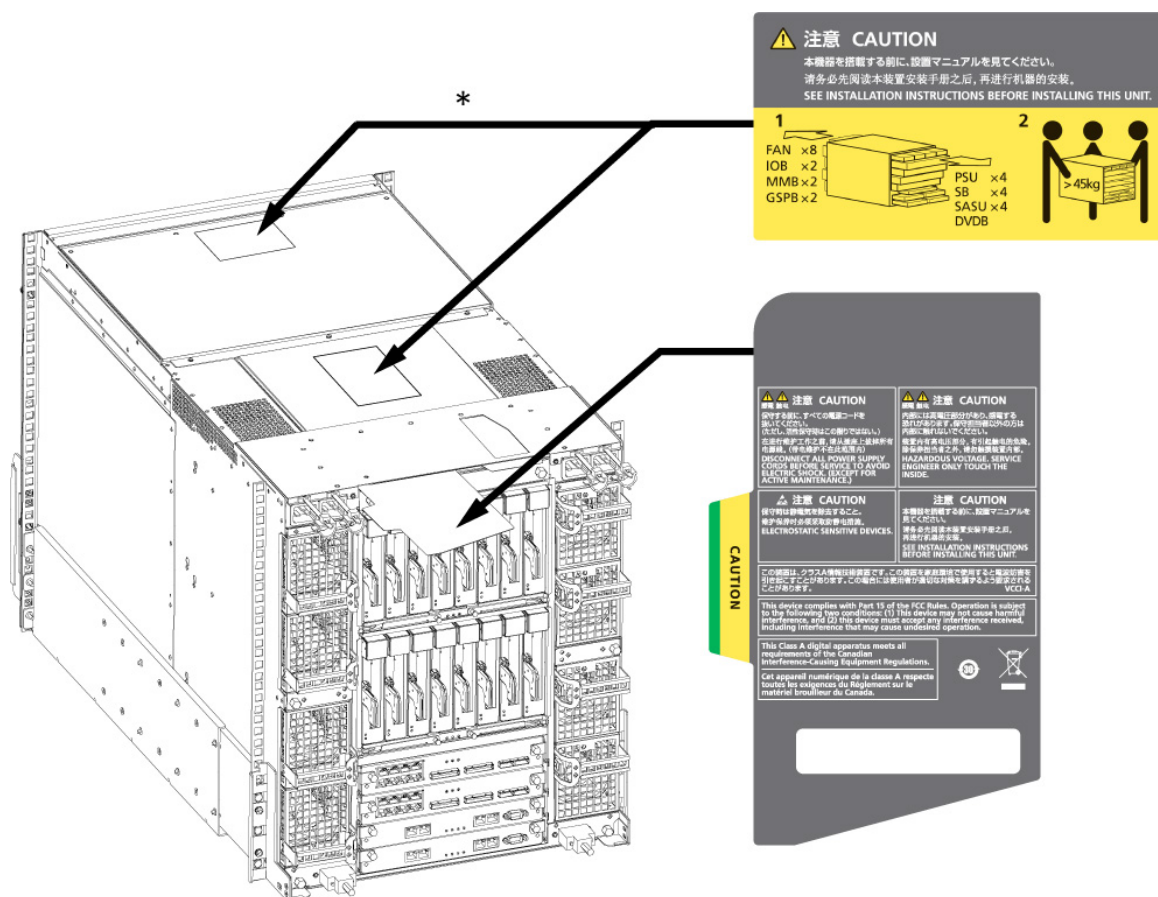
Work category	Warning	Location
Normal operation	(Damage to data) Confirm that the System Power LED of the DVDB is off before turning off the main power (e.g., UPS, power distribution box). If you turn off the main power (e.g., UPS, power distribution box) while the System Power LED of the DVDB is on, data may be damaged.	3.2.1 Powering on and off the main unit

Warning labels

The following warning labels are affixed to this product. These labels are intended for the users of this product.

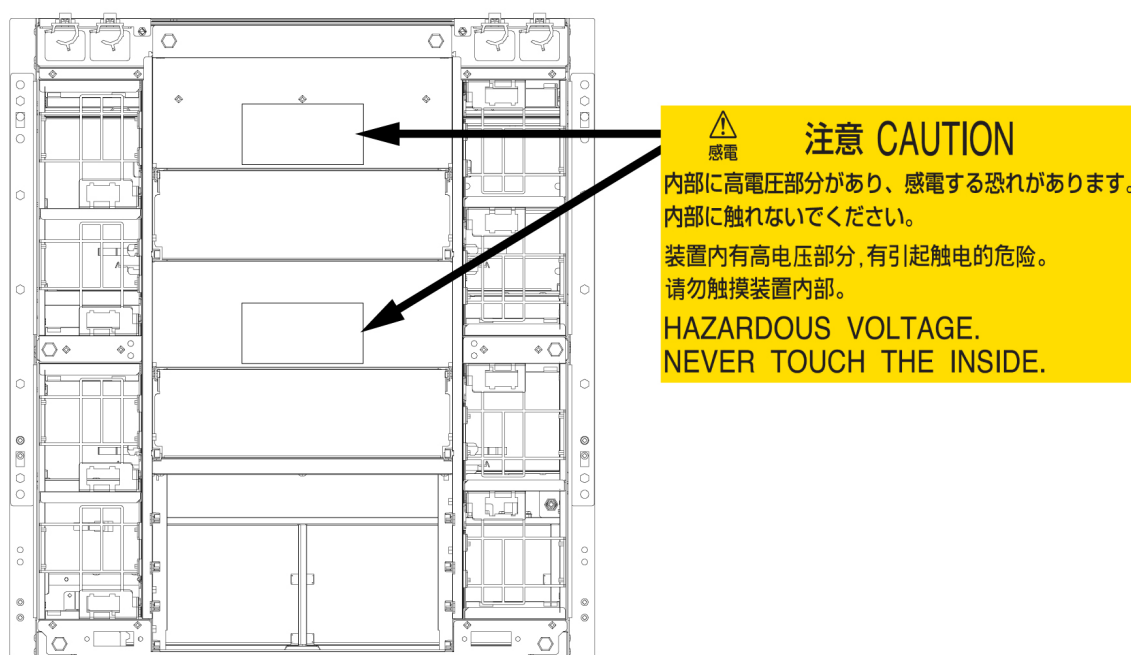


Never remove the warning labels.

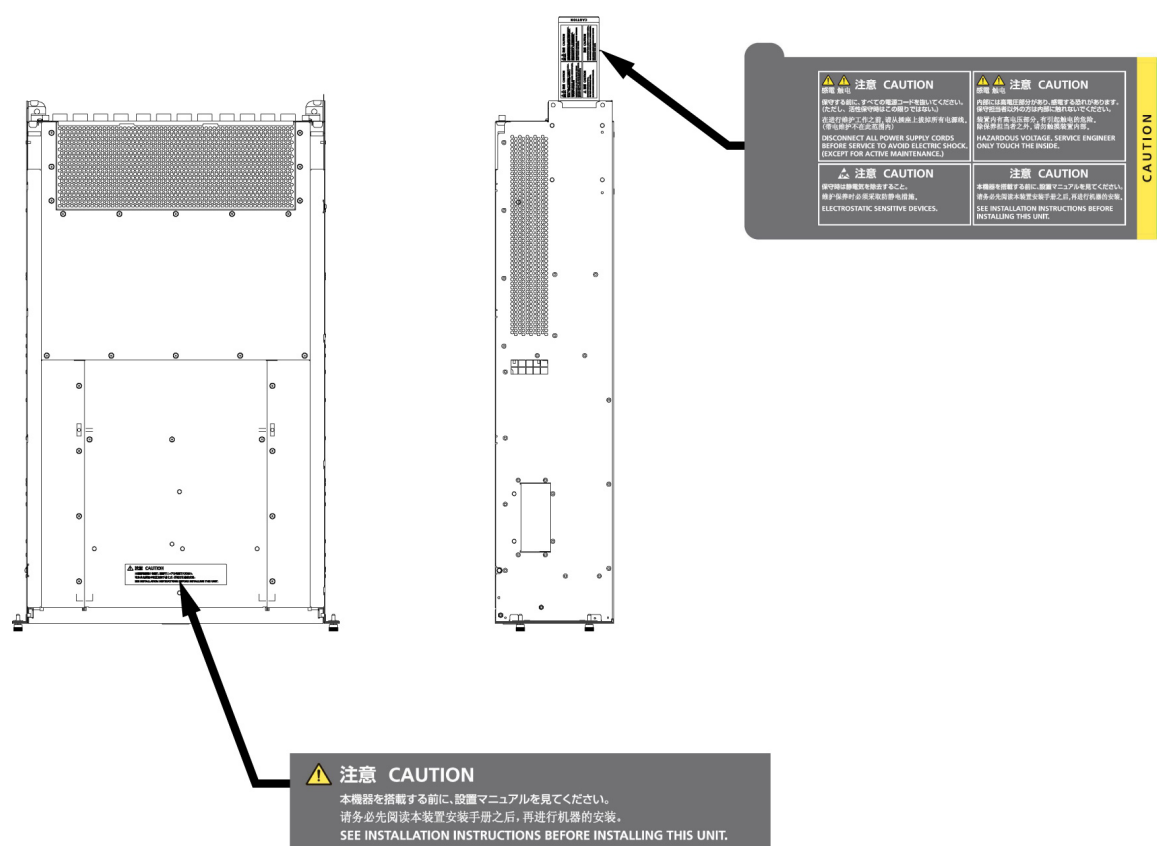


* The label is affixed at either location.

Warning label location (PRIMEQUEST 1800E2/1800E rear)



Warning label location (PRIMEQUEST 1800E2/1800E rear) (IOBs removed)



Warning label location (PCI_Box)

Notes on Handling the Product

Adding optional products

For stable operation of the PRIMEQUEST 1000 series server, use only a Fujitsu certified optional product as an added option.

Note that the PRIMEQUEST 1000 series server is not guaranteed to operate with any optional product not certified by Fujitsu.

Maintenance



Only Fujitsu certified service engineers should perform the following tasks on this product and the options provided by Fujitsu. Customers must not perform these tasks under any circumstances. Otherwise, electric shock, injury, or fire may result.

- Newly installing or moving equipment
- Removing the front, rear, and side covers
- Installing and removing built-in options
- Connecting and disconnecting external interface cables
- Maintenance (repair and periodic diagnosis and maintenance)



Only Fujitsu certified service engineers should perform the following tasks on this product and the options provided by Fujitsu. Customers must not perform these tasks under any circumstances. Otherwise, product failure may result.

- Unpacking an optional Fujitsu product, such as an optional adapter, delivered to the customer

Modifying or recycling the product



Modifying this product or recycling a secondhand product by overhauling it without prior approval may result in personal injury to users and/or bystanders or damage to the product and/or other property.

Note on erasing data from hard disks when disposing of the product or transferring it

Disposing of this product or transferring it as is may enable third parties to access the data on the hard disk and use it for unforeseen purposes. To prevent the leakage of confidential information and important data, all of the data on the hard disk must be erased before disposal or transfer of the product.

However, it can be difficult to completely erase all of the data from the hard disk. Simply initializing (reformatting) the hard disk or deleting files on the operating system is insufficient to erase the data, even though the data appears at a glance to have been erased. This type of operation only makes it impossible to access the data from the operating system. Malicious third parties can restore this data.

If you save your confidential information or other important data on the hard disk, you should completely erase the data, instead of simply carrying out the aforementioned operation, to prevent the data from being restored.

To prevent important data on the hard disk from being leaked when the product is disposed of or transferred, you will need to take care to erase all the data recorded on the hard disk on your own responsibility.

Furthermore, if a software license agreement restricts the transfer of the software (operating system and application software) on the hard disk in the server or other product to a third party, transferring the product without deleting the software from the hard disk may violate the agreement. Adequate verification from this point of view is also necessary.

Support and service

SupportDesk (available only in Japan, for a fee)

For stable system operation, we recommend concluding our SupportDesk agreement, which provides a maintenance and operation support service. SupportDesk agreement customers receive a same-day response service for hardware problems. They are eligible for regular checkups, remote notification of potential-failure predictions, and information on system problems. Moreover, they can avail themselves of other services such as troubleshooting support by phone for hardware and software problems, and access to operation support information from a dedicated website for our customers. For details, see "Product support" on the SupportDesk homepage (<http://jp.fujitsu.com/solutions/support/sdk/index.html>).

Product and service inquiries

For all product use and technical inquiries, contact the distributor where you purchased your product, or a Fujitsu sales representative or systems engineer (SE). If you do not know the appropriate contact address for inquiries about the PRIMEQUEST 1000 series, use the Fujitsu contact line.

Fujitsu contact line

We accept Web inquiries. For details, visit our website:

https://www-s.fujitsu.com/global/contact/computing/PRMQST_feedback.html

Warranty

If a component failure occurs during the warranty period, we will repair it free of charge in accordance with the terms of the warranty agreement. For details, see the warranty.

Before requesting a repair

If a problem occurs with the product, confirm the problem by referring to 11.2 Troubleshooting in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN). If the error recurs, contact your sales representative or a field engineer. Confirm the model name and serial number shown on the label affixed to the right front of the device and report it. Also check any other required items beforehand according to 11.2 Troubleshooting in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN). The system settings saved by the customer will be used during maintenance.

Revision History

Edition	Date	Revised location (type) (*)	Description
01	2010-02-09	-	-
02	2010-03-12	All pages	Incorporated differences in <i>Errata and Addenda</i> (C122-E119-01EN)

Edition	Date	Revised location (type) (*)	Description
03	2010-08-20	All pages	Incorporated differences in <i>Errata and Addenda</i> (C122-E119-02EN to C122-E119-10EN)
04	2011-04-28	All pages	- Added items about 1800E2 - Incorporated differences in <i>Errata and Addenda</i> (C122-E119-11EN to C122-E119-18EN) - Incorporated <i>Windows Server 2003/2008 NTP Client Setup Guide</i> (C122-E143-01EN) - Incorporated <i>Red Hat Enterprise Linux 6 Supplemental Manual</i> (C122-E154-01EN)
05	2011-05-31	All pages	Incorporated differences in <i>Errata and Addenda</i> (C122- E119-19EN)
06	2011-12-20	All pages	- Incorporated differences in <i>Errata and Addenda</i> (C122- E119-20EN to C122-E119-24EN) - Incorporated the contents of Appendix F(*) Quick Guide to PRIMEQUEST 1000 Installation in Chapter 4 Installing the Operating System and Bundled Software, and deleted that appendix.
07	2012-03-06	All pages	- Added and modified description of I/O space assignment. - Added and modified descriptions on confirming settings for SELinux functions.
08	2012-07-10	All pages	- Modified descriptions on Power off and Operations in 3.2.1 Powering on and off the main unit - Added note in 3.3.6 Configuring the MMB network - Added and modified description of VMware 4.x. - Added and modified description of VMware 5.x.

Edition	Date	Revised location (type) (*)	Description
09	2012-12-21	All pages	- Added descriptions about Windows Server 2012. - Added descriptions about installing SLES11 SP2.
10	2015-06-10	All pages	Incorporated differences in <i>Errata and Addenda</i> (C122- E119-37EN)

* Chapter, section, and item numbers in the "Revised location" column refer to those in the latest edition of the document. However, a number marked with an asterisk (*) denotes a chapter, section, or item in a previous edition of the document.

This manual shall not be reproduced or copied without the permission of Fujitsu Limited.
Copyright 2010 - 2015 FUJITSU LIMITED

Contents

CHAPTER 1 Installation Overview	1
1.1 Setup Workflow	2
1.1.1 Work performed by a field engineer	2
1.1.2 Work performed by the user	2
CHAPTER 2 Preparing for Main Unit Installation	5
2.1 Safety Precautions	6
2.2 Before Installing the Main Unit	7
2.3 Checking Environmental Conditions	8
2.4 Preparing the Power Supply Equipment	9
2.4.1 Electrical specifications	9
2.4.2 Facility power requirements and characteristics	9
2.4.3 Grounding	9
2.5 Checking the Installation Site	10
2.6 Preparing to Install the Main Unit	11
2.7 Confirming the Supplied Parts	12
2.8 Mounting the Main Unit in a 19-inch Rack	13
2.9 Connecting the Power Cables	14
CHAPTER 3 Work before Operating System Installation	17
3.1 Before Starting Setup	18
3.1.1 MMB settings	18
3.1.2 Partition settings	18
3.2 Starting the System	19
3.2.1 Powering on and off the main unit	19
3.3 Connecting and Configuring the MMB	20
3.3.1 Connecting the MMB console PC	21
3.3.2 Initializing MMB settings	22
3.3.3 Setting up the connection environment for actual operation	23
3.3.4 Logging in to the MMB	25
3.3.5 How to view the Web-UI window	27
3.3.6 Configuring the MMB network	32
3.3.7 Configuring telnet	33
3.3.8 Configuring a DNS server	34
3.3.9 Configuring Alarm E-Mail	35
3.3.10 Registering a user account	37
3.3.11 Setting the system name	39
3.3.12 Setting the date and time	40
3.4 Configuring a Partition	43
3.4.1 Setting a partition configuration	43
3.4.2 Setting a Home SB	46
3.4.3 Setting a Reserved SB	47
3.4.4 Setting a partition name	51
3.4.5 Setting various modes	52
3.4.6 Configuring Console Redirection	55
3.4.7 Powering off and on a partition	55
3.4.8 Checking partition information	56
3.5 Saving Configuration Information	57
3.5.1 Backing up MMB configuration information	57
CHAPTER 4 Installing the Operating System and Bundled Software	59
4.1 Installation Procedure for the Operating System and Bundled Software	60
4.2 RHEL Installation Procedures on the SAN Storage Unit	61
4.2.1 Advance setup and preparation	61
4.2.2 Preparing for Installation	61
4.2.3 Installing the operating system	62

4.2.4 Configuring bundled software after the completion of installation	64
4.2.5 Connecting the SAN and built-in HDD after the installation	66
4.3 RHEL Installation Procedures on the Built-in HDD	67
4.3.1 Advance setup	67
4.3.2 Preparing for Installation	67
4.3.3 Installing the operating system	68
4.3.4 Configuring bundled software after the completion of installation	70
4.3.5 Connecting the SAN and built-in HDD after the installation	72
4.4 Windows Installation Procedures on the SAN Storage Unit	73
4.4.1 Advance setup	73
4.4.2 Preparing for Installation	73
4.4.3 Installing the operating system	73
4.4.4 Configuring bundled software after the completion of installation	78
4.4.5 Connecting the SAN and built-in HDD after the installation	81
4.5 Windows Installation Procedures on the Built-in HDD	82
4.5.1 Advance setup	82
4.5.2 Preparing for Installation	82
4.5.3 Installing the operating system	82
4.5.4 Configuring bundled software after the completion of installation	87
4.5.5 Connecting the SAN and built-in HDD after the installation	90
4.6 VMware 4.x Installation Procedures on the SAN Storage Unit	91
4.6.1 Advance setup	91
4.6.2 Preparing for Installation	91
4.6.3 Installing VMware 4.x	92
4.6.4 Installing bundled software	92
4.6.5 Configuring bundled software	92
4.6.6 Configuring a software watchdog	93
4.6.7 Completing VMware 4.x installation	93
4.7 VMware 4.x Installation Procedures on the Built-in HDD	94
4.7.1 Advance setup	94
4.7.2 Preparing for Installation	94
4.7.3 Installing VMware 4.x	95
4.7.4 Installing bundled software	95
4.7.5 Configuring bundled software	95
4.7.6 Configuring a software watchdog	96
4.7.7 Completing VMware installation	96
4.8 VMware 5.x Installation Procedures on the SAN Storage Unit	97
4.8.1 Advance setup	97
4.8.2 Preparing for Installation	97
4.8.3 Installing VMware 5.x	98
4.8.4 Configuring a software watchdog	100
4.8.5 Completing VMware 5.x installation	100
4.8.6 Installing bundled software	100
4.9 VMware 5.x Installation Procedures on the Built-in HDD	101
4.9.1 Advance setup	101
4.9.2 Preparing for Installation	101
4.9.3 Installing VMware 5.x	102
4.9.4 Configuring a software watchdog	104
4.9.5 Completing VMware 5.x installation	104
4.9.6 Installing bundled software	104
4.10 SUSE Linux Enterprise Server 11 Service Pack 2 Installation Procedures on the SAN Storage Unit	105
4.10.1 Advance setup and preparation	105
4.10.2 Preparing for Installation	105
4.10.3 Installing the operating system	106
4.10.4 Configuring bundled software after the completion of installation	108
4.10.5 Connecting the SAN and built-in HDD after the installation	109
4.11 SUSE Linux Enterprise Server 11 Service Pack 2 Installation Procedures on the Built-in HDD	110

4.11.1 Advance setup	110
4.11.2 Preparing for Installation	110
4.11.3 Installing the operating system	110
4.11.4 Configuring bundled software after the completion of installation	113
4.11.5 Connecting the SAN and built-in HDD after the installation	114
CHAPTER 5 Work after Operating System Installation (PRIMEQUEST 1800E2)	115
5.1 Types of Work	116
5.2 Configuring SVS (SVagent/SVmco)	117
5.3 Setting of sadump	118
5.4 Setting Up the Dump Environment (Windows)	128
5.4.1 Memory dump files and paging files	128
5.5 Setting Up the Dump Environment (Linux)	129
5.5.1 How to use sadump	129
5.6 Configuring the NTP Client	132
5.7 Saving Management and Configuration Information	133
5.7.1 Saving MMB configuration information	133
5.7.2 Saving BIOS configuration information	134
5.8 Configuring Service Life Monitoring by RAS Support Service	135
5.8.1 BBU service life monitoring for a RAID card	135
5.8.2 Battery unit service life monitoring for a UPS	136
CHAPTER 6 Work after Operating System Installation (PRIMEQUEST 1800E)	139
6.1 Types of Work	140
6.2 Configuring PSA (Linux: Red Hat Enterprise Linux)	141
6.2.1 Configuring the PSA-to-MMB communication LAN	142
6.2.2 Confirming management LAN settings	146
6.2.3 Confirming SELinux function settings	146
6.2.4 Checking the firewall function (opening ports)	147
6.2.5 Setting the destinations of traps from a partition	152
6.2.6 Setting the destinations of traps and e-mail via the MMB	156
6.2.7 Setting the management LAN IP address	156
6.2.8 Configuring SNMP to use duplicate disks	157
6.2.9 Installing a PSA update	159
6.2.10 Uninstalling PSA	160
6.3 Configuring PSA (Windows Server 2003)	161
6.3.1 Configuring the PSA-to-MMB communication LAN	163
6.3.2 Confirming management LAN settings	165
6.3.3 Setting the destinations of traps from a partition	165
6.3.4 Setting the destinations of traps and e-mail via the MMB	167
6.3.5 Configuring the Windows Firewall	167
6.3.6 Setting the Watchdog Timer for monitoring after a STOP error (fatal system error)	169
6.3.7 Setting the management LAN IP address	170
6.3.8 Installing a PSA update	170
6.3.9 Uninstalling PSA	173
6.4 Configuring PSA (Windows Server 2008)	175
6.4.1 Configuring the PSA-to-MMB communication LAN	177
6.4.2 Confirming management LAN settings	177
6.4.3 Installing the PSHED Plugin driver	178
6.4.4 Setting the destinations of traps from a partition	179
6.4.5 Setting the destinations of traps and e-mail via the MMB	180
6.4.6 Configuring the Windows Firewall	180
6.4.7 Setting the Watchdog Timer for monitoring after a STOP error (fatal system error)	195
6.4.8 Setting the management LAN IP address	195
6.4.9 Installing a PSA update	196
6.4.10 Uninstalling PSA	199
6.5 Setting Up the Dump Environment (Windows)	203
6.5.1 Memory dump files and paging files	203

6.6 Setting Up the Dump Environment (Linux)	204
6.7 Configuring the NTP Client	205
6.8 Saving Management and Configuration Information	206
6.8.1 Saving PSA management information	206
6.8.2 Saving MMB configuration information	208
6.8.3 Saving BIOS configuration information	209
6.9 Configuring Service Life Monitoring by RAS Support Service	211
6.9.1 BBU service life monitoring for a RAID card	211
6.9.2 Battery unit service life monitoring for a UPS	213
6.10 Recommended Write Policy Setting for SAS Disk RAID Units	214
6.11 Recovery Procedure after the Execution of the Simple Setup Tool (editconf.sh)	215
CHAPTER 7 Work after Installation	217
7.1 Duplicate Network Adapter Configuration	218
7.2 Configuring NTP	219
7.2.1 How NTP operates in the PRIMEQUEST 1000 series	219
7.2.2 Setting an NTP server	220
7.3 Configuring a DNS Server	223
7.4 Configuring SMTP	224
7.5 Configuring Security	225
7.5.1 Configuring access control	225
7.5.2 Configuring SNMP	228
7.5.3 Configuring SSH	231
7.5.4 Configuring HTTPS	232
7.6 Scheduled Operations	234
CHAPTER 8 Powering On and Off a Partition	235
8.1 Powering On and Off a Partition	236
8.1.1 Powering on a partition	236
8.1.2 Powering off a partition	237
APPENDIX A Lists of Settings (Links)	239
A.1 MMB Settings	240
A.2 PSA Settings	241
A.3 UEFI Settings	242
A.4 BMC Settings	243
APPENDIX B Manual PSA Installation and Uninstallation	245
B.1 Manually Installing PSA (Linux: Red Hat Enterprise Linux)	246
B.1.1 Installation flow	246
B.1.2 Checks before PSA installation	246
B.1.3 Installing PSA	249
B.1.4 Automatic configuration during PSA installation	249
B.1.5 Restarting the partition	250
B.1.6 Settings after PSA installation	250
B.1.7 Installing a PSA update	254
B.1.8 Uninstalling PSA	254
B.2 Manually Installing PSA (Windows Server 2003)	255
B.2.1 Installation flow	255
B.2.2 Checks before PSA installation	256
B.2.3 Installing PSA	257
B.2.4 Automatic configuration during PSA installation	259
B.2.5 Settings after PSA installation	260
B.2.6 Installing a PSA update	260
B.2.7 Uninstalling PSA	260
B.3 Manually Installing PSA (Windows Server 2008)	261
B.3.1 Installation flow	261
B.3.2 Checks before PSA installation	262
B.3.3 Installing PSA	263

B.3.4 Automatic configuration during PSA installation	266
B.3.5 Settings after PSA installation	267
APPENDIX C Software (Links)	269
C.1 General Description and Types of Bundled Software	270
APPENDIX D Configuring the SAN Boot Environment	271
APPENDIX E Notes on VMware Installation	272
E.1 Building a RAID Environment Using VMware 4.x Built-in Disks	273
E.2 Notes on VMware 4.x Installation	274
E.3 Installing VMware 4.x Bundled Software	277
E.3.1 Installing ServerView Agent	277
E.3.2 Installing ServerView RAID	277
E.3.3 Installing RAS Support Service (PRIMEQUEST)	277
E.3.4 Installing VMware 4.x HRM/server (PRIMEQUEST)	278
E.3.5 Installing VMware 4.x PSA	280
E.3.6 Installing SVMco	281
E.4 Settings after VMware 4.x PSA Installation	282
E.4.1 Configuring the network	282
E.4.2 Configuring the firewall	288
E.4.3 Configuring the default gateway	289
E.4.4 Retrieving VMware 4.x PSA maintenance information	290
E.4.5 Notes on VMware 4.x PSA	291
E.5 Settings after VMware 4.x SVMco Installation	292
E.6 Building a RAID Environment Using VMware 5.x Built-in Disks	293
E.7 Installing VMware 5.x Bundled Software	294
E.7.1 Installing ServerView RAID	294
E.7.2 Configuring BBU service life monitoring	294
E.7.3 Installing and setting SVMcovm	294
APPENDIX F Setting up the NTP Server (Windows)	295
F.1 Overview of NTP Client Settings	296
F.2 NTP Settings in Windows Server 2003	298
F.2.1 Specifying an NTP Server	298
F.2.2 Synchronization Interval Setting	298
F.3 NTP Settings in Windows Server 2008	301
F.3.1 Specifying an NTP Server	301
F.3.2 Synchronization Interval Setting	302
F.3.3 Event Task Settings	303
F.4 NTP Settings in Windows Server 2008 R2	307
F.4.1 Specifying an NTP Server	307
F.4.2 Synchronization Interval and Startup Settings of NTP Service	308
F.4.3 Event Task Settings	309
F.5 NTP Settings in Windows Server 2012	315
F.5.1 Specifying an NTP Server	315
F.5.2 Synchronization Interval and Startup Settings of NTP Service	316
F.5.3 Event Task Settings	318
Index	325

Figures

Warning label location (PRIMEQUEST 1800E2/1800E rear)	xi
Warning label location (PRIMEQUEST 1800E2/1800E rear) (IOBs removed)	xii
Warning label location (PCI_Box)	xii
FIGURE 2.1 Power cable socket locations (PRIMEQUEST 1800E2/1800E)	15
FIGURE 2.2 Power cable socket locations (PCI_Box)	15
FIGURE 3.1 Mounting location and external interfaces of the MMB	21
FIGURE 3.2 MMB USER port location	23
FIGURE 3.3 Network configuration and IP addresses of the management LAN	24
FIGURE 3.4 MMB Web-UI login window	26
FIGURE 3.5 Information displayed in the window	27
FIGURE 3.6 Maintenance status display	28
FIGURE 3.7 Submenu area	29
FIGURE 3.8 Content area	30
FIGURE 3.9 [Network Interface] window (example)	33
FIGURE 3.10 [Network Protocols] window (example)	34
FIGURE 3.11 [Network Interface] window (example)	35
FIGURE 3.12 [Alarm E-Mail] window (example)	36
FIGURE 3.13 [Alarm E-Mail Filtering Condition] window (example)	37
FIGURE 3.14 [User List] window (example)	38
FIGURE 3.15 [Add User] window (example)	38
FIGURE 3.16 [Edit User] window (example)	39
FIGURE 3.17 [System Information] window (example)	40
FIGURE 3.18 [Date/Time] window (example)	41
FIGURE 3.19 [Management LAN Port Configuration] window (example)	42
FIGURE 3.20 [Partition Configuration] window (example)	43
FIGURE 3.21 [Add SB/IOB/GSPB to Partition] window (example)	44
FIGURE 3.22 [Partition Configuration] window (example)	45
FIGURE 3.23 [Remove SB/IOB/GSPB from Partition] window (example)	46
FIGURE 3.24 [Partition Home] window (example)	47
FIGURE 3.25 [Reserved SB Configuration] window (example)	48
FIGURE 3.26 BlueScreenTimeout setting ([Configuration] tab)	50
FIGURE 3.27 BlueScreenTimeout setting ([Misc] settings)	51
FIGURE 3.28 [Partition Configuration] window (example)	52
FIGURE 3.29 [Mode] window (example)	54
FIGURE 3.30 [Console Redirection Setup] window (example)	55
FIGURE 3.31 [Information] window (example)	56
FIGURE 3.32 Backup/Restore MMB Configuration window (example)	57
FIGURE 4.1 Example of display of the [Change Boot Order] menu	63
FIGURE 4.2 Example of display of the [Change Boot Order] menu	69
FIGURE 4.3 Example of display of the [Change Boot Order] menu	75
FIGURE 4.4 [Mode] window (example)	76
FIGURE 4.5 [Install Windows] window	77
FIGURE 4.6 [Install Windows] window	77
FIGURE 4.7 Example of display of the [Change Boot Order] menu	84
FIGURE 4.8 [Mode] window (example)	85
FIGURE 4.9 [Install Windows] window	86
FIGURE 4.10 [Install Windows] window	86
FIGURE 4.11 Example of display of the [Change Boot Order] menu	99
FIGURE 4.12 Example of display of the [Change Boot Order] menu	103
FIGURE 4.13 Example of display of the [Change Boot Order] menu	107
FIGURE 4.14 Example of display of the [Change Boot Order] menu	112
FIGURE 5.1 Example of the Device Manager menu	119
FIGURE 5.2 Main menu (sadump)	119
FIGURE 5.3 sadump setup menu	120
FIGURE 5.4 sadump setup menu	120
FIGURE 5.5 Main menu (sadump)	121

FIGURE 5.6 Dump device maintenance menu	121
FIGURE 5.7 Dump device configuration menu	122
FIGURE 5.8 Dump device selection menu	122
FIGURE 5.9 Dump device selection menu	123
FIGURE 5.10 Dump device configuration menu	124
FIGURE 5.11 Dump device maintenance menu	124
FIGURE 5.12 Dump device setting menu	125
FIGURE 5.13 Dump device list menu	125
FIGURE 5.14 Dump Device Setting Menu	126
FIGURE 5.15 Dump device maintenance menu	126
FIGURE 5.16 Main menu (sadump)	127
FIGURE 5.17 [Backup/Restore MMB Configuration] window (example)	133
FIGURE 5.18 [Backup BIOS Configuration] window (example)	134
FIGURE 5.19 RAS Support Service screens (no BBU)	135
FIGURE 5.20 RAS Support Service screens (move to another partition)	136
FIGURE 6.1 [Add a Port] dialog box (PSA)	168
FIGURE 6.2 [Add a Port] dialog box (SNMP)	169
FIGURE 6.3 Preparing to Install window	171
FIGURE 6.4 Update installation window	172
FIGURE 6.5 Update installation complete window	173
FIGURE 6.6 Confirmation message dialog box	173
FIGURE 6.7 Uninstall Complete window	174
FIGURE 6.8 Windows Firewall window	181
FIGURE 6.9 [General] tab in [SNMP Service (UDP In) Properties]	182
FIGURE 6.10 [Scope] tab in [SNMP Service (UDP In) Properties]	183
FIGURE 6.11 [IP Address] dialog box	184
FIGURE 6.12 New Inbound Rule Wizard - Rule Type	185
FIGURE 6.13 New Inbound Rule Wizard - Program	186
FIGURE 6.14 New Inbound Rule Wizard - Protocol and Ports	187
FIGURE 6.15 New Inbound Rule Wizard - Scope	188
FIGURE 6.16 New Inbound Rule Wizard - Action	189
FIGURE 6.17 New Inbound Rule Wizard - Profile	190
FIGURE 6.18 New Inbound Rule Wizard - Name	191
FIGURE 6.19 New Outbound Rule Wizard - Protocol and Ports	192
FIGURE 6.20 New Outbound Rule Wizard - Protocol and Ports	194
FIGURE 6.21 Preparing to Install window	197
FIGURE 6.22 Update installation window	197
FIGURE 6.23 Update installation complete window	198
FIGURE 6.24 Program removal window	199
FIGURE 6.25 [Program and Features] window	200
FIGURE 6.26 Preparing to Install window	201
FIGURE 6.27 Confirmation message dialog box	201
FIGURE 6.28 Uninstall Complete window	202
FIGURE 6.29 [Export List] window (example)	207
FIGURE 6.30 [Export] window (example)	208
FIGURE 6.31 [Backup/Restore MMB Configuration] window (example)	209
FIGURE 6.32 [Backup BIOS Configuration] window (example)	210
FIGURE 6.33 RAS Support Service screens (no BBU)	212
FIGURE 6.34 RAS Support Service screens (move to another partition)	212
FIGURE 7.1 External network configuration	218
FIGURE 7.2 Operation with external NTP servers (three NTP servers)	220
FIGURE 7.3 [Date/Time] window (example)	221
FIGURE 7.4 [Access Control] window (example)	226
FIGURE 7.5 [Add Filter] window (example)	227
FIGURE 7.6 [Network Protocols] window (example)	228
FIGURE 7.7 [SNMP Community] window (example)	229
FIGURE 7.8 [SNMP Trap] window (example)	230
FIGURE 7.9 [SNMP v3 Configuration] window (example)	231

FIGURE 7.10 [Network Protocols] window (example)	232
FIGURE 7.11 [Network Protocols] window (example)	233
FIGURE 8.1 [Power Control] window (example)	236
FIGURE 8.2 [Power Control] window (example)	238
FIGURE B.1 Preparing to Install window	257
FIGURE B.2 Setup window	258
FIGURE B.3 Select Features window	258
FIGURE B.4 Setup complete window	259
FIGURE B.5 Select Features window	263
FIGURE B.6 Preparing to Install window	264
FIGURE B.7 Setup window	264
FIGURE B.8 Select Features window	265
FIGURE B.9 Installation complete window	266
FIGURE E.1 Completion of VMware 4.x installation	274
FIGURE E.2 [Watchdog] tab in the VMware 4.x software window	275
FIGURE E.3 [Server Configuration] window	275
FIGURE E.4 [Software Watchdog] window	276
FIGURE E.5 Network configuration immediately after installation of OS	283
FIGURE E.6 Network configuration after setup	288
FIGURE E.7 VMware vSphere 4.x Client	289
FIGURE E.8 [DNS and Routing Configuration] dialog box	290
FIGURE F.1 [Date and Time Properties] window (1)	298
FIGURE F.2 [Date and Time Properties] window (2)	298
FIGURE F.3 [Run] window	299
FIGURE F.4 [Registry Editor] window	299
FIGURE F.5 [Services] window	300
FIGURE F.6 [Date and Time] window (1)	301
FIGURE F.7 [Date and Time] window (2)	301
FIGURE F.8 [Internet Time Settings] window	302
FIGURE F.9 [Run] window	302
FIGURE F.10 [Registry Editor] window	302
FIGURE F.11 [Services] window	303
FIGURE F.12 [Task Scheduler] window	303
FIGURE F.13 [Create Basic Task Wizard] window (Create a Basic Task)	304
FIGURE F.14 [Create Basic Task Wizard] window (Task Trigger)	304
FIGURE F.15 [Create Basic Task Wizard] window (When a Specific Event Is Logged)	304
FIGURE F.16 [Create Basic Task Wizard] window (Action)	305
FIGURE F.17 [Create Basic Task Wizard] window (Start a Program)	305
FIGURE F.18 [Create Basic Task Wizard] window (Summary)	305
FIGURE F.19 [Properties] dialog box	306
FIGURE F.20 [Select User or Group] window	306
FIGURE F.21 [Date and Time] window (1)	307
FIGURE F.22 [Date and Time] window (2)	307
FIGURE F.23 [Internet Time Settings] window	308
FIGURE F.24 [Run] window	308
FIGURE F.25 [Registry Editor] window	308
FIGURE F.26 [Services] window	309
FIGURE F.27 [Windows Time Properties] window	309
FIGURE F.28 [Task Scheduler] window	310
FIGURE F.29 [Create Basic Task Wizard] window (Create a Basic Task)	310
FIGURE F.30 [Create Basic Task Wizard] window (Task Trigger)	311
FIGURE F.31 [Create Basic Task Wizard] window (When a Specific Event Is Logged)	311
FIGURE F.32 [Create Basic Task Wizard] window (Action)	312
FIGURE F.33 [Create Basic Task Wizard] window (Start a Program)	312
FIGURE F.34 [Create Basic Task Wizard] window (Summary)	313
FIGURE F.35 [Properties] dialog box	313
FIGURE F.36 [Select User or Group] window	313
FIGURE F.37 [Date and Time] window (1)	315

FIGURE F.38 [Date and Time] window (2)	316
FIGURE F.39 [Internet Time Settings] window	316
FIGURE F.40 [Registry Editor] selection window	317
FIGURE F.41 [Registry Editor] window	317
FIGURE F.42 [Services] window	317
FIGURE F.43 [Windows Time Properties] window	318
FIGURE F.44 [Task Scheduler] window	319
FIGURE F.45 [Create Basic Task Wizard] window (Create a Basic Task)	319
FIGURE F.46 [Create Basic Task Wizard] window (Task Trigger)	320
FIGURE F.47 [Create Basic Task Wizard] window (When a Specific Event Is Logged)	320
FIGURE F.48 [Create Basic Task Wizard] window (Action)	321
FIGURE F.49 [Create Basic Task Wizard] window (Start a Program)	321
FIGURE F.50 [Create Basic Task Wizard] window (Summary)	322
FIGURE F.51 [Properties] dialog box	322
FIGURE F.52 [Select User or Group] window	323

Tables

TABLE 1.1 Work performed by the user	2
TABLE 2.1 Accessories required in main unit installation	11
TABLE 3.1 MMB connection and configuration flow	20
TABLE 3.2 External interfaces of the MMB	21
TABLE 3.3 Settings for terminal software	21
TABLE 3.4 Required settings for external LAN connections	24
TABLE 3.5 URL to enter for login	26
TABLE 3.6 Default user account and password	26
TABLE 3.7 System status indicators	28
TABLE 3.8 Buttons in the title area	31
TABLE 3.9 Status indicator types	31
TABLE 3.10 Setting various modes	52
TABLE 4.1 Operating system installation by SVIM	62
TABLE 4.2 Operating system installation by SVIM	68
TABLE 4.3 Operating system installation by SVIM	74
TABLE 4.4 If the folder contains two files	79
TABLE 4.5 If the folder contains one file	79
TABLE 4.6 Operating system installation by SVIM	83
TABLE 4.7 If the folder contains two files	88
TABLE 4.8 If the folder contains one file	88
TABLE 4.9 Operating system installation by SVIM	98
TABLE 4.10 Operating system installation by SVIM	102
TABLE 4.11 Operating system installation by SVIM	106
TABLE 4.12 Ports to open for the PSA-to-MMB communication LAN interface	108
TABLE 4.13 Operating system installation by SVIM	110
TABLE 4.14 Ports to open for the PSA-to-MMB communication LAN interface	113
TABLE 5.1 Types of work	116
TABLE 5.2 Message for advance notification of replacement and replacement notification message (RAID card)	135
TABLE 5.3 Message for advance notification of replacement and replacement notification message (UPS) 137	
TABLE 6.1 Types of work	140
TABLE 6.2 Confirmation of the required settings for PSA operation, and corresponding features about the settings	141
TABLE 6.3 Settings automatically added/changed during PSA installation	142
TABLE 6.4 Ports to open for the management LAN interfaces	147
TABLE 6.5 Ports to open for the PSA-to-MMB communication LAN interfaces	151
TABLE 6.6 secLevel settings	154
TABLE 6.7 Confirmation of the required settings for PSA operation, and corresponding features about the settings	161
TABLE 6.8 Settings automatically added/changed during PSA installation	162
TABLE 6.9 Confirmation of the required settings for PSA operation, and corresponding features about the settings	175
TABLE 6.10 Settings automatically added/changed during PSA installation	176
TABLE 6.11 [Protocol and Ports] setting items	186
TABLE 6.12 [Scope] setting items	187
TABLE 6.13 [Protocol and Ports] setting items	192
TABLE 6.14 [Scope] setting items	192
TABLE 6.15 [Scope] setting items	194
TABLE 6.16 Message for advance notification of replacement and replacement notification message (RAID card)	211
TABLE 6.17 Message for advance notification of replacement and replacement notification message (UPS) 213	
TABLE B.1 Packages required for PSA operation (RHEL5)	247
TABLE B.2 Packages required for PSA operation (RHEL6)	247
TABLE B.3 Packages required for SIRMS operation (RHEL6)	248

TABLE B.4 Settings automatically added/changed during PSA installation 249

TABLE E.1 Settings after PSA Installation (VMware 4.x) 282

TABLE E.2 IP addresses to be set for virtual ports 287

TABLE E.3 Configuring the firewall for PSA operation 288

TABLE E.4 Examples of firewall configurations 288

TABLE E.5 VMware 5.x bundled software and its installation destination 294

TABLE E.6 VMware 5.x setting procedure and setting destination 294

TABLE F.1 Settings for system clock synchronization 296

CHAPTER 1 Installation Overview

This chapter describes the workflow up to actual operation of the PRIMEQUEST 1000 series server.

For an overview of the hardware and software and the part names and functions of the server, see the *PRIMEQUEST 1000 Series General Description* (C122-B022EN).

1.1 Setup Workflow	2

1.1 Setup Workflow

This section describes the workflow for the tasks required to prepare the PRIMEQUEST 1000 series server for operation.

Setup work consists of tasks performed by a field engineer and other tasks performed by the user.

The setup workflow is described below.



Field engineers perform the following tasks on this product.

Customers must not perform these tasks under any circumstances. Otherwise, electric shock, injury, or fire may result.

- Newly installing or moving equipment
- Removing the front, rear, and side covers
- Installing and removing built-in options
- Connecting and disconnecting external interface cables
- Maintenance (repair and periodic diagnosis and maintenance)

1.1.1 Work performed by a field engineer

A field engineer sets up the unit. This includes the following tasks:

- Checking mounted components
- Preparing for main unit installation
- Checking partitions ... etc.

Remarks

The following tasks need to be completed before the user starts the setup work:

- Unit setup by a field engineer
- MMB setup within the scope of responsibility of the field engineer
- Running test programs ... etc.

1.1.2 Work performed by the user

The user performs the following tasks in the order given.

TABLE 1.1 Work performed by the user

No.	Work item	Work tasks and description	See
1.	Setup	- Initializing partition settings Perform tasks such as setting partition names and configuring partitions individually.	3.1.2 Partition settings
		- Connecting and configuring the MMB (operating environment) - Setting up the connection environment for actual operation Set up the MMB connection environment, such as by setting the IP addresses for actual operation.	3.3.3 Setting up the connection environment for actual operation

No.	Work item	Work tasks and description	See
		- Initializing MMB settings Set the parameters for the entire MMB, such as the user account names or system names.	3.3.10 Registering a user account 3.3.11 Setting the system name 3.3.12 Setting the date and time
		- Setting various modes Set modes as needed.	3.4.5 Setting various modes
		- Starting the system and confirming system startup Start the system and confirm that it has started normally.	3.2 Starting the System
		- Saving setting information Save the setting information for the MMB.	3.5 Saving Configuration Information
2.	Installing the OS and bundled software	Install the operating system and bundled software.	CHAPTER 4 Installing the Operating System and Bundled Software
3.	Work after installation	Specify the monitoring method, and save the specified information.	CHAPTER 5 Work after Operating System Installation (PRIMEQUEST 1800E2) CHAPTER 6 Work after Operating System Installation (PRIMEQUEST 1800E)
4.	Configuring SNMP and security	Configure SNMP and security.	CHAPTER 7 Work after Installation

CHAPTER 2 Preparing for Main Unit Installation

This chapter describes the preparation before main unit installation.

This preparation includes work up to power cable connection.

2.1 Safety Precautions	6
2.2 Before Installing the Main Unit	7
2.3 Checking Environmental Conditions	8
2.4 Preparing the Power Supply Equipment	9
2.5 Checking the Installation Site	10
2.6 Preparing to Install the Main Unit	11
2.7 Confirming the Supplied Parts	12
2.8 Mounting the Main Unit in a 19-inch Rack	13
2.9 Connecting the Power Cables	14

2.1 Safety Precautions

Observe the following precautions when installing the main unit.



Failure to do so cause damage to the unit or abnormal operation.

- Follow the precautions, warnings, and instructions shown on the main unit.
- Do not block the vent holes.
- Do not install the main unit in a location exposed to direct sunlight or close to a device that may generate large amounts of heat.
- Do not install the main unit in a location exposed to large amounts of dust, corrosive gas, or salt spray.
- Do not install the main unit in a location subject to strong vibration. Install the main unit on a flat surface.
- Use grounded Category 3 wiring or better. Using another type of grounded wiring may cause abnormal operation.
- Do not route cables under the main unit. Do not allow cables to become taut.
- Do not disconnect the power cables while the main unit power is on.
- If it is hard to push the connector latch of a LAN cable or other cable when attempting to disconnect the cable, push it with a flathead screwdriver. Forcibly inserting a finger may cause personal injury or damage the unit.
- Do not place anything on top of the main unit. Do not work above or on top of the main unit.
- Prevent rapid rises in the ambient temperature during winter. Such an abrupt temperature change may cause condensation to form in the main unit. Allow sufficient warm-up time before starting operation.
- Do not install the main unit close to a photocopier, air-conditioning unit, welder, or other device that generates electromagnetic noise.
- Do not install the main unit close to a device that generates large amounts of electrical noise.
- When installing the main unit, do not connect it to the power supply line for an elevator in the facility, since this would expose it to sudden voltage drops.
- Implement antistatic measures at the installation site.
- Confirm that the power supply voltage and frequency are adequate according to the respective ratings shown on the main unit.
- Do not insert or drop foreign matter into the openings of the main unit. The main unit contains high-voltage components. If any metallic matter or other electro-conductive object enters the main unit through an opening, it may cause a short circuit. This may lead to fire, electric shock, or damage to the main unit.
- For details on maintenance of the main unit, contact the distributor where you purchased your product, or your sales representative.

2.2 Before Installing the Main Unit

Be sure that you understand the system configuration and have acquired all the requisite installation information before installing the main unit.

For a system overview and details on the system configuration, see the *PRIMEQUEST 1000 Series General Description* (C122-B022EN). For details on the installation prerequisites, see the *PRIMEQUEST 1000 Series Hardware Installation Manual* (C122-H004EN).

2.3 Checking Environmental Conditions

This section describes the environmental conditions covered by the specifications for main unit installation.

The conditions of the main unit operating environment depend on the altitude at the installation site.

For details on the environmental conditions of the PRIMEQUEST 1000 series, see 1.3 Installation Specifications in the *PRIMEQUEST 1000 Series Hardware Installation Manual* (C122-H004EN).

For details on the recommended temperature and humidity of the computer room, see the *SPARC Enterprise/PRIMEQUEST Common Installation Planning Manual* (C120-H007EN).

2.4 Preparing the Power Supply Equipment

This section describes the electrical specifications, facility power requirements, and grounding for the PRIMEQUEST 1000 series.

To prevent accidents, confirm that the power supply equipment can supply enough power to the system. Electrical engineering and installation work shall conform to local ordinances and local and national government regulations. For details on the power supply equipment, see the *SPARC Enterprise/PRIMEQUEST Common Installation Planning Manual* (C120-H007EN).

2.4.1 Electrical specifications

For details on the electrical specifications of the PRIMEQUEST 1000 series, see 1.3 Installation Specifications in the *PRIMEQUEST 1000 Series Hardware Installation Manual* (C122-H004EN).

For details on the power cables, see 2.2.1 Basic interfaces and peripheral devices (PRIMEQUEST 1800E2) or 2.2.2 Basic interfaces and peripheral devices (PRIMEQUEST 1800E) in the *PRIMEQUEST 1000 Series Hardware Installation Manual* (C122-H004EN).

For details on the connectors and their shapes, see 2.4.1 PRIMEQUEST 1000 series main unit in the *PRIMEQUEST 1000 Series Hardware Installation Manual* (C122-H004EN).

2.4.2 Facility power requirements and characteristics

To obtain the required degree of redundancy, the facility must have two independent supplies of power. Connect the circuit breakers to the power receiver provided by the electric power company or to a UPS (uninterruptible power supply).

If the main unit operates in an environment that experiences frequent power failures or has a power source that often becomes unstable, the component failure rate tends to rise.

The PRIMEQUEST 1000 series supports the basic connection configurations shown in the following diagrams:

- Power line diagram for redundant power connections
- Power line diagram for dual power connections

For details on the power line configurations for redundant power connections and dual power connections, see 2.3 Power Cable Connections in the *PRIMEQUEST 1000 Series Hardware Installation Manual* (C122-H004EN).

2.4.3 Grounding

The PRIMEQUEST 1000 series is shipped with grounded (three-wire) power cables. You need to connect the power cables to outlets with ground terminals. To determine the type of power supply in your building, contact the building manager or a qualified electrical engineer.

2.5 Checking the Installation Site

Before installing the main unit, confirm that the installation site has enough space for the required service (maintenance) area and for accommodating the peripheral devices. For details on checks of the installation site, see Chapter 1 Installation Information in the *PRIMEQUEST 1000 Series Hardware Installation Manual* (C122-H004EN).

2.6 Preparing to Install the Main Unit

TABLE 2.1 Accessories required in main unit installation lists the accessories required in main unit installation. Prepare these accessories in advance.

TABLE 2.1 Accessories required in main unit installation

Accessory name	Description
No. 2 Phillips screwdriver	Used to mount the unit in a rack.
Wrist strap	Used to prevent main unit damage from static electricity discharged from your body.
Conductive mat	Required for some system configurations. To order any of the accessories, contact the distributor where you purchased your product, or your sales representative.
Ethernet Category 5 cable or better	
Console PC-to-LAN cable (for user LAN)	
External switching hub	Used to connect the PRIMEQUEST 1000 series server to an external switching hub via a LAN.
Multitester	Used to check the input AC voltage.

2.7 Confirming the Supplied Parts

Confirm that the supplied parts match the shipping list provided with the main unit.

If any of the parts listed in the shipping list or performance records are missing, incorrect, or damaged, contact the distributor where you purchased your product, or your sales representative.

Note

If you also purchased optional modules for installation, such as additional memory modules or PCI Express cards, first confirm that the main unit functions normally before mounting the optional modules in the main unit.

2.8 Mounting the Main Unit in a 19-inch Rack

The PRIMEQUEST 1000 series server is mounted for use in a 19-inch rack. For details on mounting, see Appendix A Racks in the *PRIMEQUEST 1000 Series Hardware Installation Manual* (C122-H004EN).

2.9 Connecting the Power Cables

This section describes how to connect the power cables.

The main unit and PCI_Box are shipped with (three-wire) power cables equipped with a grounded plug. You need to connect the power cables to outlets with ground terminals.

Remarks

The main unit and PCI_Box are designed to operate with a power supply facility that supports grounded wiring. Do not connect the main unit and PCI_Box to a power supply facility that does not provide grounded wiring. To determine the type of power supply in your building, contact the building manager or a qualified electrical engineer.

Operations

1. Confirm with an on-site electrical engineer that the input power satisfies power requirements. For details on the power requirements, see 1.3 Installation Specifications in the *PRIMEQUEST 1000 Series Hardware Installation Manual* (C122-H004EN).
2. Confirm that the power cables are connected to the AC inlets of the main unit and PCI_Box. Also confirm that the power cables are secured with the AC cord clamps for the AC inlets on the main unit.
3. Group all the cables that run outside the main unit and PCI_Box into power cables and signal cables, and secure them firmly to the cable holders of the 19-inch rack with cable ties.
4. Confirm that the AC power breaker is off. Then, connect the power cables to AC power. For details on the power cable connections, see [2.4.2 Facility power requirements and characteristics](#).

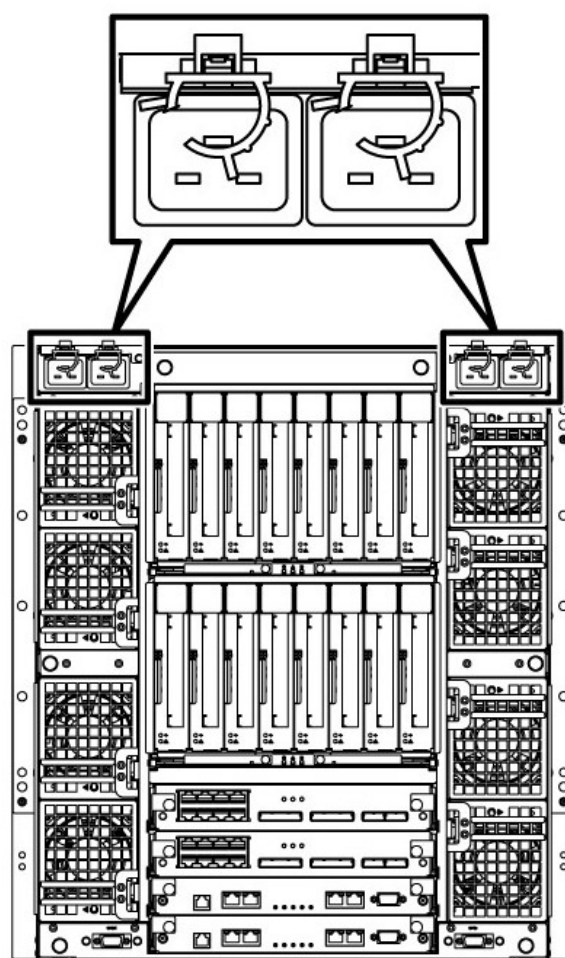


FIGURE 2.1 Power cable socket locations (PRIMEQUEST 1800E2/1800E)

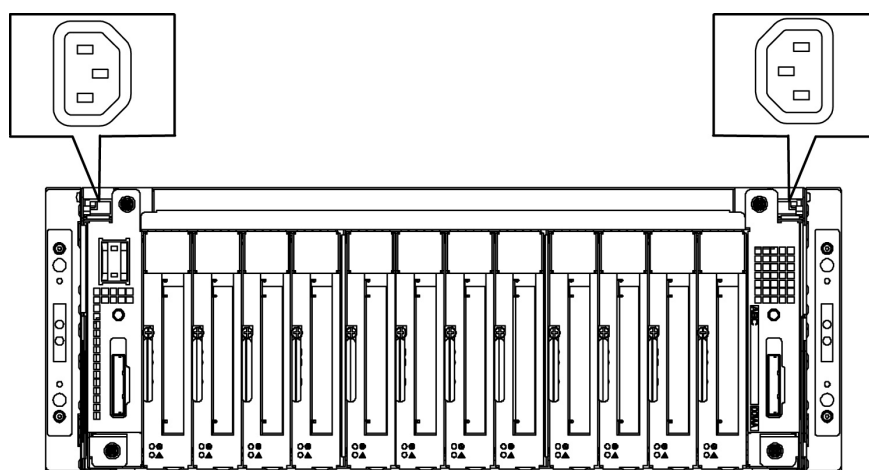


FIGURE 2.2 Power cable socket locations (PCI_Box)

CHAPTER 3 Work before Operating System Installation

This chapter describes the work that must be done before you install an operating system on the PRIMEQUEST 1000 series server. The chapter also describes the settings required for practical operation and the necessary setup work.

3.1 Before Starting Setup	18
3.2 Starting the System	19
3.3 Connecting and Configuring the MMB	20
3.4 Configuring a Partition	43
3.5 Saving Configuration Information	57

3.1 Before Starting Setup

This section describes the decisions that must be made before you start setup.

3.1.1 MMB settings

You need to decide the following to configure the MMB:

- IP address, host name, subnet mask, and gateway address
- IP address of the PC used as the MMB console (referred to below as the MMB console PC)
- User accounts
- Name of the PRIMEQUEST 1000 series system (also used as the SNMP system name)
- Management LAN environment ... etc.

For details on MMB settings, see [3.3 Connecting and Configuring the MMB](#).

Note

The management LAN, PSA-to-MMB communication LAN, and remote maintenance LAN must be configured as networks with different subnet masks.

3.1.2 Partition settings

You need to decide the following before using the partitioning functions to configure multiple partitions:

- Number of partitions
- Partition names
- Partition configuration
- Home SB

For details on partition settings, see [3.4 Configuring a Partition](#).

Remarks

If each partition has the same name as the host name of the operating system installed on the partition, partition management is easier.

3.2 Starting the System

This section describes power control for system startup.

Use the following power-on procedure only when the power to the main unit is off.

3.2.1 Powering on and off the main unit

This section describes how to power on and power off the main unit.

Power on

The system will power on when the power cable is connected to the AC inlet on the main unit and to the AC power supply (or the optional power distribution box). Confirm that the power cable is connected. The system will power on when the circuit breaker of the AC power supply is on. (For details on the power cable connections, see [2.9 Connecting the Power Cables](#).)

To power on the system again after disconnecting the power cable, connect the power cable to the AC inlet on the main unit and to the AC power supply.

Notes

- After disconnecting the power cable from the AC inlet, wait at least 10 seconds before reconnecting the power cable to power on the system again.
- The detection of an overcurrent trips the breaker of the AC power supply (or the optional power distribution box) to cut off power. The overcurrent indicates that a malfunction such as a short circuit occurred in the main unit. In such cases, do not power on the system again. Instead, contact your sales representative or a field engineer.

Power off

The procedure for turning off the main power is as follows.



(Damage to data)

Confirm that the System Power LED of the DVDB is off before turning off the main power (e.g., UPS, power distribution box). If you turn off the main power (e.g., UPS, power distribution box) while the System Power LED of the DVDB is on, data may be damaged.

Operations

1. Power off the main unit. Power it off from the MMB. For details, see [8.1.2 Powering off a partition](#).
2. Confirm that the System Power LED of the DVDB is off.

Remarks

If the System Power LED of the DVDB is on, the system cannot be powered off. If the Alarm LED is on, contact your sales representative or a field engineer.

3. Disconnect the power cable from the power distribution box.

3.3 Connecting and Configuring the MMB

A field engineer will have constructed a test environment for the MMB to run test programs in it. Therefore, you need to reconfigure the MMB to switch from the test environment to that for actual operation. Skip the steps for items already set by the field engineer.

After connecting the MMB, perform the following from the MMB Web-UI:

- Registering a user account
- Configuring security
- Setting the time ... etc.

Connect and configure the MMB by using the following procedures.

TABLE 3.1 MMB connection and configuration flow

Procedure	Item	Description	See
1.	Connecting the MMB console PC	Connect the MMB console PC to set up the environment for actual operation.	- 3.3.1 Connecting the MMB console PC
2.	Initializing MMB settings	Initialize MMB settings before setting up the connection environment for actual operation.	- 3.3.2 Initializing MMB settings
3.	Setting up the connection environment for actual operation	The MMB is set for a test connection. Set up the connection environment for actual operation.	- 3.3.3 Setting up the connection environment for actual operation
4.	Logging in to the MMB	Log in to the MMB. There is also a description of the MMB Web-UI window for reference.	- 3.3.4 Logging in to the MMB - 3.3.5 How to view the Web-UI window
5.	Configuring the network for actual operation	The MMB is set for testing purposes, so configure the network and Web servers for actual operation. Make the required settings appropriate to your operation mode.	- 3.3.6 Configuring the MMB network - 3.3.7 Configuring telnet - 3.3.8 Configuring a DNS server - 3.3.9 Configuring Alarm E-Mail
6.	Initializing MMB settings	Initialize MMB settings. - Registering a user account - Setting the system name - Setting the date and time After you initialize the above settings, we recommend backing up the setting information. For details on how to back up the specified information, see 3.5 Saving Configuration Information .	- 3.3.10 Registering a user account - 3.3.11 Setting the system name - 3.3.12 Setting the date and time

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

3.3.1 Connecting the MMB console PC

This section describes how to connect the MMB console PC.

To reconfigure the system for actual operation, connect the COM port on the MMB console PC to the RS-232C port (external interface) on the MMB by using an RS-232C crossover cable. For details on the mounting location and external interfaces of the MMB, see [FIGURE 3.1 Mounting location and external interfaces of the MMB](#).

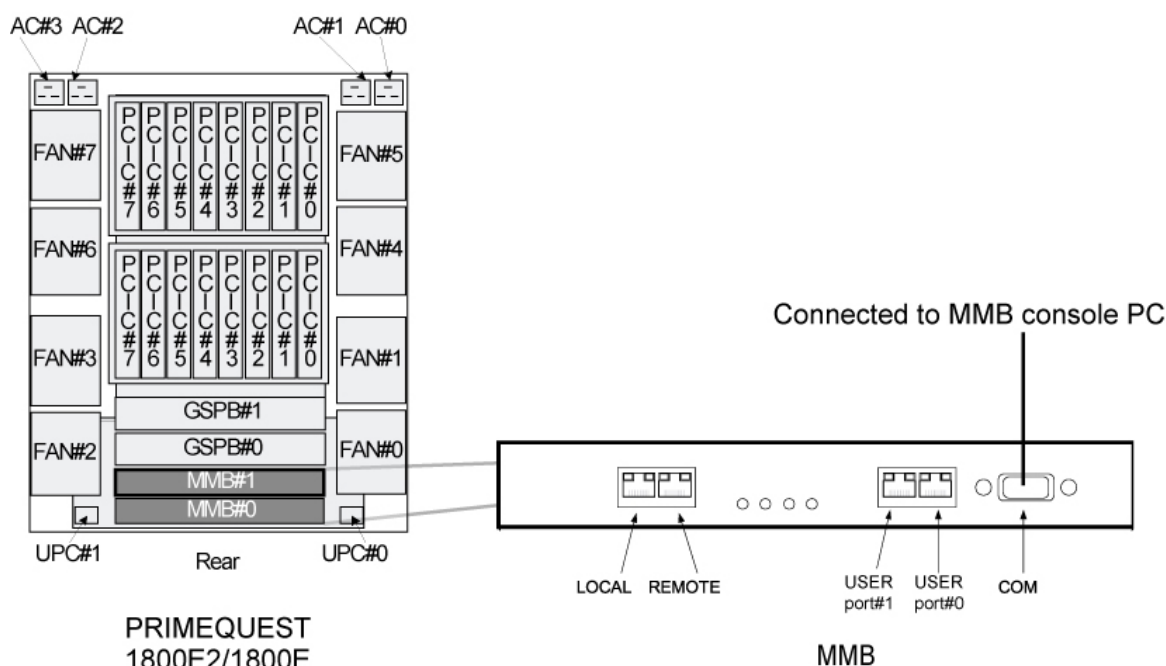


FIGURE 3.1 Mounting location and external interfaces of the MMB

TABLE 3.2 External interfaces of the MMB

External interface	Quantity	Remarks
RS-232C (COM port)	1	A field engineer uses this port to set up the device. It is not used in ordinary operation.
LAN 100Base-TX	2	Ports used for maintenance - LOCAL: CE port - REMOTE: REMCS port
LAN 1000Base-T	2	USER port

Make the following settings for the terminal software for the COM port connection.

TABLE 3.3 Settings for terminal software

Setting item	Value
Bits per second	19200

Setting item	Value
Data bit	8
Parity	None
Stop bit	1
Flow control	None
Emulation	VT100

3.3.2 Initializing MMB settings

The procedure for initializing MMB settings is as follows.

If the field engineer has already made the settings, you can skip the following procedure.

Operations

1. Power on the main unit.
>> The Alarm LED of each unit goes on while the MMB Ready LED is blinking (initialization in progress).
The login prompt appears.
2. Log in with Administrator privileges using the terminal software from the MMB console PC.
>> When you first log in, you will be asked to change the Administrator password.

3. Set a password.

Note

You need to set a hard-to-guess password consisting of at least eight characters.

If you enter an inappropriate password, you will be asked to enter another password.

4. Configure the MMB network.

Execute the command shown below to set the IP address.

```
Administrator> set ip <IPAddress> <netmask>
```

```
Administrator> set gateway<default gateway IP Address>
```

Example: The IP address is 192.168.0.10, netmask is 255.255.255.0, and gateway is 192.168.0.1.

```
Administrator> set ip 192.168.0.10 255.255.255.0
Administrator> set gateway 192.168.0.1
```

5. Execute the set http enable command to enable http.

>> The MMB Web-UI is accessible from the MMB console PC via the LAN.

```
Administrator> set http enable
```

Remarks

To enable https, use the set https command.

```
Administrator> set http enable
```


6. Execute the set telnet enable command to enable telnet.

```
Administrator> set telnet enable
```

7. Set the date and time as needed.

Use the following command.

```
Administrator> set date MMDDhhmm[[CC]YY][,ss]
```

Example: April 27, 2009 13:10:00 is set as the date and time.

```
Administrator> set date 042713102009,00
```

8. After the MMB Ready LED goes on (initialization completed), confirm that the Alarm LED on each unit is off.

3.3.3 Setting up the connection environment for actual operation

Set up the connection environment for actual operation from the configured test environment by performing the following:

[Setting the IP address of the MMB console PC](#)

[Connecting the MMB console PC to the MMB USER port](#)

[Connecting the PRIMEQUEST 1000 series server to an external LAN](#)

Setting the IP address of the MMB console PC

Set the IP address of the PC used as the MMB console. For details on how to set it, see the manuals for the PC used.

Connecting the MMB console PC to the MMB USER port

Connect your MMB console PC to MMB USER port#0 with a LAN cable. When connected, the MMB console PC can communicate with the MMB via the LAN.

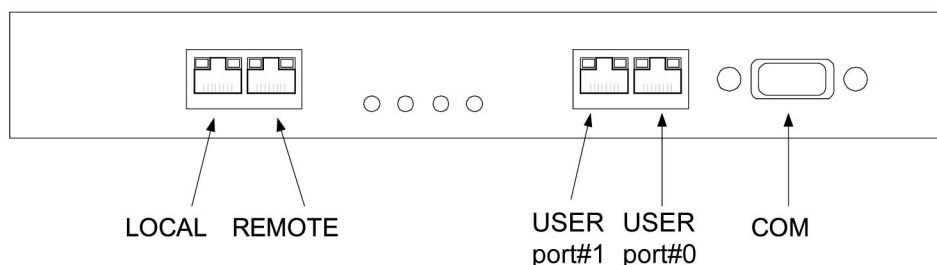


FIGURE 3.2 MMB USER port location

Connecting the PRIMEQUEST 1000 series server to an external LAN

The following describes the configuration of external LAN connections of the PRIMEQUEST 1000 series server. It also describes points to consider about the connections. We recommend you configure security before connecting an external LAN. For details on security, see [7.5 Configuring Security](#).

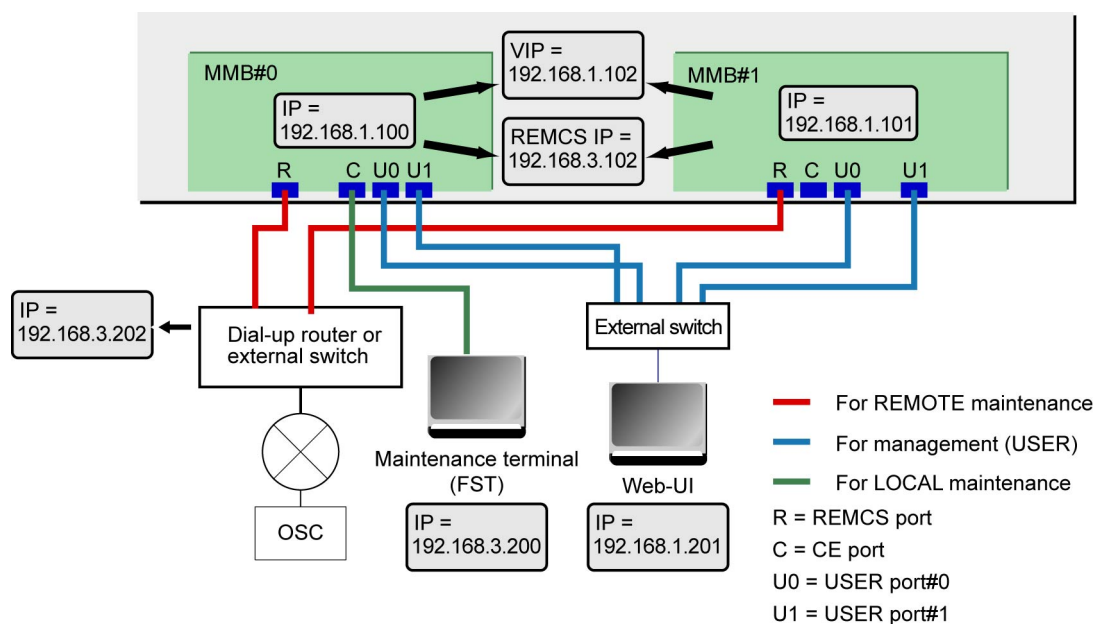


FIGURE 3.3 Network configuration and IP addresses of the management LAN

Connect the management (USER) ports of MMB#0 and MMB#1 to an external switching hub with LAN cables. At this time, also connect the MMB console PC to the external switching hub. The MMB console PC is used for MMB Web-UI operations.

Set the physical IP addresses and virtual IP addresses of MMB#0 and MMB#1 in the same subnet.

Each MMB has the following two addresses:

- Physical IP address (in the above figure, MMB#0 = 192.168.1.100, MMB#1 = 192.168.1.101)
- Virtual IP address (in the above figure, 192.168.1.102)

An external connection (e.g., Web browser, maintenance terminal, REMCS) uses the virtual IP address for communication.

TABLE 3.4 Required settings for external LAN connections

Condition	Required setting
The external switch used in the configuration is a switching hub that supports functions preventing cycling (e.g., Spanning Tree Protocol, Domain Separation).	Select [disable] for the spanning tree protocol of the ports of the switching hub and main unit. Alternatively, set domain separation to on to disable the functions preventing cycling.
Configuration that meets any of the following conditions: - The send destination server becomes an external server through the firewall. - It uses a mail server that restricts IP addresses.	The firewall or mail server settings must permit packets with the physical IP address of MMB#0 or MMB#1 to pass.
REMCS connection	The connection patterns are as follows: - Internet connection:

Condition	Required setting
	Connect the REMCS port to the external switching hub. Alternatively, connect the center from the external switch of the management port through the firewall. - P-P connection: Connect the REMCS port on each of MMB#0 and MMB#1 directly to the dial-up router. For details on REMCS linkage, see the <i>PRIMEQUEST 1000 Series REMCS Installation Manual</i> (C122-E120EN).

Remarks

- The MMB sends NTP, Alarm E-Mail, REMCS, and SNMP Trap packets. If both physical and virtual IP addresses are set for the MMB, the sender's IP address in the packets is the physical IP address of the MMB.
- PRIMECLUSTER linkage also uses the physical IP address of the MMB.

3.3.4 Logging in to the MMB

This section describes how to log in to the MMB.

Login to and logout from the MMB Web-UI

The login and logout procedures for the MMB Web-UI are described below.

Set one of the following for login to the Web-UI:

- Virtual IP address
- FQDN (fully qualified domain name) corresponding to the virtual IP address

Caution

- The MMB Web-UI supports the following browsers. Other browsers may incorrectly display the Web-UI window. Be careful about the browser used.
 - Microsoft Internet Explorer 6 (Service Pack 1) or later. FireFox 15 or later should be used for IPv6.
 - Mozilla FireFox 3.0 or later. FireFox 15 or later should be used for IPv6.
- Do not attempt multiple logins (e.g., multiple logins with the same user name) from one MMB console PC through the Web-UI to the PRIMEQUEST 1000 series system. Multiple logins may cause the following problems, depending on the browser type or version. In a tabbed browser, avoid using multiple tabs for one login session, which would be the same as multiple logins. Internet Explorer 7 or later is a tabbed browser.
 - The operating privileges of a logged-in user may change to those of a user who logs in later to the Web-UI.
 - One user logging out from the Web-UI may also log out all other users from the Web-UI.

Remarks

To specify an FQDN, you must configure a DNS server on the MMB console PC. For details on how to configure a DNS server, see [3.3.8 Configuring a DNS server](#).

Logging in

1. Start your Web browser.

Remarks

Enable JavaScript and enable Download in your browser settings.

2. Enter the following URL.

TABLE 3.5 URL to enter for login

Standard	http://nodename:adminport http://nodename:adminport/login.cgi (Windows Server 2008 and Windows Server 2012)
SSL	https://nodename:adminport
Remarks	nodename:adminport in the above URLs conforms to the following syntax: nodename specifies the FQDN or IP address of the MMB. adminport specifies the port number assigned to the MMB management port (8081 by default, and 432 for SSL).

Note

When an https connection is established, a warning message appears because the certificate is not one from a third-party organization. Ignore it and continue establishing the connection.

3. When the MMB Web-UI login window appears, enter the user account and password. Then, click the [Login] button.



FIGURE 3.4 MMB Web-UI login window

Remarks

At initial startup or if the settings have not been changed, use the following default user account and password. You will be asked to change the password to a new password.

TABLE 3.6 Default user account and password

Username	Administrator

Password	Password that was set by a field engineer during device setup

Logging out

Click the [Logout] button at the top right in the browser window.

>> You are logged out from the Web-UI.

3.3.5 How to view the Web-UI window

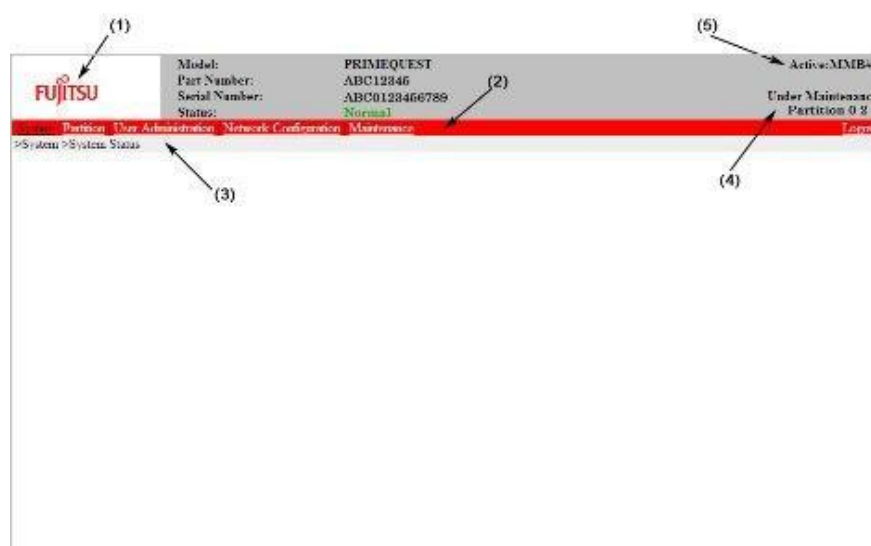
This section describes the information displayed in the Web-UI window.

Remarks

If the Web-UI window displays "Read Error," check for details on the error in 11.2 Troubleshooting in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN). If you cannot solve the problem even after referring to the manual, contact your sales representative or a field engineer.

Before making contact, confirm the model name and serial number shown on the label affixed to the main unit.

FIGURE 3.5 Information displayed in the window shows the information displayed in the window.



No.	Description
(1)	Fujitsu logo (link to Fujitsu's top page)
(2)	Navigation bar
(3)	Submenu breadcrumb trail
(4)	Maintenance status display
(5)	Active MMB display

FIGURE 3.5 Information displayed in the window

The information area always displays the following information.

Model

This field displays the model name of the PRIMEQUEST 1000 series server.

Part Number

This field displays the part number of the PRIMEQUEST 1000 series server.

Serial Number

This field displays the serial number of the PRIMEQUEST 1000 series server.

Status

This field displays the status of the entire PRIMEQUEST 1000 series system. The following table shows the three system status indicators.

TABLE 3.7 System status indicators

Status	Display color	Icon
Normal (normal status)	Green	(None)
Warning	Yellow	A black ! mark in a yellow triangle 
Error	Red	A white x mark in a red circle 

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

Active MMB display

This field displays the number of the active MMB, which is operating with the connected Web-UI.

Maintenance status display

The window displays the information area in gray to a field engineer who is performing maintenance on the PRIMEQUEST 1000 series server using the [Maintenance Wizard] menu.

Also, the area displays [Under Maintenance] in black characters and the partition number of the partition under maintenance below [Under Maintenance].



No.	Description
(1)	Partition under maintenance

FIGURE 3.6 Maintenance status display

Navigation bar

Select a menu on the navigation bar to display the menu in the submenu area.

The selected menu is displayed in black characters. The menus not selected are displayed in white characters.

Logout

Click [here](#) to log out from the Web-UI.

Submenu breadcrumb trail

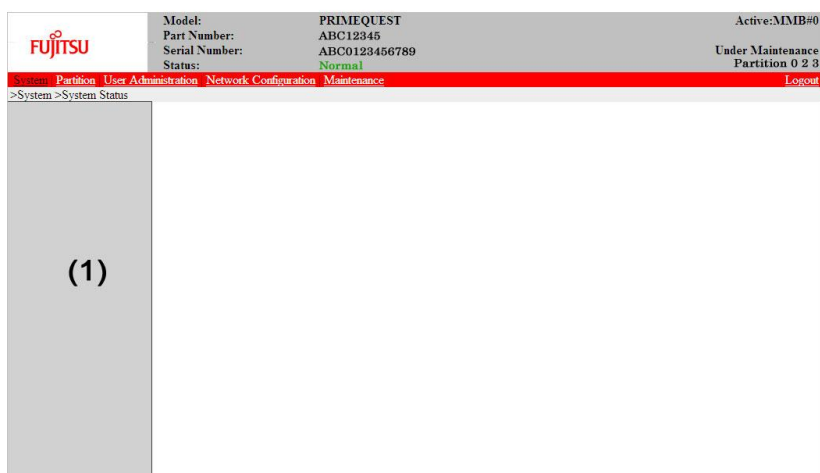
This bar displays each level on the path to the menu that is displayed in the submenu area.

Click a level to display the window for that level.

Example: > System > System Status

Submenu area

This area displays the submenu corresponding to the menu selected on the navigation bar.



No.	Description
(1)	Submenu area

FIGURE 3.7 Submenu area

The submenu area display is as follows.

- The area displays up to three menu levels.

One level is added to the submenu breadcrumb trail when the user goes deeper than three levels or when the submenu area displays a scroll bar for a large number of menu items.

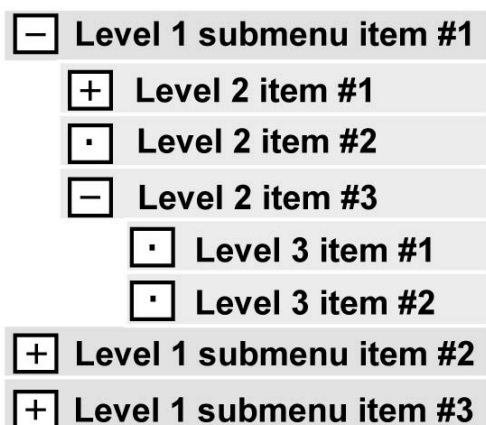
When displayed, the added submenu is the lowest menu on the submenu breadcrumb trail and the top submenu in the submenu area.

- Each submenu has one of the following icons to indicate whether it has lower-level menus.

: This symbol indicates that the submenu has lower-level menu items.

: This symbol indicates that the submenu has lower-level menu items and is currently expanded.

: This symbol indicates that the submenu has no lower-level menu items.



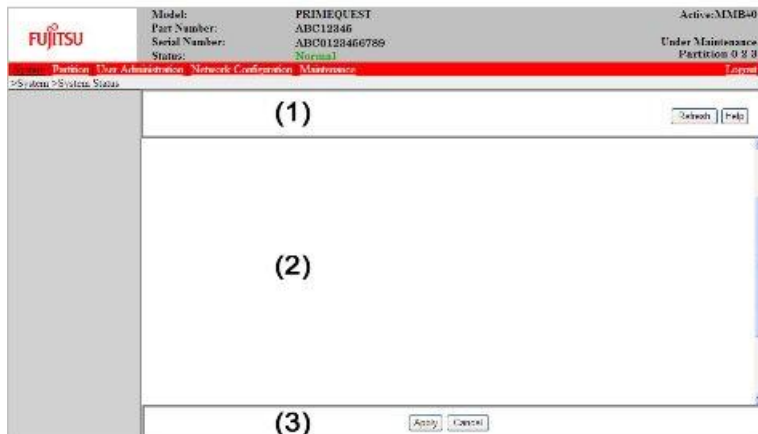
- Placing the cursor on a submenu highlights the submenu.
- The selected submenu has a different background color.
- The background colors of menus at different levels depend on the level.

Content area

The content area displays the following:

- Navigation bar
- Screen of the menu selected in the submenu area

The following figure shows the content area.



No.	Description
(1)	Title area
(2)	Status display and settings area
(3)	Button area

FIGURE 3.8 Content area

The content area is divided into the following three areas.

Title area

The title area displays information on the content.

This area also displays the [Help] button and [Refresh] button. Use the [Help] button to display the help for the content. Use the [Refresh] button to reload the content.

TABLE 3.8 Buttons in the title area

Button name	Description
[Help] button	Displays help information. When clicked, the button displays a help window.
[Refresh] button	Reloads only the content area. The window displays the [Refresh] button only if there is information to be automatically updated. If the window has no information to be automatically updated, the window displays only the functions for settings and does not display the [Refresh] button.

There is no scrolling of the title area.

Status display and settings area

The status display and settings area displays status and setting information related to the content.

A scroll bar is displayed on the screen when the area cannot display all the contents of the status and settings.

TABLE 3.9 Status indicator types

Status	Background color
Normal	Background color to the normal color in the window
Warning	Yellow
Error	Red
Not present	Grey

Input fields, radio buttons, and check boxes are grayed out and unavailable if authenticated users do not have corresponding privileges.

For details on the privileges, see TABLE 1.1 User privileges in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

Button area

This area displays buttons for setting the contents of the status display and settings area.

Usually, the area displays the [Apply] button and [Cancel] button.

In any of the following cases, the window does not display the button area.

- The current content is display only and no input is necessary.
- The user has only display privileges.

In such cases, the above [Status display and settings area](#) has an expanded display area.

Basic operations of the MMB Web-UI

The basic operation flow is as follows.

1. Select a menu on the navigation bar.

>> The submenu area displays the submenu of the selected menu.

2. Select a menu item from the submenu.

>> The content area display in the window corresponds to the selected menu item.

3. Check or set information in the displayed window.

Click the [Apply] button to set information.

Click the [Cancel] button to revert to the settings before input.

Note

The MMB Web-UI may display a confirmation dialog box for process execution or notification dialog box for process completion. If the MMB Web-UI is running in IE and the dialog box remains displayed for more than two minutes, the MMB Web-UI connection is terminated. In such cases, log in to the MMB Web-UI again.

3.3.6 Configuring the MMB network

Configure the MMB network. For the items already set at this time, confirm the setting contents. For the items not set, make the settings.

Set the following IP addresses:

- Virtual IP address used to access the Web-UI
- Physical IP address assigned to the MMB interface ... etc.

For details on how to back up the specified information, see [3.5 Saving Configuration Information](#).

Notes

- When the MMB is not duplicated and the PRIMECLUSTER linkage is disabled, the physical IP address setting for the MMB is not necessary.
- Log in with Administrator privileges to configure the MMB network.
- To change an IP address on the MMB side between PSA and the MMB, change the IP address setting on all partitions in the same cabinet. For details on how to change the setting, see [6.2.1 Configuring the PSA-to-MMB communication LAN](#) or [6.3.1 Configuring the PSA-to-MMB communication LAN](#).
- If the PSA-to-MMB communication LAN setting is Disable, the PSA Web-UI does not appear. Moreover, REMCS notifications and e-mail notifications related to PSA (PRIMEQUEST 1800E) or SVS (PRIMEQUEST 1800E2) are not output.
- If you change a value in [MMB#0 IP Address] or [MMB#1 IP Address] in the [Network Interface] window and then click the [Apply] button:
The network is suspended and the Web-UI is disconnected to enable the settings. You can connect to the Web-UI again by selecting the Web-UI menu.
- If you change the virtual IP address:
The MMB Web-UI is disconnected. You need to log in again to use the MMB Web-UI.

Remarks

Once the virtual IP address is set:

Web browsers have access through the virtual IP address of the PRIMEQUEST 1000 series server. They cannot access the MMB Web-UI through the specified physical IP address of MMB#0 or MMB#1.

The maintenance terminal and REMCS has access through the address specified in [Maintenance IP Address]. You can specify the address by selecting [Network Configuration] - [Network Interface].

Operations

1. Click [Network Configuration] - [Network Interface].
>> The [Network Interface] window appears. For details on the [Network Interface] window, see 1.5.2 [Network Interface] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

The screenshot shows the 'IPv4 Interface' configuration window. At the top, it displays system information: Model (PRIMEQUEST 1800F), Part Number (MCD3AC111), Serial Number (1486915601), and Status (Normal). The left sidebar contains a tree view with 'Network Interface' selected. The main area is titled 'IPv4 Interface' and includes a 'Help' button. Below the title, there is a note: 'Click the Apply button for all changes to take effect.' The configuration is divided into three sections: 'Virtual IP Address', 'MMB#0 IP Address', and 'MMB#1 IP Address'. Each section has a 'Hostname' field, an 'IP Address' field (with sub-fields for octets), a 'Subnet Mask' field (with sub-fields for octets), and a 'Gateway address' field (with sub-fields for octets). There are also 'Interface' checkboxes (Enable/Disable) and 'DNS (optional)' settings (DNS Server 1, 2, 3) for each section. At the bottom right, there are 'Apply' and 'Cancel' buttons.

FIGURE 3.9 [Network Interface] window (example)

2. Enter values in [IP Address], [Subnet Mask], and [Gateway Address] in [Virtual IP Address]. Also specify the host name.

Remarks

Set the physical IP addresses and virtual IP addresses of MMB#0 and MMB#1 in the same subnet.

3. Click [Enable] for [Interface] in [MMB#0 IP Address] or [MMB#1 IP Address]. Then, enter a value in each item. Specify a physical IP address to assign it at this time.
4. Specify the required fields. Then, click the [Apply] button.

Note

If the IP address or some other set value is invalid, the browser does not display the MMB Web-UI. In such cases, connect the MMB console PC to the COM port on the MMB. Then, set the correct value.

3.3.7 Configuring telnet

Configure telnet for the MMB.

For details on how to back up the specified information, see 3.5 Saving Configuration Information.

Note

Log in with Administrator privileges to make these settings.

Operations

1. Click [Network Configuration] - [Network Protocols].
>> The [Network Protocols] window appears. For details on the [Network Protocols] window, see 1.5.4 [Network Protocols] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

The screenshot shows the 'Network Protocols' configuration window. The left sidebar contains a tree view with the following items: User/Time, Network Interface, Management LAN Port Configuration, Network Protocols (selected), Network Rate, RMON Configuration, SMI, Remote Server Management, Access Control, and Alarm E-Mail. The main area is titled 'Network Protocols' and includes a 'Help' button. Below the title, it says 'Click the Apply Button to apply all changes.' The configuration is divided into four sections: Web (HTTP/HTTPS), Telnet, SSH, and SNMP. Each section has a table of settings with radio buttons for 'Enable' and 'Disable'.

Section	Item	Value	Enable/Disable
Web (HTTP/HTTPS)	HTTP		☐ Enable ☒ Disable
	HTTP Port#	1024-65535	
	HTTPS		☒ Enable ☐ Disable
	HTTPS Port#	432, 1024-65535	
	Timeout (sec)	0, 60-9999	
Telnet	Telnet		☐ Enable ☒ Disable
	Telnet Port#	23, 1024-65535	
	Timeout (sec)	0, 60-9999	
SSH	SSH		☒ Enable ☐ Disable
	SSH Port#	22, 1024-65535	
	Timeout (sec)	0, 60-9999	
SNMP	SNMP Agent		☐ Enable ☒ Disable
	Agent Port#	161, 1024-65535	
	SNMP Trap		☐ Enable ☒ Disable
	Trap Port#	162, 1024-65535	

At the bottom right, there are 'Apply' and 'Cancel' buttons.

FIGURE 3.10 [Network Protocols] window (example)

2. Specify each item in [Telnet].

Note

The MMB uses the following fixed TCP/IP port numbers. Do not change the following port numbers:

- 623/udp: Port for RMCP communication
- 664/udp: Port for RMCP communication

3. Click the [Apply] button.

3.3.8 Configuring a DNS server

To use a DNS server, configure it. You can configure a DNS server at a later time.

For details on how to back up the specified information, see [3.5 Saving Configuration Information](#).

Note

Log in with Administrator privileges to make these settings.

Operations

1. Click [Network Configuration] - [Network Interface].

>> The [Network Interface] window appears. For details on the [Network Interface] window, see 1.5.2 [Network Interface] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

FIGURE 3.11 [Network Interface] window (example)

2. Click [Enable] for [DNS] in [DNS(optional)]. Then, enter a value for each item.
3. Specify the required fields. Then, click the [Apply] button.

3.3.9 Configuring Alarm E-Mail

Make the following Alarm E-Mail settings:

- Whether to send e-mail notification if an error occurs during operation
- Error level and send destination for such e-mail notification

For details on how to back up the specified information, see [3.5 Saving Configuration Information](#).

Note

Log in with Administrator privileges to make these settings.

Operations

1. Click [Network Configuration] - [Alarm E-Mail].
>> The [Alarm E-Mail] window appears. For details on the [Alarm E-Mail] window, see 1.5.11 [Alarm E-Mail] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).



FIGURE 3.12 [Alarm E-Mail] window (example)

2. Enter values in the required fields.

Remarks

- As described below, the [From] address is sent with Alarm E-Mail notification to the SMTP server:
 - If the [Use envelope "from" address.] check box is checked
The address set in [From] in the [Alarm E-Mail] window becomes the [From] address sent to the SMTP server.
 - If the [Use envelope "from" address.] check box is unchecked (initial setting)
The following [From] address set in [Virtual IP Address] - [Hostname] in the [Network Configuration] - [Network Interface] window is sent to the SMTP server. The address should be in the same format as [Hostname].
In FQDN format: root@[Hostname]
Except in FQDN format: root@localdomain.localdomain
The e-mail address set in [From] becomes the From address of the e-mail sent to the e-mail recipient ([To]).
- To specify an FQDN as an SMTP server name, a DNS server must be set. After selecting [Network Configuration] - [Network Interface], you can set a DNS server.

3. Click the button appropriate to your needs.
 - To set conditions for sending e-mail: [Filter] button
 - To enable the settings: [Apply] button
 - To send test e-mail: [Test E-Mail] button

Specify e-mail send conditions

1. To specify e-mail send conditions, click the [Filter] button in the [Alarm E-Mail] window.

>> The [Alarm E-Mail Filtering Condition] window appears. For details on the [Alarm E-Mail Filtering Condition] window, see [Alarm E-Mail Filtering Condition] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).



FIGURE 3.13 [Alarm E-Mail Filtering Condition] window (example)

2. Select values in the required items. Multiple selected items are evaluated with the AND condition. Multiple options selected in an item are evaluated with the OR condition.
3. Click the [Apply] button.

3.3.10 Registering a user account

Register as many MMB user accounts as needed in the initial settings. You can register up to 16 accounts. For details on how to back up the specified information, see [3.5 Saving Configuration Information](#).

Operations

1. Click [User Administration] - [User List].

>> The [User List] window appears. For details on the [User List] window, see 1.4.1 [User List] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

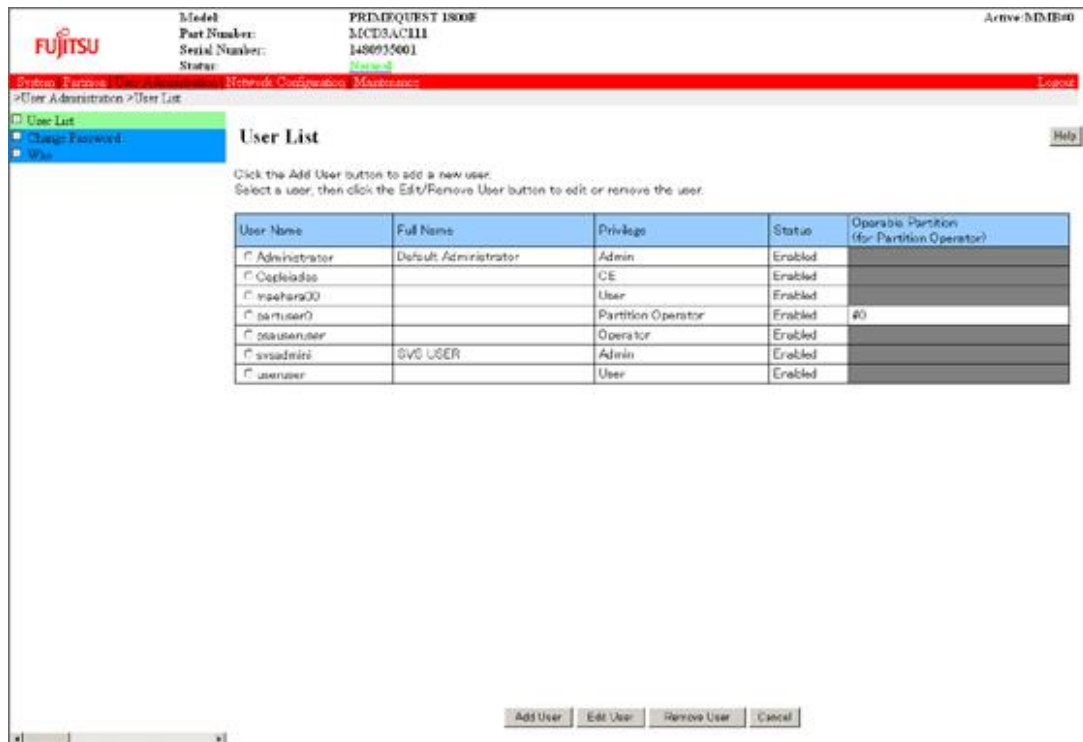


FIGURE 3.14 [User List] window (example)

2. Click the [Add User] button.

>> The [Add User] window appears. For details on the [Add User] window, see the part about the [Add User] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

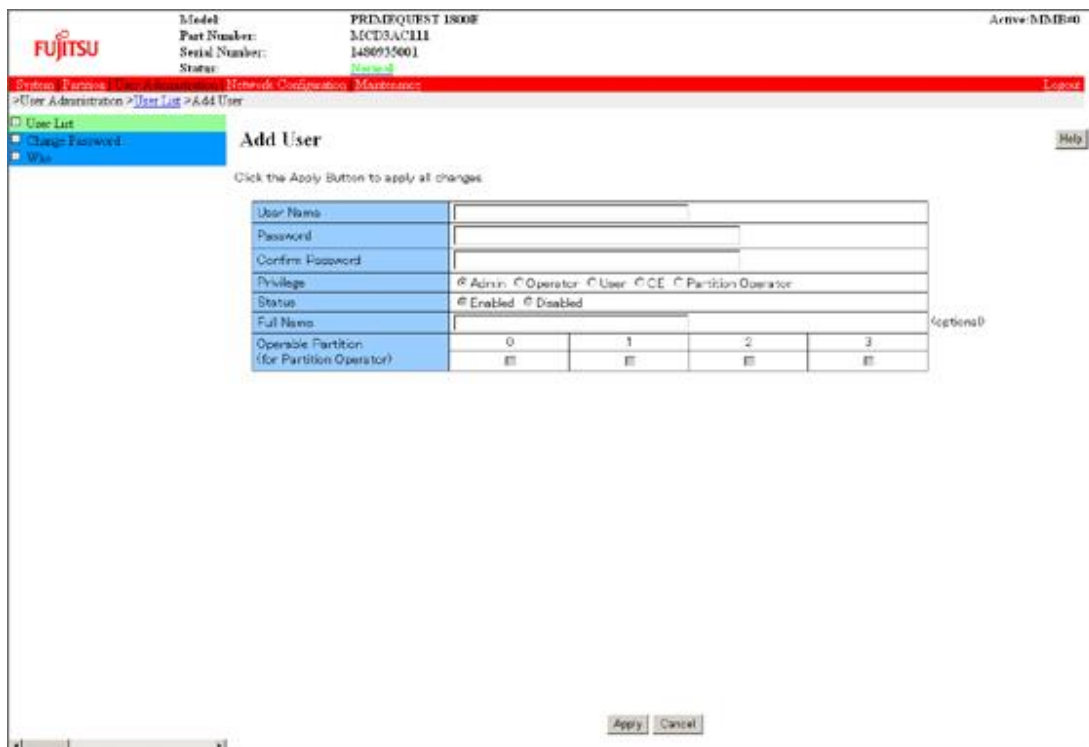


FIGURE 3.15 [Add User] window (example)

Remarks

To change an existing user account, first click the [Edit User] button in the [User List] window. Then, change the registered contents in the [Edit User] window. For details on the [Edit User] window, see the part about the [Edit User] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

FIGURE 3.16 [Edit User] window (example)

3. Enter values in the required fields.
4. Click the [Apply] button.

3.3.11 Setting the system name

Specify a name for the PRIMEQUEST 1000 series system. This name is also used as the SNMP system name. For details on how to back up the specified information, see [3.5 Saving Configuration Information](#).

Operations

1. Click [System] - [System Information].
>> The [System Information] window appears. For details on the [System Information] window, see 1.2.4 [System Information] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

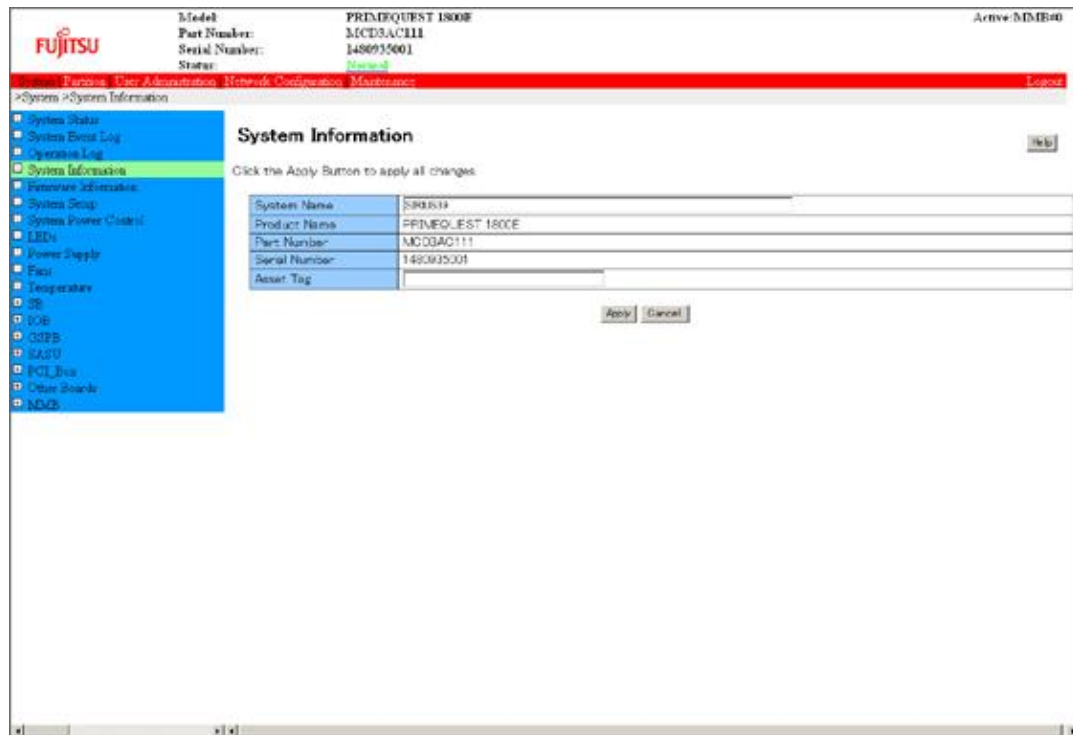


FIGURE 3.17 [System Information] window (example)

2. Enter a name in [System Name].
3. Click the [Apply] button.

3.3.12 Setting the date and time

Set the MMB date and time. Configure NTP (to use an NTP server) as needed.

The field engineer may have already done this. If so, proceed to the next setting item unless you need to change a setting.

For details on how to back up the specified information, see [3.5 Saving Configuration Information](#).

Remarks

The MMB provides the NTP client function. The NTP client function of the MMB adjusts time by using another NTP server as reference. For stable NTP operation, specify multiple NTP servers (at least three servers in RHEL) from each NTP client.

Operations in the [Date/Time] window

1. Click [Network Configuration] - [Date/Time].
>> The [Date/Time] window appears. For details on the [Date/Time] window, see 1.5.1 [Date/Time] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

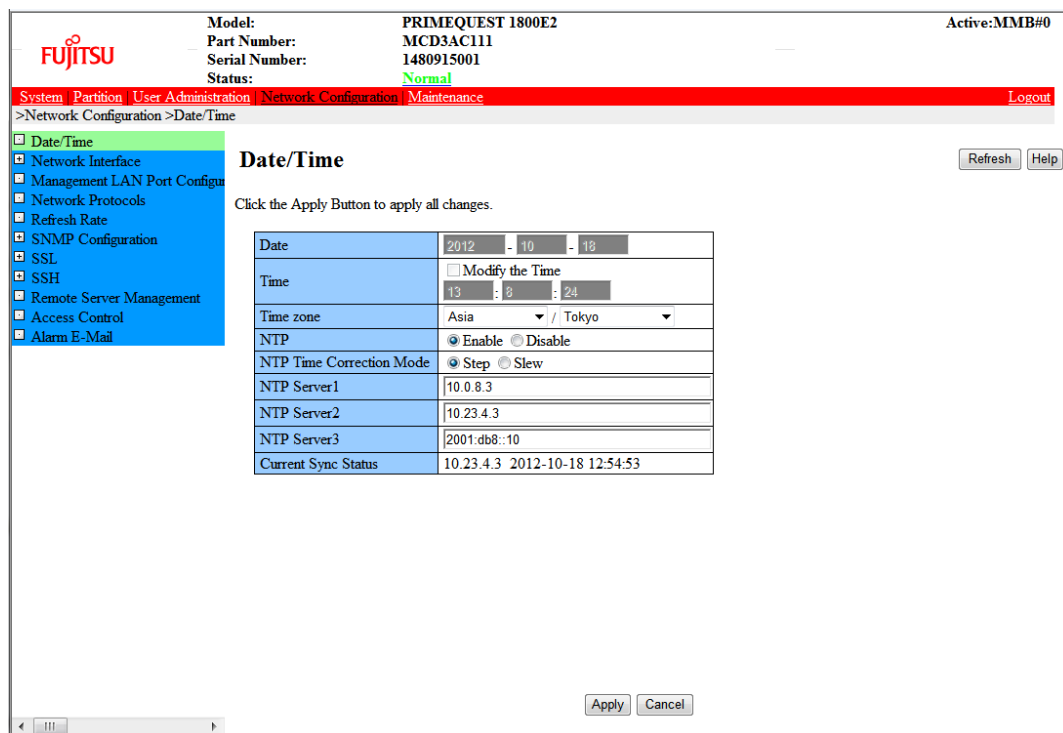


FIGURE 3.18 [Date/Time] window (example)

2. Enter values in the required fields.
3. Click the [Apply] button.

Operations in the [Management LAN Port Configuration] window

1. Click [Network Configuration] - [Management LAN Port Configuration].
>> The [Management LAN Port Configuration] window appears. For details on the [Management LAN Port Configuration] window, see 1.5.3 [Management LAN Port Configuration] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

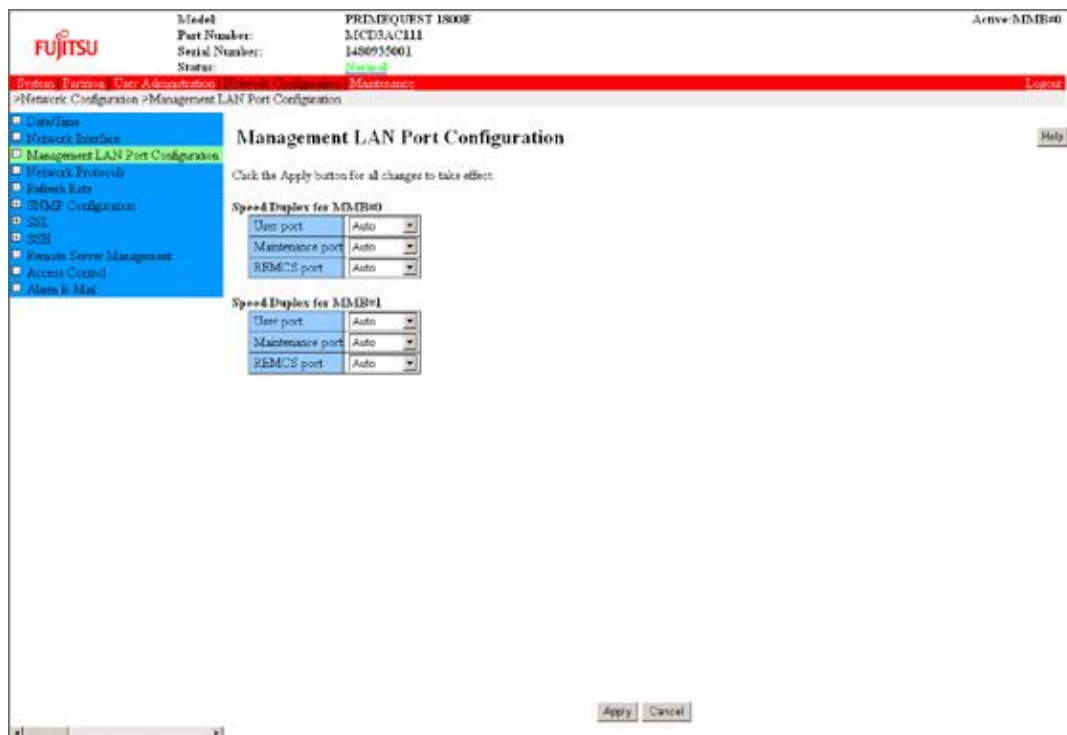


FIGURE 3.19 [Management LAN Port Configuration] window (example)

2. Enter values in the required fields.
3. Click the [Apply] button.

3.4 Configuring a Partition

This section describes various information settings for partitions. If your system has multiple partitions, configure all the partitions.

To apply the configuration changes to a partition, power off and on the partition.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

3.4.1 Setting a partition configuration

This section describes how to add and remove an SB, IOB, and GSPB.

Adding an SB, IOB, and GSPB

Add an SB, IOB, and GSPB to a partition as follows.

Operations

1. Click [Partition] - [Partition Configuration].
>> The [Partition Configuration] window appears. For details on the [Partition Configuration] window, see 1.3.4 [Partition Configuration] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

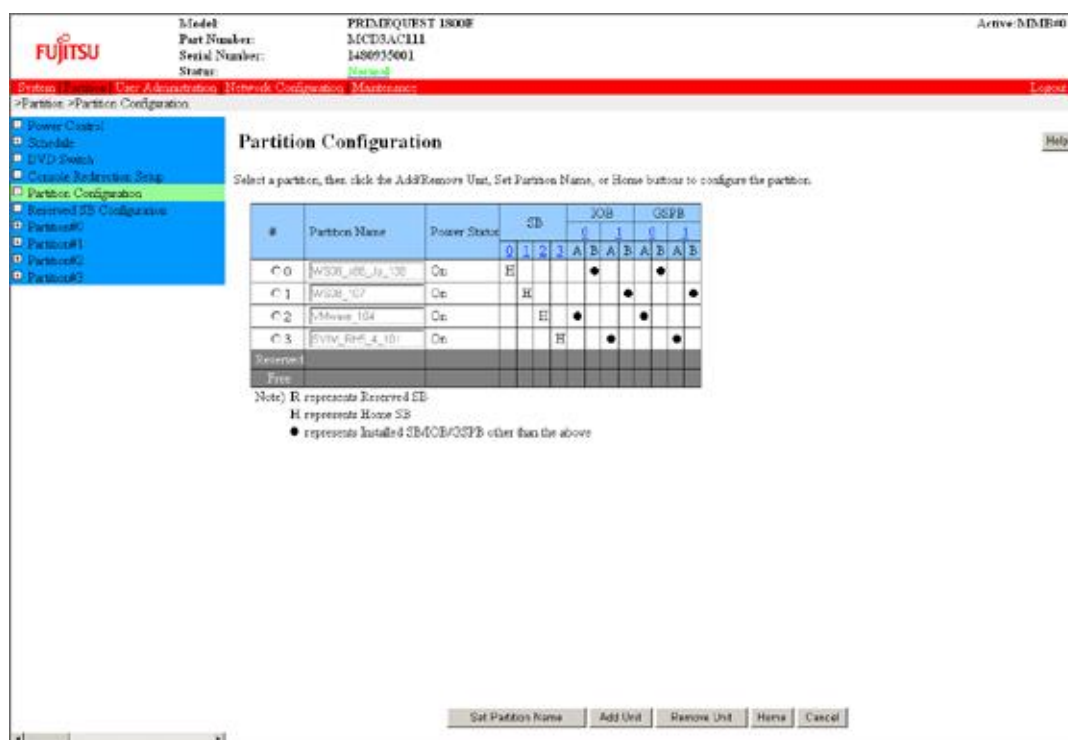


FIGURE 3.20 [Partition Configuration] window (example)

Remarks

The above window shows the maximum configuration.

2. Click the radio button of a partition number to add an SB, IOB, or GSPB to that partition.
3. Click the [Add Unit] button.
>> The [Add SB/IOB/GSPB to Partition] window appears. The window displays a list of free SBs, IOBs, and GSPBs. For details on the [Add SB/IOB/GSPB to Partition] window, see [Add SB/IOB/GSPB to

Partition] window in 1.3.4 [Partition Configuration] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

FUJITSU Model: PRIMEQUEST 1800E Active:MMB#0
Part Number: MCD3AC111
Serial Number: 1480915001
Status: Normal

System Partition User Administration Network Configuration Maintenance Logout

>Partition >Partition Configuration

Power Control
Schedule
DVD Switch
Console Redirection Setup
Partition Configuration
Reserved SB Configuration
Partition#0
Partition#1
Partition#2
Partition#3

Add SB/IOB/GSPB to Partition

Select an SB, IOB or GSPB to add to the partition #0, then click the Apply Button.

Free SB/IOB/GSPB	Status	Note
☐ SB#0	OK	Number of CPUs = 2, Memory = 16 GB
☐ IOB#0A	OK	Number of PCI-Express Slots = 4
☐ GSPB#0A	OK	

Apply Cancel

FIGURE 3.21 [Add SB/IOB/GSPB to Partition] window (example)

- Click the radio button of an SB, IOB, or GSPB to add it to the partition.
Only one SB, IOB, or GSPB can be selected at a time.
- Click the [Apply] button.
>> A confirmation dialog box appears.
- Click the [OK] button.
>> The partition incorporates the selected SB, IOB, or GSPB.

Repeat steps 2 to 6 until you finish adding all the required SBs, IOBs, and GSPBs.

Removing an SB, IOB, or GSPB

The following describes how to remove an SB, IOB, or GSPB from a partition.

Remarks

You cannot remove an SB, IOB, or GSPB while the operating system on the target partition is running. Remove the SB, IOB, or GSPB while the partition power is in the standby status.

Operations

- Click [Partition] - [Partition Configuration].
>> The [Partition Configuration] window appears. For details on the [Partition Configuration] window, see 1.3.4 [Partition Configuration] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

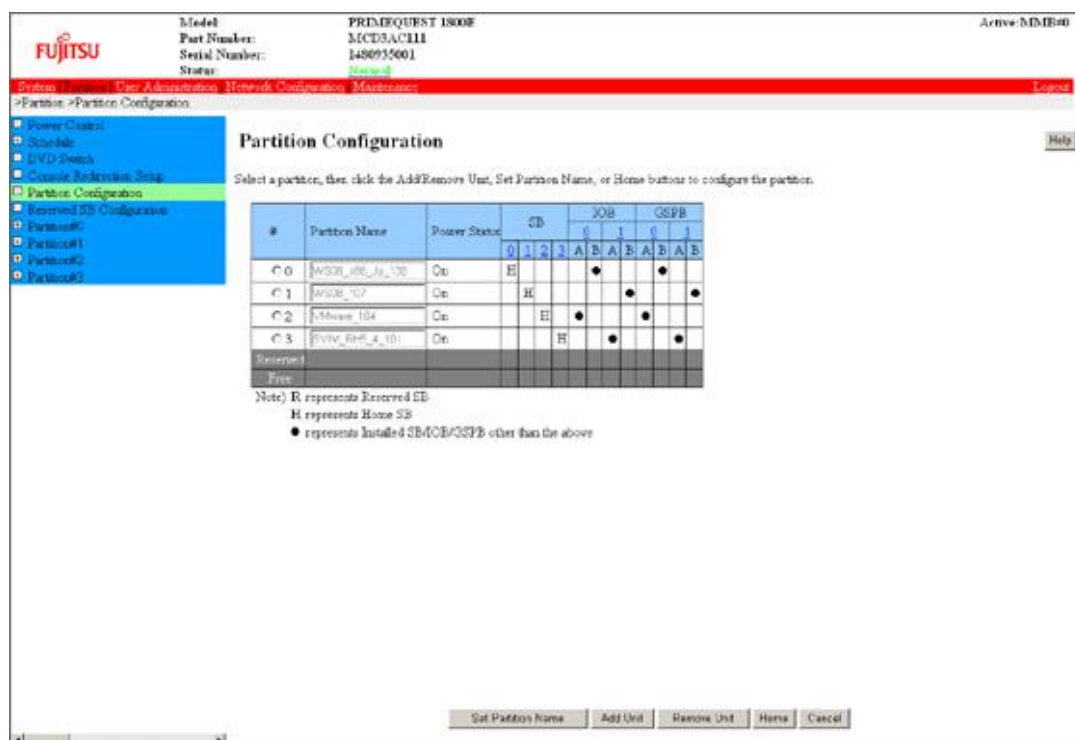


FIGURE 3.22 [Partition Configuration] window (example)

Remarks

The above window shows the maximum configuration.

2. Click the radio button of a partition number to remove an SB, IOB, or GSPB from that partition.
3. Click the [Remove Unit] button.

>> The [Remove SB/IOB/GSPB from Partition] window appears. The window displays a list of SBs, IOBs, and GSPBs. These SBs IOBs, and GSPBs are incorporated in the partition selected in step 2. For details on the [Remove SB/IOB/GSPB from Partition] window, see [Remove SB/IOB/GSPB from Partition] window in 1.3.4 [Partition Configuration] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).



FIGURE 3.23 [Remove SB/IOB/GSPB from Partition] window (example)

4. Click the radio button of an SB, IOB, or GSPB to remove it from the partition.
Only one SB, IOB, or GSPB can be selected at a time.
5. Click the [Apply] button.
>> A confirmation dialog box appears.
6. Click the [OK] button.
>> The partition releases the selected SB, IOB, or GSPB, which becomes free.

3.4.2 Setting a Home SB

The Home SB in each partition is only one type of SB in the partition. The first SB incorporated in a partition is automatically set as the Home SB.

If the Home SB is deleted, the SB that is configured in the partition, has not degraded, and has the smallest physical number is automatically set as the Home SB.

You can use the USB port and VGA port as external connectors of the Home SB.

If you want to change the Home SB, specify the change with the Web-UI. For details on the Home SB, see 5.2.4 Home SB in the *PRIMEQUEST 1000 Series General Description* (C122-B022EN).

Remarks

Windows license verification may be required depending on the combination of the SB and enable kit. For details, see "License authentication with SB and enable kit combinations" in 3.4 Adding Components in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

Operations

1. Click [Partition] - [Partition Configuration] - [Home].

>> The [Partition Home] window appears. For details on the [Partition Home] window, see [Partition Home] window in 1.3.4 [Partition Configuration] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

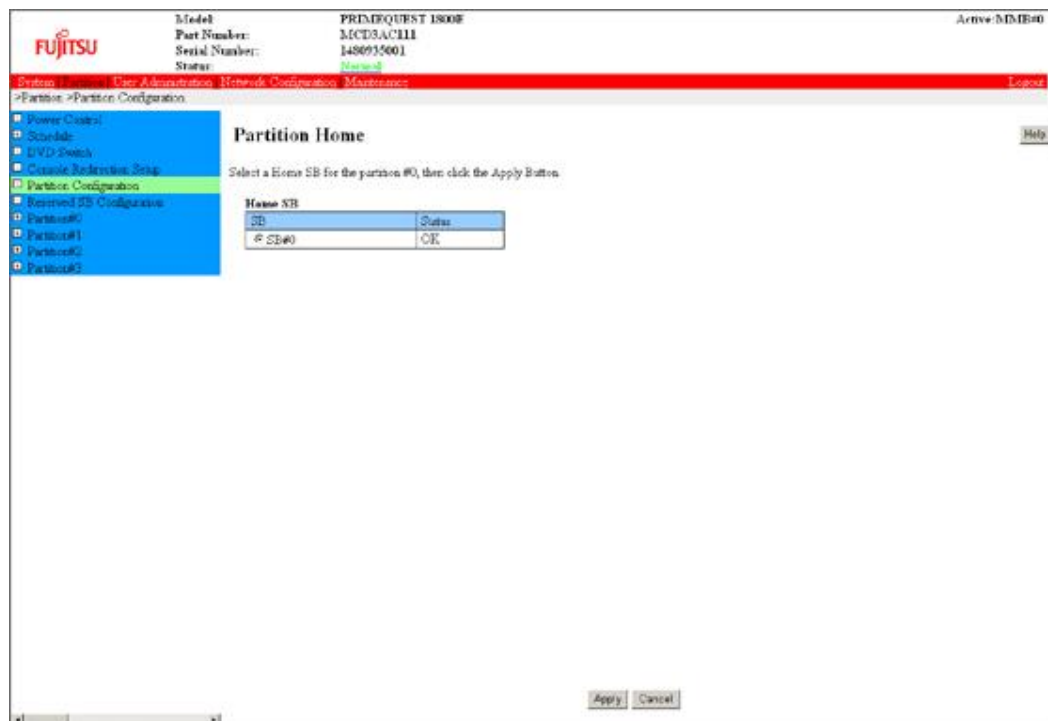


FIGURE 3.24 [Partition Home] window (example)

2. Select an SB as the Home SB of the partition. Then, click the [Apply] button to set it.
3. Select the Home SB from the radio buttons for the specified partition. An unmounted SB that is set as the Home SB is grayed out. You can switch from the selected radio button on a grayed-out row to a radio button on a row not grayed out. From the grayed-out row, you can select another radio button but cannot then select the original radio button again.

4. Click the [Apply] button.

>> A confirmation dialog box appears.

Note

While the power to the target partition is on, you cannot change the Home setting by clicking the [Apply] button. A warning dialog box would appear.

5. Click the [OK] button to continue processing or the [Cancel] button to cancel processing.

>> The browser returns to the [Partition Configuration] window.

3.4.3 Setting a Reserved SB

If a hardware failure occurs on an SB incorporated in a partition, you sometimes may need to remove the SB. A Reserved SB is the SB to be incorporated in the partition in place of the removed SB.

You can set the Reserved SB for a partition according to operating conditions.

You can also define an SB that has not been incorporated in the specified partition as the Reserved SB.

The following SBs are not incorporated in the partition:

- Free SBs
- SBs incorporated in other partitions
- SBs defined as the Reserved SBs of other partitions

For details on the Reserved SB, see 3.2.1 Reserved SB in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

Remarks

Windows license verification may be required depending on the combination of the SB and enable kit. For details, see "License authentication with SB and enable kit combinations" in 3.4 Adding Components in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

Operations

1. Click [Partition] - [Reserved SB Configuration].

>> The [Reserved SB Configuration] window appears. The window displays check boxes in the columns of the free SBs and SBs defined as Reserved SBs. For details on the [Reserved SB Configuration] window, see 1.3.5 [Reserved SB Configuration] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

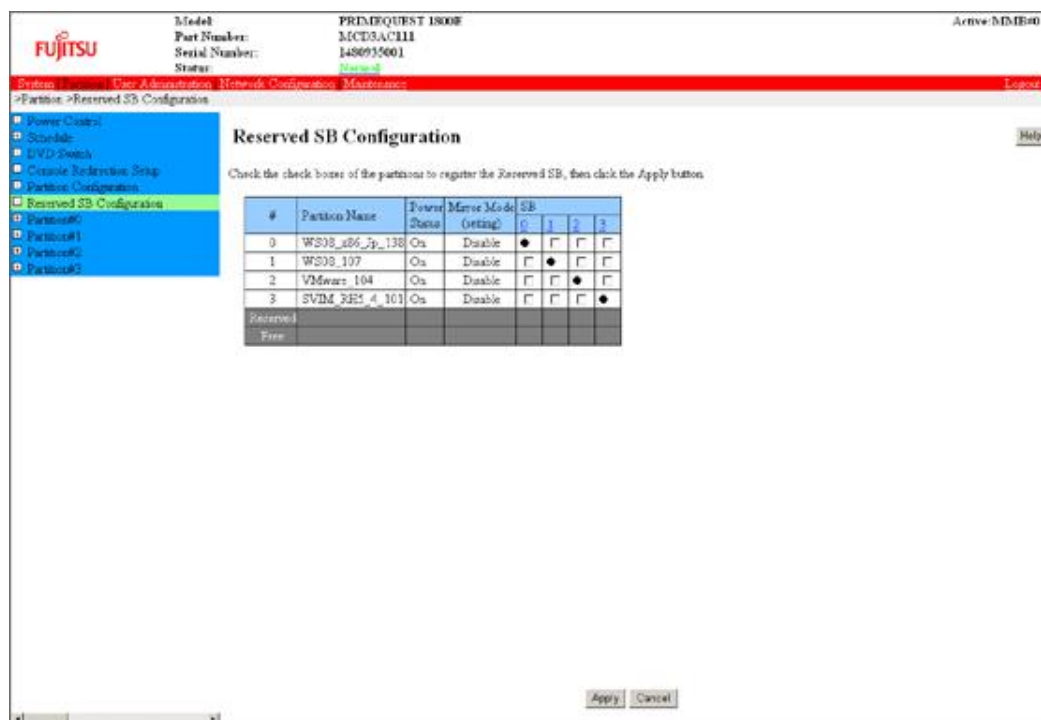


FIGURE 3.25 [Reserved SB Configuration] window (example)

2. In the SB column, check the check box of a partition to designate it as the standby partition.
3. Click the [Apply] button.

Remarks

Unchecking the check box of a Reserved SB in the [Reserved SB Configuration] window changes the SB to a free SB.

Reserved SB mounting requirements

For 1800E2/1800E, the Reserved SB must meet the following conditions regarding the number of CPUs:

- In a partition configured with one SB, one CPU mounted per SB is permitted.
- In a partition configured with multiple SBs, two CPUs mounted per SB are required.

If the above mounting conditions are not met, a message dialog box appears. This inhibits the setting of a Reserved SB.

Notes

- The type of CPU on the Reserved SB must be the same as on the other SBs configured in the partition. An SB that has a different type of mounted CPU cannot be defined as the Reserved SB.
- An SB with 8-GB DIMMs, 16-GB DIMMs, or 32-GB DIMMs mounted cannot be mixed with an SB having mounted memory of another capacity in the same partition. This means an SB with 8-GB DIMMs mounted cannot be set as the Reserved SB in a partition consisting of SBs having mounted memory of another capacity. Neither can an SB with 16-GB DIMMs mounted be set as the Reserved SB in a partition consisting of SBs having mounted memory of another capacity. Nor can an SB with 32-GB DIMMs mounted be set as the Reserved SB in a partition consisting of SBs having mounted memory of another capacity.

Notes on Windows

At the first startup after an SB is switched to the Reserved SB in a partition running Windows, the operating system may not start. Set Windows to automatically restart in the settings of the Reserved SB in the partition running Windows. For details on the settings, see 11.4.4 Setting up the dump environment (Windows) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN). Check the [Automatically restart] check box shown in FIGURE 11.18 [Startup and Recovery] dialog box.

If the SB failure causes a suspension of business for the aforementioned reason, take into account the length of time required for the restart. The restart will take twice as long since one restart is needed after the switching to the Reserved SB and one restart for the subsequent initial startup.

However, the following workaround can suppress the restart request.

Workaround for the Windows restart

You can suppress the restart request only if the PRIMEQUEST 1000 series server has already set as the Reserved SB.

Repeat the following procedure for all the partitions with Windows Server OS installed.

Note that no message requesting a restart is displayed on the screen even if an SB failure occurs during switching to the Reserved SB.

1. After completing installation of the Windows Server OS, shut down the partition.
2. Remove the SB from the partition by using the MMB Web-UI. If the partition has multiple SBs mounted, you can remove any SB. For details, see [Removing an SB, IOB, or GSPB](#) in 3.4.1 Setting a partition configuration.
3. Add an SB as the Reserved SB to the partition. For details, see [Adding an SB, IOB, and GSPB](#) in 3.4.1 Setting a partition configuration.
4. Power on the partition. Then, start the Windows Server OS.

5. Log in with Administrator privilege. After the message that the system must be restarted is displayed on the screen, follow the instructions to restart the system.
6. After the Windows restart is completed, shut down the system.
7. Remove the SB incorporated as the Reserved SB in step 3 from the partition by using the MMB Web-UI.
8. Add the SB removed once in step 2 to the partition.

Notes on VMware

At the first startup after an SB is switched to the Reserved SB in a partition running ESX, the guest operating system may not start. Set the guest operating system to automatically restart and the BlueScreen Timeout item in the settings of the Reserved SB in the partition running ESX.

For example, to reset the ESX host 20 seconds after a panic occurs, set "20" for BlueScreenTimeout.

Remarks

To not reset the ESX host after a panic occurs, set "0" for BlueScreenTimeout.

How to set BlueScreenTimeout

Set BlueScreenTimeout from vSphere Client.

1. Open the [Configuration] tab of the host in vSphere Client. Click [Advanced Settings] in the [Software] pane.

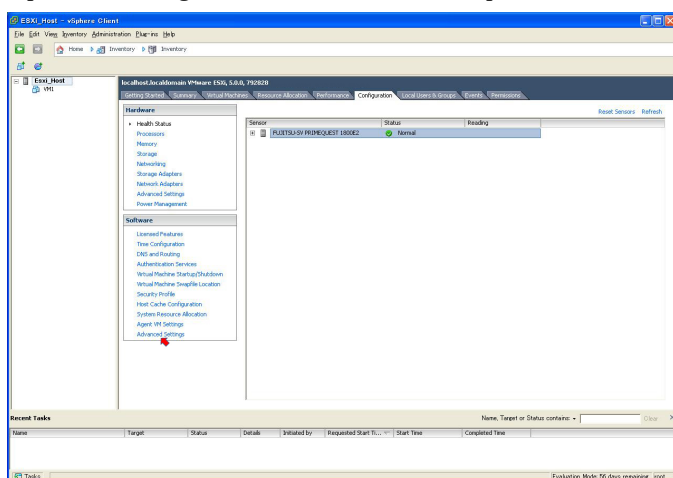


FIGURE 3.26 BlueScreenTimeout setting ([Configuration] tab)

2. The [Advanced] window opens. Click [Misc] in the left pane.
3. The right frame displays parameters. Set the BlueScreenTimeout value in [Misc. BlueScreenTimeout].

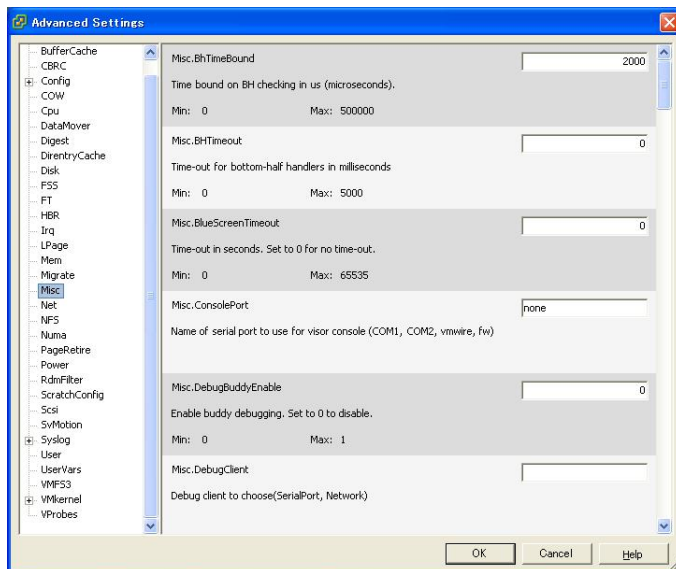


FIGURE 3.27 BlueScreenTimeout setting ([Misc] settings)

For details on the vSphere Client, see the manual of VMware.

3.4.4 Setting a partition name

Set the name for a partition. You can set it with Administrator privileges.

If the specified name is the same as the specified host name of the operating system, the partition is easy to recognize.

Operations

1. Click [Partition] - [Partition Configuration].

>> The [Partition Configuration] window appears. For details on the [Partition Configuration] window, see 1.3.4 [Partition Configuration] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

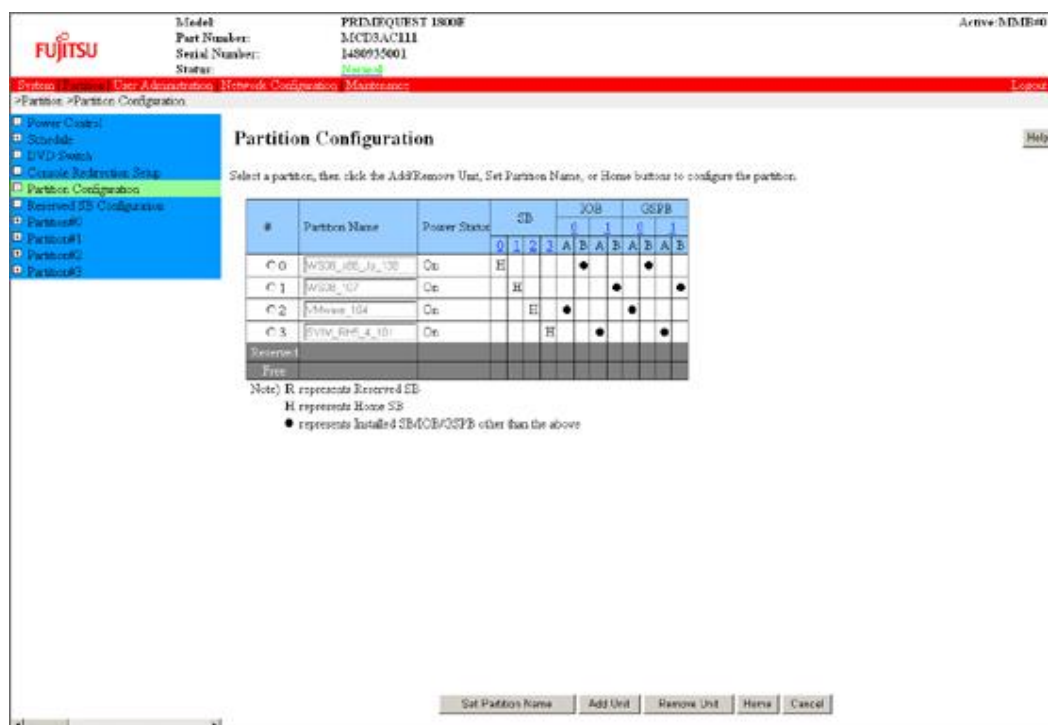


FIGURE 3.28 [Partition Configuration] window (example)

Remarks

The above window shows the maximum configuration.

2. Select the partition to be assigned a partition name. Then, enter a partition name in its [Partition Name] cell.

Remarks

- You can enter a name consisting of up to 16 characters. You can use the following characters:
0 to 9, a to z, A to Z, en space (), and
- _

3. Click the [Set Partition Name] button.

>> The MMB-Web UI sets the entered partition name.

3.4.5 Setting various modes

Set Mirror mode, Hyper Threading mode, and other modes for the partition. The MMB Web-UI and UEFI (Unified Extensible Firmware Interface) windows have settings items for these settings. The following table lists the setting items and the screen transitions. For details on each setting, see the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

TABLE 3.10 Setting various modes

Setting item	Screen Transitions	See (the <i>PRIMEQUEST 1000 Series Tool Reference</i> (C122-E110EN))
Mirror Mode	MMB Web-UI-[Partition]- [Partition#x]-[Mode]	1.3.7 [Partition#x] menu, [Mode] window

Setting item	Screen Transitions	See (the <i>PRIMEQUEST 1000 Series Tool Reference</i> (C122-E110EN))
POST	MMB Web-UI-[Partition]-[Partition#x]-[Mode]	1.3.7 [Partition#x] menu, [Mode] window
Enhanced Speed Step	UEFI-[Device Manager]-[Configure CPU]	5.5.3 [Configure CPU] menu
Turbo Boost Technology	UEFI-[Device Manager]-[Configure CPU]	5.5.3 [Configure CPU] menu
Hyper Threading	UEFI-[Device Manager]-[Configure CPU]	5.5.3 [Configure CPU] menu
Active Processor Cores	UEFI-[Device Manager]-[Configure CPU]	5.5.3 [Configure CPU] menu
Virtualization Technology	UEFI-[Device Manager]-[Configure CPU]	5.5.3 [Configure CPU] menu
Adjacent Cache Line Prefetch	UEFI-[Device Manager]-[Configure CPU]	5.5.3 [Configure CPU] menu
Hardware Prefetch	UEFI-[Device Manager]-[Configure CPU]	5.5.3 [Configure CPU] menu
I/O space assignment	UEFI-[Device Manager]-[Configure I/O Space Assignment]	5.5.1 Configure I/O Space Assignment menu
x2APIC (*)	UEFI-[Device Manager]-[Configure CPU]	5.5.3 [Configure CPU] menu

* Only for the PRIMEQUEST 1800E2

Notes

- When using SVIM on the PRIMEQUEST 1800E2 with x2APIC Disabled set, use up to 128 threads of the operating CPU in the relevant partition.
In order to use up to 128 threads, specify Disabled for Hyper Threading.
- Check whether I/O spaces have been assigned to the SAS device (SAS card, SAS array controller card, Onboard SAS controller (GSPB), SAS disk unit controller, SAS array disk unit controller) of the relevant partition.
Also, when installing the OS in the SAN storage unit, confirm that I/O spaces have also been assigned in the same manner to the FC card (for boot path only).
"Device:SAS" is displayed for an SAS device and "Device:Fibre" is displayed for an FC device. If the I/O spaces have not been assigned, cancel the LAN and Fibre Channel assignments from the [Configure I/O Space Assignment] menu.
However, if the OS is to be installed in a storage device in the SAN environment, do not cancel the I/O space assignment of the FC card to be used for the installation.
- Confirm that the Boot device to be used in the relevant partition has been recognized by the UEFI. For details on this confirmation, see 5.4 [Boot Manager] Menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-

E110EN). If the boot device has not been recognized by the UEFI, use the [Boot Manager] menu to have it recognize the Boot device.

The following describes how to configure POST and set Mirror mode and POST from the MMB Web-UI.

Operations

1. Click [Partition] - [Partition#x] - [Mode].

>> The [Mode] window appears. For details on the [Mode] window, see [Mode] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).



FIGURE 3.29 [Mode] window (example)

Remarks

The window displays the [PSA] menu only in the PRIMEQUEST 1800E.
The PRIMEQUEST 1800E2 does not display TPM.

2. Set Mirror mode, and configure POST.
3. Click the [Apply] button.
>> A confirmation dialog box appears.
4. Click the [OK] button.

Remarks

To enable the new settings in the [Mode] window, you need to power off and on the partition.

3.4.6 Configuring Console Redirection

To remotely install an operating system, you need to first configure Console Redirection.
Set Console Redirection to the same subnet as the management LAN.

1. Click [Partition] - [Console Redirection Setup].
>> The [Console Redirection Setup] window appears. For details on this window, see 1.3.6 [Console Redirection Setup] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

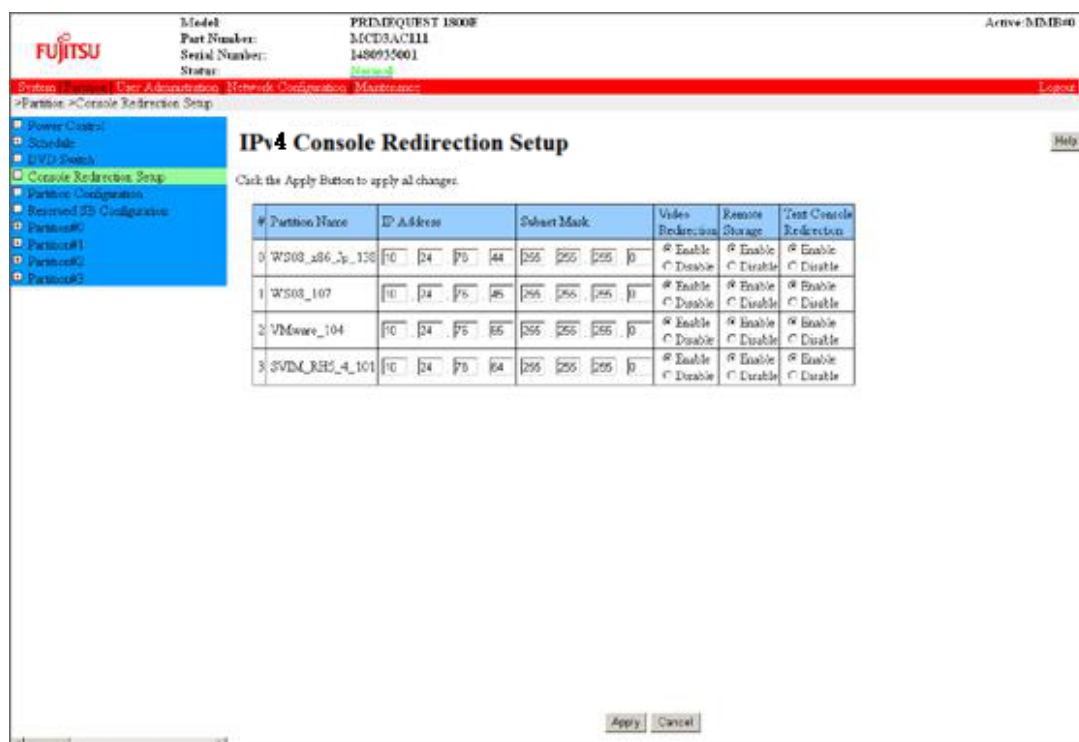


FIGURE 3.30 [Console Redirection Setup] window (example)

2. Set the IP address.
3. Enable each of video redirection, remote storage, and text console redirection.
4. Click the [Apply] button.

Note

After the installation, disable the functions that will not be used.

3.4.7 Powering off and on a partition

To apply the configuration changes to a partition, power off and on the partition.
For details on how to power off and on a partition, see [CHAPTER 8 Powering On and Off a Partition](#).

Remarks

After POST ends, processing continues until the [EFI Shell] window appears when the console is connected to the partition, and then it stops.

3.4.8 Checking partition information

Check partition information by displaying the partition status and partition-related information. You can also check the partition configuration of the entire PRIMEQUEST 1000 series system in the [Partition Configuration] window.

Operations

1. Click [Partition] - [Partition#x] - [Information].

>> The [Information] window appears. For details on the [Information] window, see [Information] window in 1.3.7 [Partition#x] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

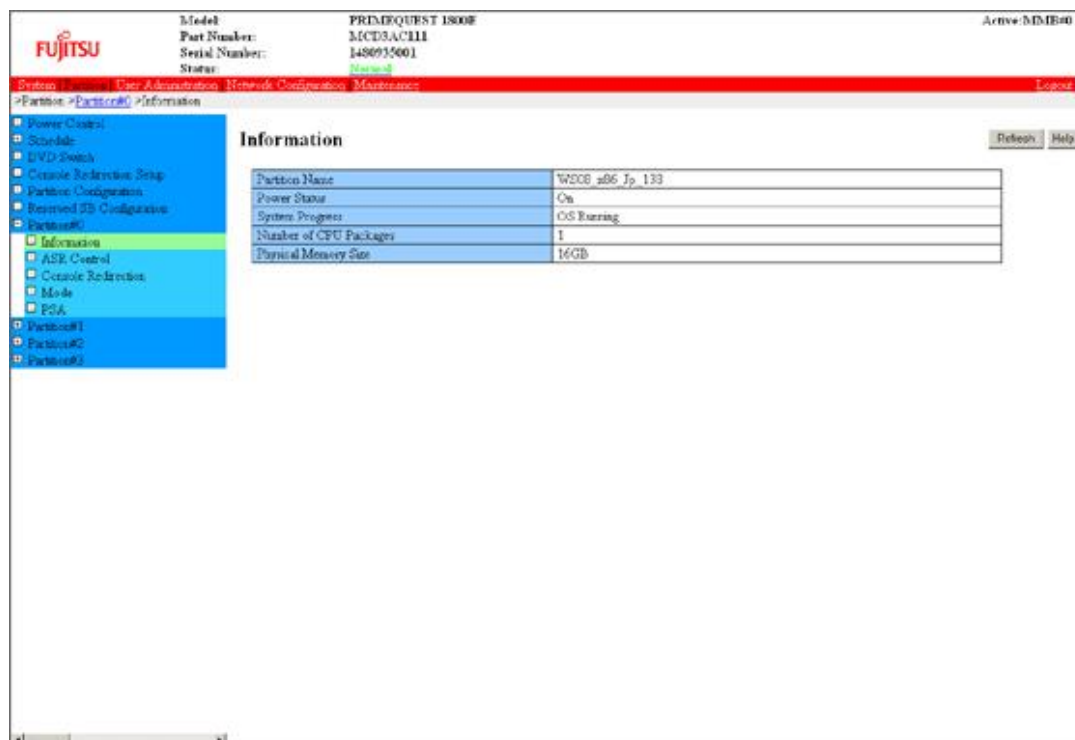


FIGURE 3.31 [Information] window (example)

Remarks

Whether the [PSA] menu is displayed depends on the model and installed operating system. For details, check with a field engineer.

3.5 Saving Configuration Information

This section describes how to save information on the settings made during installation. Be sure to back up MMB configuration information.

Remarks

- After the start of actual business operation, back up MMB configuration information regularly.
- For details on how to save PSA management and BIOS configuration information, see [6.8 Saving Management and Configuration Information](#).

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

3.5.1 Backing up MMB configuration information

This section describes how to back up MMB configuration information.

Remarks

For details on how to restore MMB configuration information, see 8.1.2 Backing up and restoring MMB configuration information in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

Operations

1. Click [Maintenance] - [Backup/Restore Configuration] - [Backup/Restore MMB Configuration].
>> The Backup/Restore MMB Configuration window appears. For details on the Backup/Restore MMB Configuration window, see Backup/Restore MMB Configuration window in 1.6.2 [Backup/Restore Configuration] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

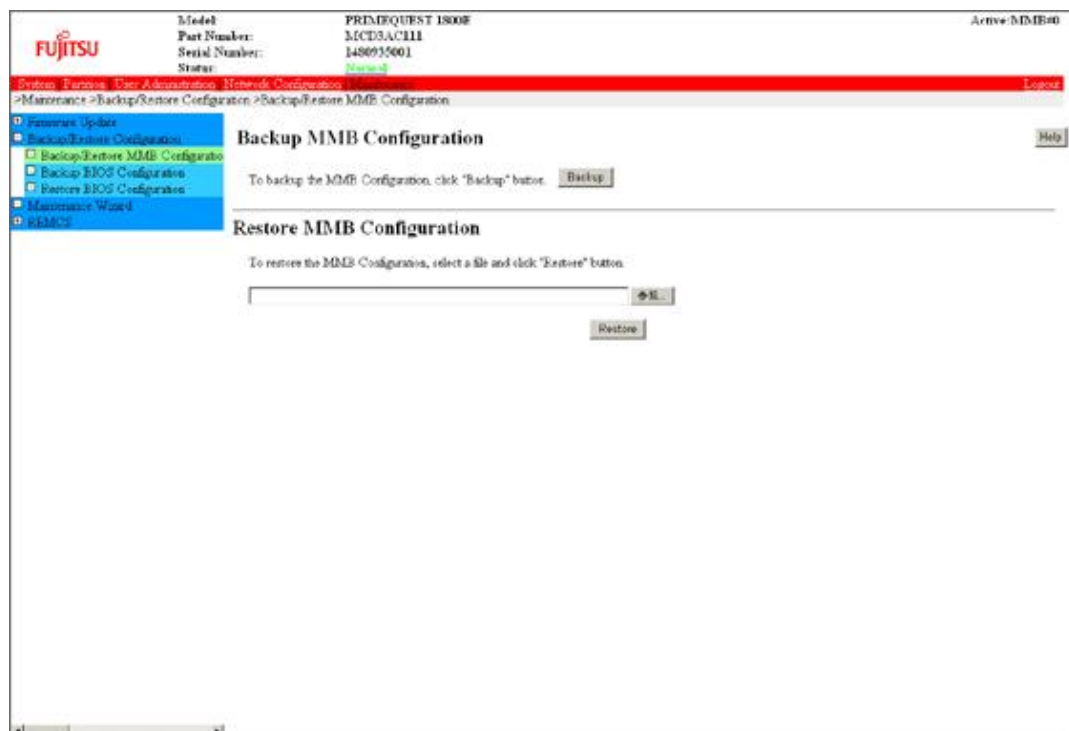


FIGURE 3.32 Backup/Restore MMB Configuration window (example)

2. Click the [Backup] button.

>> The save destination dialog box of the browser appears.

3. Select the save destination path. Then, click the [OK] button.

>> Download of the configuration information file begins.

The backup file of the MMB configuration information has the following default name:

MMB_backup date_MMB version.dat

CHAPTER 4 Installing the Operating System and Bundled Software

This appendix describes the procedures for installing RHEL, Windows, and VMware on the SAN storage unit or built-in HDD. For details on the installation procedures, see the respective references.

4.1 Installation Procedure for the Operating System and Bundled Software	60
4.2 RHEL Installation Procedures on the SAN Storage Unit	61
4.3 RHEL Installation Procedures on the Built-in HDD	67
4.4 Windows Installation Procedures on the SAN Storage Unit	73
4.5 Windows Installation Procedures on the Built-in HDD	82
4.6 VMware 4.x Installation Procedures on the SAN Storage Unit	91
4.7 VMware 4.x Installation Procedures on the Built-in HDD	94
4.8 VMware 5.x Installation Procedures on the SAN Storage Unit	97
4.9 VMware 5.x Installation Procedures on the Built-in HDD	101
4.10 SUSE Linux Enterprise Server 11 Service Pack 2 Installation Procedures on the SAN Storage Unit	105
4.11 SUSE Linux Enterprise Server 11 Service Pack 2 Installation Procedures on the Built-in HDD	110

4.1 Installation Procedure for the Operating System and Bundled Software

Before installing the operating system, deactivate BootWatchdog. For deactivation procedure details, see 9.4.1 Setting automatic partition restart conditions in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

You can set the x2APIC mode in the PRIMEQUEST 1800E2. Set Enabled or Disabled for x2APIC mode according to the operating system. For details, see G.1 CPU in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

Use SVIM to install the operating system on a partition of the PRIMEQUEST 1000 series server. SVIM is a setup support tool for the following operations:

- Installation of the operating system
- Installation of the drivers required by the operating system
- Installation of the bundled software

For details on the software installed automatically by SVIM, see 3.3 Bundled Software in the *PRIMEQUEST 1000 Series General Description* (C122-B022EN).

For an overview of SVIM, see the *ServerView Suite ServerView Installation Manager*.

There are also points to consider regarding SVIM. See the *PRIMEQUEST 1000 Series ServerView Suite Notes* (C122-E149EN).

Note

For installation in the SAN boot environment and VMware installation, also check the following.

- Configuring the SAN boot environment
If the SAN boot environment is to be installed, configure it before installing the operating system. For details on configuring the SAN boot environment, see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).
- Installing the operating system and bundled software
A different procedure applies to VMware installation. For details on the VMware installation procedure, see [APPENDIX E Notes on VMware Installation](#).

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

4.2 RHEL Installation Procedures on the SAN Storage Unit

This section describes the procedures for installing RHEL on the SAN storage unit. Confirm the MMB configuration and successful login to the MMB before starting the installation.

For details on configuring the SAN storage unit and FC card (Fibre Channel card), see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).

4.2.1 Advance setup and preparation

Set up the following as needed.

1. Set the LUN of the SAN storage unit.
2. Configure the BIOS so that the LUN of the FC card is recognized.
For details on configuring the FC card, see Chapter 2 Settings on the Fiber Channel Card (FC Card) in the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).
3. After removing the built-in HDD of the PRIMEQUEST server, confirm the partition settings with the MMB.
 - Setting the SB/IOB/GSPB configuration
(See [3.4.1 Setting a partition configuration.](#))
 - Configuring Console Redirection
(See [3.4.6 Configuring Console Redirection.](#))
 - Video redirection: Enable
 - Remote storage: Enable
 - Console redirection: Enable
 - Setting various modes
(See [3.4.5 Setting various modes.](#))
4. Connect only the LUN of the SAN storage unit, to which the OS is to be installed, to the partition of the PRIMEQUEST server.
For details on the settings for the SAN storage unit, see the manual supplied with the SAN storage unit.
5. Assign I/O spaces to the FC card (card for boot path only), SAS card, SAS array controller card, Onboard SAS controller (GSPB), SAS disk unit controller and SAS array disk unit controller.
For details on I/O space assignment, see [3.4.5 Setting various modes](#) in this manual and 5.5.1 [Configure I/O Space Assignment] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

4.2.2 Preparing for Installation

No RHEL distribution DVD is available for RHEL installation. Users who have purchased a RHEL subscription will need to create a RHEL distribution DVD.

Customer Portal :

<https://access.redhat.com/home>

Create an image of the RHEL distribution DVD.

Creating an image of the RHEL distribution DVD

Log in to Red Hat's customer portal (<https://access.redhat.com/>), download the image file of the distribution DVD to another system.

Note

The image file of the distribution DVD varies with minor releases and the architecture (for x86/for Intel64).
Download the DVD image file appropriate to your needs.

Remarks

To download the file, you will need to register a subscription to Red Hat from Red Hat's customer portal.

Preparing for boot

Change FC cabling to single path (connecting only one FC cable).

4.2.3 Installing the operating system

This section describes the operating system installation with SVIM.

SVIM can perform the following types of operating system installation. For the procedure for each mode, see the *ServerView Suite ServerView Installation Manager*.

TABLE 4.1 Operating system installation by SVIM

Mode	Functional outline	Remarks
Quick mode	You can simply use the minimum settings necessary for operating system installation. This mode uses Fujitsu's recommended settings.	Use this mode to readily install the OS.
Guide mode	You can specify setup information by following the instructions of the wizard. You can save the specified information in a configuration file for use during reinstallation.	This mode enables detailed settings. Use the mode if you want to configure installation with detailed RAID and OS settings.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

Operations

1. Make the setting for booting the partition from remote storage.
For details on the setting, see 1.6.3 Remote operation (BMC) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).
2. Insert ServerView Suite DVD1 into the DVD drive. Then, power on the partition.
When using the remote storage DVD, insert ServerView Suite DVD1 into the remote storage. Then, power on the partition.

Remarks

If the operating system supports UEFI mode, you can install it in UEFI mode by using the following procedure to change the boot order.

1. Select [Force boot from DVD] from [Boot Selector] in the [Power Control] window of the MMB Web-UI. Then, power on the partition.

2. After powering on the partition, press and hold down any key ([Space] key, for example) other than the [Enter] key while the FUJITSU logo is displayed, to display the Boot Manager Front Page.
3. Select the following items from the menu in the order given in the Boot Manager Front Page:
[Boot Maintenance Manager] - [Boot Options] - [Change Boot Order] - [Change the order]
 - Specify [UEFI: DVD/CD 0] as the highest priority device to boot from the remote storage DVD.
 - Specify [UEFI: Embedded DVD/CD] as the highest priority device to boot from the built-in DVD.

For details on how to set the boot order, see Changing the order of priority (Change Boot Order) in 5.6.1 [Boot Options] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

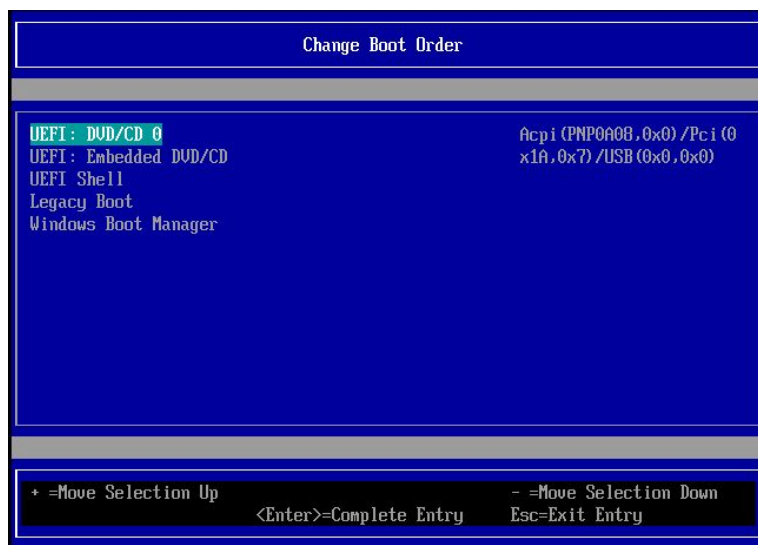


FIGURE 4.1 Example of display of the [Change Boot Order] menu

The following describes the meaning of the menu:

- UEFI: DVD/CD n (n=0, 1, 2...)
Specify this when starting the UEFI-aware OS from the external DVD/CD drive media.
The n in "UEFI: DVD/CD n" is a sequential number (starting from 0) assigned in the order that DVD/CD devices are recognized. The assigned number remains stored based on the connection location information as long as the device is not disconnected from the system.
 - UEFI: Embedded DVD/CD:
Specify this item when using the built-in DVD drive for installation in UEFI mode.
 - UEFI Shell:
Specify this menu when starting UEFI Shell. The PRIMEQUEST 1000 series does not use UEFI Shell.
 - Legacy Boot:
Specify this item for BIOS mode. Also specify [Legacy Boot] when using the built-in DVD drive for installation in BIOS mode.
4. Specify [Commit Changes and Exit].
 5. Press the [ESC] key to return to the Front Page.
 6. Specify [Boot Manager].
 7. Specify [UEFI:DVD/CD 0] to use the remote storage DVD. Specify [UEFI: Embedded DVD/CD] to use the built-in DVD.

3. After a moment, the language selection window appears. Select [English] for installation in English.

4. Click the [Next] button on the initially displayed window without setting anything.
5. Select [Deployment] in the [Welcome to ServerView Installation Manager] window.
6. Select an installation mode and the operating system to be installed. Then, set up the operating system.

Remark

The IP address of the LAN cannot be set through the operating system setup. Set the IP address after the installation of the operating system.

7. Click [Install].
Installation begins.
8. Replace the media with the operating system installation media according to the SVIM instructions.

4.2.4 Configuring bundled software after the completion of installation

After completing OS installation, configure the bundled software.

1. Confirm that the PSA management LAN IP address is not the same as the IP address used for the production network or management network. For details in the case of the PRIMEQUEST 1800E2, see the *ServerView Mission Critical Option User Manual*. For details in the case of the PRIMEQUEST 1800E, see [6.2.1 Configuring the PSA-to-MMB communication LAN](#).

Remarks

The PSA management LAN is automatically assigned an IP address. Confirm that the IP address is not the same as the IP address used for the production network or management network. If the IP addresses match, change the PSA management LAN IP address. Also, if the subnets match, change the subnet setting on the MMB side.

2. Configure and confirm the management LAN.
 - Configuring the management LAN used for communication with the MMB
(See [6.2.2 Confirming management LAN settings](#).)
If necessary, configure any duplication with bonding or PRIMECLUSTER GLS, for example.
 - Confirming SELinux function settings
(See [6.2.3 Confirming SELinux function settings](#).)
Confirm that the SELinux function is [disabled].
3. Check the firewall function. For details, see [6.2.4 Checking the firewall function \(opening ports\)](#).
 - Open the ports for the PSA-to-MMB communication LAN interfaces.
 - snmp port: udp/snmp or 161
 - web-mmb communication port: tcp/fj-webgate or 24450
 - psa-mmb communication port: tcp/5000 on the MMB side
 - icmp: echo-request
 - icmp: echo-reply

4. Set the destinations of SNMP traps from the partition.

Set the destinations of traps and PSA trap notification on the partition side as needed. For details, see [6.2.5 Setting the destinations of traps from a partition](#).

Remarks

You can confirm a trap destination setting by using the standard trap of the SNMP service. For details, see [How to confirm a trap destination setting](#) in [6.3.3 Setting the destinations of traps from a partition](#).

5. Set the destinations of SNMP traps and e-mail via the MMB.

Make settings only as needed, such as for linkage with operations management software.

1. Set the destinations of SNMP traps via the MMB.
(See [7.5.2 Configuring SNMP](#).)
2. If Alarm E-Mail is to be configured, set the notification destination and filter.
(See [3.3.9 Configuring Alarm E-Mail](#).)

6. Set the management LAN IP address.

Make this setting only if you need to change the management LAN IP address. For details, see [6.2.7 Setting the management LAN IP address](#).

7. If the FC card is installed, install HBAnyware.

Remarks

For RHEL5.6 or later, replace HBAnyware with OneCommand Manager.

1. The libnl package is required to use HBAnyware.

Execute the following command to display the libnl package information, and confirm that libnl has been installed:

```
# rpm -qi libnl
```

If libnl has not been installed, execute a search for the install medium of the distribution for the libnl package, and execute the following command to install the package:

```
# rpm -ivh libnl-<version>-<release>.<arch>.rpm
```

Remark

<version>, <release>, and <arch> must be replaced with suitable character strings.

2. Download the driver and utility of MC-0JFC11 or MC-0JFC21 from the following URL:
<http://jp.fujitsu.com/platform/server/primequest/download/>

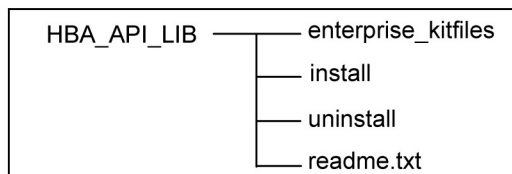
Note

The downloaded binary file has a description about the PRIMERGY, but the driver and utility can be used for the PRIMEQUEST 1000 series.

3. Copy the downloaded file to an arbitrary directory of the PRIMEQUEST 1000 series, and then expand it.

```
# tar xvzf F1010350.tar.gz
```

4. The following files are extracted:



Remark

For details on how to install "SNIA HBA API library," see the readme.txt extracted in the HBA_API_LIB folder.

5. After the installation is completed, reboot the unit.
8. Install updates of PSA and other bundled software.
Check the latest versions of the software at their download sites, and install the necessary updates. For details on PSA, see [6.2.9 Installing a PSA update](#).
9. Configure the dump area.
Confirm that the hard disk has enough free space before collecting a memory dump.
10. Configure the NTP client.
Configure the NTP server on the operating system side. For details, see [7.2 Configuring NTP](#).
11. Save management and configuration information. For details, see [6.8 Saving Management and Configuration Information](#).
12. Configure RAS Support Service. For details, see [6.9 Configuring Service Life Monitoring by RAS Support Service](#).
For service life monitoring of the BBU of a RAID card: See [6.9.1 BBU service life monitoring for a RAID card](#).
For service life monitoring of the battery of a UPS: See [6.9.2 Battery unit service life monitoring for a UPS](#).

4.2.5 Connecting the SAN and built-in HDD after the installation

For details on connecting the SAN and built-in HDD after the installation, see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).

Also, for details on driver parameters, see the readme file that comes with the driver.

4.3 RHEL Installation Procedures on the Built-in HDD

This section concisely describes the procedures for installing RHEL on the built-in HDD. Confirm the MMB configuration and successful login to the MMB before starting the installation.

4.3.1 Advance setup

Set up the following as needed.

1. Remove each built-in HDD that is not the installation destination.
2. Confirm the partition settings of the PRIMEQUEST server with the MMB. For details, see [3.4 Configuring a Partition](#).
 - Setting the SB/IOB/GSPB configuration
(See [3.4.1 Setting a partition configuration](#).)
 - Configuring Console Redirection
(See [3.4.6 Configuring Console Redirection](#).)
 - Video redirection: Enable
 - Remote storage: Enable
 - Console redirection: Enable
 - Setting various modes
(See [3.4.5 Setting various modes](#).)
3. Assign I/O spaces to the SAS card, SAS array controller card, Onboard SAS controller (GSPB), SAS disk unit controller and SAS array disk unit controller.
For details on I/O space assignment, see [3.4.5 Setting various modes](#) in this manual and 5.5.1 [Configure I/O Space Assignment] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

4.3.2 Preparing for Installation

No RHEL distribution DVD is available for RHEL installation. Users who have purchased a RHEL subscription will need to create a RHEL distribution DVD.

Create an image of the RHEL distribution DVD.

Creating an image of the RHEL distribution DVD

Log in to Red Hat's customer portal (<https://access.redhat.com/>), download the image file of the distribution DVD to another system.

Note

The image file of the distribution DVD varies with minor releases and the architecture (for x86/for Intel64). Download the DVD image file appropriate to your needs.

Remarks

To download the file, you will need to register a subscription to Red Hat from Red Hat's customer portal.

Preparing for boot

1. Disconnect all the FC cables.

2. Mount the disk image of the RHEL distribution DVD on remote storage.
3. Change the boot order to give the highest priority to booting the storage unit where the operating system is installed.

For details, see 1.3.1 [Power Control] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

4.3.3 Installing the operating system

This section describes the operating system installation with SVIM.

SVIM can perform the following types of operating system installation. For the procedure for each mode, see the *ServerView Suite ServerView Installation Manager*.

TABLE 4.2 Operating system installation by SVIM

Mode	Functional outline	Remarks
Quick mode	You can simply use the minimum settings necessary for operating system installation. This mode uses Fujitsu's recommended settings.	Use this mode to readily install the OS.
Guide mode	You can specify setup information by following the instructions of the wizard. You can save the specified information in a configuration file for use during reinstallation.	This mode enables detailed settings. Use the mode if you want to configure installation with detailed RAID and OS settings.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

Operations

1. Make the setting for booting the partition from remote storage.
For details on the setting, see 1.6.3 Remote operation (BMC) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).
2. Insert ServerView Suite DVD1 into the DVD drive. Then, power on the partition.

Remarks

You can boot from the DVD drive either by selecting [Force boot from DVD] from [Boot Selector], or by specifying the DVD drive as the highest-priority device to boot from, in UEFI mode.

If the operating system supports UEFI mode, you can install it in UEFI mode by using the following procedure to change the boot order.

1. After powering on the partition, press and hold down any key ([Space] key, for example) other than the [Enter] key while the FUJITSU logo is displayed, to display the Boot Manager Front Page.
2. Select the following items from the menu in the order given in the Boot Manager Front Page:
[Boot Maintenance Manager] - [Boot Options] - [Change Boot Order] - [Change the order]

- Specify [UEFI: DVD/CD 0] as the highest priority device to boot from the remote storage DVD.
- Specify [UEFI: Embedded DVD/CD] as the highest priority device to boot from the built-in DVD.

For details on how to set the boot order, see Changing the order of priority (Change Boot Order) in 5.6.1 [Boot Options] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

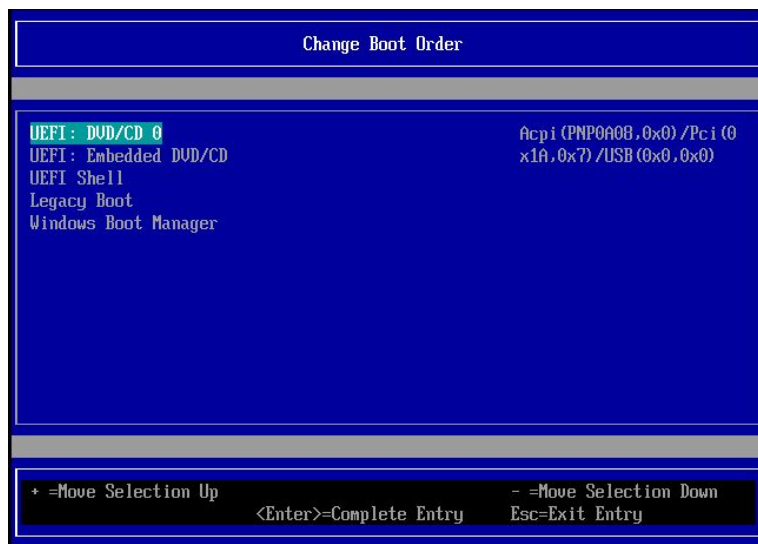


FIGURE 4.2 Example of display of the [Change Boot Order] menu

The following describes the meaning of the menu:

- UEFI: DVD/CD n (n=0, 1, 2...)
Specify this when starting the UEFI-aware OS from the external DVD/CD drive media.
The n in "UEFI: DVD/CD n" is a sequential number (starting from 0) assigned in the order that DVD/CD devices are recognized. The assigned number remains stored based on the connection location information as long as the device is not disconnected from the system.
- UEFI: Embedded DVD/CD:
Specify this item when using the built-in DVD drive for installation in UEFI mode.
- UEFI Shell:
Specify this menu when starting UEFI Shell. The PRIMEQUEST 1000 series does not use UEFI Shell.
- Legacy Boot:
Specify this item for BIOS mode. Also specify [Legacy Boot] when using the built-in DVD drive for installation in BIOS mode.

3. Specify [Commit Changes and Exit] - [Reset System] to reboot the partition.

3. After a moment, the language selection window appears. Select [English] for installation in English.
4. Click the [Next] button on the initially displayed window without setting anything.
5. Select [Deployment] in the [Welcome to ServerView Installation Manager] window.
6. Select an installation mode and the operating system to be installed. Then, set up the operating system.

Remark

The IP address of the LAN cannot be set through the operating system setup. Set the IP address after the installation of the operating system.

7. Click [Install].
Installation begins.
8. Replace the media with the operating system installation media according to the SVIM instructions.

4.3.4 Configuring bundled software after the completion of installation

After completing OS installation, configure the bundled software.

1. Confirm that the PSA management LAN IP address is not the same as the IP address used for the production network or management network. For details in the case of the PRIMEQUEST 1800E2, see the *ServerView Mission Critical Option User Manual*. For details in the case of the PRIMEQUEST 1800E, see [6.2.1 Configuring the PSA-to-MMB communication LAN](#).

Remarks

The PSA management LAN is automatically assigned an IP address. Confirm that the IP address is not the same as the IP address used for the production network or management network. If the IP addresses match, change the PSA management LAN IP address. Also, if the subnets match, change the subnet setting on the MMB side.

2. Configure and confirm the management LAN.
 - Configuring the management LAN used for communication with the MMB
(See [6.2.2 Confirming management LAN settings](#).)
If necessary, configure any duplication with bonding or PRIMECLUSTER GLS, for example.
 - Confirming SELinux function settings
(See [6.2.3 Confirming SELinux function settings](#).)
Confirm that the SELinux function is [disabled].
3. Check the firewall function. For details, see [6.2.4 Checking the firewall function \(opening ports\)](#).
 - Open the ports for the PSA-to-MMB communication LAN interfaces.
 - snmp port: udp/snmp or 161
 - web-mmb communication port: tcp/fj-webgate or 24450
 - psa-mmb communication port: tcp/5000 on the MMB side
 - icmp: echo-request
 - icmp: echo-reply
4. Set the destinations of SNMP trap from the partition.
Set the destinations of traps and PSA trap notification on the partition side as needed. For details, see [6.2.5 Setting the destinations of traps from a partition](#).

Remarks

You can confirm a trap destination setting by using the standard trap of the SNMP service. For details, see [How to confirm a trap destination setting](#) in 6.3.3 [Setting the destinations of traps from a partition](#).

5. Set the destinations of traps and e-mail via the MMB.

Make settings only as needed, such as for linkage with operations management software.

1. Set the destinations of SNMP traps via the MMB.
(See [7.5.2 Configuring SNMP](#).)
2. If Alarm E-Mail is to be configured, set the notification destination and filter.
(See [3.3.9 Configuring Alarm E-Mail](#).)

6. Set the management LAN IP address.

Make this setting only if you need to change the management LAN IP address. For details, see [6.2.7 Setting the management LAN IP address](#).

7. If the FC card is installed, install HBAnyware.

Remarks

For RHEL5.6 or later, replace HBAnyware with OneCommand Manager.

1. The libnl package is required to use HBAnyware.

Execute the following command to display the libnl package information, and confirm that libnl has been installed:

```
# rpm -qi libnl
```

If libnl has not been installed, execute a search for the install medium of the distribution for the libnl package, and execute the following command to install the package:

```
# rpm -ivh libnl-<version>-<release>.<arch>.rpm
```

Remark

<version>, <release>, and <arch> must be replaced with suitable character strings.

2. Download the driver and utility of MC-0JFC11 or MC-0JFC21 from the following URL:

<http://jp.fujitsu.com/platform/server/primequest/download/>

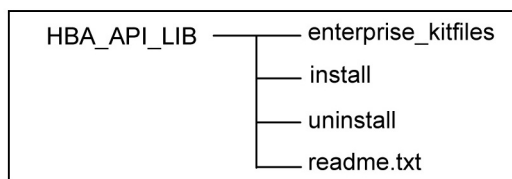
Note

The downloaded binary file has a description about the PRIMERGY, but the driver and utility can be used for the PRIMEQUEST 1000 series.

3. Copy the downloaded file to an arbitrary directory of the PRIMEQUEST 1000 series, and then expand it.

```
# tar xvzf F1010350.tar.gz
```

4. The following files are extracted:



Remark

For details on how to install "SNIA HBA API library," see the `readme.txt` extracted in the `HBA_API_LIB` folder.

5. After the installation is completed, reboot the unit.
8. Install updates of PSA and other bundled software.
Check the latest versions of the software at their download sites, and install the necessary updates. For details on PSA, see [6.2.9 Installing a PSA update](#).
9. Configure the dump area.
Confirm that the hard disk has enough free space before collecting a memory dump.
10. Configure the NTP client.
Configure the NTP server on the operating system side. For details, see [7.2 Configuring NTP](#).
11. Save management and configuration information. For details, see [6.8 Saving Management and Configuration Information](#).
12. Configure RAS Support Service. For details, see [6.9 Configuring Service Life Monitoring by RAS Support Service](#).
For service life monitoring of the BBU of a RAID card: See [6.9.1 BBU service life monitoring for a RAID card](#).
For service life monitoring of the battery of a UPS: See [6.9.2 Battery unit service life monitoring for a UPS](#).

4.3.5 Connecting the SAN and built-in HDD after the installation

For connecting the SAN and built-in HDD after the installation, see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).

Also, for details on driver parameters, see the `readme` file that comes with the driver.

4.4 Windows Installation Procedures on the SAN Storage Unit

This section concisely describes the procedures for installing Windows on the SAN storage unit. Start this work only after confirming the completion of the connection and configuration of the MMB.

For details on configuring the SAN storage unit and FC card (Fibre Channel card), see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).

4.4.1 Advance setup

Set up the following as needed.

1. Set the LUN of the SAN storage unit.
2. Configure the BIOS so that the LUN of the FC card is recognized.
For details on configuring the FC card, see Chapter 2 Settings on the Fiber Channel Card (FC Card) in the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).
3. After removing the built-in HDD of the PRIMEQUEST server, confirm the partition settings with the MMB.
 - Setting the SB/IOB/GSPB configuration
(See [3.4.1 Setting a partition configuration.](#))
 - Configuring Console Redirection
(See [3.4.6 Configuring Console Redirection.](#))
 - Video redirection: Enable
 - Remote storage: Enable
 - Console redirection: Enable
 - Setting various modes
(See [3.4.5 Setting various modes.](#))
4. Connect only the LUN of the SAN storage unit as the installation destination to the partition of the PRIMEQUEST server.
For details on the settings for the SAN storage unit, see the manual supplied with the SAN storage unit.
5. Assign I/O spaces to the FC card (card for boot path only), SAS card, SAS array controller card, Onboard SAS controller (GSPB), SAS disk unit controller and SAS array disk unit controller.
For details on I/O space assignment, see [3.4.5 Setting various modes](#) in this manual and 5.5.1 [Configure I/O Space Assignment] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

4.4.2 Preparing for Installation

Prepare the following.

1. Prepare the following disk image:
Windows operating system media
2. Change FC cabling to single path (connecting only one FC cable).

4.4.3 Installing the operating system

This section describes the operating system installation with SVIM.

SVIM can perform the following types of operating system installation. For the procedure for each mode, see the *ServerView Suite ServerView Installation Manager*.

TABLE 4.3 Operating system installation by SVIM

Mode	Functional outline	Remarks
Quick mode	You can simply use the minimum settings necessary for operating system installation. This mode uses Fujitsu's recommended settings.	Use this mode to readily install the OS.
Guide mode	You can specify setup information by following the instructions of the wizard. You can save the specified information in a configuration file for use during reinstallation.	This mode enables detailed settings. Use the mode if you want to configure installation with detailed RAID and OS settings.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

Operations

1. Make the setting for booting the partition from remote storage.

For details on the setting, see 1.6.3 Remote operation (BMC) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

2. Insert ServerView Suite DVD1 into the DVD drive. Then, power on the partition.

When using the remote storage DVD, insert ServerView Suite DVD1 into the remote storage. Then, power on the partition.

Remarks

If the operating system supports UEFI mode, you can install it in UEFI mode by using the following procedure to change the boot order.

1. Select [Force boot from DVD] from [Boot Selector] in the [Power Control] window of the MMB Web-UI. Then, power on the partition.
2. After powering on the partition, press and hold down any key ([Space] key, for example) other than the [Enter] key while the FUJITSU logo is displayed, to display the Boot Manager Front Page.
3. Select the following items from the menu in the order given in the Boot Manager Front Page:
[Boot Maintenance Manager] - [Boot Options] - [Change Boot Order] - [Change the order]
 - Specify [UEFI: DVD/CD 0] as the highest priority device to boot from the remote storage DVD.
 - Specify [UEFI: Embedded DVD/CD] as the highest priority device to boot from the built-in DVD.

For details on how to set the boot order, see Changing the order of priority (Change Boot Order) in 5.6.1 [Boot Options] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

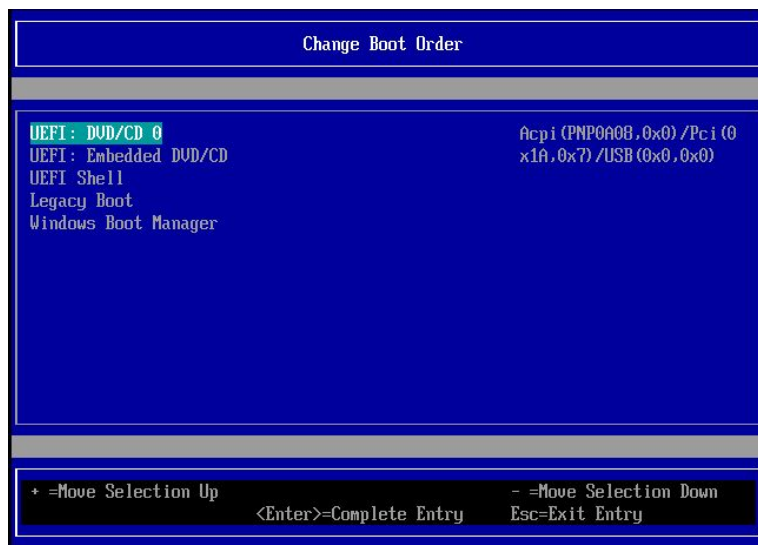


FIGURE 4.3 Example of display of the [Change Boot Order] menu

The following describes the meaning of the menu:

- UEFI: DVD/CD n (n=0, 1, 2...)
Specify this when starting the UEFI-aware OS from the external DVD/CD drive media. The n in "UEFI: DVD/CD n" is a sequential number (starting from 0) assigned in the order that DVD/CD devices are recognized. The assigned number remains stored based on the connection location information as long as the device is not disconnected from the system.
- UEFI: Embedded DVD/CD:
Specify this item when using the built-in DVD drive for installation in UEFI mode.
- UEFI Shell:
Specify this menu when starting UEFI Shell. The PRIMEQUEST 1000 series does not use UEFI Shell.
- Legacy Boot:
Specify this item for BIOS mode. Also specify [Legacy Boot] when using the built-in DVD drive for installation in BIOS mode.

4. Specify [Commit Changes and Exit].
5. Press the [ESC] key to return to the Front Page.
6. Specify [Boot Manager].
7. Specify [UEFI:DVD/CD 0] to use the remote storage DVD. Specify [UEFI: Embedded DVD/CD] to use the built-in DVD.

3. After a moment, the language selection window appears. Select [English] for installation in English.
4. Click the [Next] button on the initially displayed window without setting anything.
5. Select [Deployment] in the [Welcome to ServerView Installation Manager] window.
6. Select an installation mode and the operating system to be installed. Then, set up the operating system.

Remark

The IP address of the LAN cannot be set through the operating system setup. Set the IP address after the installation of the operating system.

7. Click [Install].
Installation begins.
8. Replace the media with the operating system installation media according to the SVIM instructions.
9. Perform the following operation by using the MMB Web-UI.

Remarks

These steps are not required in Windows Server 2012.

1. Click [Partition] - [Partition#x] - [Mode].
2. Check the [Setting OS Installation Mode] check box, and then click the [Apply] button.
3. When the confirmation message appears, click the [OK] button.

After a while, the [Setting Completed] window appears. This completes the setting procedure.



FIGURE 4.4 [Mode] window (example)

Remark

Perform the above procedure at the following times.

1. When the system goes from the [ServerView Installation Manager] window to the [Install Windows] window, after starting installation with SVIM and rebooting.

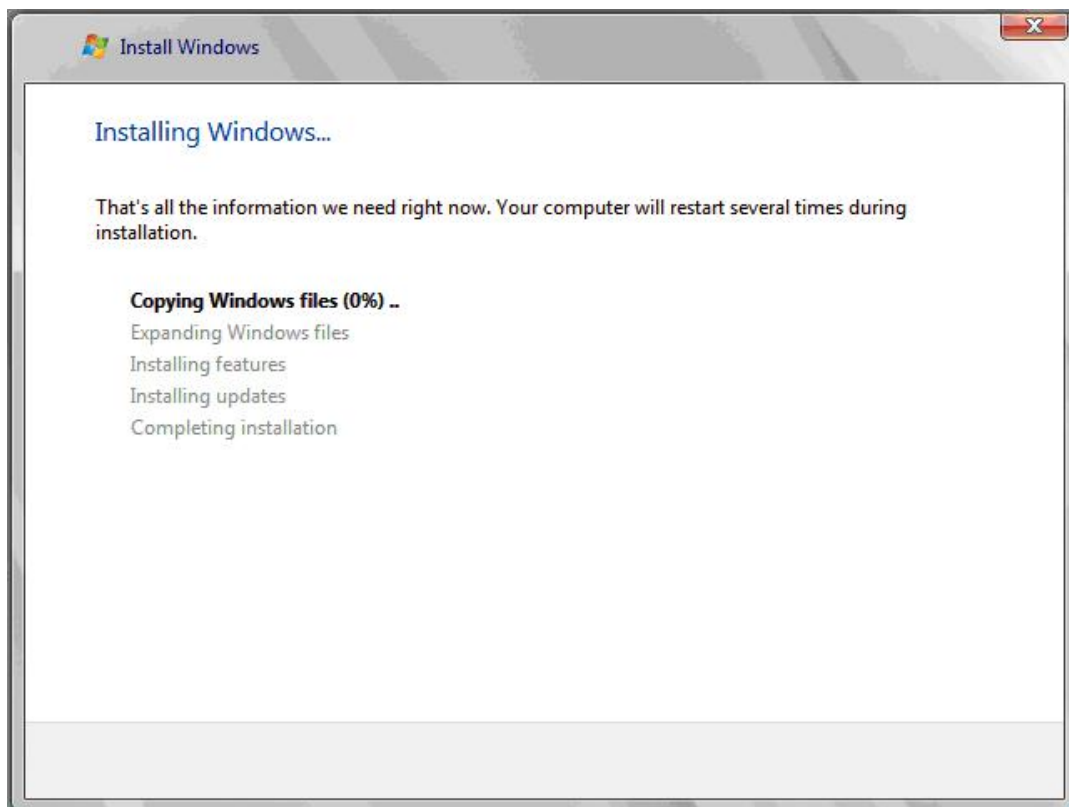


FIGURE 4.5 [Install Windows] window

2. When the [Install Windows] window appears after a system reboot following termination of the [Installing updates] window with the [Install Windows] window displayed as is in 1. above.

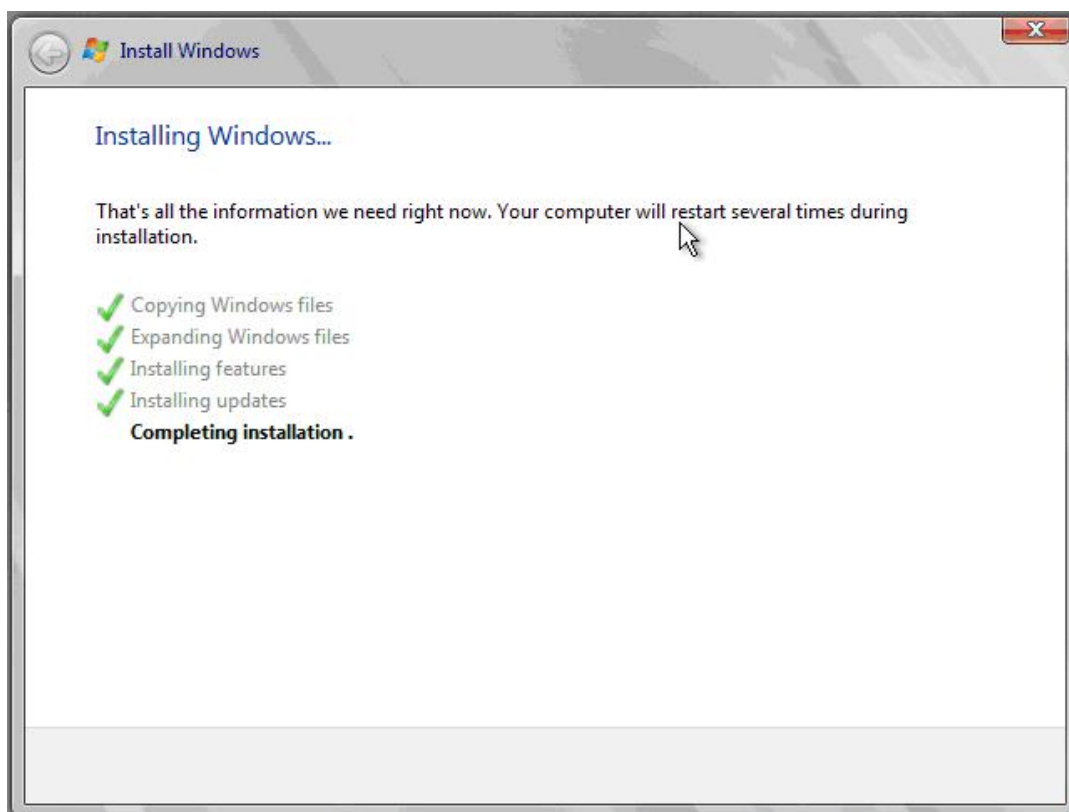


FIGURE 4.6 [Install Windows] window

4.4.4 Configuring bundled software after the completion of installation

After completing installation of the operating system, configure the bundled software.

Remarks

- Depending on the driver version, HBAnyware should be interpreted as OneCommand Manager.
- When referring to PSA-related descriptions, for the PRIMEQUEST 1800E2, see the *ServerView Mission Critical Option User Manual*, instead of the descriptions in the PSA-related sections shown in this document.

1. Install HBAnyware if the following applies:

- The FC card is installed,

and

- HBAnyware has not been installed.

The installation of HBAnyware can be confirmed by the existence of [Emulex] - [HBAnyware], which is displayed by selecting [All Programs] from the [Start] menu.

1. Download the driver and utility of MC-0JFC11 or MC-0JFC21 from the following URL:

<http://jp.fujitsu.com/platform/server/primequest/download/>

Note

The downloaded binary file has a description about the PRIMERGY, but the driver and utility can be used for the PRIMEQUEST 1000 series.

2. Execute the downloaded file by double-clicking it.

The prompt screen for the cmd.exe (a window with a black background) is displayed for a while, and then the file is extracted.

3. After the extraction is completed, the window is automatically closed.

The downloaded file is extracted and folders or files are newly created.

Remark

If the window is not closed in spite of the display of "Installation Completed" in the window, click the [Finish] button to close the window.

4. Double-click storportminiportkit_XXXXX.exe in the extracted FC_vXXXXXXX directory to run it.

Remark

"XXXXX" represents the version and must be replaced with a suitable character string.

2. For Windows 2003 or Windows 2008, make the registry setting.

Remarks

No registry setting is required for Windows Server 2012.

1. Insert the "ServerView Suite DVD1" DVD into the DVD drive.

2. Double-click the file in the <DVD drive name>:\HotFixes\SR-IO folder to run it.

- If the folder contains the following two files, select a file according to the Windows type.

TABLE 4.4 If the folder contains two files

OS type	Name of file to be run (xx: version number)
Windows Server 2003 / R2	SR-IO-registry-xx-Win2003.reg
Windows Server 2008 / R2	SR-IO-registry-xx-Win2008.reg
Windows Server 2012 / R2	- (Registry setting not required)

- If the folder contains one file, it is a common file for Windows.

TABLE 4.5 If the folder contains one file

OS type	Name of file to be run (xx: version number)
Windows Server 2003 / R2	SR-IO-registry-xx-E0.reg
Windows Server 2008 / R2	
Windows Server 2012 / R2	- (Registry setting not required)

3. Remove the "ServerView Suite DVD1" DVD from the DVD drive.

3. After completing the setting, reboot the unit.

4. Confirm that the PSA management LAN IP address is not the same as the IP address used for the production network or management network. For details, see [6.3.1 Configuring the PSA-to-MMB communication LAN](#).

Remarks

The PSA management LAN is automatically assigned an IP address. Confirm that the IP address is not the same as the IP address used for the production network or management network. If the IP addresses are identical, change the PSA management LAN IP address. Also, if the subnets are identical, change the subnet setting on the MMB side.

5. Confirm management LAN settings.

1. Confirm the management LAN settings for linkage to higher-layer software, such as Systemwalker.
2. Specify OFF for the STP function of the switch that connects to the management LAN used for communication with the MMB. (See [6.3.2 Confirming management LAN settings](#).)

6. Set the destinations of traps from the partition.

For direct transfer of a PSA expansion trap from a partition, set the SNMP trap destination and PSA trap notification. For details, see [6.3.3 Setting the destinations of traps from a partition](#).

Remarks

You can confirm a trap destination setting by using the standard trap of the SNMP service. (See [How to confirm a trap destination setting](#) in [6.3.3 Setting the destinations of traps from a partition](#).)

7. Set the destinations of SNMP traps and e-mail via the MMB.

Make settings only as needed, such as for linkage with operations management software.

1. Display the [SNMP Configuration] menu in the MMB window, and enable SNMP.
2. Set the destinations of SNMP traps via the MMB.
(See [7.5.2 Configuring SNMP](#).)

8. Configure the firewall.

For Windows Server 2003: See [6.3.5 Configuring the Windows Firewall](#).

For Windows Server 2008: See [6.4.6 Configuring the Windows Firewall](#).

For Windows Server 2012: See the *ServerView Mission Critical Option User Manual*.

9. Set the Watchdog Timer for monitoring after a STOP error. For details, see [6.3.6 Setting the Watchdog Timer for monitoring after a STOP error \(fatal system error\)](#).

1. Edit the PSA configuration file [pnwatchdog.conf].
2. Set the following key values:
Section: [WATCHDOG]
Key: [TIMER]
Setting value (unit: seconds): 0 (Watchdog Timer disabled), 1 to 6000 (Watchdog Timer monitoring time)

10. Set the management LAN IP address.

Make this setting only if you need to change the management LAN IP address. For details, see [6.3.7 Setting the management LAN IP address](#).

11. Install updates of PSA and other bundled software.

Check the latest versions of the software at their download sites, and install the necessary updates. For details on PSA, see [6.3.8 Installing a PSA update](#).

12. Configure the dump area.

Confirm that the hard disk has enough free space before collecting a memory dump. For details, see 11.4.4 Setting up the dump environment (Windows) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

13. Configure the NTP client.

Configure the NTP server on the operating system side. For details, see [7.2 Configuring NTP](#).

14. Save management and configuration information. For details, see [6.8 Saving Management and Configuration Information](#).

15. Configure RAS Support Service. For details, see [6.9 Configuring Service Life Monitoring by RAS Support Service](#).

For service life monitoring of the BBU of a RAID card: See [6.9.1 BBU service life monitoring for a RAID card](#).

For service life monitoring of the battery of a UPS: See [6.9.2 Battery unit service life monitoring for a UPS](#).

4.4.5 Connecting the SAN and built-in HDD after the installation

For details on connecting the SAN and built-in HDD after the installation, see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).

1. Change and check the setting of detailed FC card information. For details, see *the PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).
2. Start HBAnyware. Set the following driver parameters. For details on the setting values, see the manual of the SAN storage unit.
 - Topology
 - Queue Depth
 - Queue Target
 - Link Speed
3. Check registry information. For details on how to check it, see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN). For details on the setting values, see the manual of the SAN storage unit.
 - TimeOutValue

4.5 Windows Installation Procedures on the Built-in HDD

This section concisely describes the procedures for installing Windows on the built-in HDD. Confirm the MMB configuration and successful login to the MMB before starting the installation. For details on configuring the SAN storage unit and FC card (Fibre Channel card), see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).

4.5.1 Advance setup

Set up the following as needed.

1. Remove each built-in HDD that is not the installation destination.
2. Confirm the partition settings with the MMB.
 - Setting the SB/IOB/GSPB configuration
(See [3.4.1 Setting a partition configuration.](#))
 - Configuring Console Redirection
(See [3.4.6 Configuring Console Redirection.](#))
 - Video redirection: Enable
 - Remote storage: Enable
 - Console redirection: Enable
 - Setting various modes
(See [3.4.5 Setting various modes.](#))
3. Assign I/O spaces to the SAS card, SAS array controller card, Onboard SAS controller (GSPB), SAS disk unit controller and SAS array disk unit controller.
For details on I/O space assignment, see 3.4.5 Setting various modes in this manual and 5.5.1 [Configure I/O Space Assignment] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

4.5.2 Preparing for Installation

Prepare the following.

1. Prepare the following disk image:
Windows operating system media
2. Disconnect all the FC cables.
3. Mount the disk image through a video redirection connection.
4. Change the boot order so that DVD booting has the highest priority.
For details, see 1.3.1 [Power Control] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

4.5.3 Installing the operating system

This section describes the operating system installation with SVIM.

SVIM can perform the following types of operating system installation. For the procedure for each mode, see the *ServerView Suite ServerView Installation Manager*.

TABLE 4.6 Operating system installation by SVIM

Mode	Functional outline	Remarks
Quick mode	You can simply use the minimum settings necessary for operating system installation. This mode uses Fujitsu's recommended settings.	Use this mode to readily install the OS.
Guide mode	You can specify setup information by following the instructions of the wizard. You can save the specified information in a configuration file for use during reinstallation.	This mode enables detailed settings. Use the mode if you want to configure installation with detailed RAID and OS settings.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

Operations

1. Make the setting for booting the partition from remote storage.
For details on the setting, see 1.6.3 Remote operation (BMC) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).
2. Insert ServerView Suite DVD1 into the DVD drive. Then, power on the partition.

Remarks

You can boot from the DVD drive either by selecting [Force boot from DVD] from [Boot Selector], or by specifying the DVD drive as the highest-priority device to boot from, in UEFI mode.

If the operating system supports UEFI mode, you can install it in UEFI mode by using the following procedure to change the boot order.

1. After powering on the partition, press and hold down any key ([Space] key, for example) other than the [Enter] key while the FUJITSU logo is displayed, to display the Boot Manager Front Page.
2. Select the following items from the menu in the order given in the Boot Manager Front Page:
[Boot Maintenance Manager] - [Boot Options] - [Change Boot Order] - [Change the order]
 - Specify [UEFI: DVD/CD 0] as the highest priority device to boot from the remote storage DVD.
 - Specify [UEFI: Embedded DVD/CD] as the highest priority device to boot from the built-in DVD.

For details on how to set the boot order, see Changing the order of priority (Change Boot Order) in 5.6.1 [Boot Options] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

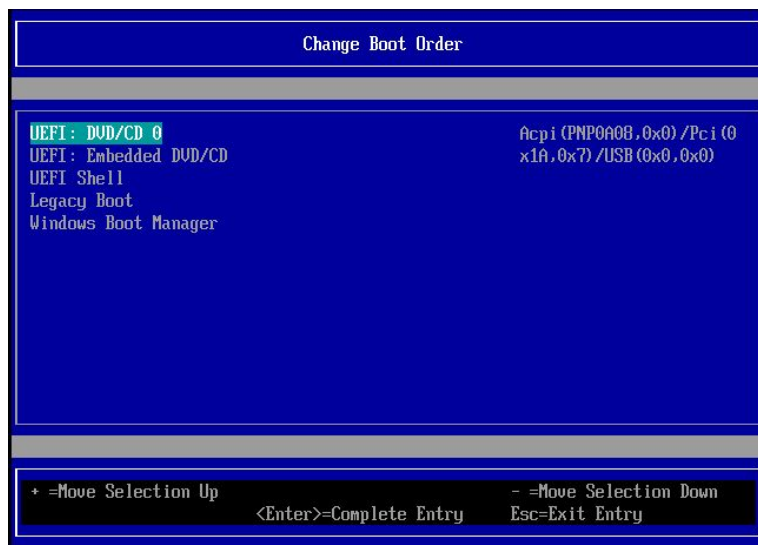


FIGURE 4.7 Example of display of the [Change Boot Order] menu

The following describes the meaning of the menu:

- UEFI: DVD/CD n (n=0, 1, 2...)
Specify this when starting the UEFI-aware OS from the external DVD/CD drive media.
The n in "UEFI: DVD/CD n" is a sequential number (starting from 0) assigned in the order that DVD/CD devices are recognized. The assigned number remains stored based on the connection location information as long as the device is not disconnected from the system.
- UEFI: Embedded DVD/CD:
Specify this item when using the built-in DVD drive for installation in UEFI mode.
- UEFI Shell:
Specify this menu when starting UEFI Shell. The PRIMEQUEST 1000 series does not use UEFI Shell.
- Legacy Boot:
Specify this item for BIOS mode. Also specify [Legacy Boot] when using the built-in DVD drive for installation in BIOS mode.

3. Specify [Commit Changes and Exit] - [Reset System] to reboot the partition.

3. After a moment, the language selection window appears. Select [English] for installation in English.

4. Click the [Next] button on the initially displayed window without setting anything.

5. Select [Deployment] in the [Welcome to ServerView Installation Manager] window.

6. Select an installation mode and the operating system to be installed. Then, set up the operating system.

Remark

The IP address of the LAN cannot be set through the operating system setup. Set the IP address after the installation of the operating system.

7. Click [Install].

Installation begins.

8. Replace the media with the operating system installation media according to the SVIM instructions.
9. Perform the following operation by using the MMB Web-UI.

Remarks

These steps are not required in Windows Server 2012.

1. Click [Partition] - [Partition#x] - [Mode].
2. Check the [Setting OS Installation Mode] check box, and then click the [Apply] button.
3. When the confirmation message appears, click the [OK] button.

After a while, the [Setting Completed] window appears. This completes the setting procedure.



FIGURE 4.8 [Mode] window (example)

Remark

Perform the above procedure at the following times.

1. When the system goes from the [ServerView Installation Manager] window to the [Install Windows] window, after starting installation with SVIM and rebooting.

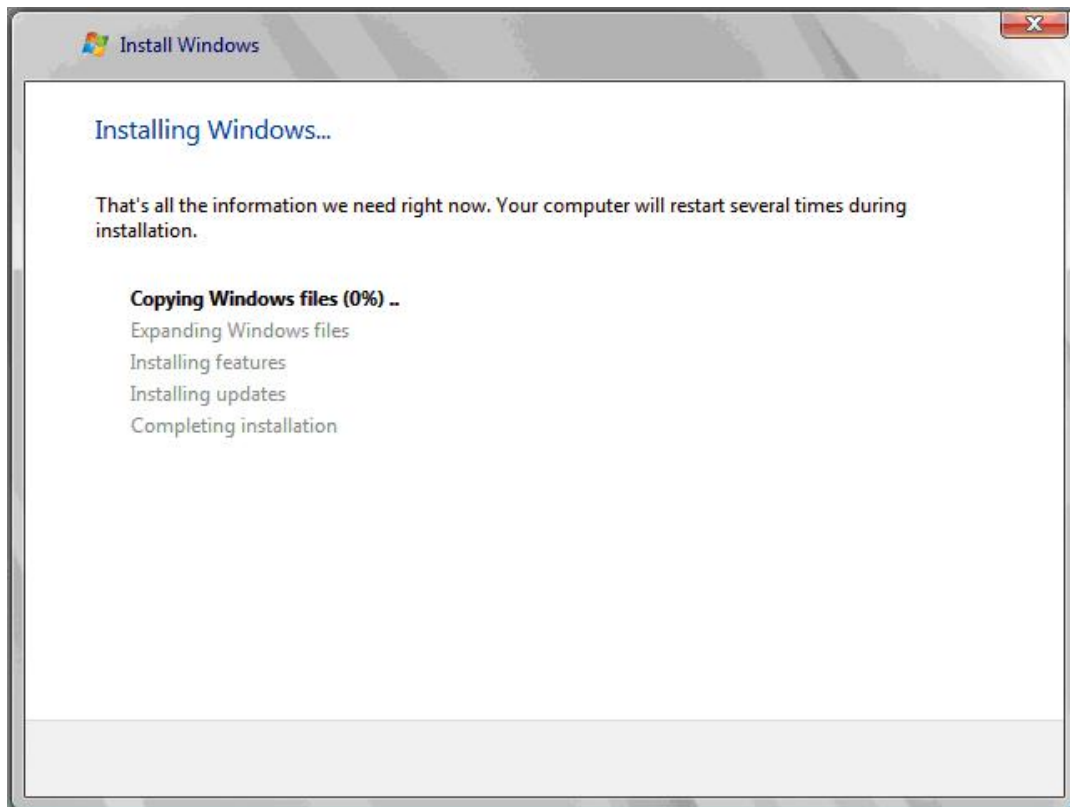


FIGURE 4.9 [Install Windows] window

2. When the [Install Windows] window appears after a system reboot following termination of the [Installing updates] window with the [Install Windows] window displayed as is in 1. above.

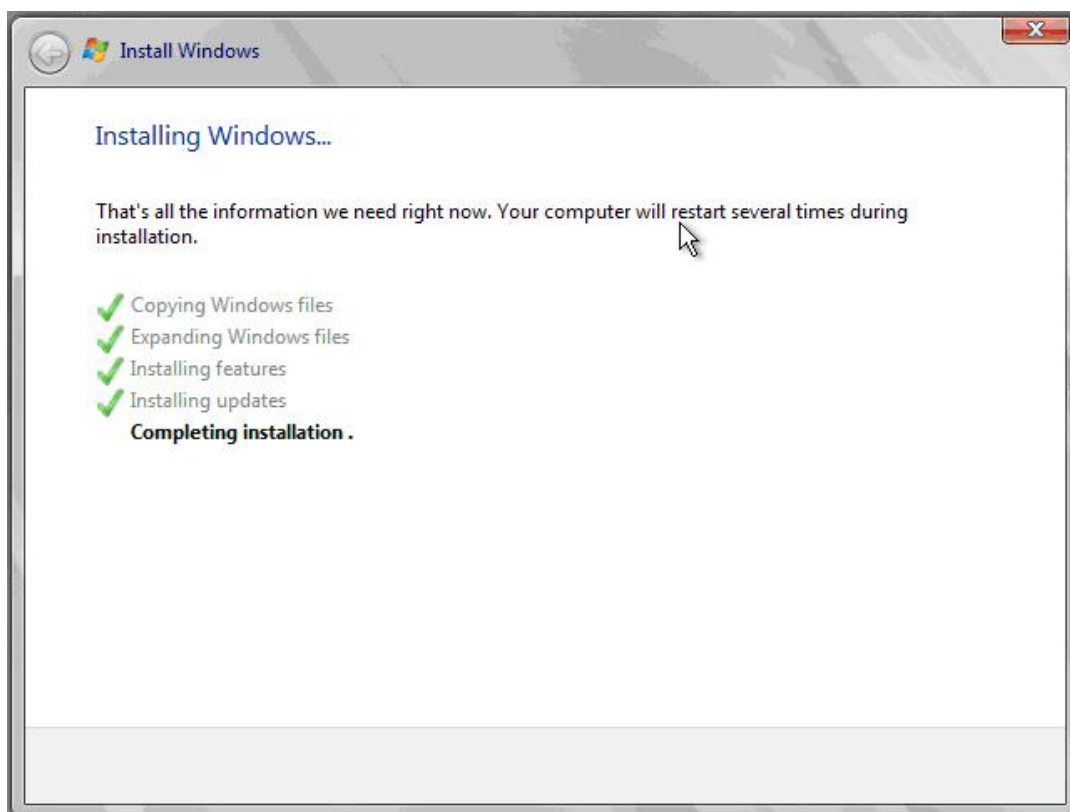


FIGURE 4.10 [Install Windows] window

4.5.4 Configuring bundled software after the completion of installation

After completing installation of the operating system, configure the bundled software.

Remarks

Depending on the driver version, interpret HBAnyware as OneCommand Manager.

1. Install HBAnyware if the following applies:

- The FC card is installed,

and

- HBAnyware has not been installed.

The installation of HBAnyware can be confirmed by the existence of [Emulex] - [HBAnyware], which is displayed by selecting [All Programs] from the [Start] menu.

1. Download the driver and utility of MC-0JFC11 or MC-0JFC21 from the following URL:

<http://jp.fujitsu.com/platform/server/primequest/download/>

Note

The downloaded binary file has a description about the PRIMERGY, but the driver and utility can be used for the PRIMEQUEST 1000 series.

2. Execute the downloaded file by double-clicking it.

The prompt screen for the cmd.exe (a window with a black background) is displayed for a while, and then the file is extracted.

3. After the extraction is completed, the window is automatically closed.

The downloaded file is extracted and folders or files are newly created.

Remark

If the window is not closed in spite of the display of "Installation Completed" in the window, click the [Finish] button to close the window.

4. Double-click storportminiportkit_XXXXX.exe in the extracted FC_vXXXXXXX directory to run it.

Remark

"XXXXX" represents the version and must be replaced with a suitable character string.

2. Make the registry setting.

Remarks

No registry setting is required for Windows Server 2012.

1. Insert the "ServerView Suite DVD1" DVD into the DVD drive.

2. Double-click the file in the <DVD drive name>:\HotFixes\SR-IO folder to run it.

- If the folder contains the following two files, select a file according to the Windows type.

TABLE 4.7 If the folder contains two files

OS type	Name of file to be run (xx: version number)
Windows Server 2003 / R2	SR-IO-registry-xx-Win2003.reg
Windows Server 2008 / R2	SR-IO-registry-xx-Win2008.reg
Windows Server 2012 / R2	- (Registry setting not required)

- If the folder contains one file, it is a common file for Windows.

TABLE 4.8 If the folder contains one file

OS type	Name of file to be run (xx: version number)
Windows Server 2003 / R2	SR-IO-registry-xx-E0.reg
Windows Server 2008 / R2	
Windows Server 2012 / R2	- (Registry setting not required)

3. Remove the "ServerView Suite DVD1" DVD from the DVD drive.

3. After completing the setting, reboot the unit.

4. Confirm that the PSA management LAN IP address is not the same as the IP address used for the production network or management network.

For details in the case of the PRIMEQUEST 1800E2, see the *ServerView Mission Critical Option User Manual*. For details in the case of the PRIMEQUEST 1800E, see [6.2.1 Configuring the PSA-to-MMB communication LAN](#).

Remarks

The PSA management LAN is automatically assigned an IP address. Confirm that the IP address is not the same as the IP address used for the production network or management network. If the IP addresses are identical, change the PSA management LAN IP address. Also, if the subnets are identical, change the subnet setting on the MMB side.

5. Confirm management LAN settings.

1. Confirm the management LAN settings for linkage to higher-layer software, such as Systemwalker.
2. Specify OFF for the STP function of the switch that connects to the management LAN used for communication with the MMB. (See [6.3.2 Confirming management LAN settings](#).)

6. Set the destinations of SNMP trap from the partition.

For direct transfer of a PSA expansion trap from a partition, set the trap destination and PSA trap notification. For details, see [6.3.3 Setting the destinations of traps from a partition](#).

Remarks

You can confirm a trap destination setting by using the standard trap of the SNMP service. (See [How to confirm a trap destination setting](#) in [6.3.3 Setting the destinations of traps from a partition](#).)

7. Set the destinations of SNMP trap and e-mail via the MMB.

Make settings only as needed, such as for linkage with operations management software.

1. Display the [SNMP Configuration] menu in the MMB window, and enable SNMP.
2. Set the destinations of SNMP traps via the MMB.

(See [7.5.2 Configuring SNMP](#).)

8. Configure the firewall.

For Windows Server 2003: See [6.3.5 Configuring the Windows Firewall](#).

For Windows Server 2008: See [6.4.6 Configuring the Windows Firewall](#).

For Windows Server 2012: See the *ServerView Mission Critical Option User Manual*.

9. Set the Watchdog Timer for monitoring after a STOP error. For details, see [6.3.6 Setting the Watchdog Timer for monitoring after a STOP error \(fatal system error\)](#).

1. Edit the PSA configuration file [pnwatchdog.conf].

2. Set the following key values:

Section: [WATCHDOG]

Key: [TIMER]

Setting value (unit: seconds): 0 (Watchdog Timer disabled), 1 to 6000 (Watchdog Timer monitoring time)

10. Set the management LAN IP address.

Make this setting only if you need to change the management LAN IP address. For details, see [6.3.7 Setting the management LAN IP address](#).

11. Install updates of PSA and other bundled software.

Check the latest versions of the software at their download sites, and install the necessary updates. For details on PSA, see [6.3.8 Installing a PSA update](#).

12. Configure the dump area.

Confirm that the hard disk has enough free space before collecting a memory dump. For details, see 11.4.4 Setting up the dump environment (Windows) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

13. Configure the NTP client.

Configure the NTP server on the operating system side. For details, see [7.2 Configuring NTP](#).

14. Save management and configuration information. For details, see [6.8 Saving Management and Configuration Information](#).

15. Configure RAS Support Service. For details, see [6.9 Configuring Service Life Monitoring by RAS Support Service](#).

For service life monitoring of the BBU of a RAID card: See [6.9.1 BBU service life monitoring for a RAID card](#).

For service life monitoring of the battery of a UPS: See [6.9.2 Battery unit service life monitoring for a UPS](#).

4.5.5 Connecting the SAN and built-in HDD after the installation

For details on connecting the SAN and built-in HDD after the installation, see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).

1. Change and check the setting of detailed FC card information. For details, see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).
2. Start HBAnyware. Set the following driver parameters. For details on the setting values, see the manual of the SAN storage unit.
 - Topology
 - Queue Depth
 - Queue Target
 - Link Speed
3. Check registry information. For details on how to check it, see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN). For details on the setting values, see the manual of the SAN storage unit.
 - TimeOutValue

4.6 VMware 4.x Installation Procedures on the SAN Storage Unit

This section concisely describes the procedures for installing VMware 4.x on the SAN storage unit. Start this work only after confirming the completion of the connection and configuration of the MMB.

For details on configuring the SAN storage unit and FC card (Fibre Channel card), see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).

4.6.1 Advance setup

Set up the following as needed.

1. Set the LUN of the SAN storage unit.
2. Configure the BIOS so that the LUN of the FC card is recognized.
For details on configuring the FC card, see Chapter 2 Settings on the Fiber Channel Card (FC Card) in the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).
3. Prepare a server running ServerView Operations Manager.
4. After removing the built-in HDD of the PRIMEQUEST server, confirm the partition settings with the MMB.
 - Setting the SB/IOB/GSPB configuration
(See [3.4.1 Setting a partition configuration.](#))
 - Configuring Console Redirection
(See [3.4.6 Configuring Console Redirection.](#))
 - Video redirection: Enable
 - Remote storage: Enable
 - Console redirection: Enable
 - Setting various modes
(See [3.4.5 Setting various modes.](#))
5. When connecting only the LUN of the SAN storage unit as the installation destination, connect it to the PRIMEQUEST partition.
For details on the settings for the SAN storage unit, see the manual supplied with the SAN storage unit.
6. Assign I/O spaces to the FC card (card for boot path only), SAS card, SAS array controller card, Onboard SAS controller (GSPB), SAS disk unit controller and SAS array disk unit controller.
For details on I/O space assignment, see [3.4.5 Setting various modes](#) and 5.5.1 [Configure I/O Space Assignment] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

4.6.2 Preparing for Installation

To prepare for installation, also see the VMware information.

For the VMware information, contact the distributor where you purchased your product, or your sales representative.

Prepare the following.

1. Prepare the following disk image:
VMware 4.x media

2. Change FC cabling to single path (connecting only one FC cable).

4.6.3 Installing VMware 4.x

Install VMware 4.x by following the instructions in the *VMware vSphere Software Handbook*.

For details on this handbook, contact your sales representative.

Before starting installation, see [E.2 Notes on VMware 4.x Installation](#).

4.6.4 Installing bundled software

After completing installation of the operating system, configure the bundled software.

- Installing ServerView Agent
(See [E.3.1 Installing ServerView Agent](#).)
- Installing ServerView RAID
(See [E.3.2 Installing ServerView RAID](#).)
- Installing RAS Support Service
(See [E.3.3 Installing RAS Support Service \(PRIMEQUEST\)](#).)
- Installing HRM/server
(See [E.3.4 Installing VMware 4.x HRM/server \(PRIMEQUEST\)](#).)
- Installing PSA (1800E)
(See [E.3.5 Installing VMware 4.x PSA](#).)
- Installing SVMco (1800E2)
(See the *ServerView Mission Critical Option User Manual*)

4.6.5 Configuring bundled software

Configure the bundled software. For details on confirming and configuring the LAN, see [E.4.1 Configuring the network](#).

1. Confirm the PSA-to-MMB communication LAN and management LAN.
The PSA-to-MMB communication LAN uses the physical adapter assigned BUS number 0000:00:19.0. The management LAN uses an arbitrary physical adapter.
Execute the `esxcfg-nics` command to confirm the physical adapters used for the PSA-to-MMB communication LAN and management LAN.
2. Configure the management LAN.
 1. Use `vswif0`, which exists by default immediately after the installation of the operating system, for the interface of the management LAN.
 2. Execute the `esxcfg-vswif` command to assign an IP address to `vswif0`.
3. Configure the PSA-to-MMB communication LAN.
 1. Execute the `esxcfg-vswitch` command to create a virtual switch (`vSwitch1`).
 2. Execute the `esxcfg-vswitch` command to connect physical adapter `vmnic0` to the virtual switch.
 3. Add a port group (PSA-MMB) to the created switch.
 4. Execute the `esxcfg-vswif` command to create a virtual port (`vswif1`).
 5. Add the following settings to the PSA-to-MMB communication LAN:
Speed: 100 Mbps
Duplex: full

6. Set the IP address of the PSA-to-MMB communication LAN in the PSA configuration file.
4. Configure the firewall. For details, see [E.4.2 Configuring the firewall](#).
5. Configure the default gateway. For details, see [E.4.3 Configuring the default gateway](#).
6. Retrieve VMware PSA maintenance information. For details, see [E.4.4 Retrieving VMware 4.x PSA maintenance information](#).
7. Install updates of PSA and other bundled software.
Check the latest versions of the software at their download sites, and install the necessary updates. For details on PSA, see [6.2.9 Installing a PSA update](#).

4.6.6 Configuring a software watchdog

Remarks

If you use SVOM 5.0, see [When using SVOM 5.0 or later](#) in [E.2 Notes on VMware 4.x Installation](#).

1. Start ServerView Operations Manager.
2. Select [ServerList].
3. Right-click the target partition in the server list on the left side. Select [Maintenance] - [ASR Properties] from the displayed menu.
4. Select [Watchdog] in the displayed window.
5. Specify the following for [Software], and click [Apply].
 - Check the [Active] check box.
 - Select [Continue] for [Action] for cases of abnormal operation.
 - Enter a value between 1 and 100 minutes for [Timeout].
6. Enter your user name and password, and press the [Enter] key.

4.6.7 Completing VMware 4.x installation

After completing the settings, reboot the partition of the PRIMEQUEST 1000 series server.

4.7 VMware 4.x Installation Procedures on the Built-in HDD

This section concisely describes the procedures for installing VMware 4.x on the built-in HDD. Start this work only after confirming the completion of the connection and configuration of the MMB.

4.7.1 Advance setup

Set up the following as needed.

1. Prepare a server running ServerView Operations Manager.
2. After removing the built-in HDD of the PRIMEQUEST server, confirm the partition settings with the MMB.
 - Setting the SB/IOB/GSPB configuration
(See [3.4.1 Setting a partition configuration.](#))
 - Configuring Console Redirection
(See [3.4.6 Configuring Console Redirection.](#))
 - Video redirection: Enable
 - Remote storage: Enable
 - Console redirection: Enable
 - Setting various modes
(See [3.4.5 Setting various modes.](#))
3. Assign I/O spaces to the SAS card, SAS array controller card, Onboard SAS controller (GSPB), SAS disk unit controller and SAS array disk unit controller.
For details on I/O space assignment, see 3.4.5 Setting various modes in this manual and 5.5.1 [Configure I/O Space Assignment] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

4.7.2 Preparing for Installation

To prepare for installation, also see the VMware information.

For the VMware information, contact the distributor where you purchased your product, or your sales representative.

Prepare the following.

1. Prepare the following disk image:
VMware 4.x media
2. Disconnect all the FC cables.
3. Mount the disk image through a video redirection connection.
4. Configure the RAID environment.
For details, see the *MegaRAID SAS Software*, the *MegaRAID SAS Device Driver Installation*, or the LSI MegaRAID (R) SAS Software contained on the SVS DVD.
5. Change the boot order to give the highest priority in startup to DVD boot.
For details, see 1.3.1 [Power Control] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

4.7.3 Installing VMware 4.x

Install VMware 4.x by following the instructions in the *VMware vSphere Software Handbook*.

For details on this handbook, contact your sales representative.

Before starting installation, see [E.2 Notes on VMware 4.x Installation](#).

4.7.4 Installing bundled software

After completing installation of the operating system, configure the bundled software.

- Installing ServerView Agent
(See [E.3.1 Installing ServerView Agent](#).)
- Installing ServerView RAID
(See [E.3.2 Installing ServerView RAID](#).)
- Installing RAS Support Service
(See [E.3.3 Installing RAS Support Service \(PRIMEQUEST\)](#).)
- Installing HRM/server
(See [E.3.4 Installing VMware 4.x HRM/server \(PRIMEQUEST\)](#).)
- Installing PSA (1800E)
(See [E.3.5 Installing VMware 4.x PSA](#).)
- Installing SVMco (1800E2)
(See the *ServerView Mission Critical Option User Manual*)

4.7.5 Configuring bundled software

Configure the bundled software. For details on confirming and configuring the LAN, see [E.4.1 Configuring the network](#).

1. Confirm the PSA-to-MMB communication LAN and management LAN.
The PSA-to-MMB communication LAN uses the physical adapter assigned BUS number 0000:00:19.0. The management LAN uses an arbitrary physical adapter.
Execute the `esxcfg-nics` command to confirm the physical adapters used for the PSA-to-MMB communication LAN and management LAN.
2. Configure the management LAN.
 1. Use `vswif0`, which exists by default immediately after the installation of the operating system, for the interface of the management LAN.
 2. Execute the `esxcfg-vswif` command to assign an IP address to `vswif0`.
3. Configure the PSA-to-MMB communication LAN.
 1. Execute the `esxcfg-vswitch` command to create a virtual switch (`vSwitch1`).
 2. Execute the `esxcfg-vswitch` command to connect physical adapter `vmnic0` to the virtual switch.
 3. Add a port group (PSA-MMB) to the created switch.
 4. Execute the `esxcfg-vswif` command to create a virtual port (`vswif1`).
 5. Add the following settings to the PSA-to-MMB communication LAN:
Speed: 100 Mbps
Duplex: full
 6. Set the IP address of the PSA-to-MMB communication LAN in the PSA configuration file.
4. Configure the firewall. For details, see [E.4.2 Configuring the firewall](#).

5. Configure the default gateway. For details, see [E.4.3 Configuring the default gateway](#).
6. Retrieve VMware PSA maintenance information. For details, see [E.4.4 Retrieving VMware 4.x PSA maintenance information](#).
7. Install updates of PSA and other bundled software.
Check the latest versions of the software at their download sites, and install the necessary updates. For details on PSA, see [6.2.9 Installing a PSA update](#).

4.7.6 Configuring a software watchdog

Remarks

If you use SVOM 5.0, see [When using SVOM 5.0 or later](#) in [E.2 Notes on VMware 4.x Installation](#).

1. Start ServerView Operations Manager.
2. Select [ServerList].
3. Right-click the target partition in the server list on the left side. Select [Maintenance] - [ASR Properties] from the displayed menu.
4. Select [Watchdog] in the displayed window.
5. Specify the following for [Software], and click [Apply].
 - Check the [Active] check box.
 - Select [Continue] for [Action] for cases of abnormal operation.
 - Enter a value between 1 and 100 minutes for [Timeout].
6. Enter your user name and password, and press the [Enter] key.

4.7.7 Completing VMware installation

After completing the settings, reboot the partition of the PRIMEQUEST 1000 series server.

4.8 VMware 5.x Installation Procedures on the SAN Storage Unit

This section concisely describes the procedures for installing VMware 5.x on the SAN storage unit. Start this work only after confirming the completion of the connection and configuration of the MMB.

For details on configuring the SAN storage unit and FC card (Fibre Channel card), see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).

4.8.1 Advance setup

Set up the following as needed.

1. Set the LUN of the SAN storage unit.
2. Configure the BIOS so that the LUN of the FC card is recognized.
For details on configuring the FC card, see Chapter 2 Settings on the Fiber Channel Card (FC Card) in the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).
3. Prepare a server running ServerView Operations Manager.
4. After removing the built-in HDD of the PRIMEQUEST server, confirm the partition settings with the MMB.
 - Setting the SB/IOB/GSPB configuration
(See [3.4.1 Setting a partition configuration.](#))
 - Configuring Console Redirection
(See [3.4.6 Configuring Console Redirection.](#))
 - Video redirection: Enable
 - Remote storage: Enable
 - Console redirection: Enable
 - Setting various modes
(See [3.4.5 Setting various modes.](#))
5. When connecting only the LUN of the SAN storage unit as the installation destination, connect it to the PRIMEQUEST partition.
For details on the settings for the SAN storage unit, see the manual supplied with the SAN storage unit.
6. Assign I/O spaces to the FC card (card for boot path only), SAS card, SAS array controller card, Onboard SAS controller (GSPB), SAS disk unit controller and SAS array disk unit controller.
For details on I/O space assignment, see 3.4.5 Setting various modes in this manual and 5.5.1 [Configure I/O Space Assignment] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

4.8.2 Preparing for Installation

To prepare for installation, also see the VMware information.

For the VMware information, contact the distributor where you purchased your product, or your sales representative.

Prepare the following.

1. Prepare the following disk image:
VMware 5.x media

2. Change FC cabling to single path (connecting only one FC cable).

4.8.3 Installing VMware 5.x

This section describes the operating system installation with SVIM.

SVIM can perform the following types of operating system installation. For the procedure for each mode, see the *ServerView Suite ServerView Installation Manager*.

TABLE 4.9 Operating system installation by SVIM

Mode	Functional outline	Remarks
Quick mode	You can simply use the minimum settings necessary for operating system installation. This mode uses Fujitsu's recommended settings.	Use this mode to readily install the OS.
Guide mode	You can specify setup information by following the instructions of the wizard. You can save the specified information in a configuration file for use during reinstallation.	This mode enables detailed settings. Use the mode if you want to configure installation with detailed RAID and OS settings.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

Operations

1. Make the setting for booting the partition from remote storage.
For details on the setting, see 1.6.3 Remote operation (BMC) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).
2. Insert ServerView Suite DVD1 into the DVD drive. Then, power on the partition.
When using the remote storage DVD, insert ServerView Suite DVD1 into the remote storage. Then, power on the partition.

Remarks

If the operating system supports UEFI mode, you can install it in UEFI mode by using the following procedure to change the boot order.

1. Select [Force boot from DVD] from [Boot Selector] in the [Power Control] window of the MMB Web-UI. Then, power on the partition.
2. After powering on the partition, press and hold down any key ([Space] key, for example) other than the [Enter] key while the FUJITSU logo is displayed, to display the Boot Manager Front Page.
3. Select the following items from the menu in the order given in the Boot Manager Front Page:
[Boot Maintenance Manager] - [Boot Options] - [Change Boot Order] - [Change the order]
 - Specify [UEFI: DVD/CD 0] as the highest priority device to boot from the remote storage DVD.
 - Specify [UEFI: Embedded DVD/CD] as the highest priority device to boot from the built-in DVD.

For details on how to set the boot order, see Changing the order of priority (Change Boot Order) in 5.6.1 [Boot Options] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

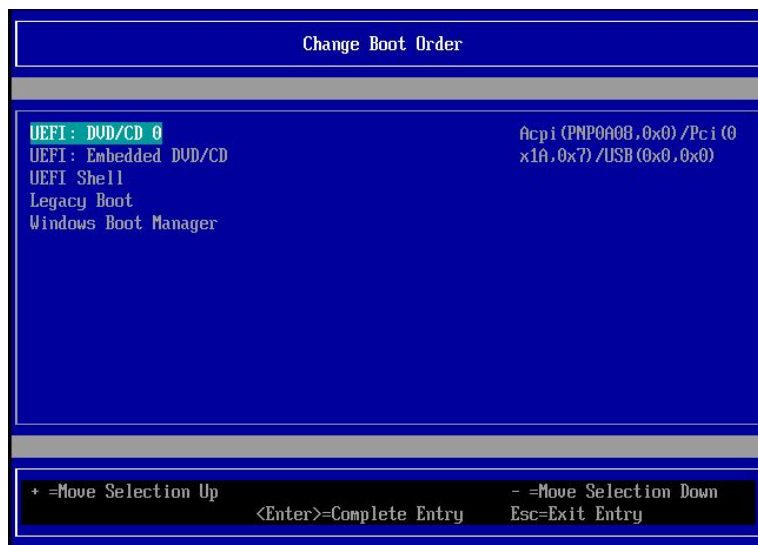


FIGURE 4.11 Example of display of the [Change Boot Order] menu

The following describes the meaning of the menu:

- UEFI: DVD/CD n (n=0, 1, 2...)
Specify this when starting the UEFI-aware OS from the external DVD/CD drive media.
The n in "UEFI: DVD/CD n" is a sequential number (starting from 0) assigned in the order that DVD/CD devices are recognized. The assigned number remains stored based on the connection location information as long as the device is not disconnected from the system.
 - UEFI: Embedded DVD/CD:
Specify this item when using the built-in DVD drive for installation in UEFI mode.
 - UEFI Shell:
Specify this menu when starting UEFI Shell. The PRIMEQUEST 1000 series does not use UEFI Shell.
 - Legacy Boot:
Specify this item for BIOS mode. Also specify [Legacy Boot] when using the built-in DVD drive for installation in BIOS mode.
4. Specify [Commit Changes and Exit].
 5. Press the [ESC] key to return to the Front Page.
 6. Specify [Boot Manager].
 7. Specify [UEFI:DVD/CD 0] to use the remote storage DVD. Specify [UEFI: Embedded DVD/CD] to use the built-in DVD.

3. After a moment, the language selection window appears. Select [English] for installation in English.
4. Click the [Next] button on the initially displayed window without setting anything.
5. Select [Deployment] in the [Welcome to ServerView Installation Manager] window.
6. Select an installation mode and the operating system to be installed. Then, set up the operating system.

Remark

The IP address of the LAN cannot be set through the operating system setup. Set the IP address after the installation of the operating system.

7. Click [Install].
Installation begins.
8. Replace the media with the operating system installation media according to the SVIM instructions.

4.8.4 Configuring a software watchdog

1. Start ServerView Operations Manager.
2. Select [ServerList].
3. Right-click the target partition in the server list on the left side. Select [Maintenance] - [ASR Properties] from the displayed menu.
4. Select [Watchdog] in the displayed window.
5. Specify the following for [Software], and click [Apply].
 - Check the [Active] check box.
 - Select [Continue] for [Action] for cases of abnormal operation.
 - Enter a value between 1 and 100 minutes for [Timeout].
6. Enter your user name and password, and press the [Enter] key.

4.8.5 Completing VMware 5.x installation

After completing the settings, reboot the partition of the PRIMEQUEST 1000 series server.

4.8.6 Installing bundled software

For bundled software installation, see [E.7 Installing VMware 5.x Bundled Software](#).

4.9 VMware 5.x Installation Procedures on the Built-in HDD

This section concisely describes the procedures for installing VMware 5.x on the built-in HDD.

Start this work only after confirming the completion of the connection and configuration of the MMB.

4.9.1 Advance setup

Set up the following as needed.

1. Prepare a server running ServerView Operations Manager.
2. After removing the built-in HDD of the PRIMEQUEST server, confirm the partition settings with the MMB.
 - Setting the SB/IOB/GSPB configuration
(See [3.4.1 Setting a partition configuration](#).)
 - Configuring Console Redirection
(See [3.4.6 Configuring Console Redirection](#).)
 - Video redirection: Enable
 - Remote storage: Enable
 - Console redirection: Enable
 - Setting various modes
(See [3.4.5 Setting various modes](#).)
3. Assign I/O spaces to the SAS card, SAS array controller card, Onboard SAS controller (GSPB), SAS disk unit controller and SAS array disk unit controller.
For details on I/O space assignment, see 3.4.5 Setting various modes in this manual and 5.5.1 [Configure I/O Space Assignment] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

4.9.2 Preparing for Installation

To prepare for installation, also see the VMware information.

For the VMware information, contact the distributor where you purchased your product, or your sales representative.

Prepare the following.

1. Prepare the following disk image:
VMware 5.x media
2. Disconnect all the FC cables.
3. Mount the disk image through a video redirection connection.
4. Configure the RAID environment.
For details, see the MegaRAID SAS Software, the MegaRAID SAS Device Driver Installation, or the LSI MegaRAID (R) SAS Software contained on the SVS DVD.
5. Change the boot order to give the highest priority in startup to DVD boot.
For details, see 1.3.1 [Power Control] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

4.9.3 Installing VMware 5.x

This section describes the operating system installation with SVIM.

SVIM can perform the following types of operating system installation. For the procedure for each mode, see the *ServerView Suite ServerView Installation Manager*.

TABLE 4.10 Operating system installation by SVIM

Mode	Functional outline	Remarks
Quick mode	You can simply use the minimum settings necessary for operating system installation. This mode uses Fujitsu's recommended settings.	Use this mode to readily install the OS.
Guide mode	You can specify setup information by following the instructions of the wizard. You can save the specified information in a configuration file for use during reinstallation.	This mode enables detailed settings. Use the mode if you want to configure installation with detailed RAID and OS settings.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

Operations

1. Make the setting for booting the partition from remote storage.
For details on the setting, see 1.6.3 Remote operation (BMC) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).
2. Insert ServerView Suite DVD1 into the DVD drive. Then, power on the partition.

Remarks

You can boot from the DVD drive either by selecting [Force boot from DVD] from [Boot Selector], or by specifying the DVD drive as the highest-priority device to boot from, in UEFI mode.

If the operating system supports UEFI mode, you can install it in UEFI mode by using the following procedure to change the boot order.

1. After powering on the partition, press and hold down any key ([Space] key, for example) other than the [Enter] key while the FUJITSU logo is displayed, to display the Boot Manager Front Page.
2. Select the following items from the menu in the order given in the Boot Manager Front Page:
[Boot Maintenance Manager] - [Boot Options] - [Change Boot Order] - [Change the order]
 - Specify [UEFI: DVD/CD 0] as the highest priority device to boot from the remote storage DVD.
 - Specify [UEFI: Embedded DVD/CD] as the highest priority device to boot from the built-in DVD.

For details on how to set the boot order, see Changing the order of priority (Change Boot Order) in 5.6.1 [Boot Options] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

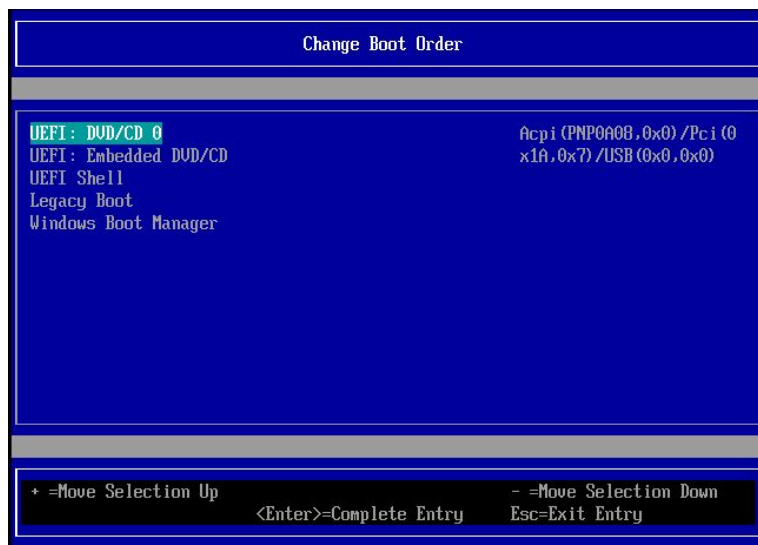


FIGURE 4.12 Example of display of the [Change Boot Order] menu

The following describes the meaning of the menu:

- UEFI: DVD/CD n (n=0, 1, 2...)
Specify this when starting the UEFI-aware OS from the external DVD/CD drive media.
The n in "UEFI: DVD/CD n" is a sequential number (starting from 0) assigned in the order that DVD/CD devices are recognized. The assigned number remains stored based on the connection location information as long as the device is not disconnected from the system.
- UEFI: Embedded DVD/CD:
Specify this item when using the built-in DVD drive for installation in UEFI mode.
- UEFI Shell:
Specify this menu when starting UEFI Shell. The PRIMEQUEST 1000 series does not use UEFI Shell.
- Legacy Boot:
Specify this item for BIOS mode. Also specify [Legacy Boot] when using the built-in DVD drive for installation in BIOS mode.

3. Specify [Commit Changes and Exit] - [Reset System] to reboot the partition.

3. After a moment, the language selection window appears. Select [English] for installation in English.

4. Click the [Next] button on the initially displayed window without setting anything.

5. Select [Deployment] in the [Welcome to ServerView Installation Manager] window.

6. Select an installation mode and the operating system to be installed. Then, set up the operating system.

Remark

The IP address of the LAN cannot be set through the operating system setup. Set the IP address after the installation of the operating system.

7. Click [Install].

Installation begins.

8. Replace the media with the operating system installation media according to the SVIM instructions.

4.9.4 Configuring a software watchdog

1. Start ServerView Operations Manager.
2. Select [ServerList].
3. Right-click the target partition in the server list on the left side. Select [Maintenance] - [ASR Properties] from the displayed menu.
4. Select [Watchdog] in the displayed window.
5. Specify the following for [Software], and click [Apply].
 - Check the [Active] check box.
 - Select [Continue] for [Action] for cases of abnormal operation.
 - Enter a value between 1 and 100 minutes for [Timeout].
6. Enter your user name and password, and press the [Enter] key.

4.9.5 Completing VMware 5.x installation

After completing the settings, reboot the partition of the PRIMEQUEST 1000 series server.

4.9.6 Installing bundled software

For bundled software installation, see [E.7 Installing VMware 5.x Bundled Software](#).

4.10 SUSE Linux Enterprise Server 11 Service Pack 2 Installation Procedures on the SAN Storage Unit

This section describes the procedures for installing SUSE Linux Enterprise Server 11 Service Pack 2 (referred to below as SLES11 SP2) on the SAN storage unit. Confirm the MMB configuration and successful login to the MMB before starting the installation.

For details on configuring the SAN storage unit and FC card (Fibre Channel card), see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).

4.10.1 Advance setup and preparation

Set up the following as needed.

1. Set the LUN of the SAN storage unit.
2. Configure the BIOS so that the LUN of the FC card is recognized.
For details on configuring the FC card, see Chapter 2 Settings on the Fiber Channel Card (FC Card) in the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).
3. After removing the built-in HDD of the PRIMEQUEST server, confirm the partition settings with the MMB.
 - Setting the SB/IOB/G
 - SPB configuration
(See [3.4.1 Setting a partition configuration.](#))
 - Configuring Console Redirection
(See [3.4.6 Configuring Console Redirection.](#))
 - Video redirection: Enable
 - Remote storage: Enable
 - Console redirection: Enable
 - Setting various modes
(See [3.4.5 Setting various modes.](#))
4. Connect only the LUN of the SAN storage unit, to which the OS is to be installed, to the partition of the PRIMEQUEST server.
For details on the settings for the SAN storage unit, see the manual supplied with the SAN storage unit.
5. Assign I/O spaces to the FC card (card for boot path only), SAS card, SAS array controller card, Onboard SAS controller (GSPB), SAS disk unit controller and SAS array disk unit controller.
For details on I/O space assignment, see 3.4.5 Setting various modes in this manual and 5.5.1 [Configure I/O Space Assignment] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

4.10.2 Preparing for Installation

Prepare a SLES11 SP2 installation DVD.

Preparing for boot

Change FC cabling to single path (connecting only one FC cable).

4.10.3 Installing the operating system

This section describes the operating system installation with SVIM.

SVIM can perform the following types of operating system installation. For the procedure for each mode, see the *ServerView Suite ServerView Installation Manager*.

TABLE 4.11 Operating system installation by SVIM

Mode	Functional outline	Remarks
Quick mode	You can simply use the minimum settings necessary for operating system installation. This mode uses Fujitsu's recommended settings.	Use this mode to readily install the OS.
Guide mode	You can specify setup information by following the instructions of the wizard. You can save the specified information in a configuration file for use during reinstallation.	This mode enables detailed settings. Use the mode if you want to configure installation with detailed RAID and OS settings.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

Operations

1. Make the setting for booting the partition from remote storage.
For details on the setting, see 1.6.3 Remote operation (BMC) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).
2. Insert ServerView Suite DVD1 into the DVD drive. Then, power on the partition.
When using the remote storage DVD, insert ServerView Suite DVD1 into the remote storage. Then, power on the partition.

Remarks

If the operating system supports UEFI mode, you can install it in UEFI mode by using the following procedure to change the boot order.

1. Select [Force boot from DVD] from [Boot Selector] in the [Power Control] window of the MMB Web-UI. Then, power on the partition.
2. After powering on the partition, press and hold down any key ([Space] key, for example) other than the [Enter] key while the FUJITSU logo is displayed, to display the Boot Manager Front Page.
3. Select the following items from the menu in the order given in the Boot Manager Front Page:
[Boot Maintenance Manager] - [Boot Options] - [Change Boot Order] - [Change the order]
 - Specify [UEFI: DVD/CD 0] as the highest priority device to boot from the remote storage DVD.
 - Specify [UEFI: Embedded DVD/CD] as the highest priority device to boot from the built-in DVD.

For details on how to set the boot order, see Changing the order of priority (Change Boot Order) in 5.6.1 [Boot Options] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

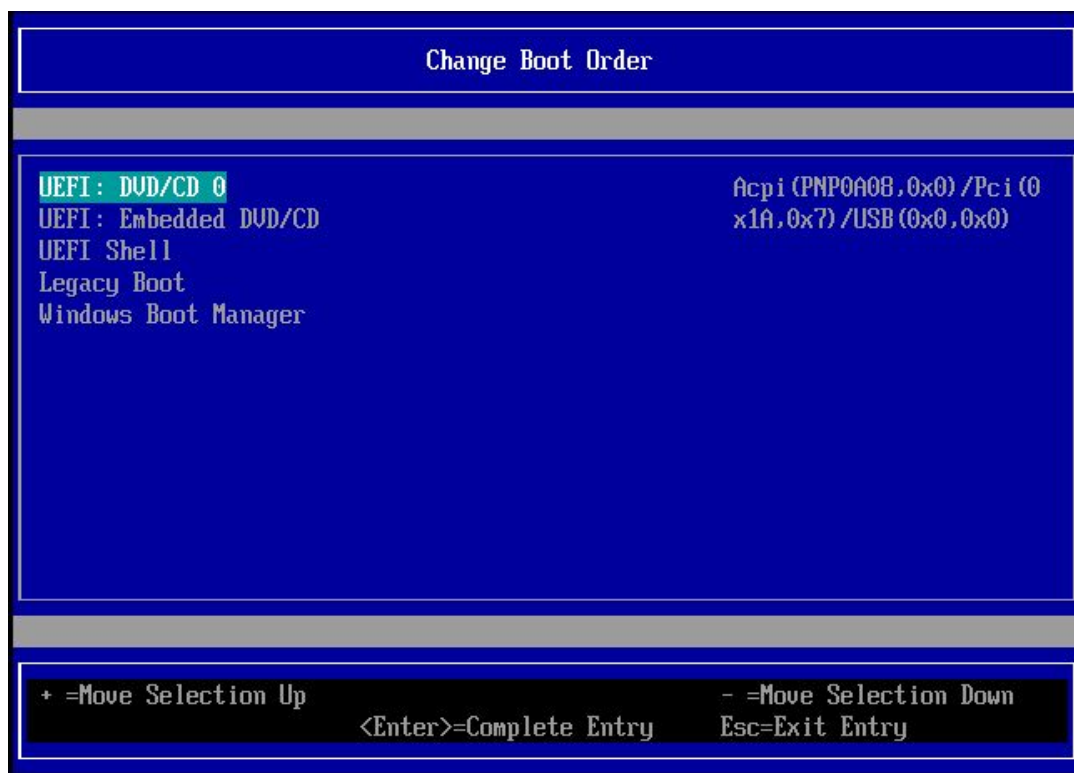


FIGURE 4.13 Example of display of the [Change Boot Order] menu

The following describes the meaning of the menu:

- UEFI: DVD/CD n (n=0, 1, 2...)
Specify this when starting the UEFI-aware OS from the external DVD/CD drive media.
The n in "UEFI: DVD/CD n" is a sequential number (starting from 0) assigned in the order that DVD/CD devices are recognized. The assigned number remains stored based on the connection location information as long as the device is not disconnected from the system.
- UEFI: Embedded DVD/CD:
Specify this item when using the built-in DVD drive for installation in UEFI mode.
- UEFI Shell:
Specify this menu when starting UEFI Shell. The PRIMEQUEST 1000 series does not use UEFI Shell.
- Legacy Boot:
Specify this item for BIOS mode. Also specify [Legacy Boot] when using the built-in DVD drive for installation in BIOS mode.

4. Specify [Commit Changes and Exit].
5. Press the [ESC] key to return to the Front Page.
6. Specify [Boot Manager].
7. Specify [UEFI:DVD/CD 0] to use the remote storage DVD. Specify [UEFI: Embedded DVD/CD] to use the built-in DVD.

3. After a moment, the language selection window appears. Select [English] for installation in English.

4. Click the [Next] button on the initially displayed window without setting anything.

5. Select [Deployment] in the [Welcome to ServerView Installation Manager] window.
6. Select an installation mode and the operating system to be installed. Then, set up the operating system.

Remark

The IP address of the LAN cannot be set through the operating system setup. Set the IP address after the installation of the operating system.

7. Click [Install].
Installation begins.
8. Replace the media with the operating system installation media according to the SVIM instructions.

4.10.4 Configuring bundled software after the completion of installation

After completing OS installation, configure the bundled software.

For details about the following settings, see the *ServerView Mission Critical Option User Manual*.

1. Configure the PSA-to-MMB communication LAN network.
For details, see the items in "Configuring the PSA-to-MMB communication LAN."
2. Configure the management LAN network.
For details, see the items in "Confirming management LAN settings."
3. Install the SVMco package.
For details, see the items in "Installing SVMco."
4. Make manual settings in the SVMco configuration file.
For details, see "Configuring SVMco."
5. Check the firewall function.
For details, see the items in "Checking the firewall function (opening ports)."
Open the following ports for use with the PSA-to-MMB communication LAN interface.

TABLE 4.12 Ports to open for the PSA-to-MMB communication LAN interface

Port	Port number	Sending / Receiving
snmp port	udp/snmp or 161	For sending and receiving
psa-mmb communication port	tcp/5000	For sending and receiving
	icmp/icmp-type0, icmp-type8	

6. Restart the partition.
For details, see the items in "Restarting the partition."
7. After installing SVMco, make the required settings.

Set the management LAN parameters.

For details, see the items in "Settings after SVMco installation."

4.10.5 Connecting the SAN and built-in HDD after the installation

For details on connecting the SAN and built-in HDD after the installation, see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN). Also, for details on driver parameters, see the readme file that comes with the driver.

4.11 SUSE Linux Enterprise Server 11 Service Pack 2 Installation Procedures on the Built-in HDD

This section concisely describes the procedures for installing SUSE Linux Enterprise Server 11 Service Pack 2 (referred to below as SLES11 SP2) on the built-in HDD. Confirm the MMB configuration and successful login to the MMB before starting the installation.

4.11.1 Advance setup

Set up the following as needed.

1. Remove each built-in HDD that is not the installation destination.
2. Confirm the partition settings of the PRIMEQUEST server with the MMB. For details, see [3.4 Configuring a Partition](#).
 - Setting the SB/IOB/G
 - Setting the SB/IOB/GSPB configuration
(See [3.4.1 Setting a partition configuration](#).)
 - Configuring Console Redirection
(See [3.4.6 Configuring Console Redirection](#).)
 - Video redirection: Enable
 - Remote storage: Enable
 - Console redirection: Enable
 - Setting various modes
(See [3.4.5 Setting various modes](#).)
3. Assign I/O spaces to the SAS card, SASarray controller card, Onboard SAS controller (GSPB), SAS disk unit controller and SAS array disk unit controller.
For details on I/O space assignment, see [3.4.5 Setting various modes](#) in this manual and 5.5.1 [Configure I/O Space Assignment] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

4.11.2 Preparing for Installation

Prepare the SLES11 SP2 installation DVD.

4.11.3 Installing the operating system

This section describes the operating system installation with SVIM.

SVIM can perform the following types of operating system installation. For the procedure for each mode, see the *ServerView Suite ServerView Installation Manager*.

TABLE 4.13 Operating system installation by SVIM

Mode	Functional outline	Remarks
Quick mode	You can simply use the minimum settings necessary for operating	Use this mode to readily install the OS.

Mode	Functional outline	Remarks
	system installation. This mode uses Fujitsu's recommended settings.	
Guide mode	You can specify setup information by following the instructions of the wizard. You can save the specified information in a configuration file for use during reinstallation.	This mode enables detailed settings. Use the mode if you want to configure installation with detailed RAID and OS settings.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

Operations

1. Make the setting for booting the partition from remote storage.
For details on the setting, see 1.6.3 Remote operation (BMC) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).
2. Insert ServerView Suite DVD1 into the DVD drive. Then, power on the partition.

Remarks

You can boot from the DVD drive either by selecting [Force boot from DVD] from [Boot Selector], or by specifying the DVD drive as the highest-priority device to boot from, in UEFI mode.

If the operating system supports UEFI mode, you can install it in UEFI mode by using the following procedure to change the boot order.

1. After powering on the partition, press and hold down any key ([Space] key, for example) other than the [Enter] key while the FUJITSU logo is displayed, to display the Boot Manager Front Page.
2. Select the following items from the menu in the order given in the Boot Manager Front Page:
[Boot Maintenance Manager] - [Boot Options] - [Change Boot Order] - [Change the order]
 - Specify [UEFI: DVD/CD 0] as the highest priority device to boot from the remote storage DVD.
 - Specify [UEFI: Embedded DVD/CD] as the highest priority device to boot from the built-in DVD.

For details on how to set the boot order, see Changing the order of priority (Change Boot Order) in 5.6.1 [Boot Options] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

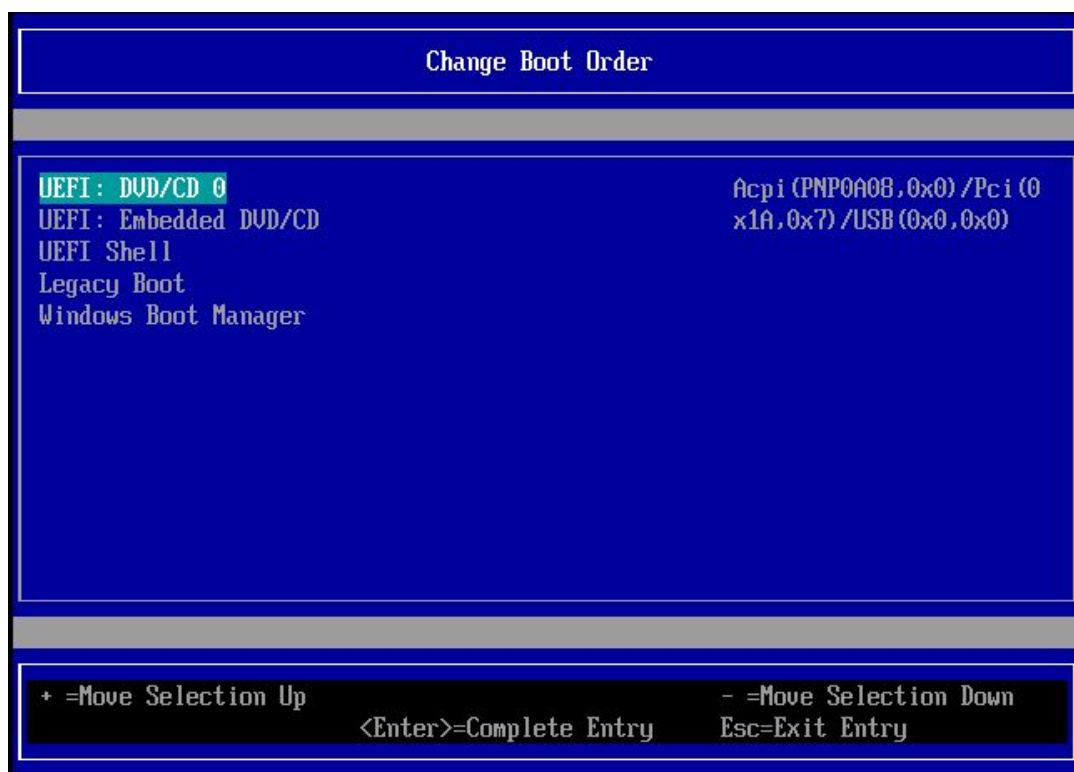


FIGURE 4.14 Example of display of the [Change Boot Order] menu

The following describes the meaning of the menu:

- UEFI: DVD/CD n (n=0, 1, 2...)
Specify this when starting the UEFI-awareOS from the external DVD/CD drive media.
The n in "UEFI: DVD/CD n" is a sequential number (starting from 0) assigned in the order that DVD/CD devices are recognized. The assigned number remains stored based on the connection location information as long as the device is not disconnected from the system.
- UEFI: Embedded DVD/CD:
Specify this item when using the built-in DVD drive for installation in UEFI mode.
- UEFI Shell:
Specify this menu when starting UEFI Shell. The PRIMEQUEST 1000 series does not use UEFI Shell.
- Legacy Boot:
Specify this item for BIOS mode. Also specify [Legacy Boot] when using the built-in DVD drive for installation in BIOS mode.

3. Specify [Commit Changes and Exit] - [Reset System] to reboot the partition.

3. After a moment, the language selection window appears. Select [English] for installation in English.

4. Click the [Next] button on the initially displayed window without setting anything.

5. Select [Deployment] in the [Welcome to ServerView Installation Manager] window.

6. Select an installation mode and the operating system to be installed. Then, set up the operating system.

Remark

The IP address of the LAN cannot be set through the operating system setup. Set the IP address after the installation of the operating system.

7. Click [Install].
Installation begins.
8. Replace the media with the operating system installation media according to the SVIM instructions.

4.11.4 Configuring bundled software after the completion of installation

After completing OS installation, configure the bundled software.

For details about the following settings, see the *ServerView Mission Critical Option User Manual*.

1. Configure the PSA-to-MMB communication LAN network.
For details, see the items in "Configuring the PSA-to-MMB communication LAN."
2. Configure the management LAN network.
For details, see the items in "Confirming management LAN settings."
3. Install the SVMco package.
For details, see the items in "Installing SVMco."
4. Make manual settings in the SVMco configuration file.
For details, see "Configuring SVMco."
5. Check the firewall function.
For details, see the items in "Checking the firewall function (opening ports)."
Open the following ports for use with the PSA-to-MMB communication LAN interface.

TABLE 4.14 Ports to open for the PSA-to-MMB communication LAN interface

Port	Port number	Sending / Receiving
snmp port	udp/snmp or 161	For sending and receiving
psa-mmb communication port	tcp/5000	For sending and receiving
	icmp/icmp-type0, icmp-type8	

6. Restart the partition.
For details, see the items in "Restarting the partition."
7. After installing SVMco, make the required settings.
Set the management LAN parameters.
For details, see the items in "Settings after SVMco installation."

4.11.5 Connecting the SAN and built-in HDD after the installation

For connecting the SAN and built-in HDD after the installation, see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN). Also, for details on driver parameters, see the readme file that comes with the driver.

CHAPTER 5 Work after Operating System Installation (PRIMEQUEST 1800E2)

This chapter describes how to make settings after operating system installation on the PRIMEQUEST 1800E2.

5.1 Types of Work	116
5.2 Configuring SVS (SVagent/SVmco)	117
5.3 Setting of sadump	118
5.4 Setting Up the Dump Environment (Windows)	128
5.5 Setting Up the Dump Environment (Linux)	129
5.6 Configuring the NTP Client	132
5.7 Saving Management and Configuration Information	
133	
5.8 Configuring Service Life Monitoring by RAS Support Service	135

5.1 Types of Work

TABLE 5.1 Types of work lists the types and details of the work performed after operating system installation.

TABLE 5.1 Types of work

Task	Description	Installed operating system	See
Configuring SVS (SVagent/SVmco)	Configuring (SVagent/SVmco)	Linux or Windows	5.2 Configuring SVS (SVagent/SVmco)
Configuring PSA-to-MMB LAN (Linux)	Configuring PSA-to-MMB LAN	Linux	<i>ServerView Mission Critical Option User Manual</i>
Configuring PSA-to-MMB LAN (Windows)	Configuring PSA-to-MMB LAN	Windows	<i>ServerView Mission Critical Option User Manual</i>
Setting up the dump environment	Setting up the dump environment	Windows	5.3 Setting of sadump
Setting up the dump environment	Setting up the dump environment	Linux	5.5 Setting Up the Dump Environment (Linux)
Configuring an NTP client	Configuring an NTP client	Linux or Windows	5.6 Configuring the NTP Client
Saving management and configuration information	Saving PSA management information and UEFI configuration information	Linux or Windows	5.7 Saving Management and Configuration Information
Setting service life monitoring by RAS Support Service	Setting service life monitoring of battery units on RAID cards and UPSs	Linux or Windows	5.8 Configuring Service Life Monitoring by RAS Support Service

5.2 Configuring SVS (SVagent/SVmco)

After installing the operating system, you need to configure SVS (SVagent/SVmco) for operation.

For details on SVagent/SVmco settings, see the SVmco manual.

- SVagent:
 - ServerView Operations Manager Installation ServerView Agents for Linux
 - ServerView Operations Manager Installation ServerView Agents for Windows
- SVmco:
 - ServerView Mission Critical Option user manual

5.3 Setting of sadump

The following items in sadump are set for each partition:

- Validation of sadump
- Dump collection address
- Compression at the time of dump collection
- Transition after dump collection
- Re-use of the dump collection address

Make the sadump settings from the BIOS setup menu.

Before making the settings, you need to reserve an area for the dump device at the dump collection address. Register information and memory contents are output to the dump device when there is a system fault. For this reason, the capacity of the device that outputs the dump is determined by matching the memory size. Obtain an estimate of the required area from the formula given below, and reserve the area.

Amount of memory installed + 512 MB

The dump device can use disks and disk partitions. To create a dump device on a disk partition, create the disk partition when installing the operating system.

To set a device on the ETERNUS as the dump device, you need to configure the UEFI driver in advance.

For details on the setting procedure, see the *PRIMEQUEST 1000 Series SAN Boot Environment Configuration Manual* (C122-E155EN).

All the screenshots are examples of what is displayed. The displayed contents differ according to the system configuration.

All the windows shown here are examples of what is displayed. The displayed contents differ according to the system configuration.

Operations

1. Display the Device Manager menu of the UEFI.

For details on displaying the Device Manager menu, see Chapter 5 UEFI Menu Operations in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

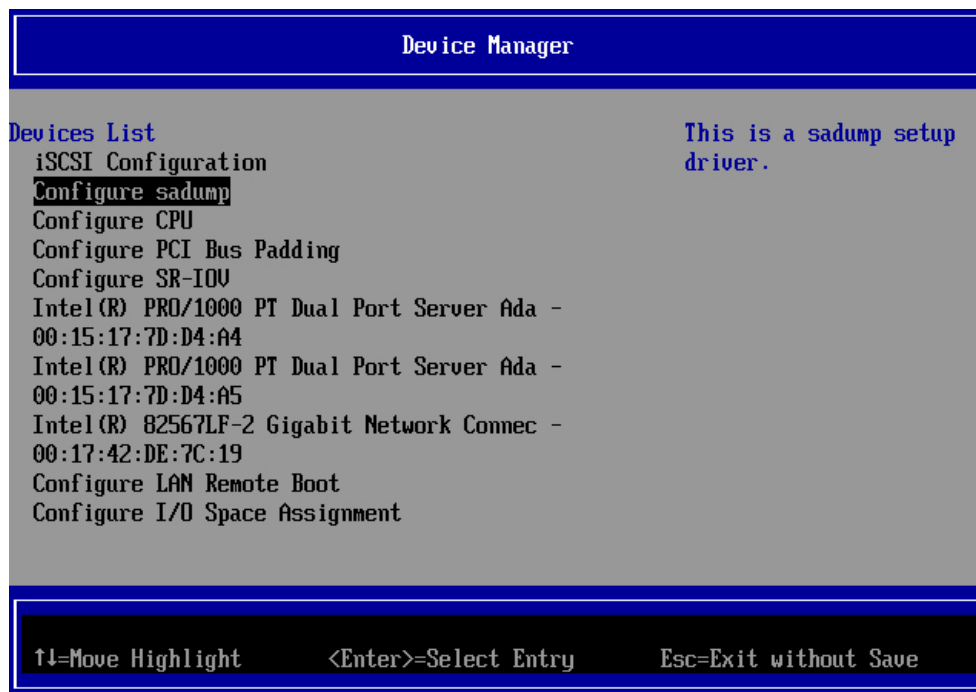


FIGURE 5.1 Example of the Device Manager menu

2. Select [Configure sadump], and press the [Enter] key.

>> The main menu (sadump) appears.

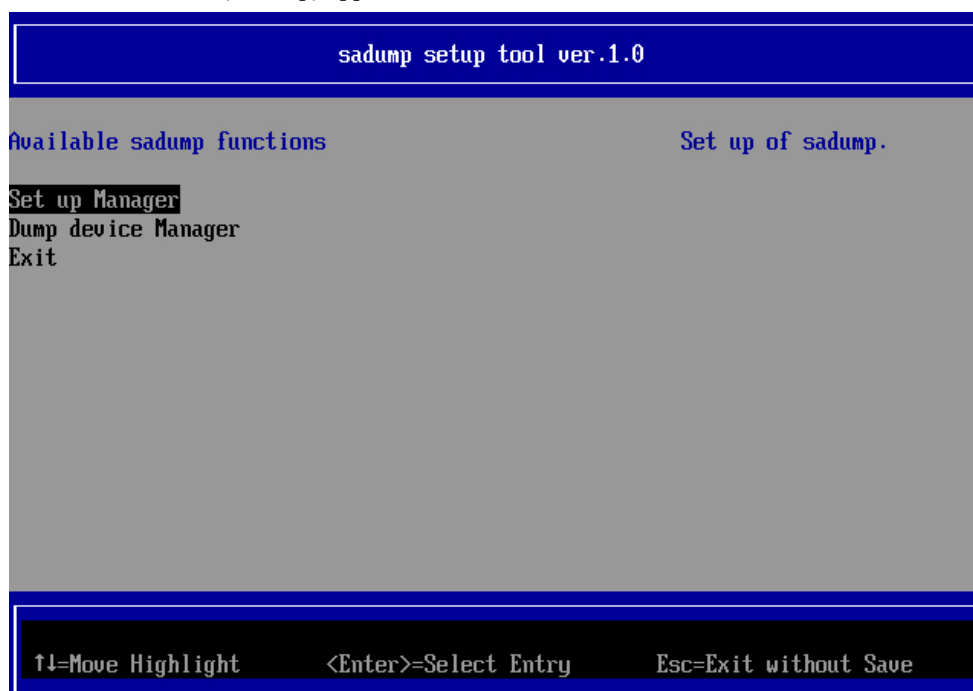


FIGURE 5.2 Main menu (sadump)

3. Select [Set up Manager], and press the [Enter] key

>> The sadump setup menu appears.

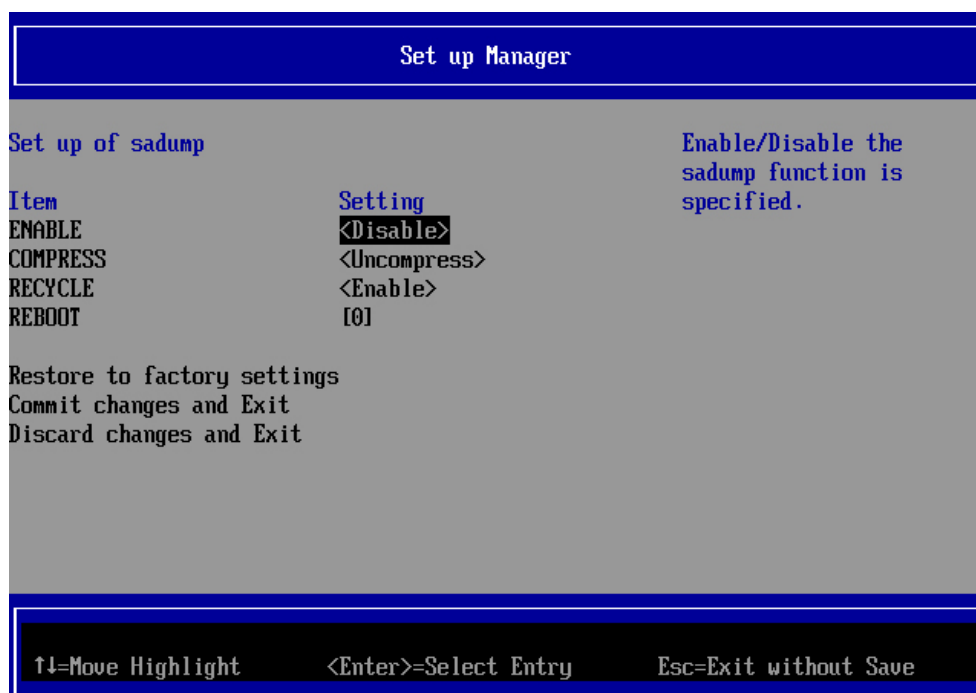


FIGURE 5.3 sadump setup menu

4. Select <Enable> for [ENABLE].

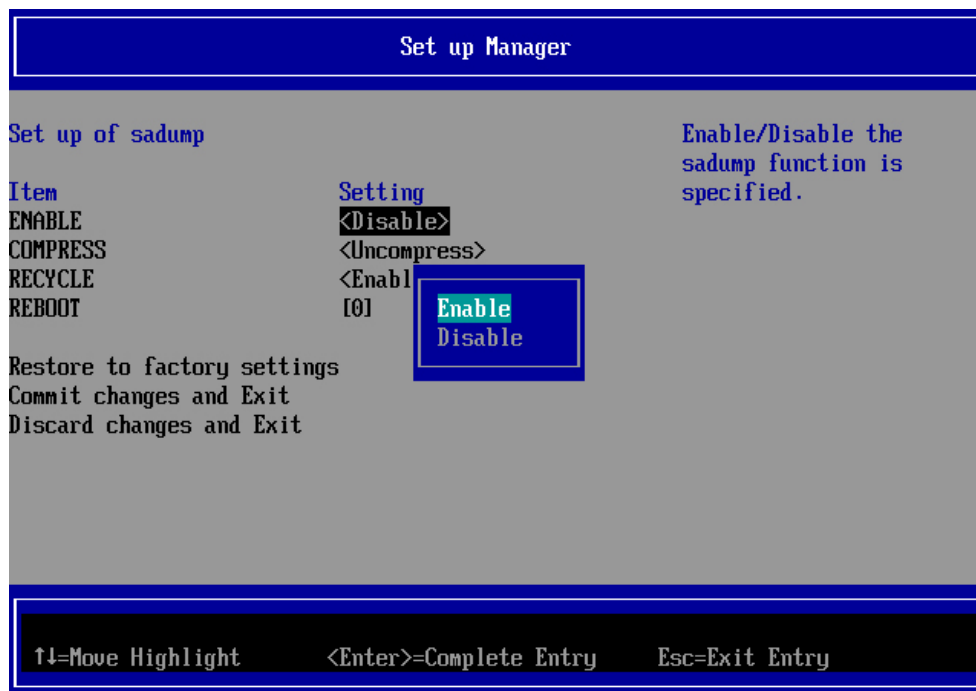


FIGURE 5.4 sadump setup menu

5. Select [Commit changes and Exit], and press the [Enter] key.
>> After the settings are reflected, the screen returns to the main menu (sadump).

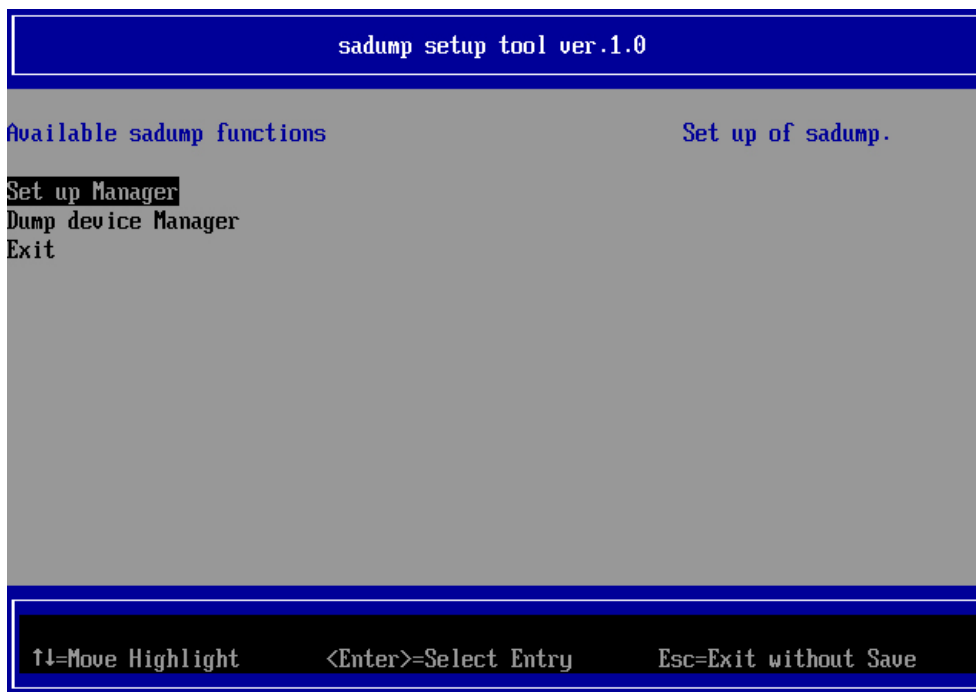


FIGURE 5.5 Main menu (sadump)

6. Select [Dump device Manager] on the main menu (sadump), and press the [Enter] key.
>> The dump device maintenance menu appears.

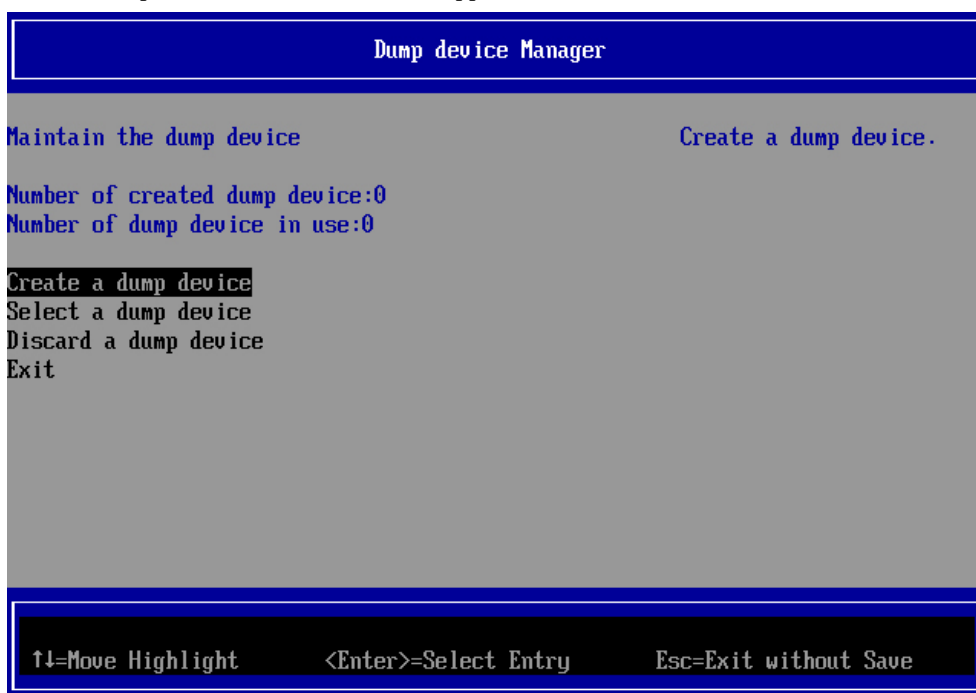


FIGURE 5.6 Dump device maintenance menu

7. Select [Create a dump device], and press the [Enter] key.
>> The dump device configuration menu appears.

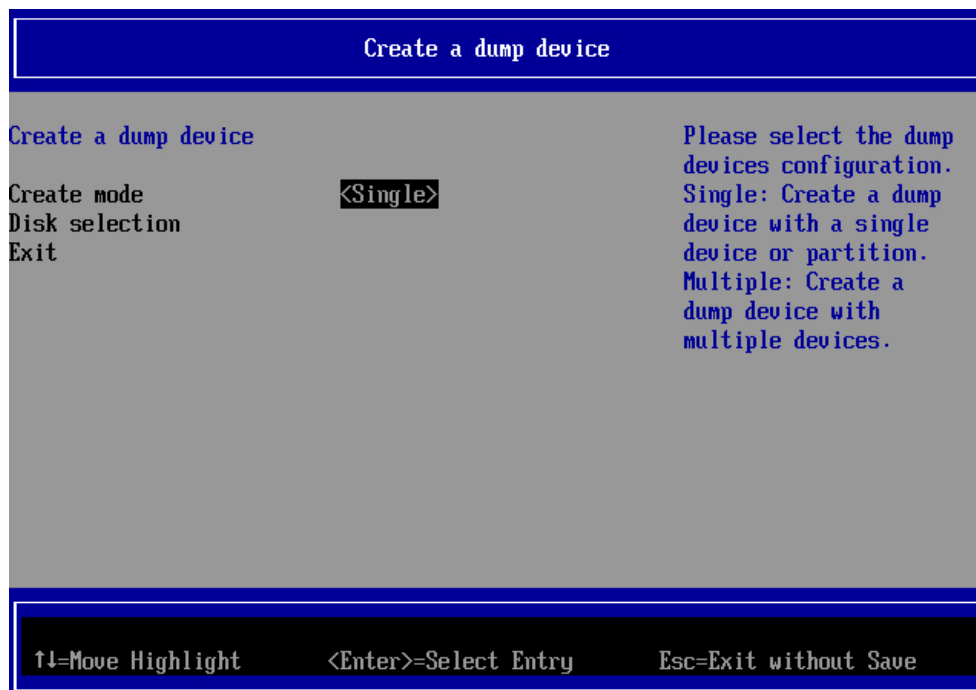


FIGURE 5.7 Dump device configuration menu

8. Select [Disk selection], and press the [Enter] key.

>> The dump device selection menu appears.

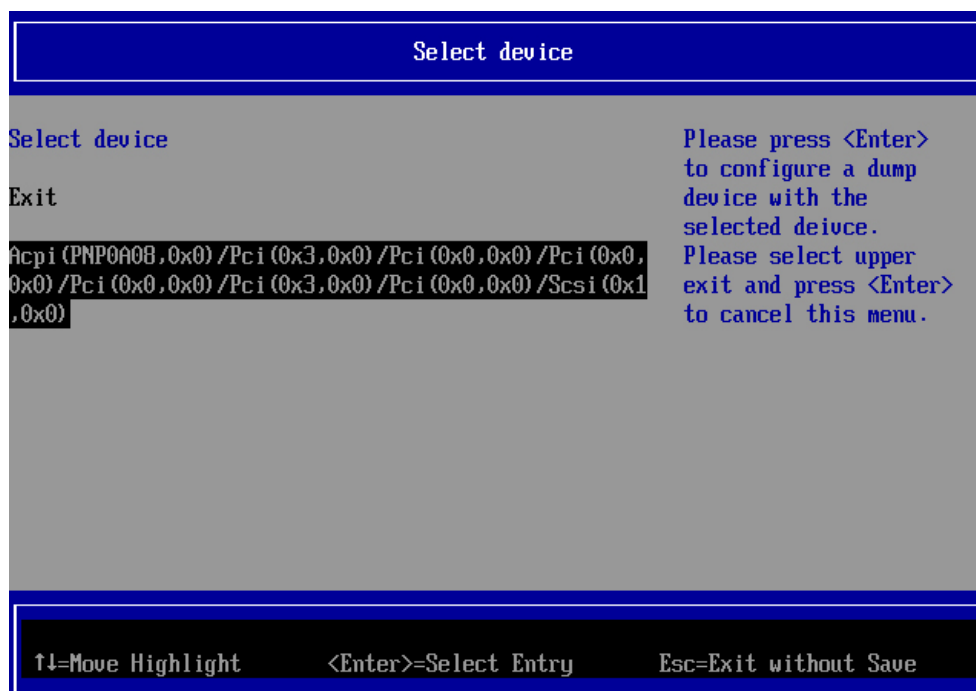


FIGURE 5.8 Dump device selection menu

9. Select a disk or disk partition to set it in the dump device configuration.

>> The dump device selection menu appears.



(Data corruption)

When selecting the dump device, reconfirm that the selected disk is correct. If the selected disk is incorrect during the dump operation, data will be corrupted.

Remarks

For details on the ACPI name indicating the disk or disk partition, see 5.7 Device Path in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

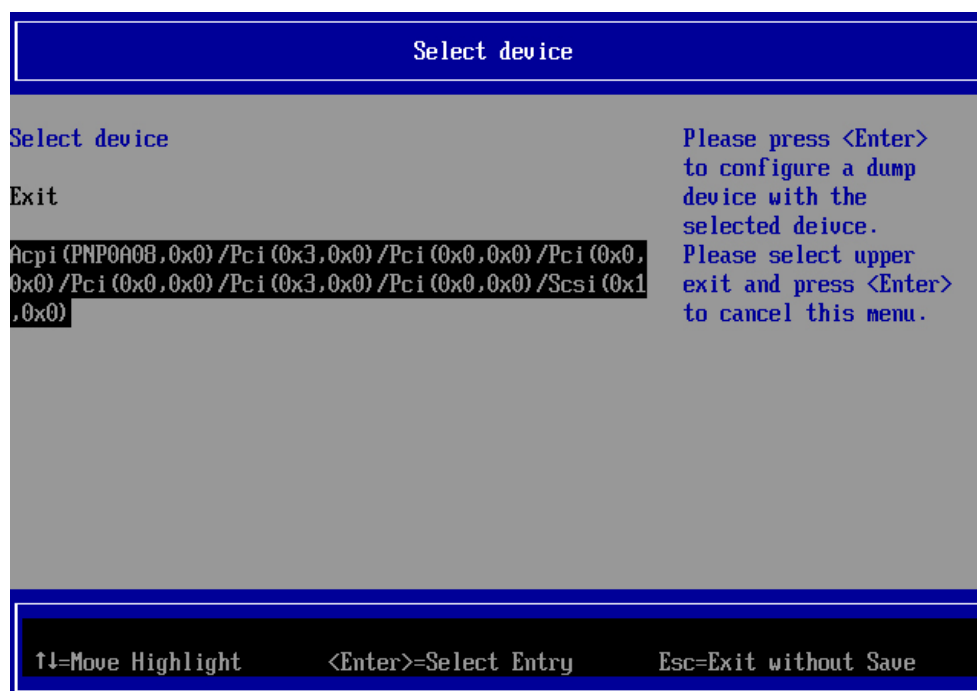


FIGURE 5.9 Dump device selection menu

10. Press the [Enter] key.

>> The dump device is created. The screen returns to the dump device configuration menu.

Warning

When created, the dump device is initialized. The time required for the initialization varies depending on the size of the selected disk or disk partition. In some cases, the initialization takes time, so the transition to the next screen takes a few minutes or more.

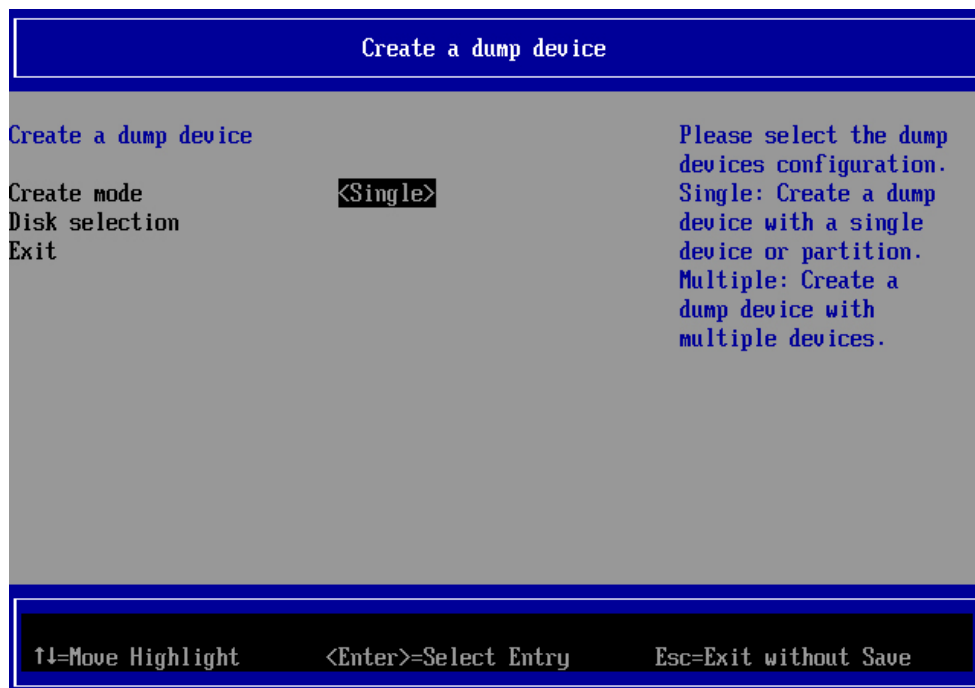


FIGURE 5.10 Dump device configuration menu

11. Select [Exit], and press the [Enter] key.
>> The screen returns to the dump device maintenance menu.

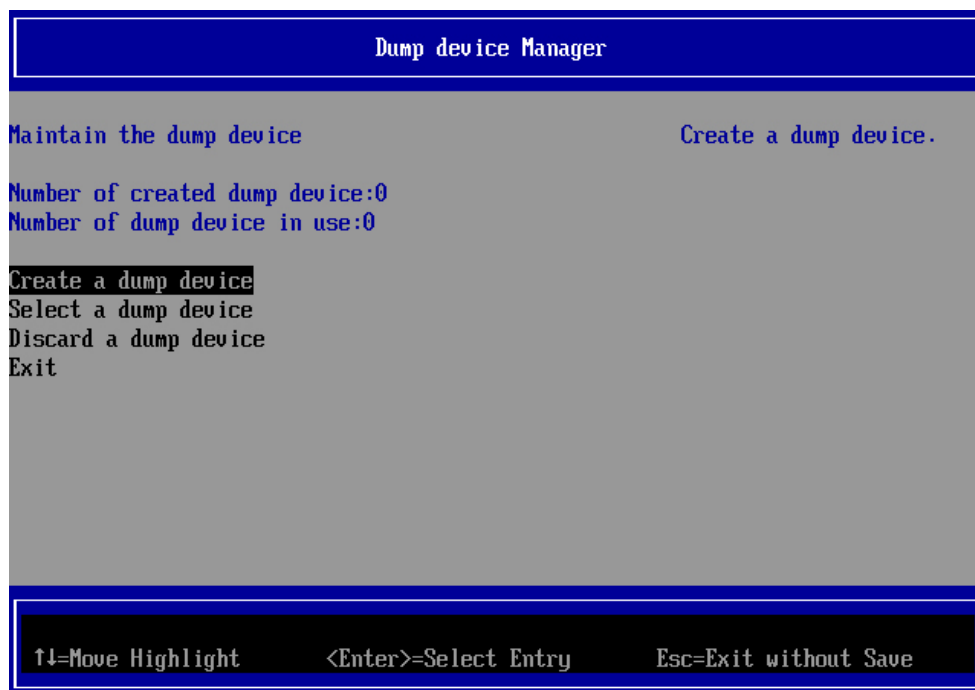


FIGURE 5.11 Dump device maintenance menu

12. Select [Select a dump device] on the dump device maintenance menu, and press the [Enter] key.
>> The dump device setting menu appears.



FIGURE 5.12 Dump device setting menu

13. Select the first dump device, which is where [1] is specified, and press the [Enter] key.
>> The dump device list menu appears.

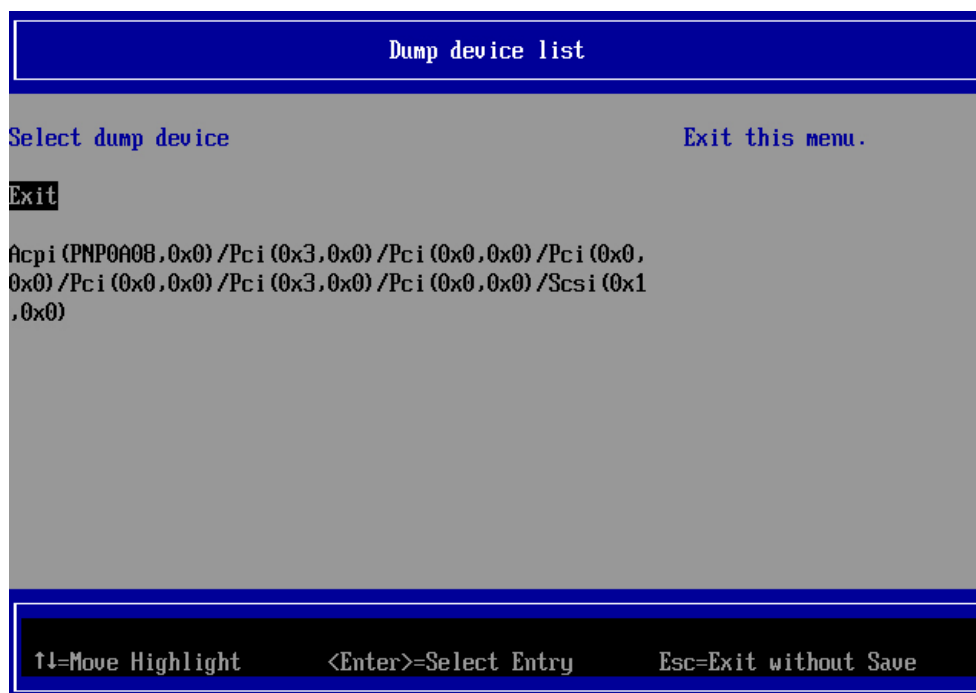


FIGURE 5.13 Dump device list menu

14. Select the disk or disk partition used for the dump device, and press the [Enter] key.
>> The dump device is set, and the screen returns to the dump device setting menu.



FIGURE 5.14 Dump Device Setting Menu

15. Select [Commit changes and Exit], and press the [Enter] key.
 >> The dump device is set, and the screen returns to the dump device maintenance menu.

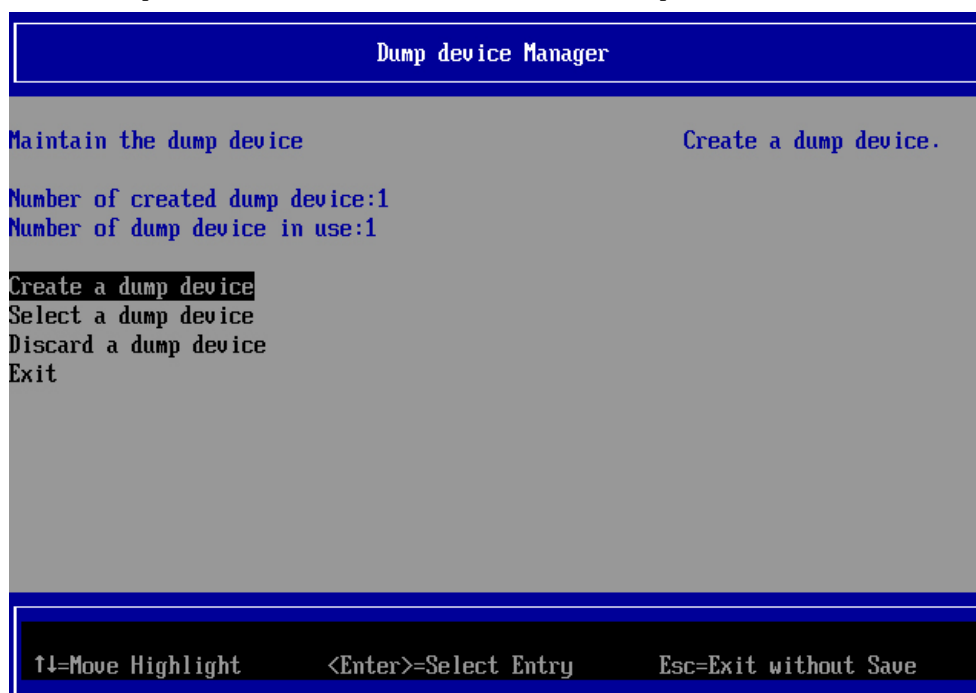


FIGURE 5.15 Dump device maintenance menu

16. Select [Exit], and press the [Enter] key.
 >> The screen returns to the main menu (sadump).

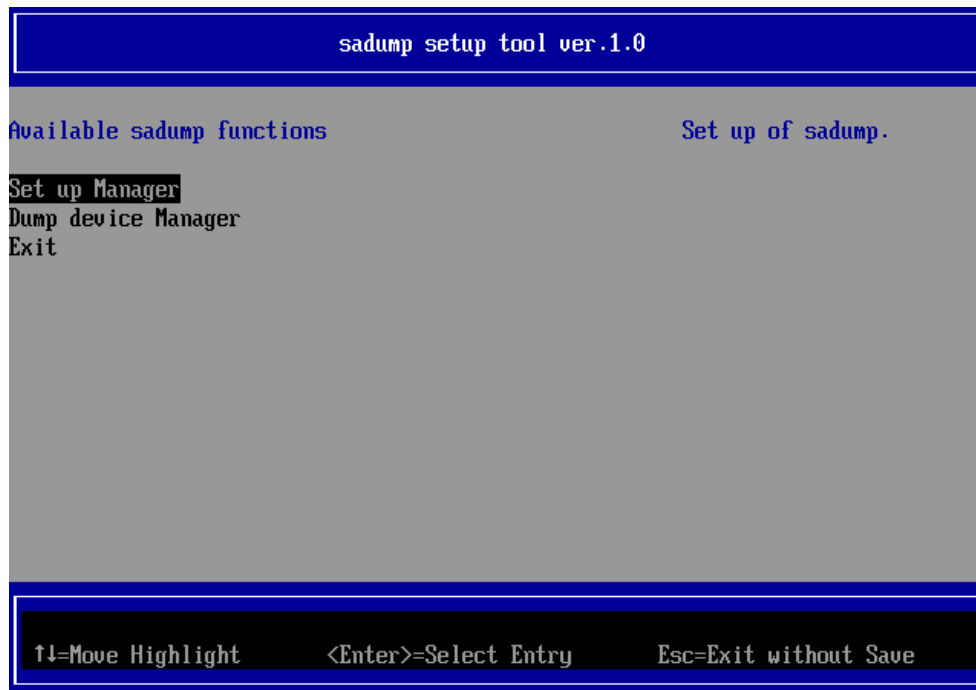


FIGURE 5.16 Main menu (sadump)

17. Select [Exit], and press the [Enter] key
>> You have completed the setting of sadump.

5.4 Setting Up the Dump Environment (Windows)

You can use the standard operating system functions of Windows to acquire dumps. Before you can acquire dumps, you need to allocate an area for them in the system.

For details on how to set up the dump environment, see 11.4.4 Setting up the dump environment (Windows) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

5.4.1 Memory dump files and paging files

A memory dump file stores debug information on any STOP error (fatal system error) that has occurred in the system. After installing the operating system and applications for operations, make settings for acquiring memory dumps.

For details on memory dumps and paging files, see 11.4.4 Setting up the dump environment (Windows) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

5.5 Setting Up the Dump Environment (Linux)

In RHEL, you can prepare an environment enabling the most reliable acquisition of dumps by combining the kdump function, which is a standard operating system function, and the sadump function of hardware.

5.5.1 How to use sadump

This section describes the procedure for sadump. sadump allows you to store memory dumps under situations like the following, whereas the standard RHEL function kdump does not allow this:

- OS panic or hang before the kdump service starts
- Error while kdump is running

1. Prepare

Install the following two packages corresponding to the kernel version used:

- kernel-debuginfo-common
- kernel-debuginfo

2. Configure the UEFI

Referring to [5.3 Setting of sadump](#), configure the UEFI for sadump. Note the following points.

- Set [RECYCLE] in Set up Manager to <Enable>. Otherwise, every time after sadump acquires a memory dump, the dump device must be configured again.
- Select [Create a dump device] in Dump device Manager, and set [Create mode] to <Single>. <Multiple> is not supported.

3. Configure the OS

To use sadump, kdump must be configured beforehand. After configuring kdump, you need to make the following additional settings.

- Setting to not reboot after panic
Set the kernel parameter "kernel.panic" to 0 (the default is 0). Otherwise, the system automatically reboots after panic, and there is no chance to start sadump. Configure /etc/sysctl.conf as follows.

```
kernel.panic=0
```

- Setting to stop the system after kdump
Set "default" in /etc/kdump.conf to "halt" or "shell". Otherwise, the system automatically reboots when kdump fails, and there is no chance to start sadump.
- Setting to start sadump
Set "blacklist kvm-intel" in /etc/kdump.conf. Otherwise, SMI is blocked, and sadump cannot start.

Example of /etc/kdump.conf

```
ext4 LABEL=/dump
path /
core_collector makedumpfile -c --message-level 1 -d 31
disk_timeout 60
default shell
blacklist kvm-intel
```

- Setting for an NMI to start kdump

A kdump start by an NMI is needed at the beginning of the procedure to start sadump. Configure `/etc/sysctl.conf` as follows.

```
kernel.unknown_nmi_panic=1
```

4. Start sadump and check

Start sadump as follows.

1. Send an NMI to start kdump.

Select [Partition] from the MMB Web-UI. Then, select [NMI] in [Power Control], and click [Apply].

2. If kdump does not start, start sadump.

Select [Partition] from the MMB Web-UI. Then, select [sadump] in [Power Control], and click [Apply].

The console screen displays the following message when sadump starts a memory dump, and the number increases gradually.

```
[ 0.0%]
```

The number reaches 100 and the following message appears when the memory dump is finished.

```
Dumping Complete
```

After the memory dump is finished and the OS reboots, check the memory dump by using the crash command. The example here checks the memory dump saved on `/dev/sdb1`. "DATE" shows the date and time that the memory dump was captured.

```
# crash /usr/lib/debug/lib/modules/2.6.32-358.el6.x86_64/vmlinux /dev/sdb1
(snip)
  KERNEL: /usr/lib/debug/lib/modules/2.6.32-358.el6.x86_64/vmlinux
  DUMPFILE: /dev/sdb1
  CPUS: 2
  DATE: Fri Oct 11 09:10:39 2013
  UPTIME: 00:19:04
  LOAD AVERAGE: 0.14, 0.03, 0.01
  TASKS: 125
  NODENAME: localhost
  RELEASE: 2.6.32-358.el6.x86_64
  VERSION: #1 SMP Tue Jan 29 11:47:41 EST 2013
  MACHINE: x86_64 (1861 Mhz)
  MEMORY: 4 GB
  PANIC: "Oops: 0002 [#1] SMP " (check log for details)
  PID: 7866
  COMMAND: "bash"
```

```
TASK: ffff8801387c8aa0 [THREAD_INFO: ffff8801394e2000]  
CPU: 0  
STATE: TASK_RUNNING (PANIC)
```

5. Send the memory dump to a vendor

Send the memory dump to a vendor supporting RHEL. You can convert the memory dump to a normal file by using the `makedumpfile` command. `makedumpfile` can generate a small dump file through compression or filtering. For details on `makedumpfile`, see the man manual. The example here saves the memory dump on `/dev/sdb1` to a `vmcore` file by using compression and filtering out memory regions except kernel memory. (The following command is written on one line.)

```
# makedumpfile -c -d 31 -x  
/usr/lib/debug/lib/modules/2.6.32-358.el6.x86_64/vmlinux /dev/  
sdb1 vmcore
```

5.6 Configuring the NTP Client

For details on how to configure the NTP client, see [7.2 Configuring NTP](#).

5.7 Saving Management and Configuration Information

This section describes how to save the following information. Be sure to save UEFI configuration information.

- 5.7.1 Saving MMB configuration information
- 5.7.2 Saving BIOS configuration information

Remarks

After the start of actual business operation, save UEFI configuration information regularly. For details on how to save UEFI configuration information, see 5.7.2 Saving BIOS configuration information.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

5.7.1 Saving MMB configuration information

This section describes how to back up MMB configuration information to a remote PC.

Use the [Maintenance] menu in the [MMB Web-UI] window to save MMB configuration information.

Operations

1. Select [Maintenance] - [Backup/Restore Configuration] - [Backup/Restore MMB Configuration].
>> The Backup/Restore MMB Configuration window appears.

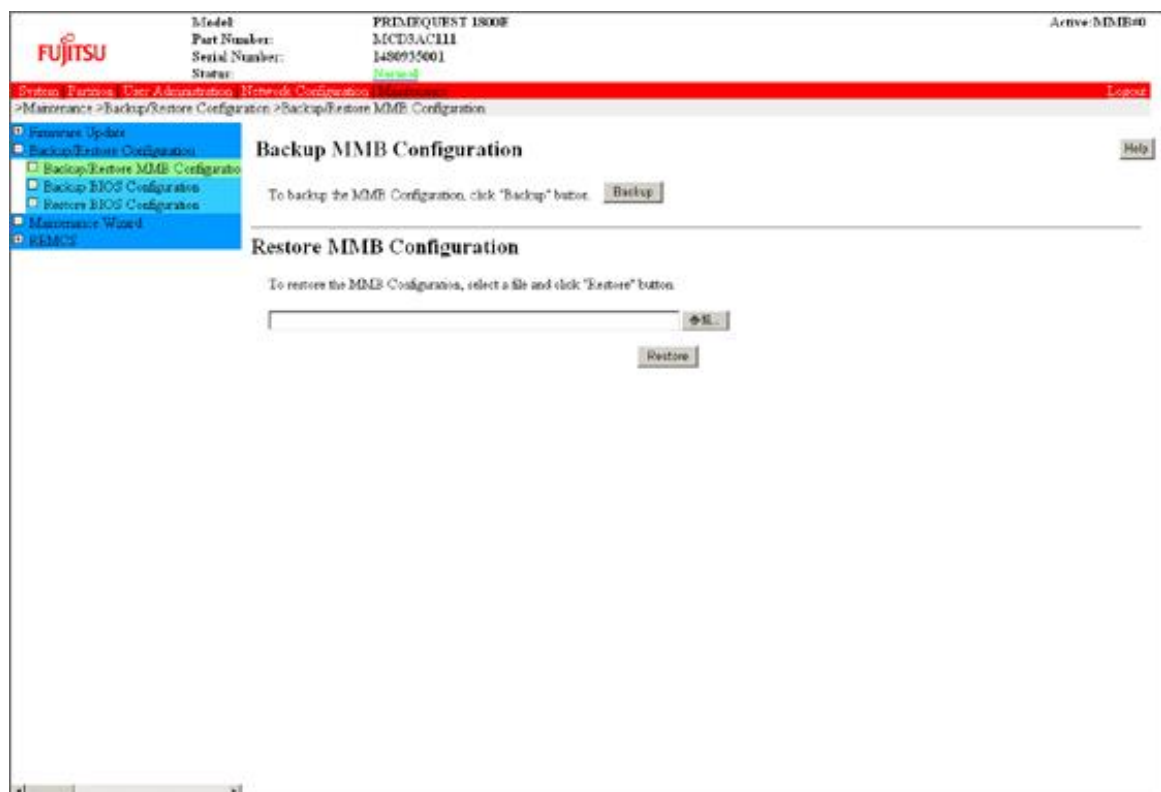


FIGURE 5.17 [Backup/Restore MMB Configuration] window (example)

2. Click the [Backup] button.
>> The save destination dialog box of the browser appears.
3. Select the save destination path. Then, click the [OK] button.
>> Download of the configuration information file begins.

The backup file of the MMB configuration information has the following default name:
MMB_backup date_MMB version.dat

5.7.2 Saving BIOS configuration information

This section describes how to back up BIOS configuration information to a remote PC.
Use the [Maintenance] menu in the [MMB Web-UI] window to save BIOS configuration information.

Operations

1. Select [Maintenance] - [Backup/Restore Configuration] - [Backup BIOS Configuration].
>> The [Backup BIOS Configuration] window appears.

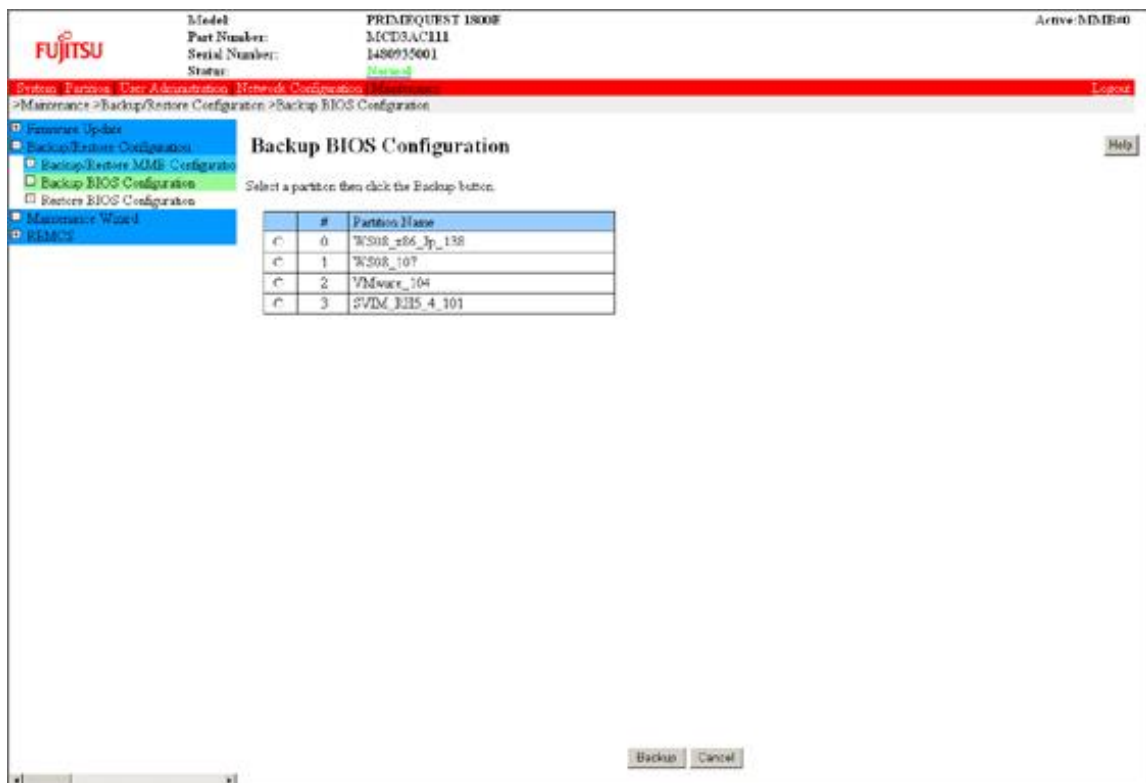


FIGURE 5.18 [Backup BIOS Configuration] window (example)

2. Select the radio button of the partition to which to back up the configuration information. Then, click the [Backup] button.
>> The save destination dialog box appears.

3. Select the save destination path. Then, click the [OK] button.

The backup file of the BIOS configuration has the following default name:
partition number_backup date_BIOS version.dat

5.8 Configuring Service Life Monitoring by RAS Support Service

For the use of RAID cards and UPSs, configure the BBU (Battery Backup Unit) service life monitoring by RAS Support Service.

SVIM automatically installs the RAS Support Service. For details on the manual installation and service life monitoring setting procedures for RAS Support Service, see the *RAS Support Service User's Guide (for Linux or Windows)*.

For details on SVIM, see the *ServerView Installation Manager*.

5.8.1 BBU service life monitoring for a RAID card

The BBU on a RAID card is a service life component. RAS Support Service performs service life monitoring. When starting, RAS Support Service checks for the RAID cards that have a BBU in order of PCI bus number, according to ServerView RAID information. It will monitor those RAID cards.

RAS Support Service performs service life monitoring and sends messages for replacement notification at the following times.

TABLE 5.2 Message for advance notification of replacement and replacement notification message (RAID card)

Start time for sending messages for advance notification of replacement	Time for sending replacement notification message
After about 2 years from the start of use or replacement of the battery unit	After about 3 years

Operations

1. Start the GUI of RAS Support Service.
 - Windows: Log in to the operating system. Start the GUI.
 - Linux: Open a Web browser. Access the specified URL. Log in.

For details on operations, see the *RAS Support Service User's Guide (for Linux or Windows)*.

2. The Service Life Component Names list on the Component Service Life Information and Settings screen of RAS Support Service displays [Battery (RAID_Card#xx)] in order of PCI bus number.

You can enter a value (for a RAID card) in the Mounting Dates list to enable battery service life monitoring. In the Mounting Dates list, enter the mounting dates of the RAID cards for which to set service life monitoring.

Notes

Note the following points about BBU service life monitoring for a RAID card in the PRIMEQUEST 1800E2.

- Of the mounted RAID cards shown in [FIGURE 5.19 RAS Support Service screens \(no BBU\)](#), the RAID card without a BBU is not monitored by RAS Support Service.

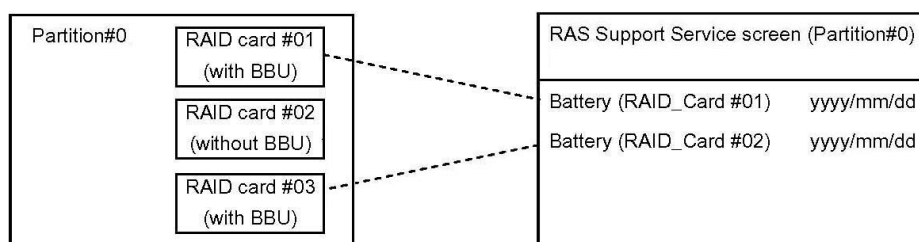


FIGURE 5.19 RAS Support Service screens (no BBU)

- After moving a monitored RAID card to another partition through a partition configuration change, you need to correct the RAS Support Service settings. First, in the Mounting Dates list, clear the RAID card mounting date on the original source partition. Then, set the RAID card mounting date on the destination partition.

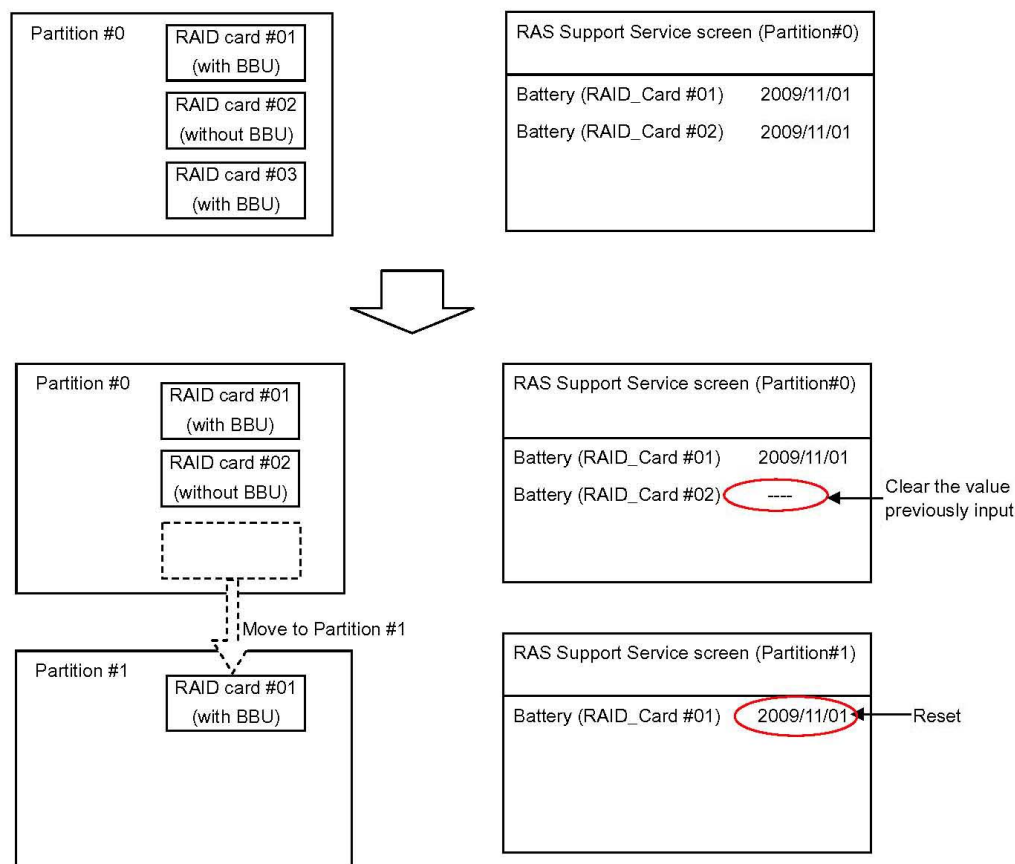


FIGURE 5.20 RAS Support Service screens (move to another partition)

- The PRIMEQUEST 1800E2 can have multiple partition configurations.
 For example, suppose a partition requires many CPUs during the day and a lot of I/O at night, the partition configuration must change between day and night. This means changes in the SB and IOB connection configuration.
 In this case, to move a RAID card to another partition, determine the primary partition for service life monitoring and then set the partition in RAS Support Service.
 If both partitions are set by mistake, notifications from both partitions will be issued in service life monitoring for the same RAID card.

5.8.2 Battery unit service life monitoring for a UPS

The battery unit on a UPS is a service life component. RAS Support Service performs service life monitoring. RAS Support Service sends messages for replacement notification at the following times.

TABLE 5.3 Message for advance notification of replacement and replacement notification message (UPS)

Start time for sending messages for advance notification of replacement	Time for sending replacement notification message
After about 1 year and 9 months from the start of use or replacement of the battery unit	After about 2 years

Operations

1. Determine which partitions to set for service life monitoring. Then, start the GUI of RAS Support Service.
 - Windows: Log in to the operating system. Start the GUI.
 - Linux: Open a Web browser. Access the specified URL. Log in.

For details on operations, see the *RAS Support Service User's Guide (for Linux or Windows)*.

2. The Service Life Component Names list on the RAS Support Service screen displays [UPS (battery)]. Since you can enter a value in the Mounting Dates list, enter the battery unit mounting date in the list.

Notes

Note the following points about service life monitoring of the battery unit for a UPS in the PRIMEQUEST 1800E2.

- If there are multiple partition configurations, set battery unit service life monitoring for a UPS for only one partition (arbitrary).

Otherwise, advance notifications of replacement will be issued from multiple partitions.

CHAPTER 6 Work after Operating System Installation (PRIMEQUEST 1800E)

This chapter describes how to make PSA and other settings after operating system installation on the PRIMEQUEST 1800E.

6.1 Types of Work	140
6.2 Configuring PSA (Linux: Red Hat Enterprise Linux)	
141	
6.3 Configuring PSA (Windows Server 2003)	161
6.4 Configuring PSA (Windows Server 2008)	175
6.5 Setting Up the Dump Environment (Windows)	203
6.6 Setting Up the Dump Environment (Linux)	204
6.7 Configuring the NTP Client	205
6.8 Saving Management and Configuration Information	
206	
6.9 Configuring Service Life Monitoring by RAS Support	
Service	211
6.10 Recommended Write Policy Setting for SAS Disk RAID	
Units	214
6.11 Recovery Procedure after the Execution of the Simple	
Setup Tool (editconf.sh)	215

6.1 Types of Work

TABLE 6.1 Types of work lists the types and details of the work performed after operating system installation.

TABLE 6.1 Types of work

Task	Description	Installed operating system	See
Configuring PSA	Configuring PSA for operation	Linux	6.2 Configuring PSA (Linux: Red Hat Enterprise Linux)
Configuring PSA	Configuring PSA for operation	Windows Server 2003	6.3 Configuring PSA (Windows Server 2003)
Configuring PSA	Configuring PSA for operation	Windows Server 2008	6.4 Configuring PSA (Windows Server 2008)
Setting up the dump environment	Setting up the dump environment	Windows	6.5 Setting Up the Dump Environment (Windows)
Setting up the dump environment	Setting up the dump environment	Linux	6.6 Setting Up the Dump Environment (Linux)
Configuring an NTP client	Configuring an NTP client	Linux or Windows	6.7 Configuring the NTP Client
Saving management and configuration information	Saving PSA management information and UEFI configuration information	Linux or Windows	6.8 Saving Management and Configuration Information
Setting service life monitoring by RAS Support Service	Setting service life monitoring of battery units on RAID cards and UPSs	Linux or Windows	6.9 Configuring Service Life Monitoring by RAS Support Service
Recovery procedure after the execution of the simple setup tool (editconf.sh)	Recovery procedure after the simple setup of ServerView Linux agent (including PRIMEQUEST-specific work)	Linux	6.11 Recovery Procedure after the Execution of the Simple Setup Tool (editconf.sh)

6.2 Configuring PSA (Linux: Red Hat Enterprise Linux)

This section describes confirmation of the required settings for PSA operation after operating system installation, and corresponding features about the settings.

TABLE 6.2 Confirmation of the required settings for PSA operation, and corresponding features about the settings

Required/ As needed	Setting item	Automatic setting (*1)/ Manual setting (*2)	See
Required	Configuring the PSA-to-MMB communication LAN	Automatic setting	6.2.1 Configuring the PSA-to-MMB communication LAN
	Confirming management LAN settings	Manual setting	6.2.2 Confirming management LAN settings
	Confirming SELinux function settings	Automatic setting	6.2.3 Confirming SELinux function settings
	Checking the firewall function (opening ports)	Automatic setting	6.2.4 Checking the firewall function (opening ports)
	Setting the management LAN IP address	Manual setting	6.2.7 Setting the management LAN IP address
As needed	Setting the destinations of traps from a partition	Manual setting	6.2.5 Setting the destinations of traps from a partition
	Setting the destinations of traps and e-mail via the MMB	Manual setting	6.2.6 Setting the destinations of traps and e-mail via the MMB
	Configuring SNMP to use duplicate disks	Manual setting	6.2.8 Configuring SNMP to use duplicate disks
	Installing a PSA update	Not applicable	6.2.9 Installing a PSA update
	Uninstalling PSA (*3)	Not applicable	6.2.10 Uninstalling PSA

*1 Automatic setting: Values are automatically set during PSA installation. You may need to change an automatically set value. See the section listed in the table.

*2 Manual setting: Values are not automatically set during PSA installation. Make settings as described in the section referred to in the table.

*3 To operate the PRIMEQUEST 1000 series server, you need to first install PSA. Otherwise, the following restrictions apply.

- I/O (e.g., PCI Express card, hard disk) failure notification and trap notification to the administrator are disabled.
- Failure notification using symptom detection and trap notification to the administrator are disabled.
 - Threshold exceeded in S.M.A.R.T. monitoring of HDDs

- Operations management software cannot collect information on the partition side.
- Even under an REMCS agreement, no software errors are reported.
- Hot maintenance of hard disks is disabled. The partition must be stopped for maintenance.
- PRIMECLUSTER linkage is disabled.

Remarks

- SVIM installs PSA as it installs the operating system. For details on SVIM, see the *ServerView Suite ServerView Installation Manager*.
- For details on how to manually install PSA, see [APPENDIX B Manual PSA Installation and Uninstallation](#).
- The following table lists settings for PSA operation. The installer automatically adds or updates these settings during PSA installation.

TABLE 6.3 Settings automatically added/changed during PSA installation

Target	Action	Remarks
syslog.conf file	Add setting	
snmpd.conf file	Add setting	
snmptrapd.conf file	Add setting	
services files	Add setting	Added port: The installer does not check for duplicate port numbers when a setting is added to the fj-webgate (24450) services file. Change settings as needed.
snmptrapd start option	Change	
snmpd start option	Change	
Dedicated PSA-to-MMB communication LAN interface	Set IP address	Referring to 6.2.1 Configuring the PSA-to-MMB communication LAN , change settings as needed.
iptables setting	Add setting	
SELinux configuration file (/etc/selinux/config)	Change	SELinux is disabled only for RHEL5. If SELinux is disabled, do not change the settings.
SELinux setting	Add setting	The policy module is added for RHEL6 or later only.

Note

If you change the IP address of the dedicated PSA-to-MMB communication LAN on the MMB side or partition side, you need to then restart PSA. Otherwise, a display error may occur in the [PSA] window of the MMB Web-UI. Moreover, PSA would not be able to report any detected errors.

6.2.1 Configuring the PSA-to-MMB communication LAN

This section describes how to confirm the settings for the PSA-to-MMB communication LAN.

Communication between PSA and the MMB requires an active NIC (network interface card) connected to the PSA-to-MMB communication LAN.

The PSA-to-MMB communication LAN is usually set with the following values during PSA installation.

<IP address>

172.30.0.<partition ID + 2>/24

Example: Partition ID of 2

172.30.0.4/24

<Communication settings>

Auto Negotiation off

Speed 100 Mbps

Duplex full

In the following cases, change the IP address setting.

1. The automatically set IP address is the same as the IP address or subnet used for a production network or management network.
2. You are configuring a new partition using a duplicate disk from another partition.
3. The partition ID changes because a disk installed in a partition was moved to another partition.

Change the IP address setting by using the following procedure. If you are changing the setting because of the above reason 1, you need to change the IP addresses of all partitions in the cabinet and the IP address of the PSA-to-MMB communication LAN on the MMB side to IP addresses in the same subnet. Change the IP addresses on the MMB side from the MMB Web-UI.

Notes

- Do not change the automatically set communication values. Otherwise, PSA-MMB communication may be disabled, making PSA functions unavailable.
- Change PSA-to-MMB LAN settings only after PSA installation. If changed before PSA installation, the settings are overwritten by the installation.
- If [Interface] of [MMB-PSA IP Address] in the [Network Configuration] - [Network Interface] window of the MMB Web-UI is Disable, you can use neither the screen display nor event notification function of PSA. After changing it from Disable to Enable, the OS must be restarted.

Confirming the NIC of the PSA-to-MMB communication LAN

Confirm the interface name assigned to the NIC of the PSA-to-MMB communication LAN by using the following procedure.

Operations

1. Execute the ifconfig command to confirm the interface name. This command lists the network interfaces recognized by the system.

Syntax

```
/sbin/ifconfig -a
```

Example of output

eth0, eth1, and lo shown on the left side are the interface names.

```
# /sbin/ifconfig -a
eth0  Link encap:Ethernet  HWaddr 00:D0:B7:53:89:C3
      inet addr:10.24.17.149  Bcast:10.24.17.255  Mask:255.255.255.0
      inet6 addr: fe80::2d0:b7ff:fe53:89c3/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500    Metric:1
      RX packets:1107704 errors:0    dropped:0 overruns:0 frame:0
      TX packets:2653820 errors:0    dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:390009908 (371.9 MiB)  TX bytes:809006934 (771.5 MiB)

eth1  Link encap:Ethernet  HWaddr 00:0E:0C:21:83:97
      inet addr:192.168.0.162  Bcast:10.24.17.255  Mask:255.255.255.0
      inet6 addr: fe80::20e:cff:fe21:8397/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500    Metric:1
      RX packets:1538726 errors:0    dropped:0 overruns:0 frame:0
      TX packets:356 errors:0 dropped:0    overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:341051195 (325.2 MiB)  TX bytes:22862 (22.3 KiB)
      Base address:0x5cc0    Memory:fbfe0000-fc000000

lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:16436    Metric:1
      RX packets:3865 errors:0 dropped:0    overruns:0 frame:0
```

2. Execute the `ethtool` command to find the NIC of the PSA-to-MMB communication LAN. Enter the command as shown below for each interface displayed in step 1. Then, check the results.

The NIC of the PSA-to-MMB communication LAN is bus-info (SEG:BUS:DEV.FUNC number) 0000:00:19:00.0.

Syntax

```
/sbin/ethtool -i <interface name>
```

Example of output

The execution results for `eth0` in the example show the matching NIC for the PSA-to-MMB communication LAN.

```
# /sbin/ethtool -i eth0
      driver: e100
      version: 3.0.27-k2-NAPI
      firmware-version: N/A
```

bus-info: 0000:00:19.0 (Corresponds to NIC of PSA-to-MMB communication LAN)

Configuring the NIC of the PSA-to-MMB communication LAN

Configure the NIC of the PSA-to-MMB communication LAN by using the following procedure.

Operations

1. Edit the ifcfg file of the corresponding interface in /etc/sysconfig/network-scripts.
 - NIC interface file name for the PSA-to-MMB communication LAN: ifcfg-<NIC interface name>
Example: ifcfg-eth0

Change the IP address by editing the ifcfg file of the interface.

The following example shows a command for editing the ifcfg file of the NIC interface for the PSA-to-MMB communication LAN.

```
# vi /etc/sysconfig/network-scripts/ifcfg-<NIC
interface name>

Change the following lines:
BROADCAST=<BROADCAST address of PSA-to-MMB
communication LAN>
IPADDR=<IP address of PSA-to-MMB communication LAN>
NETMASK=<Subnet mask of PSA-to-MMB communication LAN>
```

Notes

- Before changing the settings, confirm that the settings in the ifcfg file have the values that were automatically set during PSA installation. If they do not have the automatically set values, PSA may not have been installed. Always change the settings after PSA installation.
- Do not change any line, including comment lines, except those with the items that must be changed (BROADCAST, IPADDR, and NETMASK). Otherwise, PSA-MMB communication may be disabled, making PSA functions unavailable. Moreover, a PSA update may overwrite the automatically set values.

2. Restart the network service to activate the network interface.

Syntax

```
/sbin/service network restart
```

3. Restart PSA to reflect the new NIC settings for the PSA-to-MMB communication LAN.

Syntax

```
/sbin/service y30FJSVpsa stop
/sbin/service y30FJSVpsa start
```

6.2.2 Confirming management LAN settings

Make network settings for the management LAN. If necessary, also configure any duplication with bonding or PRIMECLUSTER GLS, for example.

After completing the above network settings for the management LAN, perform the operations described in [6.2.4 Checking the firewall function \(opening ports\)](#) and [6.2.7 Setting the management LAN IP address](#).

Note

In the PRIMEQUEST environment, it is necessary to specify OFF for the STP function of the switch that connects to the management LAN used for communication with the MMB.

6.2.3 Confirming SELinux function settings

This section describes the SELinux settings and how to confirm them.

Other OS settings

- For RHEL5
If the partition OS with PSA installed is running RHEL5, disable the SELinux functions. When installing PSA, the SELinux functions are automatically disabled. Confirm that the SELinux functions are disabled. If the SELinux functions are enabled, disable them.
- For RHEL6.0/RHEL6.1
If the partition OS with PSA installed is running RHEL6.0/RHEL6.1, disable the SELinux functions. When installing PSA, the SELinux functions are not automatically disabled. Check the SELinux function setting. If the SELinux functions are enabled, disable them.
- For RHEL6.2 or later
If the partition OS with PSA installed is running RHEL6.2 or later, it operates irrespective of whether the SELinux functions are enabled or disabled.

The procedure for confirming the SELinux function setting and disabling the SELinux functions is as follows. Confirm that the following command displays "disabled" when operating the system with the SELinux functions disabled. If the command displays anything other than "disabled," disable the functions by editing the config file (/etc/selinux/config).

Confirming settings

```
#cd /etc/selinux/  
#more config  
.....  
.....  
SELinux=disabled ← Confirm this.
```

Changing settings

```
# vi /etc/selinux/config  
.....  
.....  
SELinux=disabled ← Edit this.
```

6.2.4 Checking the firewall function (opening ports)

Open any partition port that is required for operating PSA but is not open because of firewall settings. Configure the management LAN interfaces and PSA-to-MMB communication LAN interfaces.

Settings related to the PSA-to-MMB communication LAN interface are required. Usually, the interfaces are automatically set during PSA installation.(*1)

The settings related to the management LAN interface are required only for PRIMECLUSTER linkage. Open the ports by executing the supplied shell script for these settings. Alternatively, use the iptables command or another command to make the settings manually.(*2)

For RHEL6, see the information [For PSA version 2.6 or later].

*1 In PSA version 2.6 and later, the ports are configured only when PSA is automatically installed from SVIM.

*2 In PSA version 2.6 and later, only a chain for the management LAN (MMLAN) is created by execution of the shell script for settings (setmlanfw.sh). Add the jump setting for the management LAN to INPUT or OUTPUT in iptables. For details, see Using the shell script (setmlanfw.sh) for these settings.

Management LAN interfaces

Open the following ports for use with the management LAN interfaces.

Perform the operations described in [6.2.7 Setting the management LAN IP address](#) before making the settings.

Open the ports by executing the shell script (setmlanfw.sh) for these settings. Alternatively, use the iptables command or another command to make the settings manually.

TABLE 6.4 Ports to open for the management LAN interfaces

Port	Port number	Description	Remarks
snmptrap port	udp/snmptrap or 162	Open the port only for linkage with a cluster (e.g., PCL linkage).	For the IP addresses, specify the physical IP addresses of the MMBs (MMB#0/MMB#1) belonging to all cluster nodes.
rmcp+ port	udp/7000 to 7100		

Using the shell script (setmlanfw.sh) for these settings

Note

- setmlanfw.sh is a tool for setting a management LAN port in iptables. If a firewall other than iptables is used, the ports specified in [TABLE 6.4 Ports to open for the management LAN interfaces](#) must be opened individually.
- If PSA version 2.8.0 or earlier is installed and the shell script (setmlanfw.sh) for these settings is used, the existing settings are cleared when the iptables service stops.
- The shell script (setmlanfw.sh) for these settings adds settings to iptables. To make settings with this script, start the iptables service.

1. Confirm the completion of the operations described in [6.2.7 Setting the management LAN IP address](#).
2. Prepare a configuration file.

The following is a sample configuration file.

```
/opt/FJSVpsa/sh/sample_conf_setmlanfw.txt
```

Remarks

A PSA update will overwrite the above sample file. Save a copy of the configuration file to retain the original values.

In the configuration file, write [PCL] only on the first line. Then, on separate lines, write the physical IP addresses of the MMBs (MMB#0/MMB#1) belonging to all the cluster nodes defined for PRIMECLUSTER, or write the network IP addresses including the physical IP addresses of the aforementioned MMBs.

Sample configuration file:

```
[PCL]
192.168.0.0/24
192.168.1.5
```

3. Execute the shell script.

In the first variable, specify the path to the configuration file prepared in step 2.

A confirmation message appears for the contents of the configuration file. Enter "Y".

```
Execution example: (The prepared configuration file "fwconf.txt" is
assumed to be in the current directory.)
# /opt/FJSVpsa/sh/setmlanfw.sh ./fwconf.txt
Management LAN IP address:
192.168.0.1
Source IPs for PRIMECLUSTER Service:
192.168.0.0/24
192.168.1.5.
Press "Y" to confirm above settings, "N" to cancel all settings
> Y
#####
# Created the MMLAN chain on your                                     #
# firewall(iptables)                                                 #
# For more detail on how to set firewall, refer to the Installation #
# Manual.                                                            #
#####
The setting was completed
```

4. Execute iptables -L -n. Then, confirm that the "MMLAN" chain exists.

```
Execution example:
# iptables -L -n
Chain INPUT (policy DROP)
target    prot opt source                destination
```

```

MMLAN    all    --    0.0.0.0/0    0.0.0.0/0

Chain FORWARD (policy DROP)
target    prot    opt    source        destination

Chain OUTPUT (policy DROP)
target    prot    opt    source        destination
MMLAN    all    --    0.0.0.0/0    0.0.0.0/0

Chain MMLAN (2 references)
target    prot    opt    source        destination
ACCEPT    udp    --    192.168.0.0/24  192.168.0.1    udp dpts:7000:7100
ACCEPT    udp    --    192.168.0.1    192.168.0.0/24  udp spts:7000:7100
ACCEPT    udp    --    192.168.0.0/24  192.168.0.1    udp dpt:162
ACCEPT    udp    --    192.168.0.1    192.168.0.0/24  udp spt:162
ACCEPT    udp    --    192.168.1.5    192.168.0.1    udp dpts:7000:7100
ACCEPT    udp    --    192.168.0.1    192.168.1.5    udp spts:7000:7100
ACCEPT    udp    --    192.168.1.5    192.168.0.1    udp dpt:162
ACCEPT    udp    --    192.168.0.1    192.168.1.5    udp spt:162
  
```

Note

After changing the IP address of the management LAN interface, delete the settings once, and set their values again. For details on how to delete the settings, see (7) Configuration deletion procedure in 4.11 Firewall Setting Command for the Management LAN Interface (setmlanfw.sh) in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

[For PSA version 2.6 or later]

Add the "MMLAN" setting chain to INPUT and OUTPUT chains. At this time, take care to prevent interruptions by an existing REJECT setting in an INPUT or OUTPUT chain or by a user definition chain.

```

Example: REJECT setting in INPUT and FORWARD
# iptables -L
Chain INPUT (policy ACCEPT)
target    prot    opt    source        destination
ACCEPT    all    --    0.0.0.0/0    0.0.0.0/0    state RELATED,ESTABLISHED
ACCEPT    icmp  --    0.0.0.0/0    0.0.0.0/0
ACCEPT    all    --    0.0.0.0/0    0.0.0.0/0
ACCEPT    tcp    --    0.0.0.0/0    0.0.0.0/0    state NEW tcp dpt:22

REJECT    all    --    0.0.0.0/0    0.0.0.0/0    reject-with icmp-host-
prohibited

Chain FORWARD (policy ACCEPT)
target    prot    opt    source        destination

REJECT    all    --    0.0.0.0/0    0.0.0.0/0    reject-with icmp-host-
prohibited
  
```

```
Chain OUTPUT (policy ACCEPT)
target  prot  opt  source      destination

Chain MMLAN (2 references)
target  prot  opt  source      destination
ACCEPT  udp   --   192.168.0.0/24  192.168.0.1      udp dpts:7000:7100
ACCEPT  udp   --   192.168.0.1     192.168.0.0/24  udp spts:7000:7100
ACCEPT  udp   --   192.168.0.0/24  192.168.0.1      udp dpt:162
ACCEPT  udp   --   192.168.0.1     192.168.0.0/24  udp spt:162
ACCEPT  udp   --   192.168.1.5     192.168.0.1      udp dpts:7000:7100
ACCEPT  udp   --   192.168.0.1     192.168.1.5      udp spts:7000:7100
ACCEPT  udp   --   192.168.1.5     192.168.0.1      udp dpt:162
ACCEPT  udp   --   192.168.0.1     192.168.1.5      udp spt:162
```

5. Add "MMLAN" to the fifth INPUT chain (before the REJECT setting) and to the OUTPUT chain. (For details on the iptables option, see the man manual.)

```
# /sbin/iptables -I INPUT 5 -j MMLAN
# /sbin/iptables -A OUTPUT -j MMLAN
```

6. Execute the iptables -L command, and confirm that the MMLAN chains added to the INPUT and OUTPUT chains are not interrupted by the previous REJECT, DROP, or other settings.

```
Example of settings:
# iptables -L
Chain INPUT (policy ACCEPT)
target  prot  opt  source      destination
ACCEPT  all   --   0.0.0.0/0    0.0.0.0/0    state RELATED,ESTABLISHED
ACCEPT  icmp  --   0.0.0.0/0    0.0.0.0/0
ACCEPT  all   --   0.0.0.0/0    0.0.0.0/0
ACCEPT  tcp   --   0.0.0.0/0    0.0.0.0/0    state NEW tcp dpt:22

MMLAN   all   --   0.0.0.0/0    0.0.0.0/0
REJECT  all   --   0.0.0.0/0    0.0.0.0/0    reject-with icmp-host-
prohibited

Chain FORWARD (policy ACCEPT)
target  prot  opt  source      destination
REJECT  all   --   0.0.0.0/0    0.0.0.0/0    reject-with icmp-host-
prohibited

Chain OUTPUT (policy ACCEPT)
target  prot  opt  source      destination
```



```
MMLAN    all    --    0.0.0.0/0  0.0.0.0/0
```

Chain MMLAN (2 references)

target	prot	opt	source	destination	
ACCEPT	udp	--	192.168.0.0/24	192.168.0.1	udp dpts:7000:7100
ACCEPT	udp	--	192.168.0.1	192.168.0.0/24	udp spts:7000:7100
ACCEPT	udp	--	192.168.0.0/24	192.168.0.1	udp dpt:162
ACCEPT	udp	--	192.168.0.1	192.168.0.0/24	udp spt:162
ACCEPT	udp	--	192.168.1.5	192.168.0.1	udp dpts:7000:7100
ACCEPT	udp	--	192.168.0.1	192.168.1.5	udp spts:7000:7100
ACCEPT	udp	--	192.168.1.5	192.168.0.1	udp dpt:162
ACCEPT	udp	--	192.168.0.1	192.168.1.5	udp spt:162

7. Save the firewall configuration.

```
# /sbin/service iptables save
```

PSA-to-MMB communication LAN interfaces

Open the following ports for use with the PSA-to-MMB communication LAN interfaces.

Usually, the ports are automatically opened during PSA installation.(*)

* In PSA version 2.6 and later, the ports are automatically configured only when PSA is installed from SVIM.

TABLE 6.5 Ports to open for the PSA-to-MMB communication LAN interfaces

Port	Port number	Description	Remarks
snmp port	udp/snmp or 161		For sending and receiving
web-mmb communication port	tcp/fj-webgate or 24450	web-mmb communication port	For sending and receiving
psa-mmb communication port	tcp/5000 on MMB side	Communication using port 5000 on the MMB side. The partition acts as the client in this type of communication, so the partition uses a dynamic port number (one of the ports in the range tcp/1025 to 65535). Under certain circumstances, there is no need to set port number 5000. One example is a setting that permits a connection to be established from the partition. Another example is a setting permitting communication through an established connection with the partition.	For sending and receiving

Port	Port number	Description	Remarks
		Example of a case where port 5000 need not be set: iptables -A OUTPUT -m state --state NEW,ESTABLISH -j ACCEPT iptables -A INPUT -m state --state ESTABLISH -j ACCEPT	
icmp	echo-request		For sending only
icmp	echo-reply		For receiving only

Syntax

```
/sbin/iptables -L
```

Use a command such as iptables to open ports. For details on how to use the command, see the respective manual (such as with the man command).

```
/usr/bin/man iptables
```

6.2.5 Setting the destinations of traps from a partition

Direct transfer of a PSA expansion trap from a partition requires that the trap destination and PSA trap notification be set on the partition.

Remarks

- Make settings only as needed.
- Even if this setting is skipped, traps are sent via the MMB.
- Operations management software needs these settings to manage events by partition.

Operations

1. Edit the /etc/opt/FJSVpsa/user/psatrap.conf file.

Example of setting PSA trap notification

```
#vi /etc/opt/FJSVpsa/usr/psatrap.conf
```

Change the following line.

```
[PSATRAP]
```

```
PSATRAP_SET=<0 or 1>
```

Setting value

- 1: Enables PSA trap notification from the partition.
- 0: Disables PSA trap notification from the partition.

Example of input

```
[PSATRAP]
PSATRAP_SET=1
```

2. Set trap destinations in the snmpd.conf file.

For details, see [Editing snmpd.conf](#).

3. Restart PSA to apply the settings.

Syntax

```
#!/sbin/service y30FJSVpsa stop
#!/sbin/service y30FJSVpsa start
```

Editing snmpd.conf

```
# vi /etc/snmp/snmpd.conf

Add the following lines according to the SNMP version used.
* The lines of definitions can be in any order.
trapsink HOST [COMMUNITY [PORT]]      # SNMPv1 trap setting
trap2sink HOST [COMMUNITY [PORT]]     # SNMPv2 trap setting
trapsest SNMPCMD_ARGS HOST[:PORT]    # SNMPv3 trap setting
```

The following describes the settings in detail.

SNMPv1/SNMPv2 trap setting

```
trapsink HOST [COMMUNITY [PORT]]      # SNMPv1 trap setting
trap2sink HOST [COMMUNITY [PORT]]     # SNMPv2 trap setting
```

The setting defines the host receiving the trap (i.e., the trap destination).

- A Cold Start trap is sent to the defined host during snmpd startup. If the partition is set to send SNMP traps, a trap is sent from the partition following any authentication failure.
- You can specify multiple trap destinations by specifying multiple hosts on the trapsink and trap2sink lines. As an alternative to specifying COMMUNITY, you can specify a character string on the trapcommunity line. The trapcommunity command defines a default community character string for sending traps. To use trapcommunity to set a community character string, specify the string before the trapsink and trap2sink lines.

```
trapcommunity STRING                  # Community name setting
```

- As an alternative to specifying PORT, you can use the general-purpose SNMP trap port (162).

The following example shows how to send traps with "public" as the community name. The traps are sent to the manager of port 162 with IP address 192.168.0.162.

```
trapsink 192.168.0.162 public 162    ##SNMPv1 trap setting
trap2sink 192.168.0.162 public 162    ##SNMPv2 trap setting
```

SNMPv3 trap setting

```
trapssess SNMPCMD_ARGS HOST[:PORT]# SNMPv3 trap setting
```

The setting defines the host receiving the trap (i.e., the trap destination). As an alternative to specifying PORT, you can use the general-purpose SNMP trap port (162).

The following options are the main options specified with SNMPCMD_ARGS.

-v version:

This option specifies the SNMP version. For SNMPv3, specify 3.

-e engineID:

This option specifies the oldEngineID value. The /var/net-snmp/snmpd.conf file at the trap source contains this value.

-u secName:

This is the account for SNMPv3. This setting must match that on the manager side.

-l secLevel:

This option specifies one of the values listed in [TABLE 6.6 secLevel settings](#) according to the security level of SNMPv3 messages.

TABLE 6.6 secLevel settings

Setting value	Authentication	Encryption
noAuthNoPriv	Not set	Not set
authNoPriv	Set	Not set
authPriv	Set	Set

-a authProtocol:

This is the protocol for SNMPv3 message authentication. Either MD5 or SHA is specified. To use SHA, install openssl and create a package with openssl. The option takes effect only if the security level in the -l option includes authentication. Otherwise, you can omit the option.

-A authPassword:

This is the authentication password (at least eight characters). This setting must match that on the manager side. The option takes effect only if the security level in the -l option includes authentication. Otherwise, you can omit the option.

-x privProtocol:

This is the protocol for SNMPv3 message encryption. Currently, the only supported privacy protocol is DES. The option takes effect only if the security level in the -l option includes encryption. Otherwise, you can omit the option.

-X privPassword:

This is the encryption password (at least eight characters). This setting must match that on the manager side. The option takes effect only if the security level in the -l option includes encryption. Otherwise, you can omit the option.

The following example shows how to send SNMPv3 traps with the "PRIMEQUEST" account to enable authentication and encryption. The traps are sent to the manager of port 162 with IP address 192.168.0.162.

```
#trapsess -v 3 -e 0x800007e58026577a9f421950a4 -u PRIMEQUEST -l \  
authPriv -a MD5  
-A 00000000 -x DES -X 11111111 192.168.0.162:162 \  
## SNMPv3 trap setting
```

\: This indicates that there is no line feed.

After setting the trap destination, restart snmpd with the following command.

```
#!/etc/rc.d/init.d/snmpd restart
```

After the snmpd restart is completed, restart PSA.

```
#!/sbin/service y30FJSVpsa stop  
#!/sbin/service y30FJSVpsa start
```

How to confirm a trap destination setting

To confirm a trap destination setting, use the standard net-snmp trap that was sent during the snmp restart. You can confirm the correct trap setting by checking whether the trap was received.

Remarks

The trap destination must be running both a trap receiving application and a trap manager to be able to receive standard net-snmp traps.

Restart snmpd with the following command on the trap source machine.

```
# /etc/rc.d/init.d/snmpd restart
```

After that operation, a Cold Start trap is posted to the trap receiving application at the trap destination. Cold Start is a standard net-snmp trap.

In the following example, the trap destination is a Linux machine. snmptrapd runs on the Linux machine that is the trap destination to receive traps. snmptrapd outputs the following message to the system log. Confirm that the Linux machine received the trap normally.

```
Aug 17 12:00:53 pq-server snmptrapd[2600]: 2005-08-17 12:00:53 \
pq-server.
fujitsu.com [192.168.0.162](via 192.168.0.162) TRAP, SNMP v1, \
community
public NET-SNMP-MIB::netSnmpAgentOIDs.10 Cold Start Trap (0) \
Uptime: 0:00:00.17
```

\\: This indicates that there is no line feed.

6.2.6 Setting the destinations of traps and e-mail via the MMB

You can set the destinations of traps and e-mail via the MMB by using the MMB Web-UI.

For details on MMB trap destinations, see [7.5.2 Configuring SNMP](#). For details on e-mail destinations, see [7.4 Configuring SMTP](#).

Remarks

- Make settings only as needed.
- Operations management software (e.g., Systemwalker) needs these settings to manage events by partition.

6.2.7 Setting the management LAN IP address

Set the partition management LAN IP address in PSA. For details on the management LAN, see 1.3 Management LAN in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

Note

Here, set the IP address on the partition instead of the IP address on the MMB.

Edit the /etc/opt/FJSVpsa/usr/ipsetup.conf file.

Example of changing the management LAN IP address

```
# vi /etc/opt/FJSVpsa/usr/ipsetup.conf

Change the following line.
[NETWORK]
ManagementIP=<management LAN IP address>
```

Syntax

```
[NETWORK]
ManagementIP=192.168.0.1
```

Restart PSA to reflect the new NIC setting for the management LAN.

Syntax

```
/sbin/service y30FJSVpsa stop
/sbin/service y10FJSVpsa start
/sbin/service y30FJSVpsa start
```

For details on how to specify any duplication of the management LAN with PRIMECLUSTER GLS, see the applicable PRIMECLUSTER manuals.

To use PRIMECLUSTER linkage, configure the firewall for the management LAN interfaces. After making those settings, follow the procedure in 5.2.4 Checking the firewall function (opening ports). Then, configure the management LAN interfaces.

6.2.8 Configuring SNMP to use duplicate disks

This section describes the required settings for using duplicate disks.

Remarks

Make settings only as needed.

You can use duplicate disks from a partition in a single cabinet to configure a new partition. To do so, you need to manually change EngineID of SNMPv3 for internal PSA communication.

Change EngineID by using the following procedure. Perform the procedure with root privileges.

Operations

1. Execute the ps command to check whether PSA is active.

Syntax

```
ps ax | grep psa
```

Example of output

If the command displays the processes in /opt/FJSVpsa/bin/ as follows, PSA is running.

```
# ps ax | grep psa
4562 ?      S        0:00 /opt/FJSVpsa/bin/pm -o 70 /etc/opt/\
FJSVpsa/
global/pmpsa.conf
4563 ?      S        0:18 /opt/FJSVpsa/bin/loggetd -p /
4564 ?      S        0:06 /opt/FJSVpsa/bin/sisp -p /
4565 ?      S        0:00 /opt/FJSVpsa/bin/mmbm -p /
```

```
4566 ?      S      0:01 /opt/FJSVpsa/bin/mmbs -p /
4567 ?      S      0:02 /opt/FJSVpsa/bin/fs  -p /
4568 ?      S      0:00 /opt/FJSVpsa/bin/ciipmi -p /
4569 ?      S      7:40 /opt/FJSVpsa/bin/cilog -p /
4570 ?      S      8:47 /opt/FJSVpsa/bin/cios  -p /
.
.
4578 ?      S      0:00 /opt/FJSVpsa/bin/cisalchild 1 /
4819 ?      Sl     0:00 /opt/FJSVpsa/bin/webgate -p /
21670 pts/5  S+     0:00 grep psa
```

\: This indicates that there is no line feed.

2. If PSA startup is in progress, execute the service command to stop PSA.

Syntax

```
/sbin/service y30FJSVpsa stop
```

3. Execute the ps command to check whether snmpd is active.

Syntax

```
ps ax | grep snmpd
```

Example of output

If the command displays /usr/sbin/snmpd as follows, snmpd startup is in progress.

```
# ps ax | grep snmpd
32611 ?      S      0:04 /usr/sbin/snmpd -Lsd -Lf /dev/null -p \
var/run/snmpd -a
```

\: This indicates that there is no line feed.

4. If snmpd startup is in progress, execute the service command to stop snmpd.

Syntax

```
/sbin/service snmpd stop
```

5. Change the oldEngineID value defined in the /var/net-snmp/snmpd.conf file.

Change it to an appropriate hexadecimal value consisting of up to 34 digits. However, be sure to use a value that is unique in the partitions in the same cabinet.

Example of changing the oldEngineID value to 0x19760523


```
#vi /var/net-snmp/snmpd.conf  
oldEngineID 0x19760523
```

6. Execute the service command to start snmpd.

Syntax

```
/sbin/service snmpd start
```

7. Move to the /opt/FJSVpsa/sh/ directory to generate another SNMPv3 password for internal PSA communication.

Syntax

```
cd /opt/FJSVpsa/sh/
```

8. Execute snmpsetup.sh in this directory.

When executed, snmpsetup.sh automatically generates an SNMPv3 password for internal PSA communication.

Syntax

```
./snmpsetup.sh install
```

9. Start PSA.

Syntax

```
/sbin/service y30FJSVpsa start
```

6.2.9 Installing a PSA update

This section describes how to install a PSA update in Red Hat Enterprise Linux.

Execute the following commands in the order shown to first stop PSA services and then install the PSA package to update PSA.

The following description assumes that the work directory (in the example below, \$WORK_DIR) has the PSA package (FJSVpsa-\$VER-\$REL.tar.gz) already mapped.

Syntax

```
/sbin/service y30FJSVpsa stop  
cd $WORK_DIR/FJSVpsa  
./INSTALL.sh
```

```
/sbin/service y30FJSVpsa start
```

6.2.10 Uninstalling PSA

This section describes how to uninstall PSA in Red Hat Enterprise Linux.

Execute the following commands in the order shown to first stop PSA services and then uninstall the PSA package.

Syntax

```
/sbin/service y30FJSVpsa stop  
/bin/rpm -e FJSVpsa
```

Note

Stopping the iptables service does not delete the settings of the ports to open with the PSA-to-MMB communication LAN interfaces that were specified at installation. Delete them manually as needed. For details on the ports to open, see [TABLE 6.5 Ports to open for the PSA-to-MMB communication LAN interfaces](#).

6.3 Configuring PSA (Windows Server 2003)

This section describes confirmation of the required settings for PSA operation after operating system installation, and corresponding features about the settings.

TABLE 6.7 Confirmation of the required settings for PSA operation, and corresponding features about the settings

Required/ As needed	Setting item	Automatic setting (*1)/ Manual setting (*2)	See
Required	Configuring the PSA-to-MMB communication LAN	Manual setting	6.3.1 Configuring the PSA-to-MMB communication LAN
	Confirming management LAN settings	Manual setting	6.3.2 Confirming management LAN settings
	Configuring the Windows Firewall	Manual setting	6.3.5 Configuring the Windows Firewall
	Setting the management LAN IP address	Manual setting	6.3.7 Setting the management LAN IP address
As needed	Setting the destinations of traps from a partition	Manual setting	6.3.3 Setting the destinations of traps from a partition
	Setting the destinations of traps and e-mail via the MMB	Manual setting	6.3.4 Setting the destinations of traps and e-mail via the MMB
	Setting Watchdog for monitoring after a STOP error (fatal system error)	Manual setting	6.3.6 Setting the Watchdog Timer for monitoring after a STOP error (fatal system error)
	Installing a PSA update	Not applicable	6.3.8 Installing a PSA update
	Uninstalling PSA (*3)	Not applicable	6.3.9 Uninstalling PSA

*1 Automatic setting: Values are automatically set during PSA installation. You may need to change an automatically set value. See the section listed in the table.

*2 Manual setting: Values are not automatically set during PSA installation. Make settings as described in the section referred to in the table.

*3 To operate the PRIMEQUEST 1800E server, you need to first install PSA. Otherwise, the following restrictions apply.

- I/O (e.g., PCI Express card, hard disk) failure notification and trap notification to the administrator are disabled.
- Failure notification using symptom detection and trap notification to the administrator are disabled.
 - Threshold exceeded in S.M.A.R.T. monitoring of HDDs
- Operations management software cannot collect information on the partition side.
- Even under an REMCS agreement, no software errors are reported.

Remarks

- SVIM installs PSA as it installs the operating system. For details on SVIM, see the *ServerView Installation Manager*.
- For details on how to manually install PSA, see [APPENDIX B Manual PSA Installation and Uninstallation](#).
- The following table lists settings for PSA operation. The installer automatically adds or updates these settings during PSA installation.

Note

Do not change the settings that were automatically added or changed during PSA installation. Otherwise, PSA may not operate normally.

TABLE 6.8 Settings automatically added/changed during PSA installation

Item	Description
1. Service settings	- PRIMEQUEST Server Agent - PRIMEQUEST PEM Command Service - PRIMEQUEST PSA Environment Control Service
2. Environment variable settings	- PATH variable: Adds the value used by PSA to the existing PATH variable. - FJSVpsa_INSTALLPATH variable: Adds a new variable.
3. Port settings	It sets PSA to use the TCP:24450 port.
4. SNMP security settings	Security is set for SNMP Service because PSA needs to accept SNMP packets from the MMB. The settings depend on the selected items on the [Security] tab in the [SNMP Service Properties] window during PSA installation: - With [Accept SNMP packets from any host] selected: SNMP security is not configured. - With [Accept SNMP packets from these hosts] selected: The MMB IP address is set. If no value is specified for localhost, localhost and SNMP security are configured.
5. WMI (Windows Management Instrumentation) settings	PSA uses WMI to acquire information on PCI Express cards and SCSI devices. WMI is installed as standard with Windows. These settings include settings on the size of memory and number of internal handles used by WMI to collect this information. If the system has many LUNs for devices such as RAIDs, it may not have sufficient memory or internal handles. For this reason, the settings are changed to the following values: - Upper limit on memory used: 536,870,912 bytes - Upper limit on internal handles: 65,536

Remarks

- Execute the SNMP security setting command (setsnmpsec) in the following situations. For details on the command, see 4.8 SNMP Security Setting Command (setsnmpsec) in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).
 - Having installed PSA, you will be changing the SNMP Service security setting from [Accept SNMP packets from any host] to [Accept SNMP packets from these hosts].
 - You will be changing the MMB IP address.
- In the initial startup of PSA following installation, the Web-UI may display the error message "E_33077 PSA is Not Active. (01:0000)" in the [PSA] window. This happens because PSA requires extra time to acquire system sensor data only during the initial startup. Wait a few minutes. Then, refresh the display.
- If you change the MMB IP address or the management LAN IP address on the partition, be sure to then restart PSA. Otherwise, a display error may occur in the [PSA] window of the Web-UI. Moreover, PSA would not be able to report detected errors.

Notes on configuring Windows Server 2003

- Do not enable [Visual Notification] in the options of Dr. Watson (diagnosis software bundled with Windows). Otherwise, if a PSA error occurs, a message box appears. You cannot restart PSA until you close this box.
- From [Properties] in the Event Viewer, do not change the operation in [When maximum log size is reached] for the system log or application log to [Do not overwrite events (clear log manually)]. Otherwise, after the log reaches the maximum log size, no errors are output to the log, so PSA will be unable to detect any errors.
- Do not stop the Windows Print Spooler service. The information collection function of the operating system uses WMI (Windows Management Instrumentation). If the Print Spooler service is stopped, the function cannot collect the correct configuration information because WMI reports an error.
- If the set value of the following registry key is less than 20000 (20 seconds), the system may hang during operating system shutdown. Be sure to set a value equal to or greater than 20000 (20 seconds). The default is 20000.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ WaitToKillServiceTimeout

You can use the above registry key to specify the wait time (ms) before the service is terminated in the shutdown sequence.

6.3.1 Configuring the PSA-to-MMB communication LAN

This section describes how to confirm the settings for the PSA-to-MMB communication LAN.

Communication between PSA and the MMB requires that the partition have an active NIC connected to the PSA-to-MMB communication LAN.

For the setting of the PSA-to-MMB communication LAN, use the following procedure.

Note

In the following cases, you can use neither the screen display nor event notification function of PSA:

- [Interface] of [MMB-PSA IP Address] in the [Network Configuration] - [Network Interface] window of the MMB Web-UI is Disable
- The following operation (execution of the configuration command of PSA-to-MMB communication LAN) is not performed

1. Execute the PSA-to-MMB communication LAN setting command.

[PSA installation folder]\opt\FJSVpsa\sh\setpsalan.bat

Note

If the operating system has not been restarted after PSA installation, the PSA-to-MMB communication LAN setting command in step 1 will fail.

Execute the PSA-to-MMB communication LAN setting command after restarting the operating system.

2. Restart the operating system.

Performing the above procedure sets the following values.

<IP address>

172.30.0.<partition ID + 2>/24

Example: Partition ID of 2

172.30.0.4/24

<Communication settings>

Auto Negotiation off

Speed 100 Mbps

Duplex full

In the following cases, change the IP address setting.

- The automatically set IP address is the same as the IP address or subnet used for a production network or management network.
- You are configuring a new partition using a duplicate disk from another partition.
- The partition ID changes because a disk installed in a partition was moved to another partition.
- You are configuring a Windows cluster (MSCS) with partitions assigned the same number, with the cluster spanning cabinets. (The same IP addresses are assigned, so a configuration check detects an error indicating that a duplicate IP address was found.)

Change the IP address setting by using the following procedure. If you are changing the setting because of the above reason 1, you need to change the IP addresses of all partitions in the cabinet and the IP address of the PSA-to-MMB communication LAN on the MMB side to IP addresses in the same subnet. Change the IP addresses on the MMB side from the MMB Web-UI.

Notes

- Do not change the automatically set communication values. Otherwise, PSA-MMB communication may be disabled, making PSA functions unavailable.
- Change PSA-to-MMB LAN settings only after PSA installation. If changed before PSA installation, the settings are overwritten by the installation.

Configuring the network adapter for the PSA-to-MMB communication LAN

Configure the network adapter by using the following procedure.

Operations

1. Select [Control Panel] - [Network Connections].
>> A window displays a list of networks.

2. Select [PSANIF] from the displayed list. Then, select [Properties] from the right-click menu.

Notes

- If there is no connection named [PSANIF], PSA has probably not been installed. Always change the settings after PSA installation.
- Do not change the connection name [PSANIF]. Otherwise, the settings can be overwritten by the automatically set values in a PSA update.

3. Select [Internet Protocol (TCP/IP)]. Then, click the [Properties] button.

>> The [Internet Protocol (TCP/IP) Properties] dialog box appears.

4. Set the IP address and subnet mask.

5. To apply the NIC settings for the dedicated PSA-to-MMB communication LAN, restart PSA by using the following steps.

Select [Control Panel] - [Administrative Tools] - [Services].

Right-click [PRIMEQUEST Server Agent] in the right side of the window. Then, select [Restart].

Making settings through a remote desktop connection

To configure the PSA-to-MMB communication LAN through a remote desktop connection, you need a console session connection. Establish this connection by using the following procedure.

1. Select [Start] - [Run].

>> The [Run] dialog box appears.

2. Enter "mstsc /v:<servername/ip address>/console" in the [Open] field. Then, click the [OK] button.

Specify the connected server name or the IP address in <servername/ip address>. (You cannot specify its virtual IP address in the cluster.)

You can check the details of mstsc options by entering "mstsc /?".

6.3.2 Confirming management LAN settings

Make settings for the management LAN. If necessary, also configure any duplication with teaming or GLS, for example.

After completing the above network settings for the management LAN, perform the operations in [6.3.7 Setting the management LAN IP address](#).

Note

In the PRIMEQUEST environment, it is necessary to specify OFF for the STP function of the switch that connects to the management LAN used for communication with the MMB.

6.3.3 Setting the destinations of traps from a partition

For direct transfer of a PSA expansion trap from a partition, set the trap destination and PSA trap notification by using the following procedure.

Remarks

- SNMPv3 is not supported in Windows.

- Make settings only as needed. Operations management software needs these settings to manage events by partition.
- Even if this setting is skipped, traps are sent via the MMB.
- The trap destination must be running both a trap receiving application and a trap manager to be able to receive standard SNMP Service traps.

Operations

1. Edit the PSA installation folder\etc\opt\FJSPsa\usr\psatrap.conf file.

Example of setting PSA trap notification

```
[PSATRAP]
PSATRAP_SET=<0 or 1>
```

Setting value

- 1: Enables PSA trap notification from the partition.
- 0: Disables PSA trap notification from the partition.

Example of input

```
[PSATRAP]
PSATRAP_SET=1
```

2. Restart PSA to apply the settings.
For details on how to restart PSA, see [Restarting PSA](#).
3. Select [Control Panel] - [Administrative Tools].
4. Click [Computer Management].
5. Click [Services and Applications] - [Services] in the tree on the left.
6. Double-click [SNMP Service] in the right side of the window.
>> The [SNMP Service] dialog box appears.
7. Click the [Trap] tab.
8. Enter the specified community name in the [Community Name] field. Then, click [Add to List].
9. Click [Add] in [Trap Send Destination].
10. Enter the host name or IP address of the server receiving the trap (i.e., the trap destination). Then, click [Add].
11. Click [OK].

12. Click [Action] - [Restart] to restart SNMP Service.

Restarting PSA

1. Click [Start menu] - [Administrative Tools] - [Services].
2. Select [PRIMEQUEST Server Agent] in the right side of the window.
3. Select [Action] - [Restart] from the menu bar to restart PRIMEQUEST Server Agent.

How to confirm a trap destination setting

To confirm a trap destination setting, use the standard SNMP Service trap sent to restart SNMP Service in the above step 12. You can confirm the correct trap setting by checking whether the trap was received.

Remarks

The trap destination must be running both a trap receiving application and a trap manager to be able to receive standard SNMP Service traps.

The operation performed in step 12 on the trap source machine restarts SNMP Service.

After that operation, a Cold Start trap is posted to the trap receiving application at the trap destination. Cold Start is a standard SNMP Service trap.

snmptrapd runs on the Linux machine that is the trap destination to receive traps. snmptrapd outputs the following message to the system log. Confirm that the Linux machine received the trap normally.

```
Aug 17 14:50:03 pq-server snmptrapd[2600]: 2005-08-17 14:50:03 \  
pq-server.fujitsu.com  
[192.168.0.162] (via 192.168.0.162) TRAP,    SNMP v1, community \  
public SNMPv2-SMI::  
enterprises.211.1.31.1.2.100.3 Cold Start  Trap (0) Uptime: 0:00:00.00
```

\\: This indicates that there is no line feed.

6.3.4 Setting the destinations of traps and e-mail via the MMB

You can set the destinations of traps and e-mail via the MMB by using the MMB Web-UI.

For details on MMB trap destinations, see [7.5.2 Configuring SNMP](#). For details on e-mail destinations, see [3.3.9 Configuring Alarm E-Mail](#).

Remarks

- Make settings only as needed.
- Linkage to operations management software requires these settings.

6.3.5 Configuring the Windows Firewall

For operation with the Windows Firewall enabled, the following two ports must be set as exceptions to enable them to send and receive data from the MMB:

- TCP port 24450 used by PSA
- UDP port 161 used via SNMP

Add these ports by using the following procedure.

Operations

1. Select [Control Panel] - [Windows Firewall].
>> The [Windows Firewall] window appears.
2. Click the [Exceptions] tab. Then, click the [Add Port] button.
>> The [Add a Port] dialog box appears.

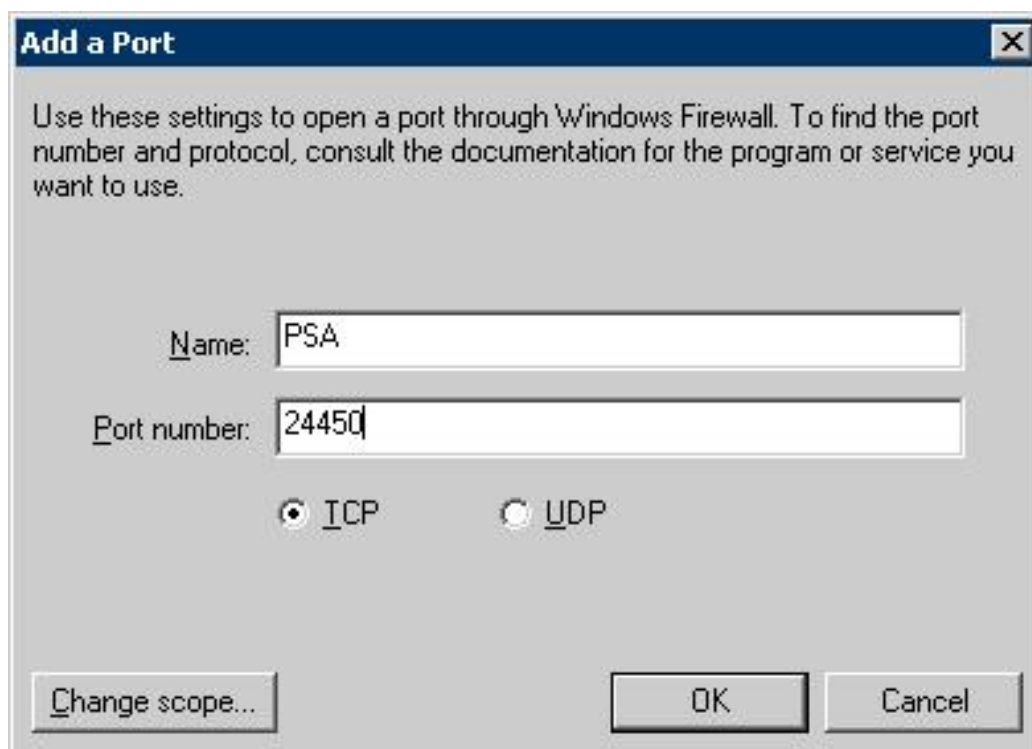


FIGURE 6.1 [Add a Port] dialog box (PSA)

3. Enter the port number used by PSA. Then, click the [OK] button.
4. Click the [Add Port] button again in the [Windows Firewall] window.
>> The [Add a Port] dialog box appears.

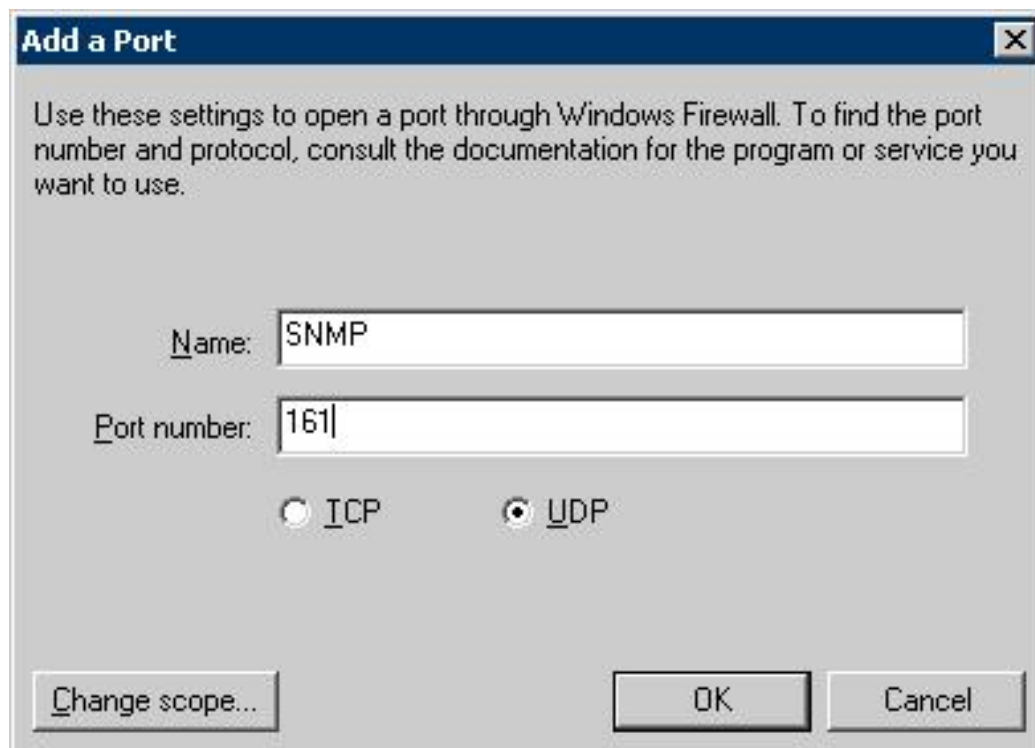


FIGURE 6.2 [Add a Port] dialog box (SNMP)

5. Enter the port number used by SNMP. Then, click the [OK] button.
6. Click the [OK] button in the [Windows Firewall] window.

6.3.6 Setting the Watchdog Timer for monitoring after a STOP error (fatal system error)

If a STOP error (fatal system error) occurs in the system, the following situation results.

- After you select [Partition] - [Power Control] from the MMB Web-UI, the window displays "Stop Error" under [System Progress] for the relevant partition.
- The system acquires a memory dump.

You can set monitoring with the Watchdog Timer to perform recovery after the system freezes or otherwise becomes unresponsive in the above event.

Immediately after the specified time elapses, the MMB performs a Hard Reset to reboot the operating system.

Operations

1. Open the following file:
PSA installation folder\etc\opt\FJSVpsa\usr\pnwatchdog.conf
Example: C:\fujitsu\FJSVpsa\etc\opt\FJSVpsa\usr\pnwatchdog.conf
2. Specify the value of the following key. The default is 0.
Section: [WATCHDOG]
Key: [TIMER]
Setting value (unit: seconds): 0 (Watchdog Timer disabled), 1 to 6000 (Watchdog Timer monitoring time)

Remarks

Determine the setting value by measuring the time taken for a memory dump in the applicable partition. If the measured time exceeds 6000 seconds (one hour and 40 minutes), specify 0 (Watchdog Timer disabled). If the specified time is too short for a memory dump, the Watchdog Timer times out and triggers a Hard Reset. In such cases, a memory dump cannot normally be acquired.

6.3.7 Setting the management LAN IP address

Set the partition management LAN IP address in PSA. For details on the management LAN, see 1.3 Management LAN in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

Note

Here, set the IP address on the partition instead of the IP address on the MMB.

Edit the *PSA installation folder* \etc\opt\FJSVpsa\usr\ipsetup.conf file.

Change the following IP address in an editor or similar application.

Syntax

```
[NETWORK]
ManagementIP=<management LAN IP address>
```

Example of input

```
[NETWORK]
ManagementIP=192.168.0.1
```

Restart PSA to reflect the new NIC settings for the management LAN.

Restarting PSA

1. Click [Start] - [Administrative Tools] - [Services].
2. Select [PRIMEQUEST Server Agent] in the right side of the window.
3. Select [Action] - [Restart] from the menu bar to restart PRIMEQUEST Server Agent.

6.3.8 Installing a PSA update

This section describes the PSA update installation procedure.

Remarks

For details on how to acquire fix programs, contact the distributor where you purchased your product, or your sales representative.

Operations

1. Save the fix program (fjpsaxxxx.exe) to your chosen folder.

Remarks

"xxxx" indicates the PSA version.

2. Start the saved fix program. The following window appears for installation preparations.

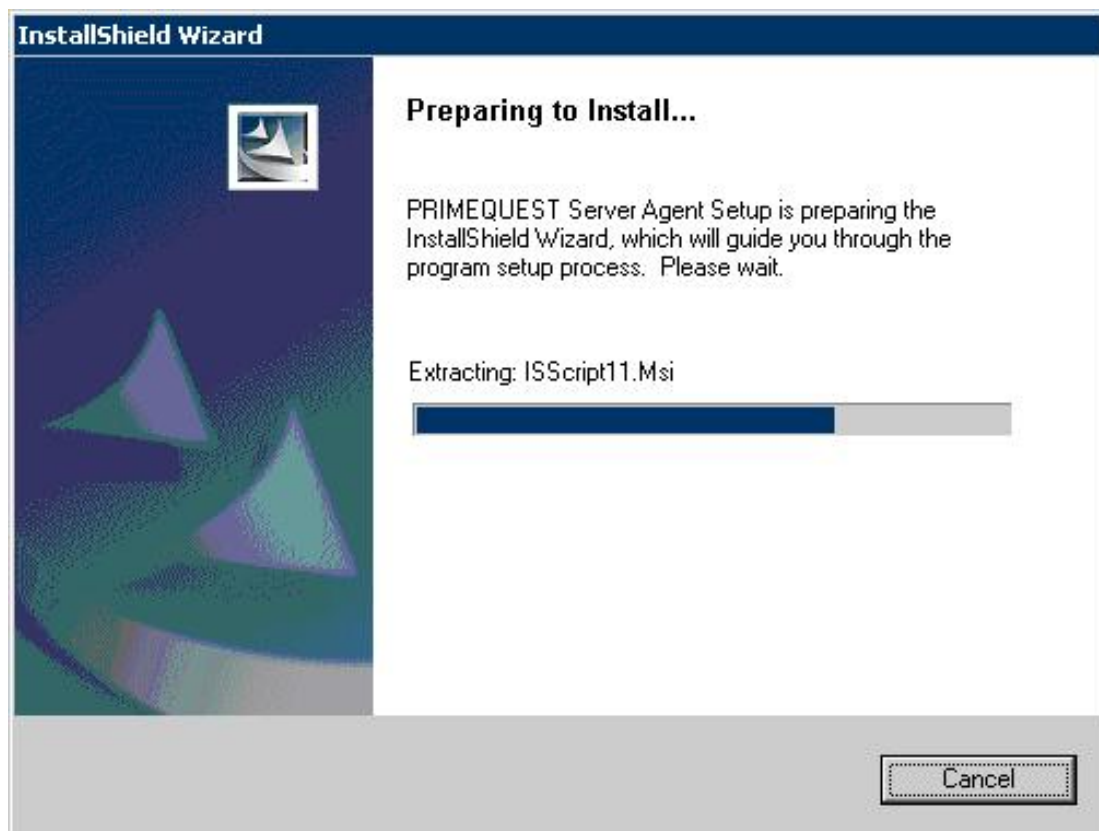


FIGURE 6.3 Preparing to Install window

3. The following window appears when installation preparations are completed. Click the [Next] button to proceed. The program update begins.

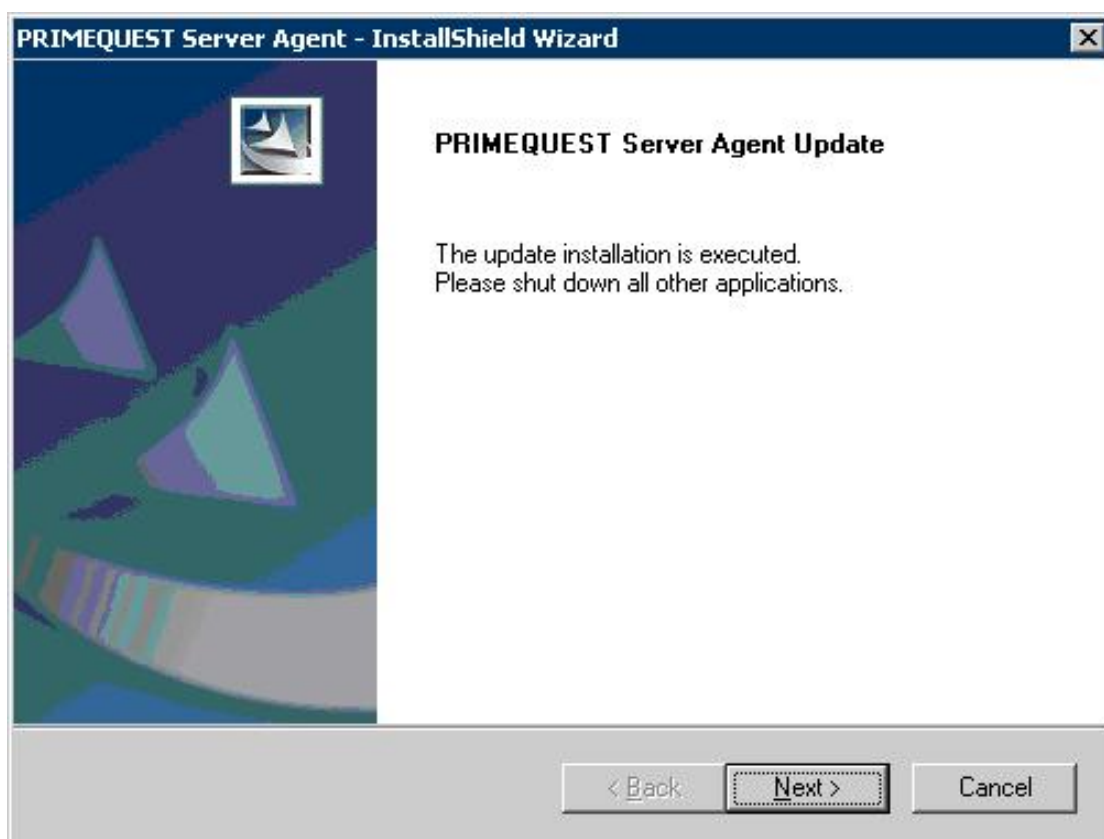


FIGURE 6.4 Update installation window

4. Click the [Finish] button.

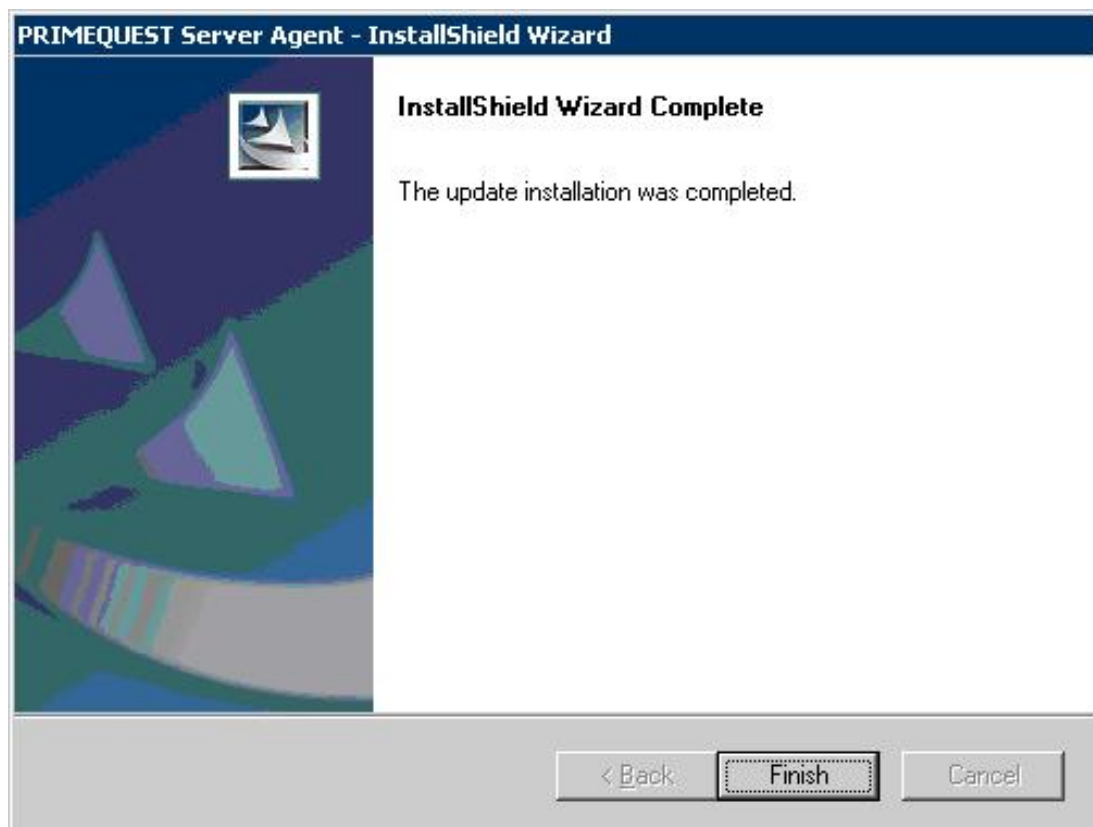


FIGURE 6.5 Update installation complete window

5. You may need to restart your computer. If so, a confirmation dialog box appears. The dialog box asks whether you want to restart the computer immediately. Check whether the computer can be restarted at this time. If the computer can be restarted, select the restart option and click the [Finish] button.

6.3.9 Uninstalling PSA

This section describes the PSA uninstallation procedure.

Remarks

Uninstalling PSA deletes all the files in the PSA installation folder. Save the necessary files before uninstallation. To confirm the PSA installation folder, check the environment variable (FJSVpsa_INSTALLPATH).

Operations

1. Select [Control Panel] - [Add or Remove Programs].
2. Select [PRIMEQUEST Server Agent] from the list of currently installed programs. Then, click [Change/Remove].
>> A deletion confirmation message appears.

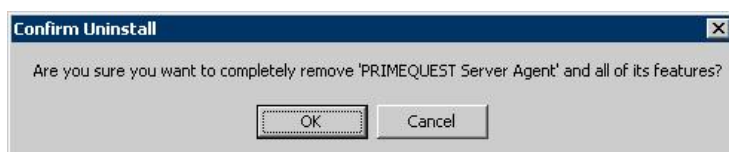


FIGURE 6.6 Confirmation message dialog box

3. Click the [OK] button.

>> Uninstallation begins.

Immediately after uninstallation is completed, the maintenance complete window appears.

4. Click the [Finish] button.

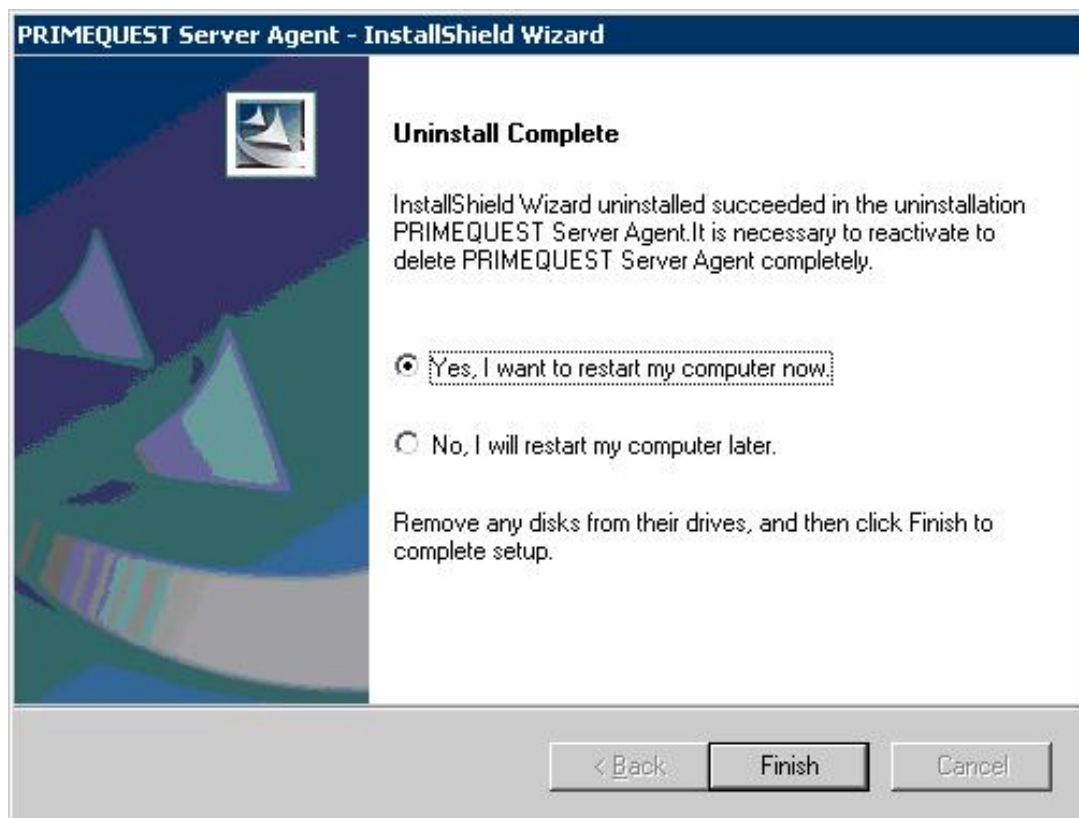


FIGURE 6.7 Uninstall Complete window

5. You may need to restart your computer. If so, a confirmation dialog box appears. The dialog box asks whether you want to restart the computer immediately. Check whether the computer can be restarted at this time. If the computer can be restarted, select the restart option and click the [Finish] button.

6.4 Configuring PSA (Windows Server 2008)

This section describes confirmation of the required settings for PSA operation after operating system installation, and corresponding features about the settings.

TABLE 6.9 Confirmation of the required settings for PSA operation, and corresponding features about the settings

Required/ As needed	Setting item	Automatic setting (*1)/ Manual setting (*2)	See
Required	Configuring the PSA-to-MMB communication LAN	Manual setting	6.4.1 Configuring the PSA-to-MMB communication LAN
	Confirming management LAN settings	Manual setting	6.4.2 Confirming management LAN settings
	Installing the PSBED Plugin driver	Manual setting	6.4.3 Installing the PSBED Plugin driver
	Configuring the Windows Firewall	Manual setting	6.4.6 Configuring the Windows Firewall
	Setting the management LAN IP address	Manual setting	6.4.8 Setting the management LAN IP address
As needed	Setting trap destinations	Manual setting	6.4.4 Setting the destinations of traps from a partition
	Setting the destinations of traps and e-mail via the MMB	Manual setting	6.4.5 Setting the destinations of traps and e-mail via the MMB
	Setting Watchdog for monitoring after a STOP error (fatal system error)	Manual setting	6.4.7 Setting the Watchdog Timer for monitoring after a STOP error (fatal system error)
	Installing a PSA update	Not applicable	6.4.9 Installing a PSA update
	Uninstalling PSA (*3)	Not applicable	6.4.10 Uninstalling PSA

*1 Automatic setting: Values are automatically set during PSA installation. You may need to change an automatically set value. See the section listed in the table.

*2 Manual setting: Values are not automatically set during PSA installation. Make settings as described in the section referred to in the table.

*3 To operate the PRIMEQUEST 1800E server, you need to first install PSA. Otherwise, the following restrictions apply.

- I/O (e.g., PCI Express card, hard disk) failure notification and trap notification to the administrator are disabled.
- Failure notification using symptom detection and trap notification to the administrator are disabled.
 - Threshold exceeded in S.M.A.R.T. monitoring of HDDs
- Operations management software cannot collect information on the partition side.

- Even under an REMCS agreement, no software errors are reported.

Remarks

- SVIM installs PSA as it installs the operating system. For details on SVIM, see the *ServerView Installation Manager*.
- The installer installs some components for REMCS function on the operating system side during PSA installation. Only Fujitsu certified service engineers make settings for REMCS.
 The following table lists settings for PSA operation. The installer automatically adds or updates these settings during PSA installation.

Note

Do not change the settings that were automatically added or changed during PSA installation. Otherwise, PSA may not operate normally.

TABLE 6.10 Settings automatically added/changed during PSA installation

Item	Description
1. Service settings	- PRIMEQUEST Server Agent - PRIMEQUEST PEM Command Service - PRIMEQUEST PSA Environment Control Service
2. Environment variable settings	- PATH variable: Adds the value used by PSA to the existing PATH variable. - FJSVpsa_INSTALLPATH variable: Adds a new variable.
3. Port settings	It sets PSA to use the TCP:24450 port.
4. SNMP security settings	Security is set for SNMP Service because PSA needs to accept SNMP packets from the MMB. The task varies depending on the parameter selected on the [Security] tab in the [SNMP Service Properties] window during PSA installation. - With [Accept SNMP packets from any host] selected: SNMP security is not configured. - With [Accept SNMP packets from these hosts] selected: If neither the MMB IP address nor localhost is specified, localhost and SNMP security are configured.
5. WMI (Windows Management Instrumentation) settings	PSA uses WMI to acquire information on PCI Express cards and SCSI devices. WMI is installed as standard with Windows. These settings include settings on the size of memory and number of internal handles used by WMI to collect this information. If the system has many LUNs for devices such as RAIDs, it may not have sufficient memory or internal handles. For this reason, the settings are changed to the following values: - Upper limit on memory used: 536,870,912 bytes (default of the operating system) - Upper limit on internal handles: 65,536

Remarks

- Execute the SNMP security setting command (setsnmpsec) in the following situations. For details on the command, see 4.8 SNMP Security Setting Command (setsnmpsec) in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).
 - Having installed PSA, you will be changing the SNMP Service security setting from [Accept SNMP packets from any host] to [Accept SNMP packets from these hosts].
 - You will be changing the MMB IP address.
- In the initial startup of PSA following installation, the Web-UI may display the error message "E_33077 PSA is Not Active. (01:0000)" in the [PSA] window. This happens because PSA requires extra time to acquire system sensor data only during the initial startup. Wait a few minutes. Then, refresh the display.
- If you change the MMB IP address or the management LAN IP address on the partition, be sure to then restart PSA. Otherwise, a display error may occur in the [PSA] window of the Web-UI. Moreover, PSA would not be able to report detected errors.

Notes on configuring Windows Server 2008

- From [Properties] in the Event Viewer, do not change the operation in [When maximum log size is reached] for the system log or application log to [Do not overwrite events (clear log manually)]. Otherwise, after the log reaches the maximum log size, no errors are output to the log, so PSA will be unable to detect any errors.
- Do not stop the Windows Print Spooler service. The information collection function of the operating system uses WMI to collect configuration information. If the Print Spooler service is stopped, the function cannot collect the correct configuration information because WMI reports an error.
- If the set value of the following registry key is less than 20000 (20 seconds), the system may hang during operating system shutdown. Be sure to set a value equal to or greater than 20000 (20 seconds).

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control "WaitToKillServiceTimeout" (Type: REG_DWORD / Default;20000)

You can use the above registry key to specify the wait time (ms) before the service is terminated in the shutdown sequence.

6.4.1 Configuring the PSA-to-MMB communication LAN

You can configure the PSA-to-MMB communication LAN by using the same procedure as that for Windows Server 2003. For details, [6.3.1 Configuring the PSA-to-MMB communication LAN](#).

6.4.2 Confirming management LAN settings

Make settings for the management LAN. If necessary, also configure any duplication with teaming or GLS, for example.

After completing the above network settings for the management LAN, perform the operations in [6.4.8 Setting the management LAN IP address](#).

Note

In the PRIMEQUEST environment, it is necessary to specify OFF for the STP function of the switch that connects to the management LAN used for communication with the MMB.

6.4.3 Installing the PSHER Plugin driver

The PSHER Plugin driver expands the WHEA (Windows Hardware Error Architecture) functions.

This driver is not automatically installed. Manually install the driver with the batch file (plugin_install.bat) stored in the following folder.

PSA installation folder \fjpsaplg\plugin_install.bat
(Example: C:\Program Files (x86)\Fujitsu\FJSVpsa\fjpsaplg\plugin_install.bat)

Remarks

The following functions do not work unless the driver is installed:

- Suppression of logging of Correctable Error events to the Event Viewer (Windows system event log)
- State transition to Stop Error for a Blue Screen of Death event ([System Progress] in the [Power Control] window of the MMB Web-UI)

Notes

- Do not execute the installation batch more than once.
If it is executed more than once, as many PRIMEQUEST PSHER Plugin drivers as the number of times executed are installed.
- If the installation batch is executed multiple times, no operational problems occur but multiple PRIMEQUEST PSHER Plugin drivers are displayed by the Device Manager.
In this case, uninstall all the PRIMEQUEST PSHER Plugin drivers and then reinstall one according to the following procedure. After the reinstallation, the operating system must be restarted.
 1. Record the number of times [PRIMEQUEST PSHER Plugin Driver] appears under [System Devices] in the Device Manager.
 2. Execute the following PSHER Plugin driver uninstallation batch as many times as the number recorded in step 1.

PSHER Plugin driver uninstallation batch storage location:
PSA uninstallation folder \fjpsaplg\plugin_uninstall.bat
(Default: C:\Program Files (x86)\Fujitsu\FJSVpsa\fjpsaplg
\plugin_uninstall.bat)

3. Restart the operating system.
4. Confirm that no [PRIMEQUEST PSHER Plugin Driver] appears under [System Devices] in the Device Manager.
5. Reinstall the PRIMEQUEST PSHER Plugin driver according to [Operations](#) below.

Operations

1. Open the following folder, and double-click [plugin_install.bat].

PSA installation folder \fjpsaplg
(Example: C:\Program Files (x86)\Fujitsu\FJSVpsa\fjpsaplg)

2. Restart the operating system. Then, the driver starts running.

3. Confirm that [PRIMEQUEST PSHED Plugin Driver] appears under [System Devices] in the Device Manager. If the Device Manager does not display the driver, repeat the procedure from step 1.

6.4.4 Setting the destinations of traps from a partition

For direct transfer of a PSA expansion trap from a partition, set the trap destination and PSA trap notification by using the following procedure.

Remarks

- SNMPv3 is not supported in Windows.
- Make settings only as needed. Operations management software needs these settings to manage events by partition.
- Even if this setting is skipped, traps are sent via the MMB.
- The trap destination must be running both a trap receiving application and a trap manager to be able to receive standard SNMP Service traps.

Operations

1. Edit the *PSA installation folder\etc\opt\FJSVpsa\usr\psatrap.conf* file.

Example of setting PSA trap notification

```
[PSATRAP]
PSATRAP_SET=<0 or 1>
```

Setting value

- 1: Enables PSA trap notification from the partition.
- 0: Disables PSA trap notification from the partition.

Example of input

```
[PSATRAP]
PSATRAP_SET=1
```

2. Restart PSA to apply the settings.
For details on how to restart PSA, see [Restarting PSA](#).
3. Click [Start] - [Administrative Tools] - [Services].
4. Double-click [SNMP Service] in the right side of the window.
>> The [SNMP Service Properties] dialog box appears.
5. Click the [Trap] tab.
6. Enter the specified community name in the [Community Name] field. Then, click [Add to List].

7. Click [Add] in [Trap Send Destination].

Enter the host name or IP address of the server receiving the trap (i.e., the trap destination). Then, click [Add].
Click the [OK] button.

8. Select [Action] - [Restart] from the menu bar to restart SNMP Service.

Restarting PSA

1. Click [Start menu] - [Administrative Tools] - [Services].
2. Select [PRIMEQUEST Server Agent] in the right side of the window.
3. Select [Action] - [Restart] from the menu bar to restart PRIMEQUEST Server Agent.

How to confirm a trap destination setting

To confirm a trap destination setting, use the standard SNMP Service trap sent to restart SNMP Service in the above step 8. You can confirm the correct trap setting by checking whether the trap was received.

Remarks

The operation performed in step 8 on the trap source machine restarts SNMP Service.

After that operation, a Cold Start trap is posted to the trap receiving application at the trap destination. Cold Start is a standard SNMP Service trap.

snmptrapd runs on the Linux machine that is the trap destination to receive traps. snmptrapd outputs the following message to the system log. Confirm that the Linux machine received the trap normally.

```
Aug 17 14:50:03 pq-server snmptrapd[2600]: 2005-08-17 14:50:03 \  
pq-server.fujitsu.com  
[192.168.0.162] (via 192.168.0.162) TRAP, SNMP v1, community \  
public SNMPv2-SMI::  
enterprises.211.1.31.1.2.100.3 Cold Start Trap (0) Uptime: 0:00:00.00
```

\: This indicates that there is no line feed.

6.4.5 Setting the destinations of traps and e-mail via the MMB

You can set the destinations of traps and e-mail via the MMB by using the MMB Web-UI.

For details on MMB trap destinations, see [7.5.2 Configuring SNMP](#). For details on e-mail destinations, see [7.4 Configuring SMTP](#).

Remarks

- Make settings only as needed.
- Operations management software needs these settings to manage events by partition.

6.4.6 Configuring the Windows Firewall

For operation with the Windows Firewall enabled, the following ports must be open to enable them to send and receive data from the MMB.

- SNMP Service uses UDP port 161 (to receive data from the MMB).
- fipsawg.exe uses TCP port 24450 (to receive data from the MMB).
- fipsammbs.exe uses a port to send data to the MMB (TCP port 5000 on the MMB side).
- fipsammbs.exe uses ICMP as the protocol for the MMB.

Operations

1. Select [Start] - [Administrative Tools] - [Windows Firewall with Advanced Security].
2. The [Windows Firewall with Advanced Security] window appears. Click [Inbound Rules] in the left pane. The [Inbound Rules] list appears in the center pane.

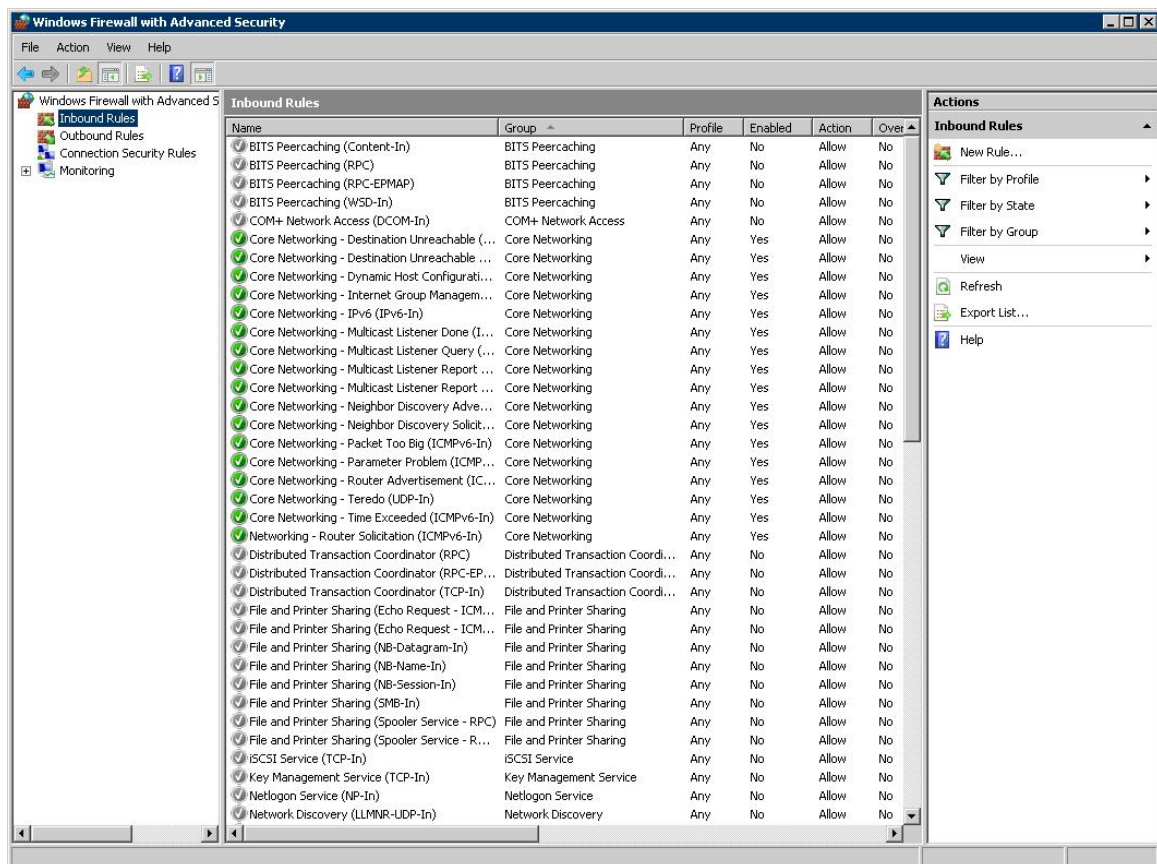


FIGURE 6.8 Windows Firewall window

3. Select and right-click [SNMP Service (UDP In)] in the [Inbound Rules] list. Then, click [Properties]. The two default profiles for SNMP Service (UDP In) are [Domain] and [Private, Public]. Perform steps 3 to 7 for both profiles.
4. The [SNMP Service (UDP In) Properties] dialog box appears. Click the [General] tab. Then, check the [Enabled] check box in [General] (checked by default).

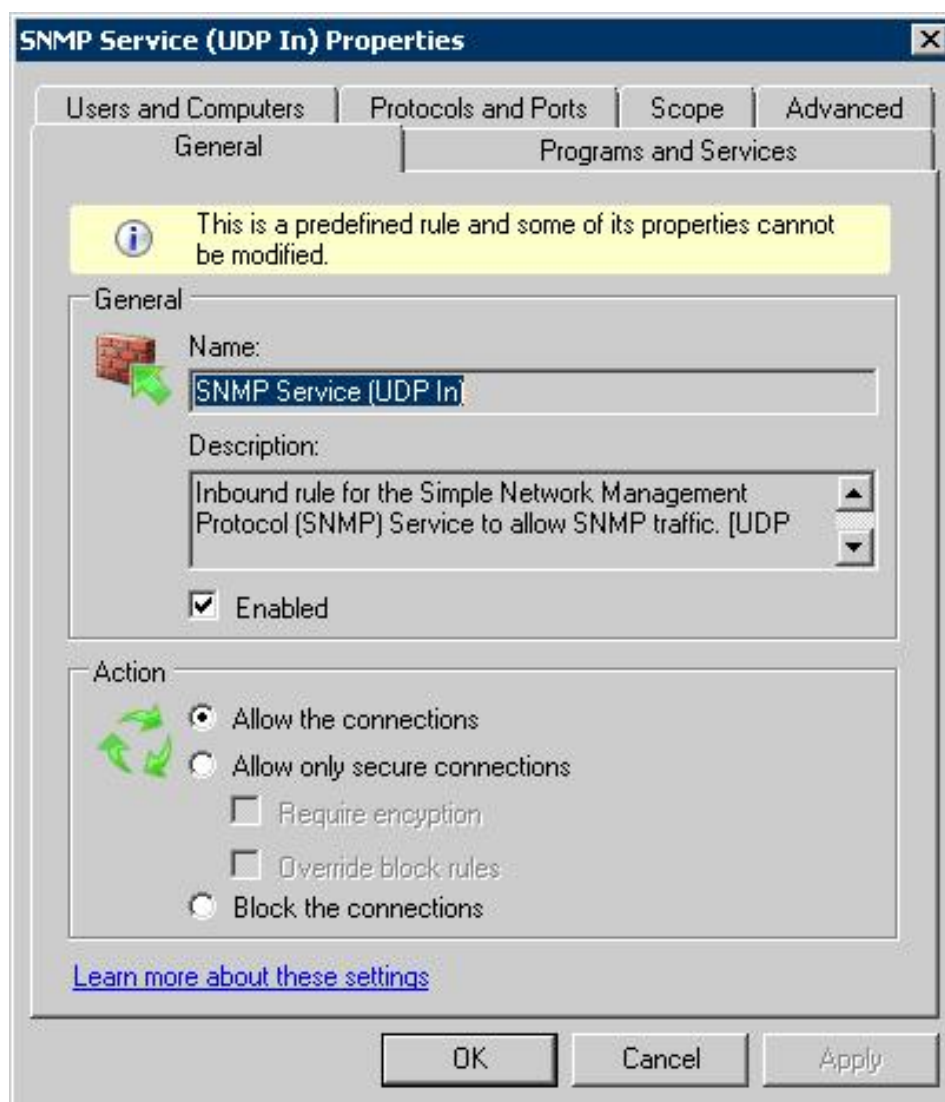


FIGURE 6.9 [General] tab in [SNMP Service (UDP In) Properties]

5. Click the [Scope] tab.
Select [Any IP address] for [Local IP Address].
Select [These IP Addresses] in [Remote IP Address]. Then, click the [Add] button.

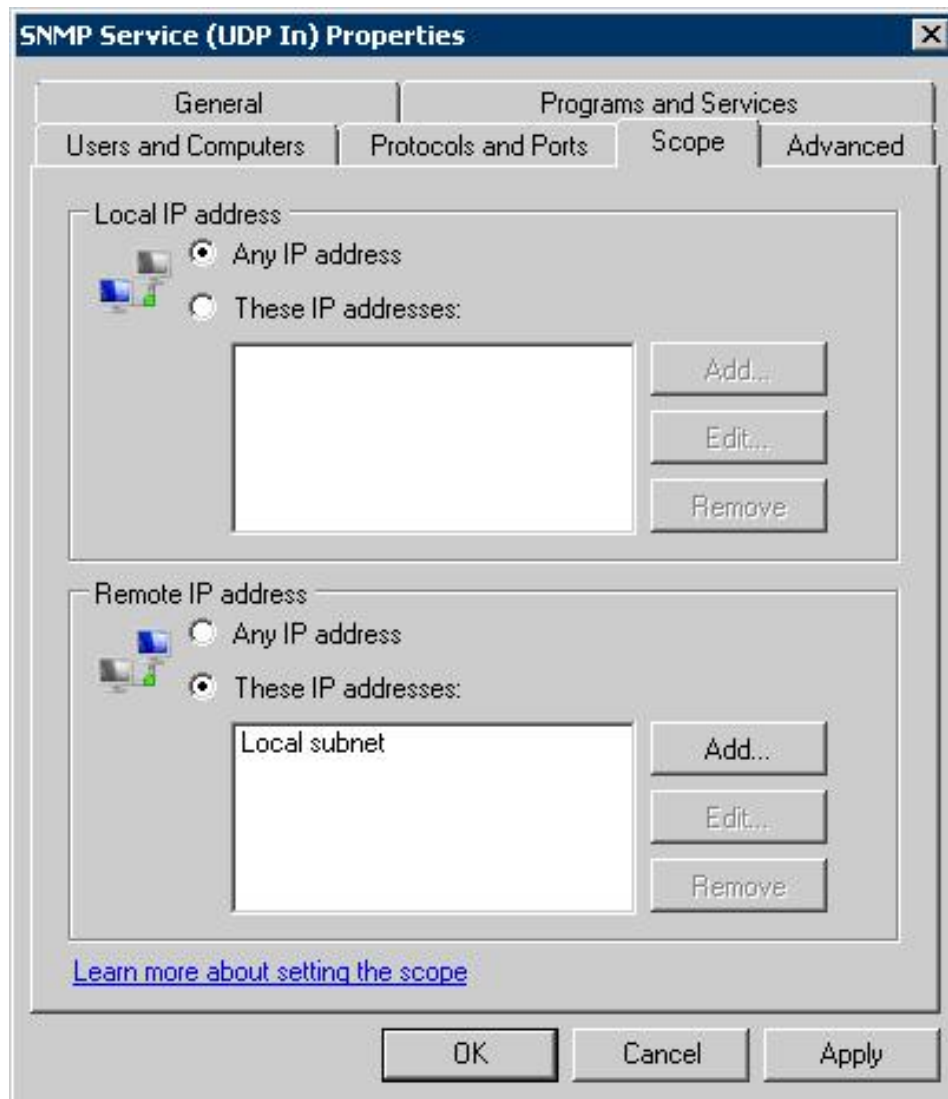


FIGURE 6.10 [Scope] tab in [SNMP Service (UDP In) Properties]

6. The [IP Address] dialog box appears. Click [Predefined set of computers].
Select [Local subnet] from the list. Then, click the [OK] button.

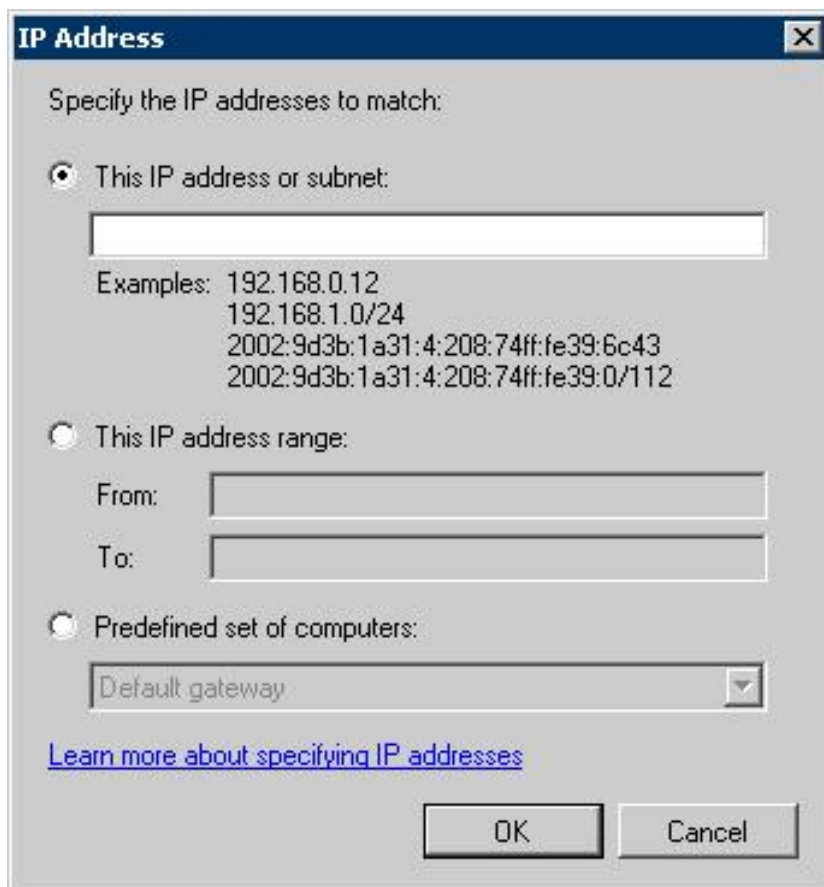


FIGURE 6.11 [IP Address] dialog box

7. Click the [OK] button to close the [SNMP Service (UDP In) Properties] dialog box.
8. Click [New Rule] in the right pane of the [Windows Firewall with Advanced Security] window. The [New Inbound Rule Wizard] window appears with [Rule Type] displayed at the top left. Select [Custom]. Then, click the [Next] button.

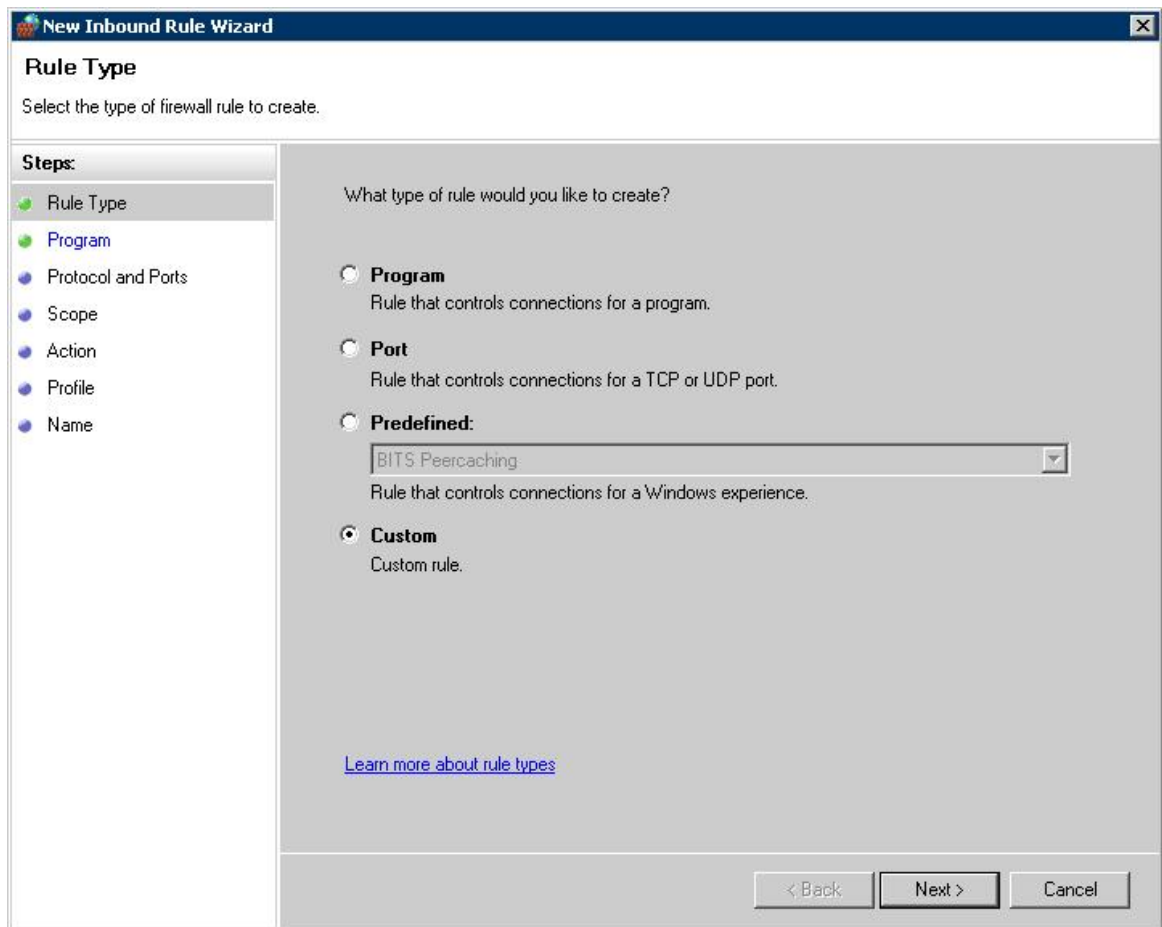


FIGURE 6.12 New Inbound Rule Wizard - Rule Type

9. The wizard displays the [Program] window, as indicated at the upper left. Select [This program path]. Then, click the [Browse] button.
Select "fjpsawg.exe." Then, click the [Next] button.

Remarks

fjpsawg.exe is in opt\FJSVpsa\bin\ in the PSA installation path. The default installation path for PSA is Program Files\fujitsu\FJSVpsa\ or Program Files (x86)\Fujitsu.

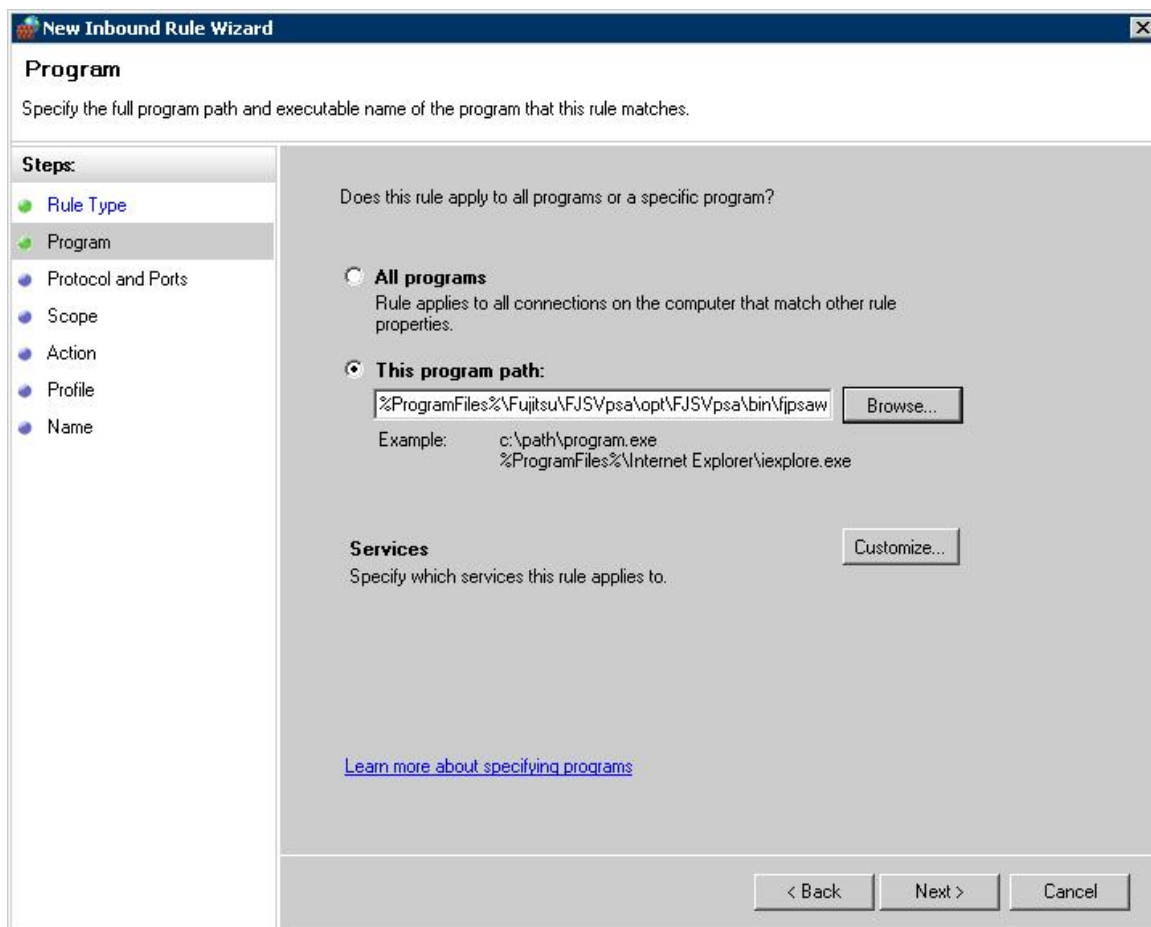


FIGURE 6.13 New Inbound Rule Wizard - Program

- The wizard displays the [Protocol and Ports] window, as indicated at the upper left. Select or enter values for the following items. Then, click the [Next] button.

TABLE 6.11 [Protocol and Ports] setting items

Window item	Selected or entered value
Protocol type	TCP
Local port	Select [Specific Ports]. Then, enter 24450 in the text box below it.
Remote port	All Ports

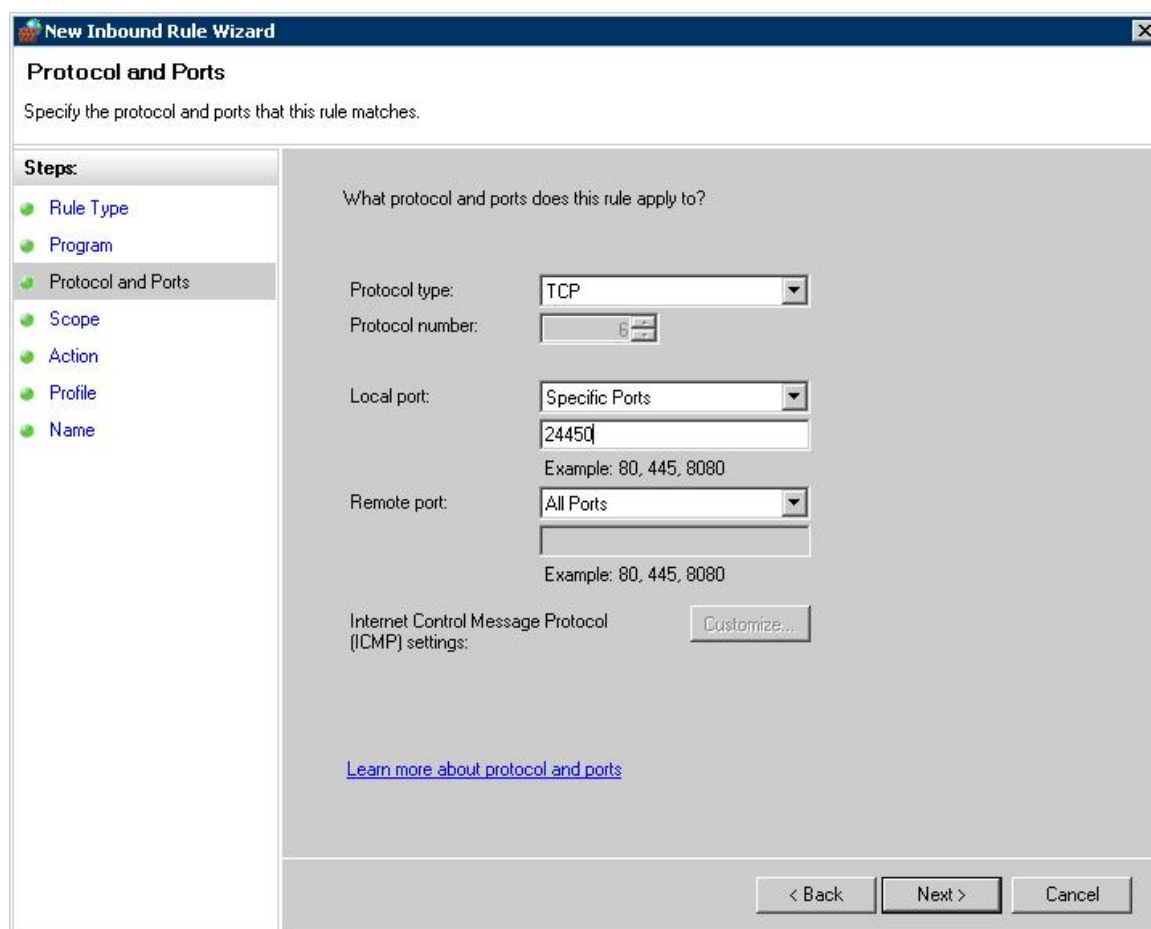


FIGURE 6.14 New Inbound Rule Wizard - Protocol and Ports

11. The wizard displays the [Scope] window, as indicated at the upper left. Select or enter values for the following items. Then, click the [Next] button.

TABLE 6.12 [Scope] setting items

Window item	Selected or entered value
Which local IP addresses does this rule match?	Any IP address
Which remote IP addresses does this rule match?	Select [These IP addresses]. Then, click the [Add] button. Enter the IP address of the PSA-to-MMB communication LAN on the MMB side.

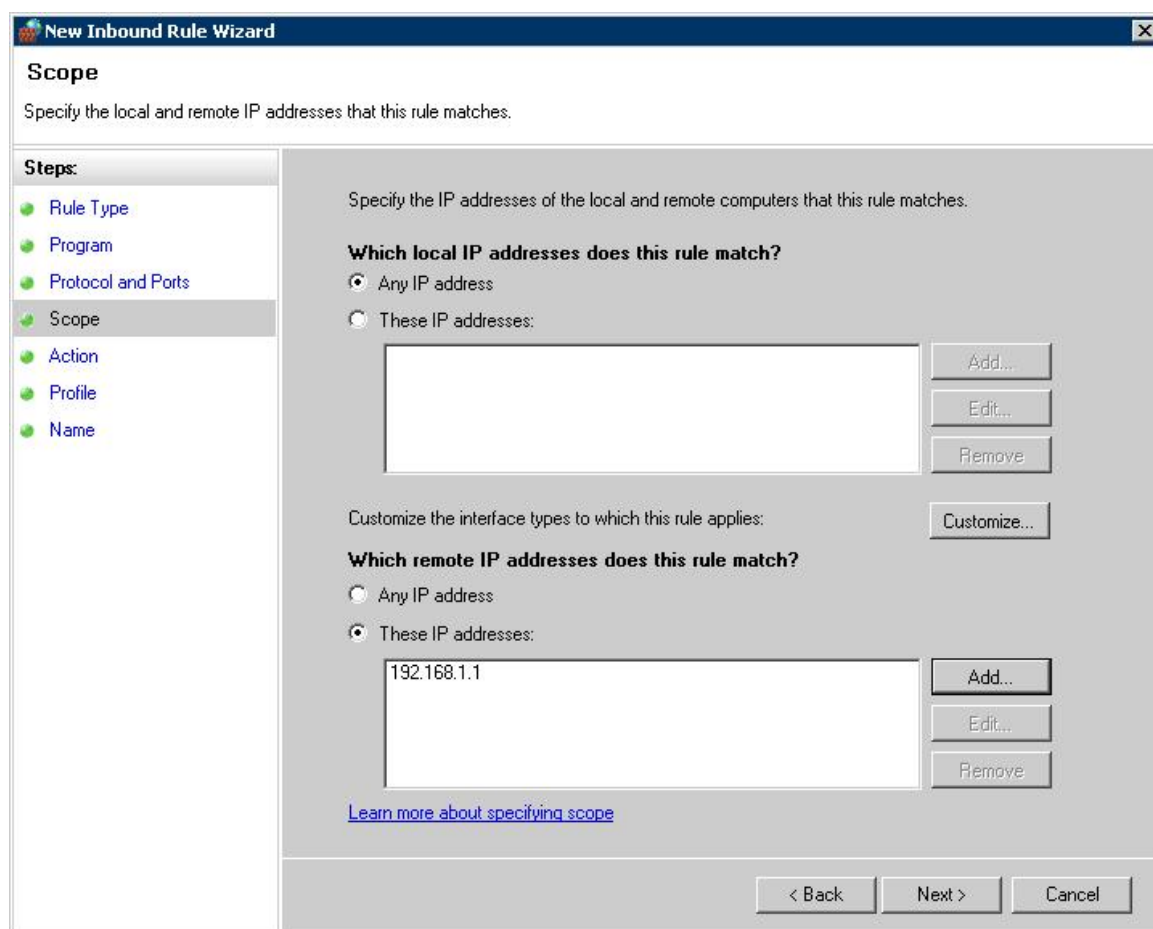


FIGURE 6.15 New Inbound Rule Wizard - Scope

12. The wizard displays the [Action] window, as indicated at the upper left. Select [Allow the connection]. Then, click the [Next] button.

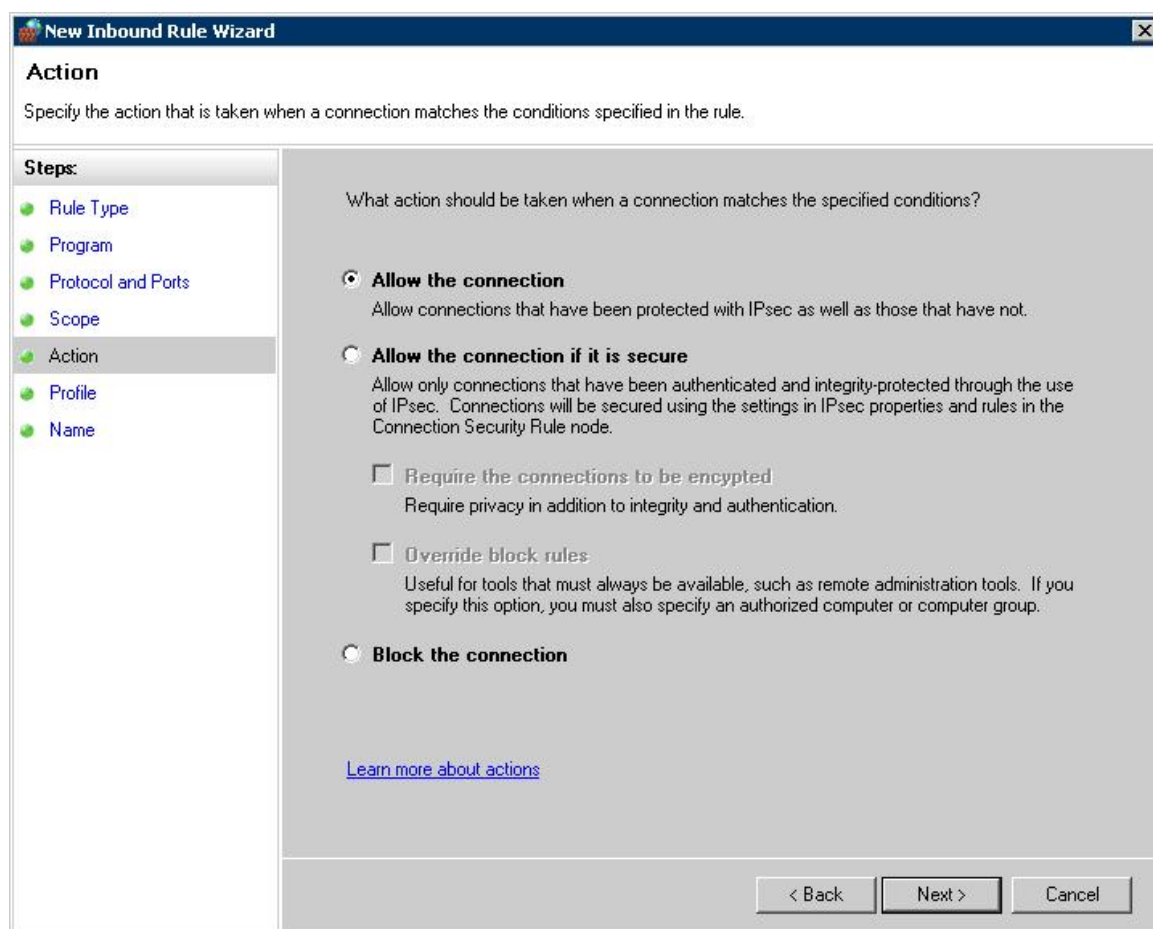


FIGURE 6.16 New Inbound Rule Wizard - Action

13. The wizard displays the [Profile] window, as indicated at the upper left. Check all the [Domain], [Private], and [Public] check boxes. Then, click the [Next] button.

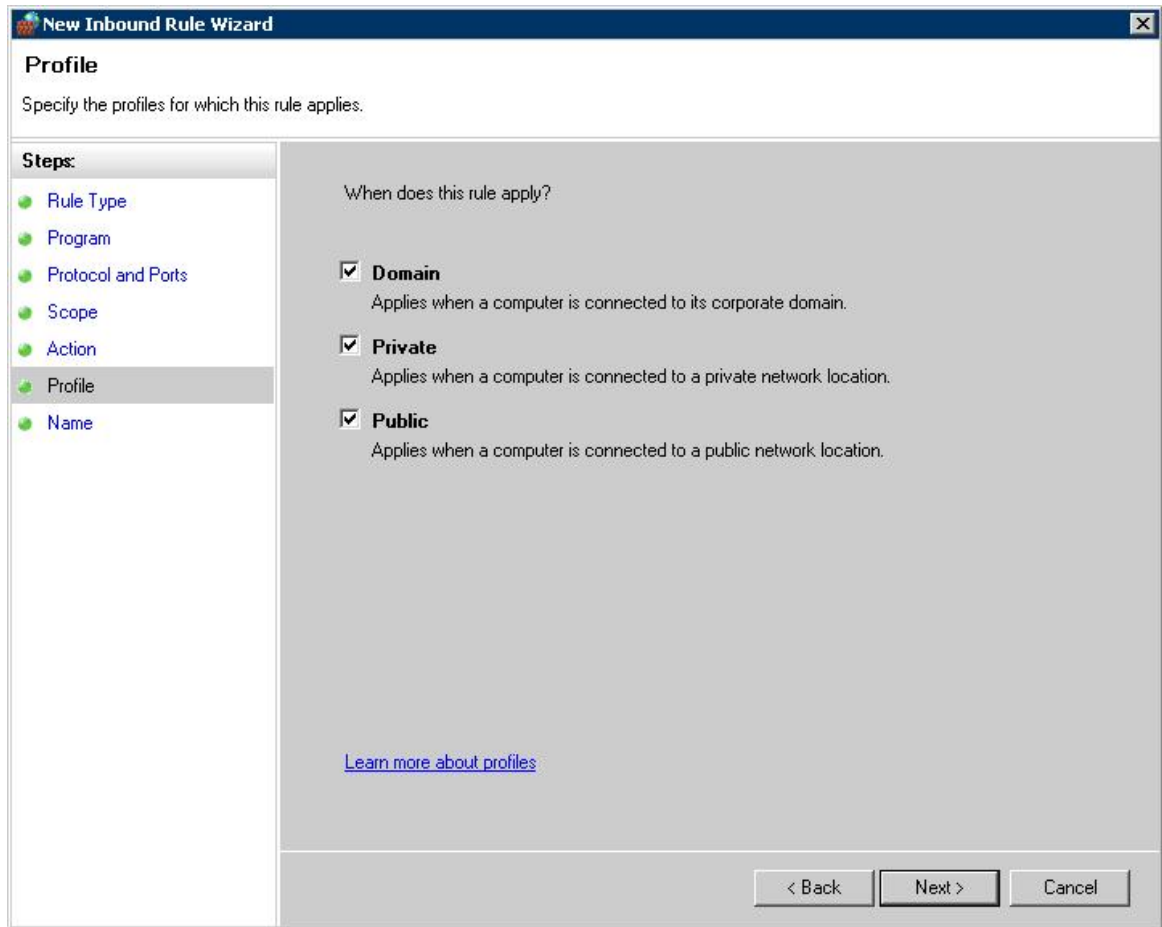


FIGURE 6.17 New Inbound Rule Wizard - Profile

14. The wizard displays the [Name] window, as indicated at the upper left. Enter "PSAWG" in [Name]. Then, click the [Finish] button.

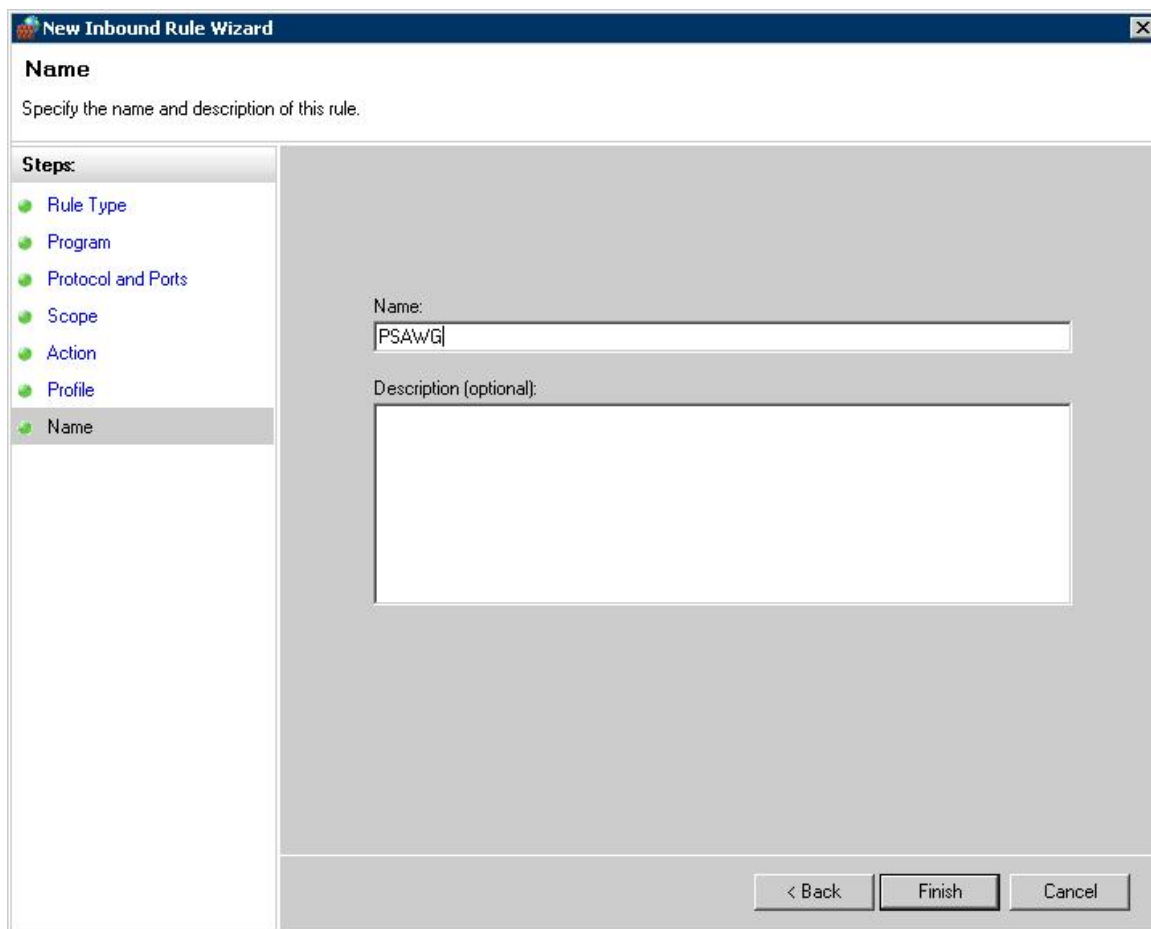


FIGURE 6.18 New Inbound Rule Wizard - Name

15. Click [Outbound Rules] in the left pane of the [Windows Firewall with Advanced Security] window. The [Outbound Rules] list appears in the center pane.
16. Click [New Rule] in the right pane of the [Windows Firewall with Advanced Security] window. The [New Outbound Rule Wizard] window appears with [Rule Type] displayed at the top left. Select [Custom]. Then, click the [Next] button.
17. The wizard displays the [Program] window, as indicated at the upper left. Select [This program path]. Then, click the [Browse] button. Select "fjpsammb.exe." Then, click the [Next] button.

Remarks

fjpsammb.exe is in opt\FJSVpsa\bin\ in the PSA installation path. The default installation path for PSA is Program Files\fujitsu\FJSVpsa\.

18. The wizard displays the [Protocol and Ports] window, as indicated at the upper left. Select or enter values for the following items. Then, click the [Next] button.

TABLE 6.13 [Protocol and Ports] setting items

Window item	Selected or entered value
Protocol type	TCP
Local port	All Ports
Remote port	Select [Specific Ports]. Then, enter 5000 in the text box below it.

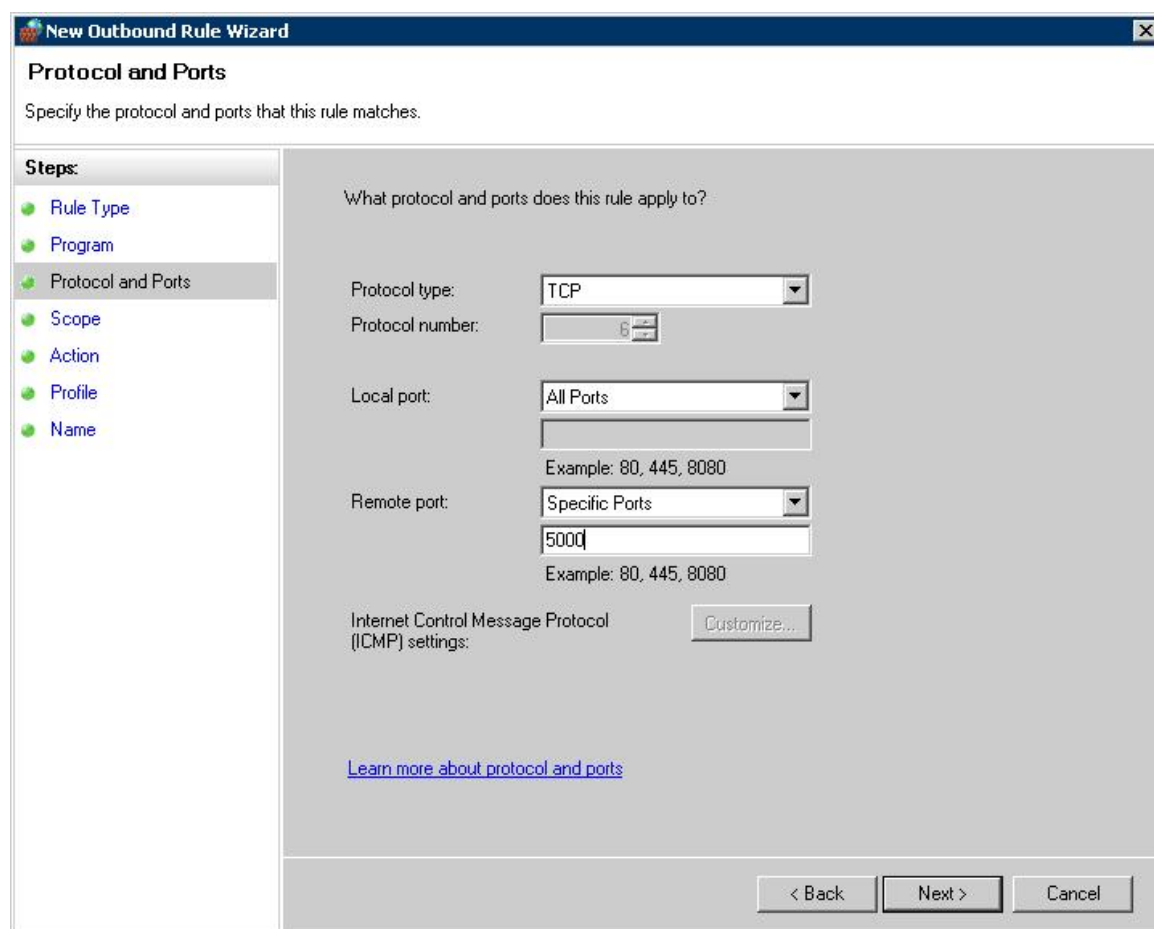


FIGURE 6.19 New Outbound Rule Wizard - Protocol and Ports

- The wizard displays the [Scope] window, as indicated at the upper left. Select or enter values for the following items. Then, click the [Next] button.

TABLE 6.14 [Scope] setting items

Window item	Selected or entered value
Which local IP addresses does this rule match?	Any IP address
Which remote IP addresses does this rule match?	Select [These IP addresses]. Then, click the [Add] button.

Window item	Selected or entered value
	Enter the IP address of the PSA-to-MMB communication LAN on the MMB side.

20. The wizard displays the [Action] window, as indicated at the upper left. Select [Allow the connection]. Then, click the [Next] button.
21. The wizard displays the [Profile] window, as indicated at the upper left. Check all the [Domain], [Private], and [Public] check boxes. Then, click the [Next] button.
22. The wizard displays the [Name] window, as indicated at the upper left. Enter "PSAMMBS" in the [Name] field. Then, click the [Finish] button.
23. Click [New Rule] in the right pane of the [Windows Firewall with Advanced Security] window. The [New Outbound Rule Wizard] window appears with [Rule Type] displayed at the top left. Select [Custom]. Then, click the [Next] button.
24. The wizard displays the [Program] window, as indicated at the upper left. Select [This program path]. Then, click the [Browse] button. Select "fjpsammbs.exe." Then, click the [Next] button.

Remarks

fjpsammbs.exe is in opt\FJSVpsa\bin\ in the PSA installation path. The default installation path for PSA is Program Files\fujitsu\FJSVpsa\.

25. The wizard displays the [Protocol and Ports] window, as indicated at the upper left. Select [ICMPv4] in [Protocol type]. Then, click the [Next] button.

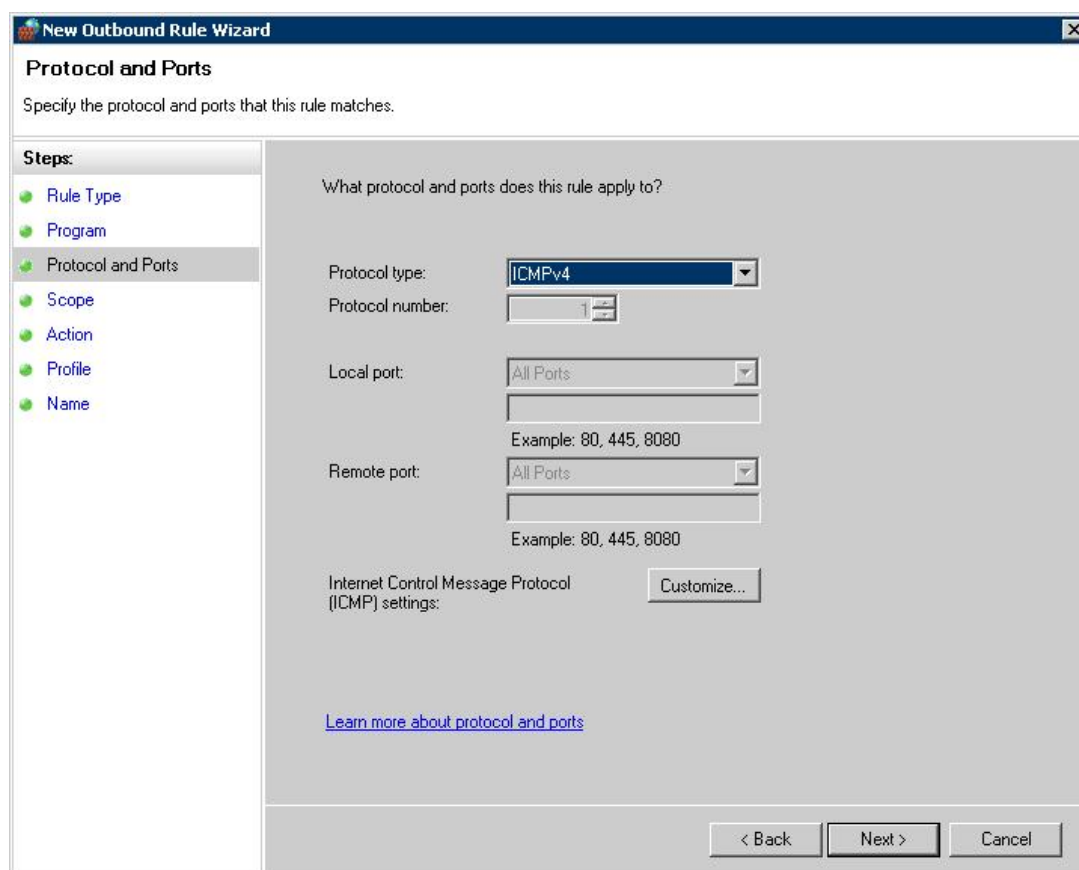


FIGURE 6.20 New Outbound Rule Wizard - Protocol and Ports

26. The wizard displays the [Scope] window, as indicated at the upper left. Select or enter values for the following items. Then, click the [Next] button.

TABLE 6.15 [Scope] setting items

Window item	Selected or entered value
Which local IP addresses does this rule match?	Any IP address
Which remote IP addresses does this rule match?	Select [These IP addresses]. Then, click the [Add] button. Enter the IP address of the PSA-to-MMB communication LAN on the MMB side.

27. The wizard displays the [Action] window, as indicated at the upper left. Select [Allow the connection]. Then, click the [Next] button.
28. The wizard displays the [Profile] window, as indicated at the upper left. Check all the [Domain], [Private], and [Public] check boxes. Then, click the [Next] button.
29. The wizard displays the [Name] window, as indicated at the upper left. Enter "PSAICMP" in [Name]. Then, click the [Finish] button.

6.4.7 Setting the Watchdog Timer for monitoring after a STOP error (fatal system error)

If a STOP error (fatal system error) occurs in the system, the following situation results.

- After you select [Partition] - [Power Control] from the MMB Web-UI, the window displays "Stop Error" under [System Progress] for the relevant partition.
- The operating system acquires a memory dump.

You can set monitoring with the Watchdog Timer to perform recovery after the system freezes or otherwise becomes unresponsive in the above event.

Immediately after the specified time elapses, the MMB performs a Hard Reset to reboot the operating system.

Operations

1. Open the following file:

PSA installation folder\etc\opt\FJSVpsa\usr\pnwatchdog.conf

Example: C:\fujitsu\FJSVpsa\etc\opt\FJSVpsa\usr\pnwatchdog.conf

2. Specify the value of the following key. The default is 0.

Section: [WATCHDOG]

Key: [TIMER]

Setting value (unit: seconds): 0 (Watchdog Timer disabled),

1 to 6000 (Watchdog Timer monitoring time)

Remarks

Determine the setting value by measuring the time taken for a memory dump in the applicable partition. If the measured time exceeds 6000 seconds (one hour and 40 minutes), specify 0 (Watchdog Timer disabled).

If the specified time is too short for a memory dump, the Watchdog Timer times out and triggers a Hard Reset. In such cases, a memory dump cannot normally be acquired.

6.4.8 Setting the management LAN IP address

Set the partition management LAN IP address in PSA. For details on the management LAN, see 1.3 Management LAN in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

Note

Here, set the IP address on the partition instead of the IP address on the MMB.

Edit the *PSA installation folder* \etc\opt\FJSVpsa\usr\ipsetup.conf file.

Change the following IP address in an editor or similar application.

Syntax

```
[NETWORK]
ManagementIP=<management LAN IP address>
```

Example of input

[NETWORK] Management IP=192.168.0.1

Restart PSA to reflect the new NIC settings for the management LAN.

Restarting PSA

1. Click [Start] - [Administrative Tools] - [Services].
2. Select [PRIMEQUEST Server Agent] in the right side of the window.
3. Select [Action] - [Restart] from the menu bar to restart PRIMEQUEST Server Agent.

6.4.9 Installing a PSA update

This section describes the PSA update installation procedure.

Remarks

- Using a fix program of the same version as the installed PSA version:
PSA uninstallation begins when you click the [OK] button in the confirmation message dialog box. After that, PSA is reinstalled.
- For details on how to acquire fix programs, contact the distributor where you purchased your product, or your sales representative.

Operations

1. Save the fix program (fjpsaxxxx.exe) to your chosen folder.
2. Start the saved fix program.
>> The following window appears for installation preparations.



FIGURE 6.21 Preparing to Install window

3. The following window appears when installation preparations are completed. Click the [Next] button to proceed.
>> The program update begins.

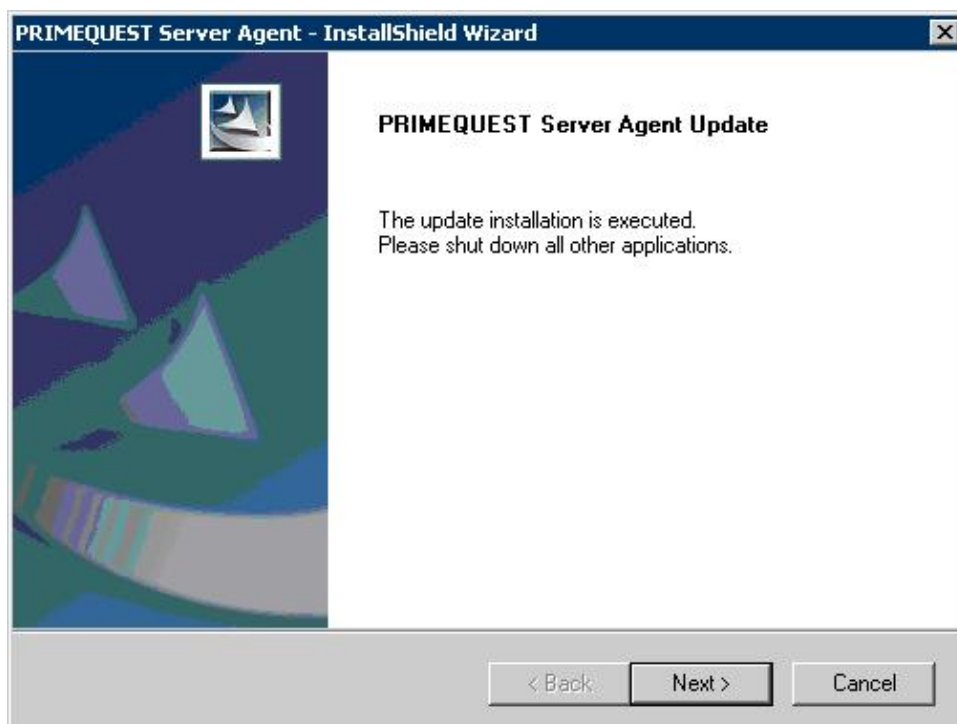


FIGURE 6.22 Update installation window

4. Click the [Install] button.

After completing PSA installation including an update to the PSLED Plugin driver, be sure to confirm that the operating system can be restarted before you restart the operating system.

5. Click the [Finish] button.



FIGURE 6.23 Update installation complete window

6. You may need to restart your computer. If so, a confirmation dialog box appears. The dialog box asks whether you want to restart the computer immediately. Check whether the computer can be restarted at this time. If the computer can be restarted, select the restart option and click the [Finish] button.

Remarks

If a fix program of the same version as the installed PSA was applied, the PSA uninstallation procedure begins. If you do not want to uninstall PSA, click the [Cancel] button in the program removal window.

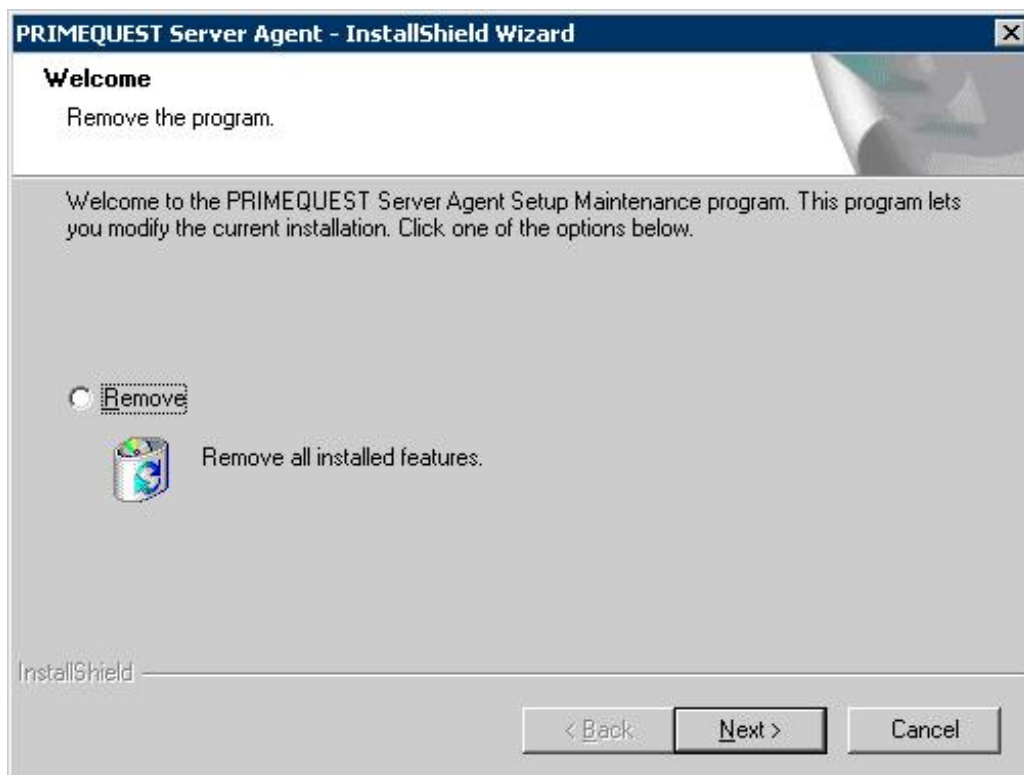


FIGURE 6.24 Program removal window

6.4.10 Uninstalling PSA

This section describes the PSA uninstallation procedure.

Remarks

Uninstalling PSA deletes all the files in the PSA installation folder. Save the necessary files before uninstallation. To confirm the PSA installation folder, check the environment variable (FJSVpsa_INSTALLPATH).

Operations

1. Select [Control Panel] - [Programs and Features].
The [Programs and Features] window appears.

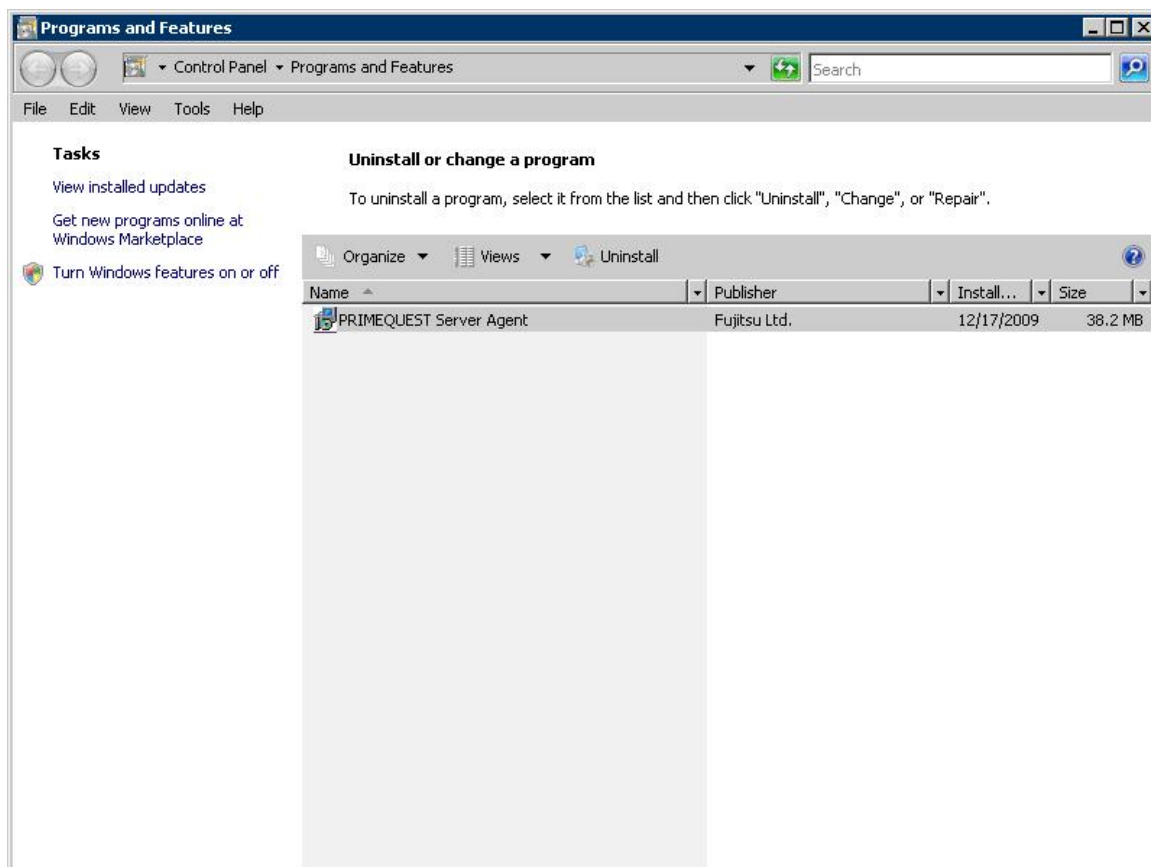


FIGURE 6.25 [Program and Features] window

2. Select [PRIMEQUEST Server Agent] from the list of currently installed programs. Then, click [Remove]. The Preparing to Install window appears. Then, a deletion confirmation message appears.

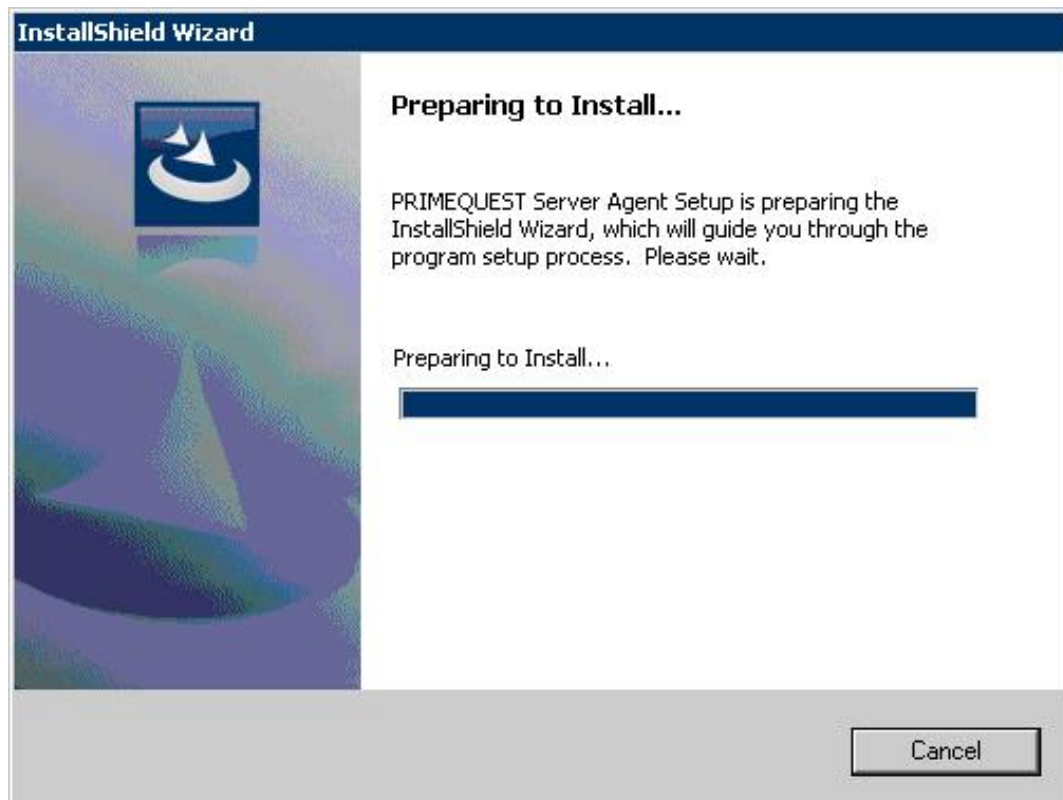


FIGURE 6.26 Preparing to Install window

3. Click the [Yes] button.
>> Uninstallation begins.

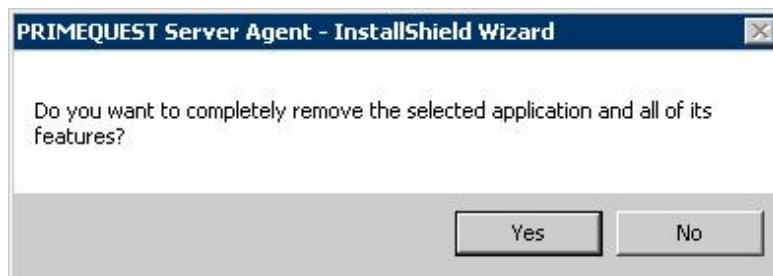


FIGURE 6.27 Confirmation message dialog box

Immediately after uninstallation is completed, the Uninstall Complete window appears.

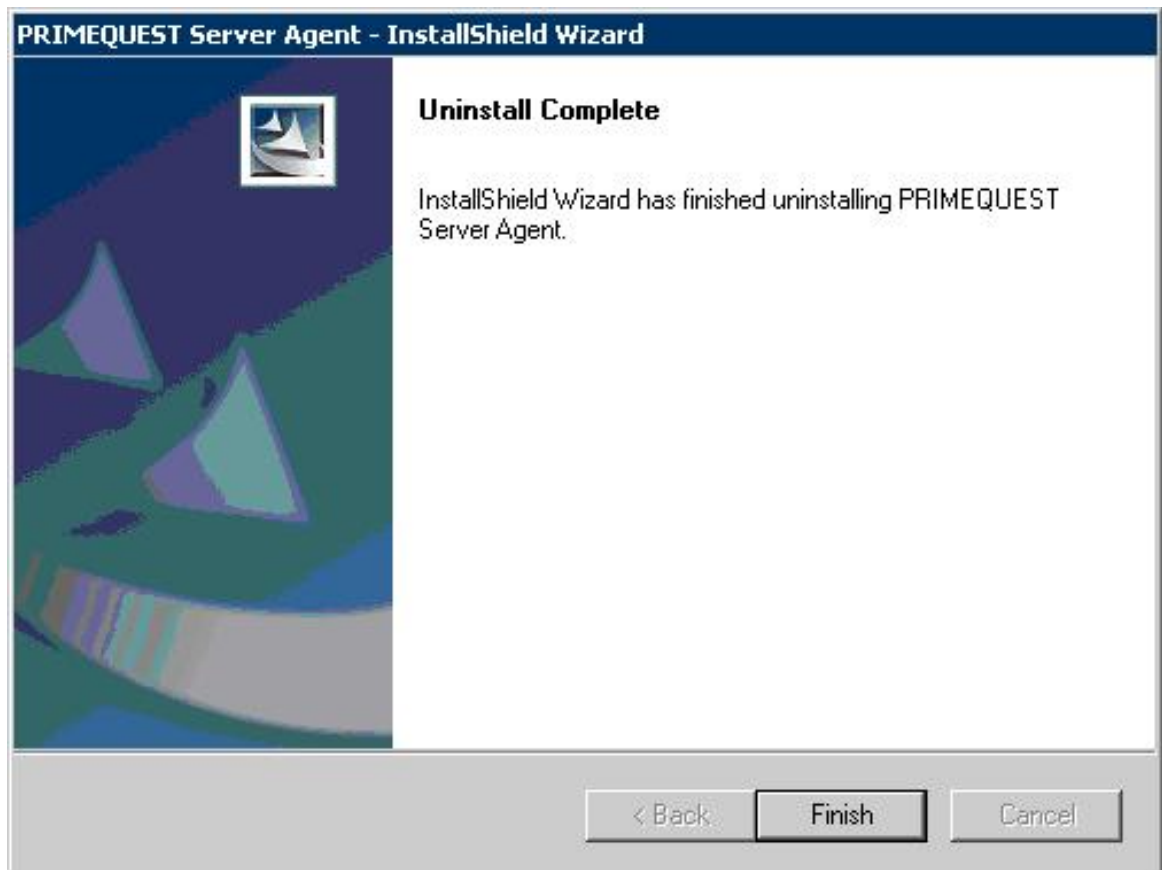


FIGURE 6.28 Uninstall Complete window

4. Click the [Finish] button.
5. To delete the PSLED Plugin driver, you need to restart the operating system. Be sure to confirm that the operating system can be restarted, before restarting it.

6.5 Setting Up the Dump Environment (Windows)

You can use the standard operating system functions of Windows to acquire dumps. Before you can acquire dumps, you need to allocate an area for them in the system.

For details on how to set up the dump environment, see 11.4.4 Setting up the dump environment (Windows) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

6.5.1 Memory dump files and paging files

A memory dump file stores debug information on any STOP error (fatal system error) that has occurred in the system. After installing the operating system and applications for operations, make settings for acquiring memory dumps.

For details on memory dumps and paging files, see 11.4.4 Setting up the dump environment (Windows) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

6.6 Setting Up the Dump Environment (Linux)

In RHEL, you can prepare an environment to enable secure acquisition of dumps by using the standard operating system function `kdump`.

6.7 Configuring the NTP Client

For details on how to configure the NTP client, see [7.2 Configuring NTP](#).

6.8 Saving Management and Configuration Information

This section describes how to save the following information. Be sure to save PSA management information and UEFI configuration information.

- [6.8.1 Saving PSA management information](#)
- [6.8.2 Saving MMB configuration information](#)
- [6.8.3 Saving BIOS configuration information](#)

Remarks

- Save PSA management information when changing the hardware or network configuration.
- Only the PRIMEQUEST 1800E supports the saving of PSA management information.
- After the start of actual business operation, save UEFI configuration information regularly. For details on how to save UEFI configuration information, see [6.8.3 Saving BIOS configuration information](#).

6.8.1 Saving PSA management information

You can save a snapshot of information in PSA by exporting it to the partition management area in CSV format. The export function can save up to 100 data files. After reaching 100 files, the function deletes the oldest file before saving a new file.

The exported data remains stored until deleted intentionally or deleted because the maximum number of files is exceeded.

Listing exported files

This section describes how to list the files. A window lists the current exported files in order with the latest files at the top.

The window displaying this list enables the following operations:

- Saving a snapshot of information in PSA to a file in CSV format
- Downloading an exported file to a terminal
- Deleting an exported file from the partition management area

Operations

1. Select [Partition] - [Partition#x] - [PSA] - [Export List].
>> The [Export List] window appears. For details on the [Export List] window, see 3.11 [Export List] Window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).



FIGURE 6.29 [Export List] window (example)

2. Click the button appropriate to your operation.
 - Saving a snapshot to a file in CSV format:
Click the [Export] button.
 - Downloading an exported file to a terminal:
Select the radio button of the chosen file. Then, click the [Download] button. Multiple files cannot be selected.
 - Deleting all exported files:
Click the [Delete All] button.
 - Deleting a specific file:
Select the radio button of the chosen file. Then, click the [Delete] button. Multiple files cannot be selected.
- For details on the subsequent operations, see [Saving a snapshot to a file in CSV format](#) below.

Saving a snapshot to a file in CSV format

This section describes how to save a snapshot of information in PSA to a file in CSV format.

You can perform this operation by clicking the [Export] button as described in step 2 in [Listing exported files](#).

Operations

1. Enter a key phrase in the [Export] window. Then, click the [Export] button.
>> After export is completed successfully, the browser returns to the [Export List] window.

Remarks

The keyword is a supplementary phrase assigned to the exported data. Enter a keyword consisting of up to 50 characters. If you do not want to enter a keyword, leave the field blank.

You can use the following characters in a keyword:

Single-byte alphanumeric characters

Single-byte space

Single-byte symbols (except < > % & " , \)

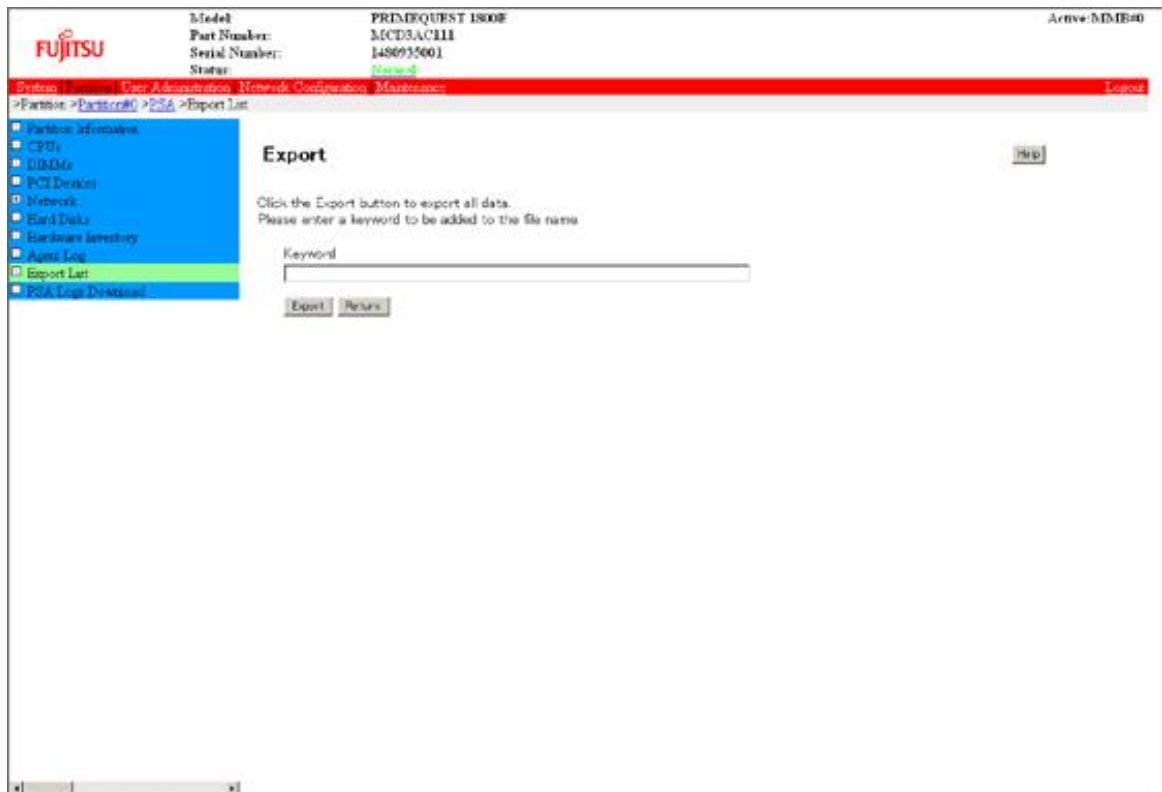


FIGURE 6.30 [Export] window (example)

2. If an export failure occurs, click [OK] in the [Export Failure Notice] dialog box.
>> The browser returns to the [Export List] window. The list shows the latest status.

6.8.2 Saving MMB configuration information

This section describes how to back up MMB configuration information to a remote PC.

Use the [Maintenance] menu in the [MMB Web-UI] window to save MMB configuration information.

Operations

1. Select [Maintenance] - [Backup/Restore Configuration] - [Backup/Restore MMB Configuration].
>> The Backup/Restore MMB Configuration window appears.

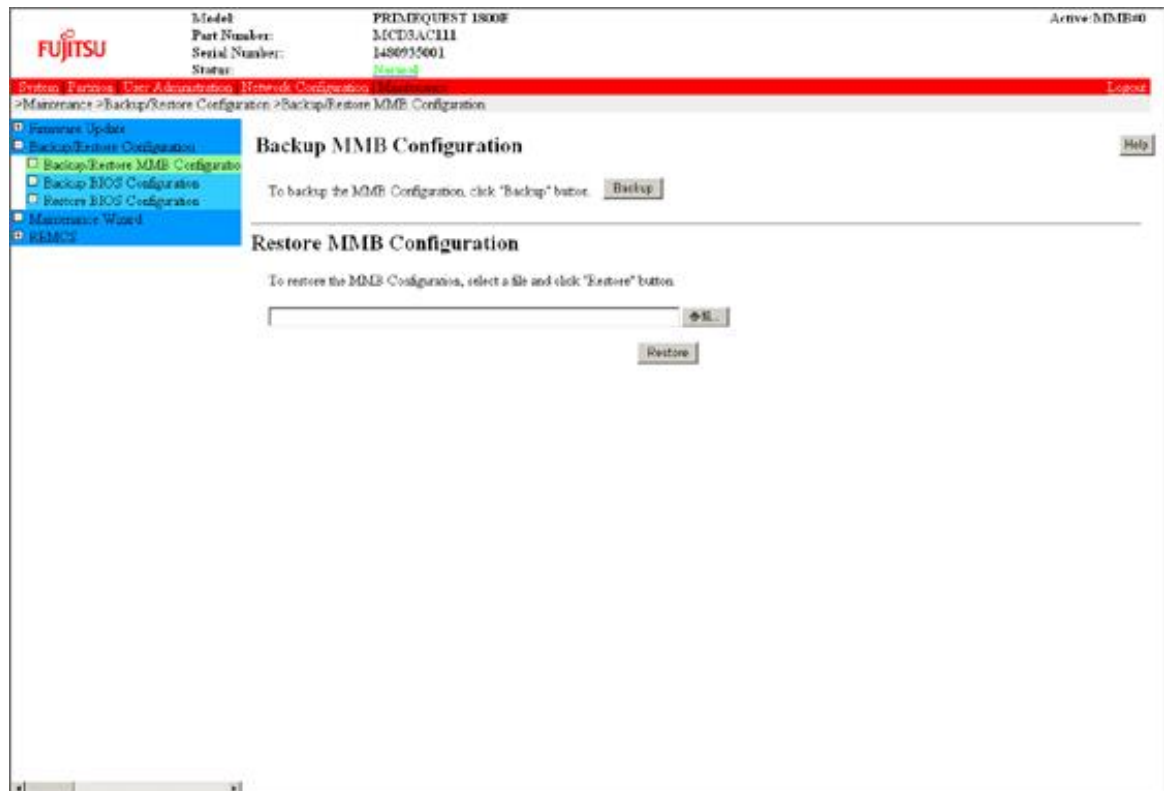


FIGURE 6.31 [Backup/Restore MMB Configuration] window (example)

2. Click the [Backup] button.
>> The save destination dialog box of the browser appears.
3. Select the save destination path. Then, click the [OK] button.
>> Download of the configuration information file begins.
The backup file of the MMB configuration information has the following default name:
MMB_backup_date_MMB version.dat

6.8.3 Saving BIOS configuration information

This section describes how to back up BIOS configuration information to a remote PC.

Use the [Maintenance] menu in the [MMB Web-UI] window to save BIOS configuration information.

Operations

1. Select [Maintenance] - [Backup/Restore Configuration] - [Backup BIOS Configuration].
>> The [Backup BIOS Configuration] window appears.

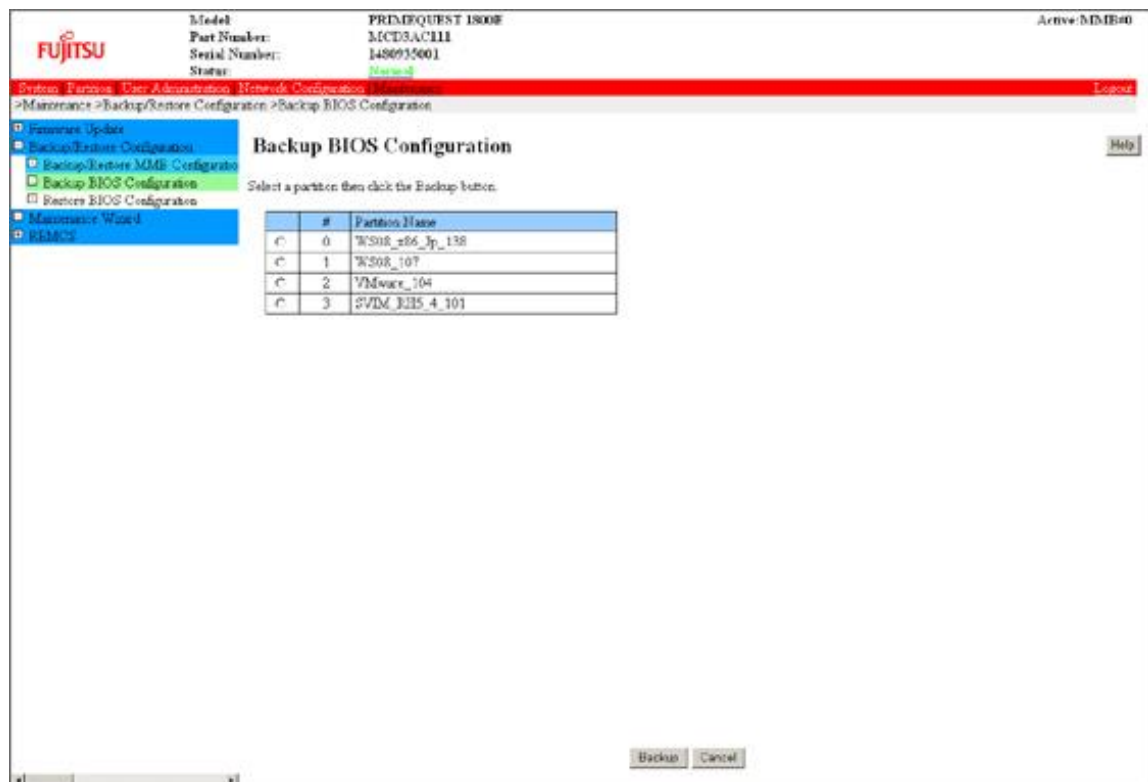


FIGURE 6.32 [Backup BIOS Configuration] window (example)

2. Select the radio button of the partition to which to back up the configuration information. Then, click the [Backup] button.

>> The save destination dialog box appears.

3. Select the save destination path. Then, click the [OK] button.

The backup file of the BIOS configuration has the following default name:

partition number_backup date_BIOS version.dat

6.9 Configuring Service Life Monitoring by RAS Support Service

For the use of RAID cards and UPSs, configure the BBU (Battery Backup Unit) service life monitoring by RAS Support Service.

SVIM automatically installs the RAS Support Service. For details on the manual installation and service life monitoring setting procedures for RAS Support Service, see the *RAS Support Service User's Guide (for Linux or Windows)*.

For details on SVIM, see the *ServerView Installation Manager*.

6.9.1 BBU service life monitoring for a RAID card

The BBU on a RAID card is a service life component. RAS Support Service performs service life monitoring. When starting, RAS Support Service checks for the RAID cards that have a BBU in order of PCI bus number, according to ServerView RAID information. It will monitor those RAID cards.

RAS Support Service performs service life monitoring and sends messages for replacement notification at the following times.

TABLE 6.16 Message for advance notification of replacement and replacement notification message (RAID card)

Start time for sending messages for advance notification of replacement	Time for sending replacement notification message
After about 2 years from the start of use or replacement of the BBU	After about 3 years

Operations

1. Start the GUI of RAS Support Service.
 - Windows: Log in to the operating system. Start the GUI.
 - Linux: Open a Web browser. Access the specified URL. Log in.

For details on operations, see the *RAS Support Service User's Guide (for Linux or Windows)*.

2. The Service Life Component Names list on the Component Service Life Information and Settings screen of RAS Support Service displays [Battery (RAID_Card#xx)] in order of PCI bus number.

You can enter a value (for a RAID card) in the Mounting Dates list to enable battery service life monitoring. In the Mounting Dates list, enter the mounting dates of the RAID cards for which to set service life monitoring.

Notes

Note the following points about BBU service life monitoring for a RAID card in the PRIMEQUEST 1000 series server.

- Of the mounted RAID cards shown in [FIGURE 6.33 RAS Support Service screens \(no BBU\)](#), the RAID card without a BBU is not monitored by RAS Support Service.

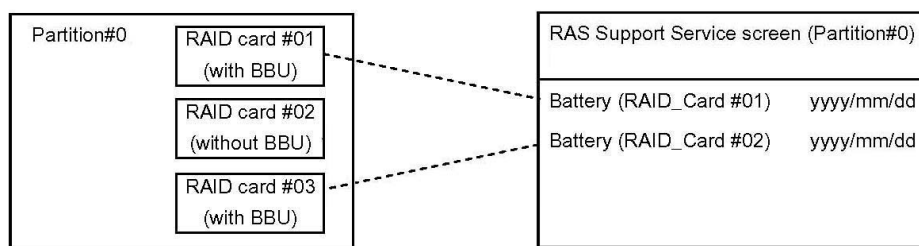


FIGURE 6.33 RAS Support Service screens (no BBU)

- After moving a monitored RAID card to another partition through a partition configuration change, you need to correct the RAS Support Service settings. First, in the Mounting Dates list, clear the RAID card mounting date on the original source partition. Then, set the RAID card mounting date on the destination partition.

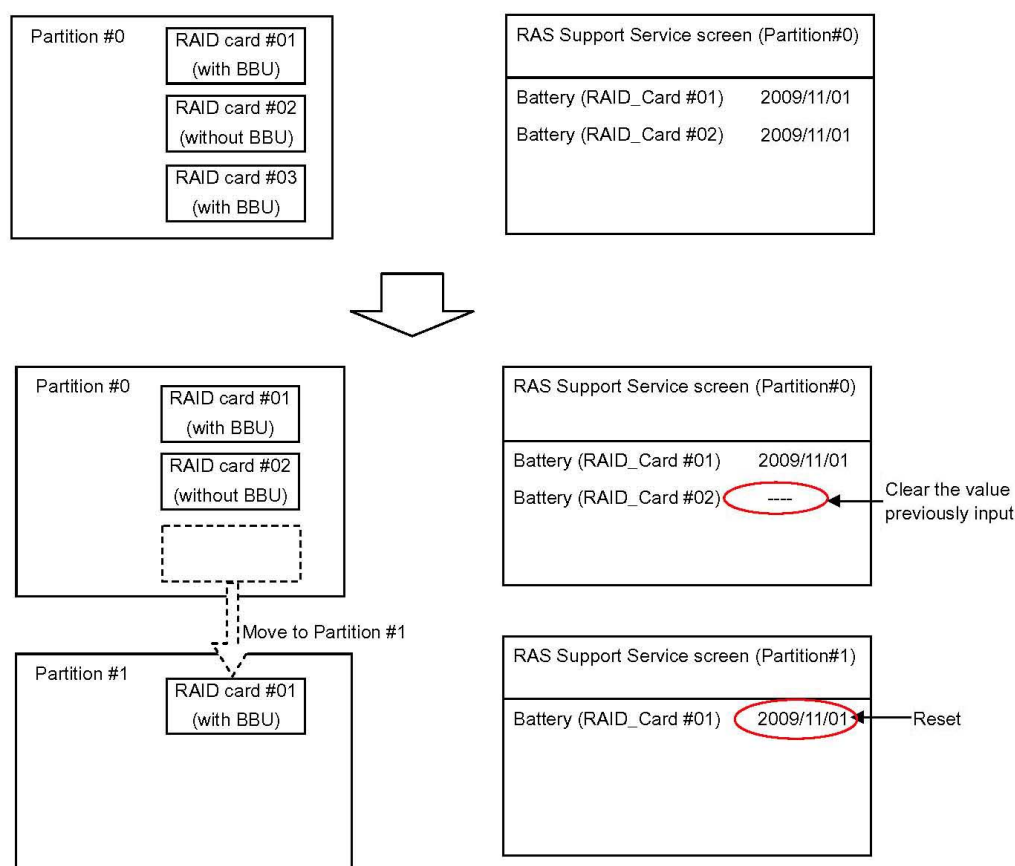


FIGURE 6.34 RAS Support Service screens (move to another partition)

- The PRIMEQUEST 1000 series server can have multiple partition configurations. For example, suppose a partition requires many CPUs during the day and a lot of I/O at night, the partition configuration must change between day and night. This means changes in the SB and IOB connection configuration.
- In this case, to move a RAID card to another partition, determine the primary partition for service life monitoring and then set the partition in RAS Support Service.
- If both partitions are set by mistake, notifications from both partitions will be issued in service life monitoring for the same RAID card.

6.9.2 Battery unit service life monitoring for a UPS

The battery unit on a UPS is a service life component. RAS Support Service performs service life monitoring. RAS Support Service sends messages for replacement notification at the following times.

TABLE 6.17 Message for advance notification of replacement and replacement notification message (UPS)

Start time for sending messages for advance notification of replacement	Time for sending replacement notification message
After about 1 year and 9 months from the start of use or replacement of the battery unit	After about 2 years

Operations

1. Determine which partitions to set for service life monitoring. Then, start the GUI of RAS Support Service.
 - Windows: Log in to the operating system. Start the GUI.
 - Linux: Open a Web browser. Access the specified URL. Log in.

For details on operations, see the *RAS Support Service User's Guide (for Linux or Windows)*.

2. The Service Life Component Names list on the RAS Support Service screen displays [UPS (battery)]. Since you can enter a value in the Mounting Dates list, enter the battery unit mounting date in the list.

Notes

Note the following points about battery unit service life monitoring for a UPS in the PRIMEQUEST 1000 series server.

- If there are multiple partition configurations, set battery unit service life monitoring for a UPS for only one partition (arbitrary). Otherwise, advance notifications of replacement will be issued from multiple partitions.

6.10 Recommended Write Policy Setting for SAS Disk RAID Units

You can attach the Battery Backup Unit to SAS disk RAID units.

The following table lists the recommended setting for Write Policy. The setting is different depending on whether the SAS disk RAID unit has the Battery Backup Unit.

For details on functions and the setting method, see the *LSI MegaRAID(R) SAS Software User Guide*.

Flash backup unit	Recommended Write Policy recommended setting
SAS disk RAID unit	Write Through
SAS disk RAID unit (with Battery Backup Unit)	Write Back

Before setting Write Policy to Write Back, examine the adequateness with the following considerations.

In the default setting, the battery is recalibrated every 30 days.

The performance during the recalibration is the same as for Write Through.

The recalibration might take a maximum of about 9 hours.

6.11 Recovery Procedure after the Execution of the Simple Setup Tool (editconf.sh)

The operations described in this section are required only if SVS (SVIM) 10.10.04 or previous version is used. When the simple setup tool is executed, the PSA setting in /etc/snmp/snmpd.conf is disabled. Perform the following recovery procedure:

1. Delete "#sv#" in the lines below (indicated with <-)

Before the modification

```
## Setup for FJSVpsa Please do not remove the following lines ##
#sv#com2sec psalocal localhost psaprivate <-
#sv#group PsarWGroup v1 psalocal <-
#sv#view fujitsu included .1.3.6.1.4.1.211.1.31.1 ff.c0 <-
#sv#access PsarWGroup "" any noauth exact fujitsu fujitsu none <-

rouser fjsvpsa

master agentx
agentxTimeout 360
agentxRetries 0

sysobjectid .1.3.6.1.4.1.211.1.31.1.2.100.2.0
## End of Setup for FJSVpsa ##
```

After the modification

```
## Setup for FJSVpsa Please do not remove the following lines ##
com2sec psalocal localhost psaprivate
group PsarWGroup v1 psalocal
view fujitsu included .1.3.6.1.4.1.211.1.31.1 ff.c0
access PsarWGroup "" any noauth exact fujitsu fujitsu none

rouser fjsvpsa

master agentx
agentxTimeout 360
agentxRetries 0

sysobjectid .1.3.6.1.4.1.211.1.31.1.2.100.2.0
## End of Setup for FJSVpsa ##
```

2. To reflect the change of snmpd.conf, restart snmpd.

```
/sbin/service snmpd restart
```

3. To reflect the setting, restart PSA.

```
/sbin/service y30FJSVpsa stop  
/sbin/service y30FJSVpsa start
```

CHAPTER 7 Work after Installation

This chapter describes the work performed after PRIMEQUEST 1000 series installation. This work includes configuring NTP and security.

7.1 Duplicate Network Adapter Configuration	218
7.2 Configuring NTP	219
7.3 Configuring a DNS Server	223
7.4 Configuring SMTP	224
7.5 Configuring Security	225
7.6 Scheduled Operations	234

7.1 Duplicate Network Adapter Configuration

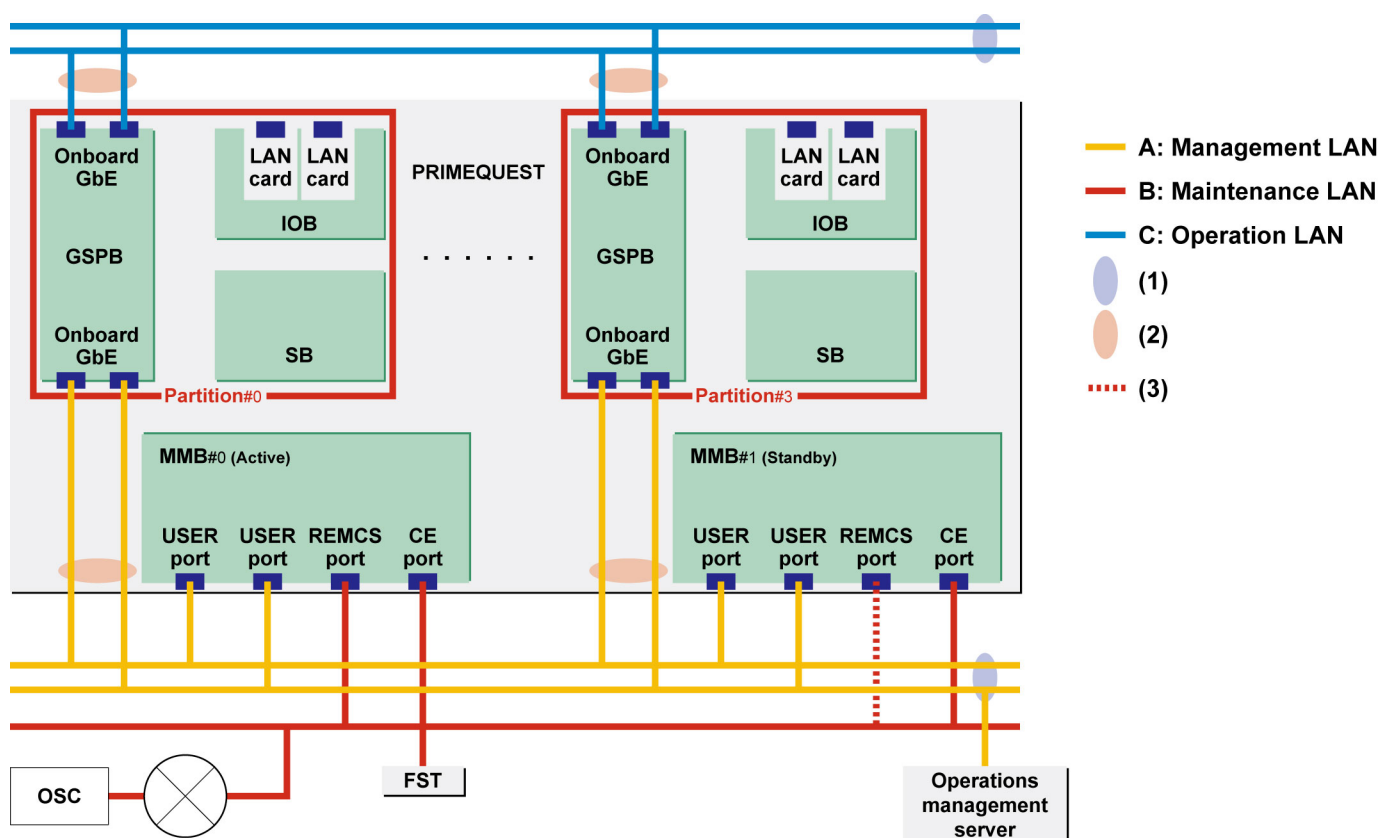
For the network configuration after installation, make teaming (multipath) settings as follows by using a utility compatible with each network adapter.

Network adapter (Intel Gigabit Ethernet (GbE)) settings

Make the network redundancy settings for the management LAN and production LAN. The target networks are shown in (2) in the following figure.

For Windows, configure teaming using Intel PROSet(R) (*1). For details, see the help for Intel PROSet(R).

*1 NIC teaming, a standard operating system function, is available in Windows Server 2012 or later.



No.	Description
(1)	SW redundancy
(2)	Redundancy by teaming (GLS or equivalent)
(3)	Disabled on the standby side

FIGURE 7.1 External network configuration

Note

There are some precautions on teaming with Intel PROSet(R). For details on the precautions, see APPENDIX G. 8 NIC (Network Interface Card) in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

7.2 Configuring NTP

This section describes how to correct the time with NTP (Network Time Protocol) in the PRIMEQUEST 1000 series.

NTP is a protocol for exchanging time information between computers. The time correction function references the correct time on another system at system startup. Then, it sets the time and keeps it within the specified error range.

A system with the correct source time is called an NTP server. A system that references that server is called an NTP client. The NTP server must be running NTP Service to respond to requests from the NTP client.

For details on time correction using NTP when the operating system is Windows, see [APPENDIX F Setting up the NTP Server \(Windows\)](#).

Note

- Be sure to use the NTP when using a reserved SB.
For details on the notes on the use of reserved SBs, see Notes on Reserved SB function in 3.2.1 Reserved SB in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).
- A partition configured with more than one SB (2 or more SBs) must use NTP.
- If an SB failure causes SB degradation and the Home SB is replaced, the operating system reads the RTC value of the new Home SB. This may result in a difference between the times before and after the Home SB replacement.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

7.2.1 How NTP operates in the PRIMEQUEST 1000 series

This section describes how NTP is used to correct the time of each partition in the PRIMEQUEST 1000 series. The time is set at the following two types of units in the PRIMEQUEST 1000 series server:

- MMB
- Each partition

For details on how to set the MMB as an NTP client, see [7.2.2 Setting an NTP server](#).

The NTP client of the installed operating system corrects the time of each partition.

For stable NTP operation, specify multiple NTP servers (at least three servers in RHEL5) from each NTP client.

[FIGURE 7.2 Operation with external NTP servers \(three NTP servers\)](#) shows a diagram outlining operation with NTP servers other than the MMB.

Note:

When using two or more NTP servers, match the stratum (layer) of the servers.

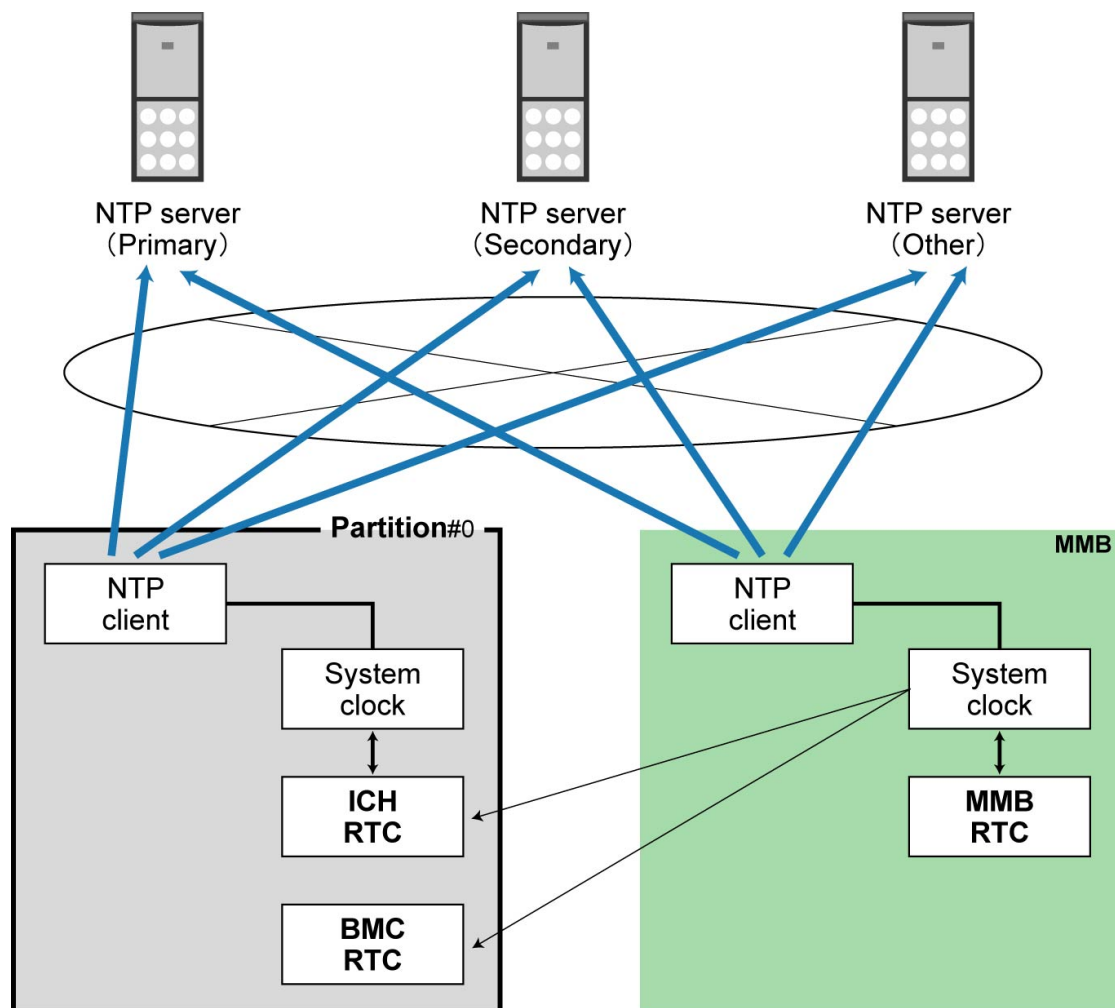


FIGURE 7.2 Operation with external NTP servers (three NTP servers)

Only a single NTP server can be specified for a client. In this case, if the NTP client is no longer able to communicate with the specified server, NTP server communication is lost because no other synchronized server is available. Time correction via NTP is disabled during the time taken for recovery of communication between the NTP client and NTP server. Time is measured based on system clock precision. Since system clock precision varies with the system, in cases where the time is not corrected via NTP, middleware, or application problems may occur due to an increasing time difference between systems.

Remarks

NTP servers 1 to 3 provide highly precise time over the Internet or intranet.

7.2.2 Setting an NTP server

Set another NTP server for time synchronization using the NTP client function of the MMB.

Note

The MMB time and the partition time are managed separately by independent clocks.

The MMB clock does not report or adjust the partition time. Keep the MMB time and the partition time the same, or at least close, because they are needed for the following cases:

- When checking the MMB log against the OS log in a partition at the hardware failure time
- When conducting a system audit or security audit

- When an error occurs regarding the maintenance time of the battery in a partition

Use either of the following ways to adjust the times.

- Adjust the time manually from the MMB Web-UI.
- Use the NTP client function of the MMB to adjust the time.

Remarks

If the NTP is not used, set the time in the operating system.

Operations

1. Click [Network Configuration] - [Date/Time].

The [Date/Time] window appears. For details on the [Date/Time] window, see 1.5.1 [Date/Time] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

The screenshot displays the MMB Web-UI interface. At the top, the Fujitsu logo is on the left, and system information (Model: PRIMEQUEST 1800E2, Part Number: MCD3AC111, Serial Number: 1480915001, Status: Normal) is on the right. Below this is a navigation bar with tabs: System, Partition, User Administration, Network Configuration, and Maintenance. The 'Network Configuration' tab is active, and the 'Date/Time' sub-tab is selected. A left sidebar contains a tree view with 'Date/Time' highlighted. The main content area is titled 'Date/Time' and includes a 'Refresh' and 'Help' button. Below the title is a message: 'Click the Apply Button to apply all changes.' The configuration fields are as follows:

Date	2012 - 10 - 18
Time	☐ Modify the Time 13 : 08 : 24
Time zone	Asia / Tokyo
NTP	☒ Enable ☐ Disable
NTP Time Correction Mode	☒ Step ☐ Slew
NTP Server1	10.0.8.3
NTP Server2	10.23.4.3
NTP Server3	2001:db8::10
Current Sync Status	10.23.4.3 2012-10-18 12:54:53

At the bottom right of the window are 'Apply' and 'Cancel' buttons.

FIGURE 7.3 [Date/Time] window (example)

2. Click [Enable] for [NTP].
3. Enter the IP address of another NTP server.
NTP Server1: Specify the Primary NTP server.
NTP Server2: Specify the Secondary NTP server.
NTP Server3: Specify the Other (Tertiary) NTP server.
4. Click the [Apply] button.
The MMB ensures time synchronization with the NTP servers specified in [NTP Server1] to [NTP Server3].

5. After several minutes elapse, click the [Refresh] button. Then, confirm that the window displays the correct time.

7.3 Configuring a DNS Server

For details on how to configure a DNS server, see [3.3.8 Configuring a DNS server](#).

7.4 Configuring SMTP

For details on how to configure SMTP, see [3.3.9 Configuring Alarm E-Mail](#).

7.5 Configuring Security

This section describes how to make the necessary settings to ensure security and notification of errors during operation.

Configure the security necessary for operation.

We recommend backing up the setting information after completing the following settings. For details on how to back up the specified information, see [3.5 Saving Configuration Information](#).

- [7.5.1 Configuring access control](#)
- [7.5.2 Configuring SNMP](#)
- [7.5.3 Configuring SSH](#)
- [7.5.4 Configuring HTTPS](#)

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

7.5.1 Configuring access control

To ensure MMB security, configure access control for the network protocol.

To ensure security, we recommend configuring it during installation. Access control can be configured even after installation.

Selecting the filter to edit

Operations

1. Click [Network Configuration] - [Access Control].

The [Access Control] window appears. For details on the [Access Control] window, see 1.5.10 [Access Control] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).



FIGURE 7.4 [Access Control] window (example)

2. Select the radio button of the filter you want to edit.

Adding or editing a filter

Operations

1. To add a filter, click the [Add Filter] button. To edit a filter, click the [Edit Filter] button.

Depending on whether you are adding or editing the filter, the [Add Filter] window or [Edit Filter] window appears. For details on the [Add Filter] and [Edit Filter] windows, see [Add Filter]/[Edit Filter] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).



FIGURE 7.5 [Add Filter] window (example)

2. Enter values in the required fields.
You can set up to 64 filters.

Remarks

Specify the IP address while taking account of the proxy setting for the Web browser on the PC or workstation.

3. Click the [Apply] button.

Deleting a filter

Operations

1. Select the filter. Then, click the [Remove Filter] button.
A deletion confirmation window appears.
2. Click the [OK] button to delete the filter.
The browser returns to the [Access Control] window. Confirm that the filter was deleted from the list. To cancel the deletion, click the [Cancel] button.

7.5.2 Configuring SNMP

Configure SNMP (Simple Network Management Protocol). Use Administrator privileges to configure SNMP. Set whether to report any operational failure to an external destination, the notification destination, and other information. You can make the following four types of setting:

[Enabling SNMP](#)

[Making advanced SNMP settings](#)

[Setting SNMP trap destinations](#)

[Configuring SNMP v3](#)

Enabling SNMP

Operations

1. Click [Network Configuration] - [Network Protocols].

The [Network Protocols] window appears. For details on the [Network Protocols] window, see 1.5.4 [Network Protocols] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

The screenshot shows the 'Network Protocols' configuration window. The left sidebar lists various network settings, with 'Network Protocols' selected. The main area displays configuration options for Web (HTTP/HTTPS), Telnet, SSH, and SNMP. The SNMP section is expanded, showing the following settings:

SNMP Agent	Enable/Disable
Agent Port# [161, 1024-65535]	161
SNMP Trap	Enable/Disable
Trap Port# [162, 1024-65535]	162

FIGURE 7.6 [Network Protocols] window (example)

2. Enter values for each item in [SNMP].
3. Click the [Apply] button.

Making advanced SNMP settings

Operations

1. Click [Network Configuration] - [SNMP Configuration] - [Community].

The [SNMP Community] window appears. For details on the [SNMP Community] window, see [SNMP Community] window in 1.5.6 [SNMP Configuration] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

FUJITSU Model: PRIMEQUEST 1800E2 Active:MMB#0
Part Number: MCD3AC111
Serial Number: 1480915001
Status: Normal

System Partition User Administration Network Configuration Maintenance Logout
>Network Configuration >SNMP Configuration >Community

SNMP Community Help

Click the Apply Button to apply all changes.

System Information

System Name	PRIMEQUEST1480915001
System Location	
System Contact	

Note)System Name can be configured in System->[System Information](#) page.

Community

Community/User	IP Address/MASK	SNMP Version	Access
public	10.24.6.94	1 ▼	Read Only ▼
public	10.24.17.150	1 ▼	Read Only ▼
public	10.24.111.243	1 ▼	Read Only ▼
public	10.24.77.65	1 ▼	Read Only ▼
public	10.24.12.0/24	1 ▼	Read Only ▼
public	10.26.64.0/24	1 ▼	Read Only ▼
public	10.24.77.0/24	1 ▼	Read Only ▼
public	10.24.2.0/24	1 ▼	Read Only ▼
public	2001:db8:0:f101::414	1 ▼	Read Only ▼
		1 ▼	Read Only ▼
		1 ▼	Read Only ▼
		1 ▼	Read Only ▼
		1 ▼	Read Only ▼
		1 ▼	Read Only ▼
		1 ▼	Read Only ▼
		1 ▼	Read Only ▼

Apply Cancel

FIGURE 7.7 [SNMP Community] window (example)

2. Enter values in the required fields.
You can set up to 16 Community lines. Enter values for the specified community, accessible IP addresses, SNMP version, access permission, and authentication.
To delete a line, clear the [Community] and [IP address] items.

3. Click the [Apply] button.

Setting SNMP trap destinations

Operations

1. Click [Network Configuration] - [SNMP Configuration] - [Trap].
The [SNMP Trap] window appears. For details on the [SNMP Trap] window, see [SNMP Trap] window in 1.5.6 [SNMP Configuration] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).



FIGURE 7.8 [SNMP Trap] window (example)

2. Enter destinations.

You can set up to 16 trap destinations.

Set the community or user name, IP address of the trap destination, SNMP version, and authentication level.

3. Click the [Apply] button.

Click the [Test Trap] button to send a test trap to the specified trap destination.

Configuring SNMP v3

Specify the ID of the engine specific to SNMP v3, and the user.

Remarks

If you change the engine ID or IP address, you need to specify again all the users that are set for SNMP v3 access. The changes for the specified users take effect only after the SNMP Service is stopped and restarted. For this reason, clicking the [Apply] button in the window temporarily stops SNMP Service.

Operations

1. Click [Network Configuration] - [SNMP Configuration] - [SNMP v3 Configuration].

The [SNMP v3 Configuration] window appears. For details on the [SNMP v3 Configuration] window, see [SNMP v3 Configuration] window in 1.5.6 [SNMP Configuration] menu in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

The screenshot shows the 'SNMP v3 Configuration' window. At the top, there's a header with 'Fujitsu' logo and device information: Model: PRIMEQUEST 1800E, Part Number: MCD3AC111, Serial Number: 1486935001, Status: Normal. Below this is a navigation bar with tabs: System, Settings, User Administration, Network Configuration, Maintenance, and Logout. The 'Network Configuration' tab is active, and the 'SNMP v3 Configuration' sub-tab is selected. The main content area is titled 'SNMP v3 Configuration' and includes a note: 'Click the Apply Button to apply all changes.' Below this is a form with an 'Engine ID' field (value: 1234567890) and a 'Trap' checkbox. The 'User' section contains a table with the following columns: 'User Name', 'Auth Type', 'Auth passphrase', 'Auth passphrase (confirm)', 'Priv passphrase', and 'Priv passphrase (confirm)'. The table has 10 rows, with the first two rows filled with 'root' and 'test' users. At the bottom right are 'Apply' and 'Cancel' buttons.

FIGURE 7.9 [SNMP v3 Configuration] window (example)

2. Enter values for SNMP v3 users.
You can register up to 16 users.

3. Click the [Apply] button.

This restarts the SNMP Service to apply the values for the selected users.

7.5.3 Configuring SSH

Configure SSH for the MMB. You can set it with Administrator privileges.

Operations

1. Click [Network Configuration] - [Network Protocols].

The [Network Protocols] window appears. For details on the [Network Protocols] window, see 1.5.4 [Network Protocols] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

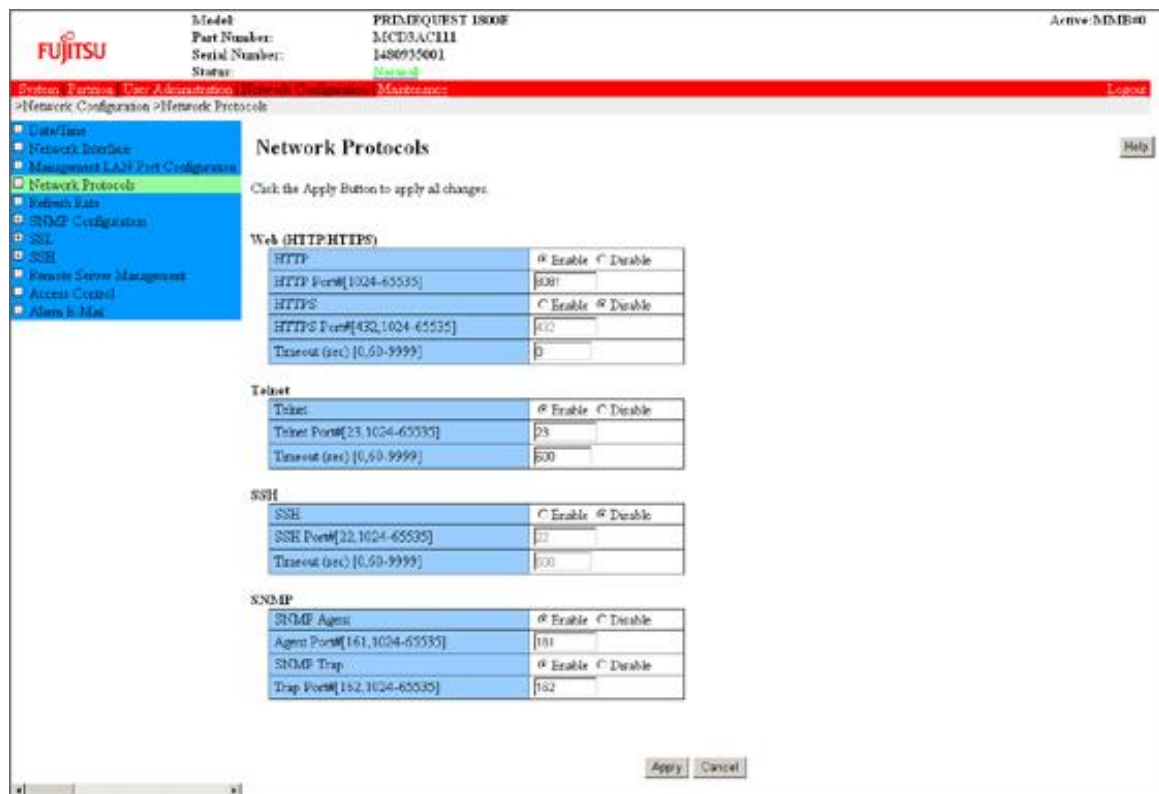


FIGURE 7.10 [Network Protocols] window (example)

2. Specify each item in [SSH].
3. Click the [Apply] button.

7.5.4 Configuring HTTPS

Configure HTTPS for the MMB. You can configure it with Administrator privileges.

To enable HTTPS, a valid SSL certificate must have been registered. If no valid SSL certificate is registered, any attempt to enable HTTPS results in an error.

Specify a "verified certificate" as the valid SSL certificate. Alternatively, specify a "self-signed certificate" created in the MMB window.

A Fujitsu certified service engineer may have already configured HTTPS. If no change is needed, proceed to the next setting item.

Operations

1. Click [Network Configuration] - [Network Protocols].

The [Network Protocols] window appears. For details on the [Network Protocols] window, see 1.5.4 [Network Protocols] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

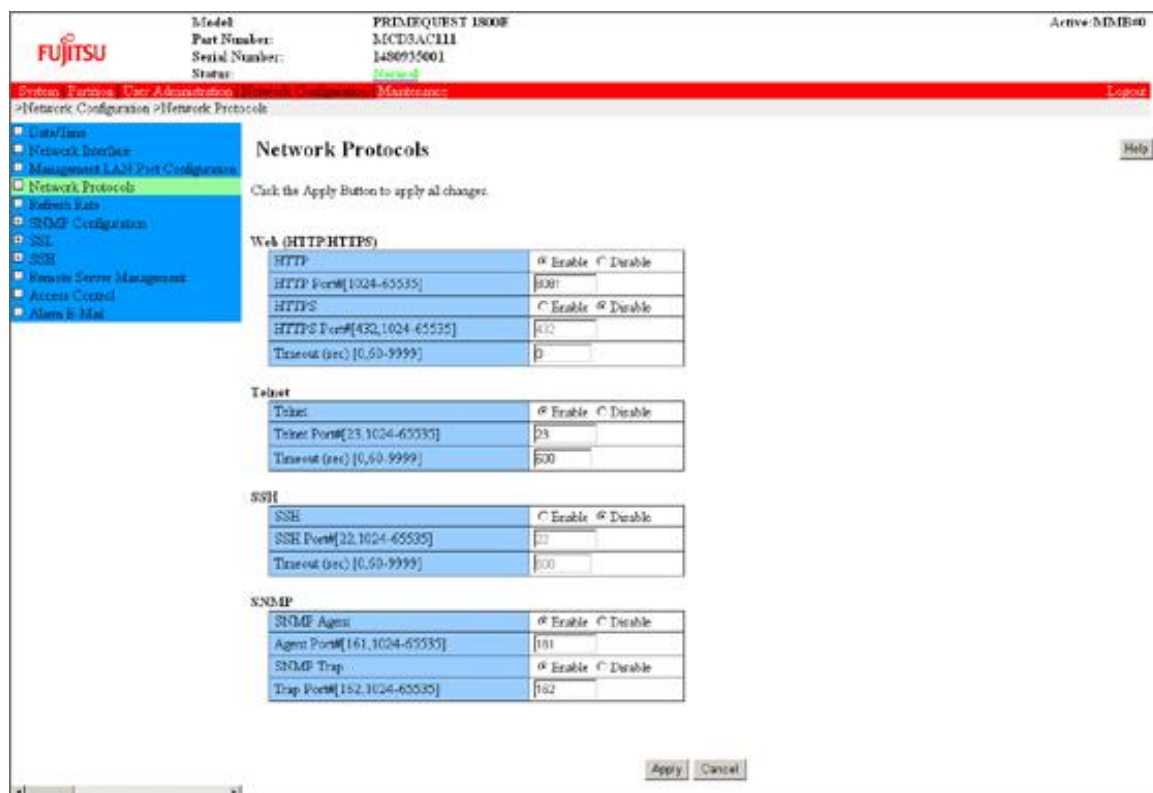


FIGURE 7.11 [Network Protocols] window (example)

2. Specify each HTTPS-related item in [HTTP].
3. Click the [Apply] button.

7.6 Scheduled Operations

For details on scheduled operations, see 9.3 Scheduled Operations in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

CHAPTER 8 Powering On and Off a Partition

This chapter describes partition power control.

8.1 Powering On and Off a Partition	236

8.1 Powering On and Off a Partition

This section describes how to power on and power off partitions.

- 8.1.1 Powering on a partition
- 8.1.2 Powering off a partition

You can power on or off a partition from a Partition Operator account with Administrator or Operator privileges for the partition.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

8.1.1 Powering on a partition

The procedure for powering on the partition is as follows.

Operations

1. Log in to the MMB Web-UI.

The [MMB Web-UI] window appears.

2. Click [Partition] - [Power Control].

The [Power Control] window appears. For details on the [Power Control] window, see 1.3.1 [Power Control] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

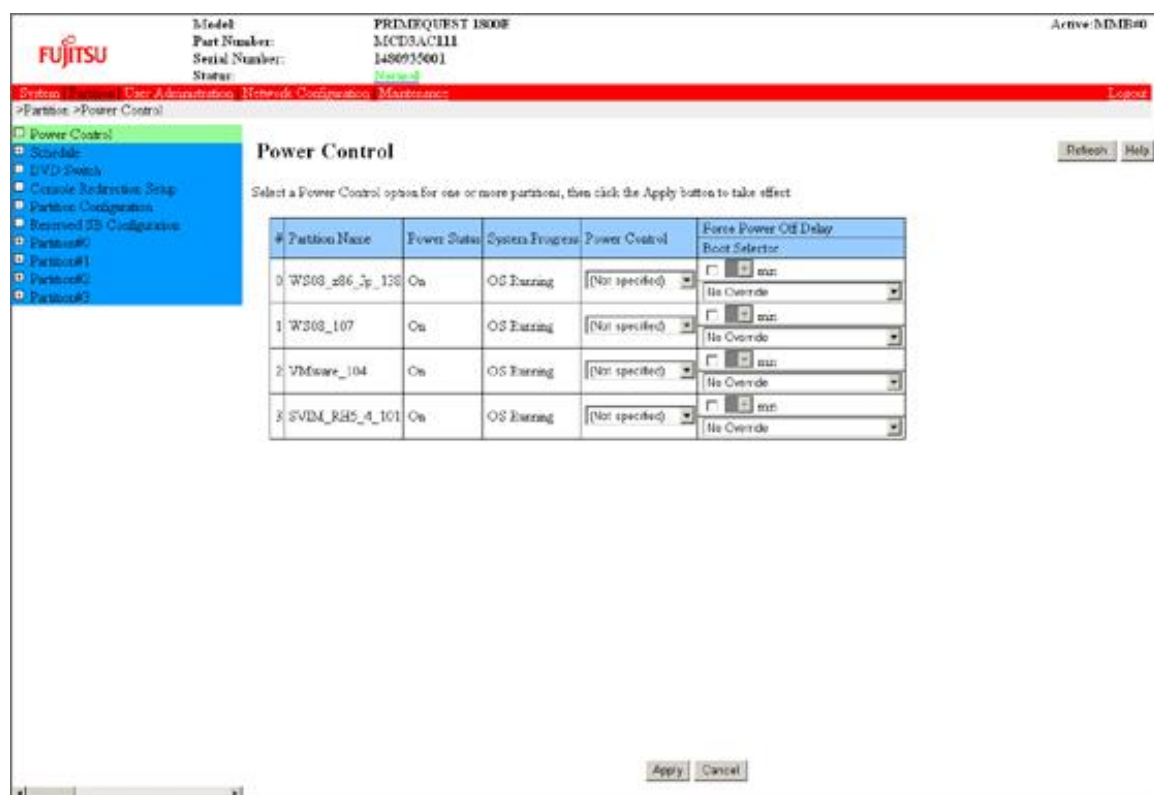


FIGURE 8.1 [Power Control] window (example)

3. Select [Power On] in [Power Control] for the partition that you are going to power on. Then, click the [Apply] button.

4. A confirmation dialog box appears. Click the [OK] button to continue processing or the [Cancel] button to cancel processing.

Remarks

- If the power to the partition is already on or if the specified control fails because the power is currently off, a warning message appears.
- If the power to all partitions is off, the partitions cannot be powered on for some time.

8.1.2 Powering off a partition

The procedure for powering off the partition is as follows.

In Windows, ServerView Agent is required to execute a shutdown from the MMB Web-UI.

For details on setting ServerView Agent, see the explanation regarding the [System Shutdown] tab in the *ServerView Operations Manager Installation ServerView Agents for Windows*.

If the following problems occur, check for details on the problem in 11.2.11 Problems with partition operations in the *PRIMEQUEST 1000 Series Administration Manual* (C122-E108EN).

- The MMB Web-UI displays [Error] for [Status] (information area) because either of the following was executed:
 - [Power Off], [Reset], or [Force Power Off] of the partition
 - Shutdown from the operating system
- The [MMB Web-UI] window displays "Read Error" for [Part Number] or [Serial Number] to indicate the component status.

Operations

1. Log in to the MMB Web-UI.

The [MMB Web-UI] window appears.

2. Click [Partition] - [Power Control] from the MMB menu.

The [Power Control] window appears. The number in the [#] column is the partition number.

For details on the [Power Control] window, see 1.3.1 [Power Control] window in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

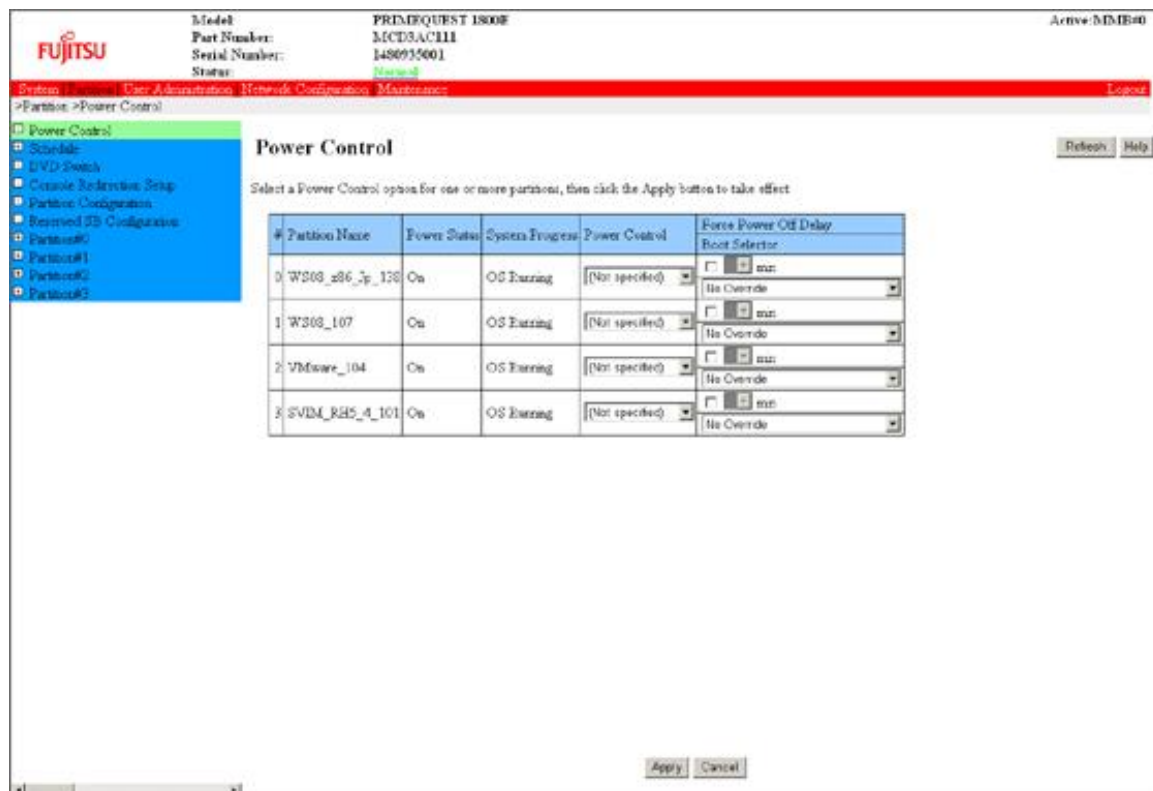


FIGURE 8.2 [Power Control] window (example)

3. Select [Power Off] in [Power Control] for the partition that you are going to power off. Then, click the [Apply] button.

The power to the specified partition is turned off.

Remarks

If the operating system supports ACPI, selecting [Power Off] enables you to automatically power off the partition after operating system shutdown. However, even if the operating system supports ACPI, you may be unable to power off the partition as long as an application that does not support it is running on the operating system. This depends on the specifications of the operating system and application. For details, see the manual of the operating system or application.

If the operating system does not support ACPI, the power-off sequence powers off the partition without shutting down the operating system.

For the above reason, be sure to shut down the operating system on the partition.

APPENDIX A Lists of Settings (Links)

See Appendix A Lists of Settings in the *PRIMEQUEST 1000 Series
Tool Reference* (C122-E110EN).

A.1 MMB Settings	240
A.2 PSA Settings	241
A.3 UEFI Settings	242
A.4 BMC Settings	243

A.1 MMB Settings

See A.1 MMB Web-UI Settings in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

A.2 PSA Settings

See A.2 PSA Settings in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

A.3 UEFI Settings

See A.3 UEFI Settings in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

A.4 BMC Settings

See A.4 BMC Settings in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).

APPENDIX B Manual PSA Installation and Uninstallation

This appendix describes how to manually install and uninstall PSA for a specific operating system.

If you use SVIM to install the operating system, you need not manually install PSA.

Remarks

PSA is provided only with the PRIMEQUEST 1800E.

B.1 Manually Installing PSA (Linux: Red Hat Enterprise Linux)	
.....	246
B.2 Manually Installing PSA (Windows Server 2003)	
255	
B.3 Manually Installing PSA (Windows Server 2008)	
261	

B.1 Manually Installing PSA (Linux: Red Hat Enterprise Linux)

This section describes how to manually install PSA in Linux (Red Hat Enterprise Linux).

Remarks

Be sure to install PSA for PRIMEQUEST 1800E. Otherwise, the following restrictions apply.

- I/O (e.g., PCI Express card, hard disk) failure notification and trap notification to the administrator are disabled.
- Failure notification using symptom detection and trap notification to the administrator are disabled.
 - Threshold exceeded in S.M.A.R.T. monitoring of HDDs
- Operations management software cannot collect information on the partition side.
- Even under an REMCS agreement, no software errors are reported.
- Hot maintenance of hard disks is disabled. The partition must be stopped for maintenance.
- PRIMECLUSTER linkage is disabled.

B.1.1 Installation flow

For details on how to install PSA, see [CHAPTER 4 Installing the Operating System and Bundled Software](#). For details on how to configure PSA, see [B.1 Manually Installing PSA \(Linux: Red Hat Enterprise Linux\)](#).

Remarks

- After changing the MMB IP address on a partition or the management LAN IP address, restart PSA. Otherwise, a display error may occur in the [PSA] window of the Web-UI. Moreover, PSA would not be able to report any detected errors.
- If you use SVIM to install the operating system, you need not manually install PSA. However, after installation with SVIM, you will need to check and make settings according to [B.1.2 Checks before PSA installation](#) and [B.1.6 Settings after PSA installation](#).

B.1.2 Checks before PSA installation

This section describes the checks to make before PSA installation.

[Confirming PSA-to-MMB communication LAN settings](#)

[Confirming management LAN settings](#)

[Confirming the functions required for PSA operation](#)

[Confirming the status of the iptables service](#)

Confirming PSA-to-MMB communication LAN settings

For details on how to confirm PSA-to-MMB communication LAN settings, see [6.2.1 Configuring the PSA-to-MMB communication LAN](#) and [6.2.7 Setting the management LAN IP address](#).

Confirming management LAN settings

For details on how to confirm management LAN settings, see [6.2.2 Confirming management LAN settings](#).

Confirming the functions required for PSA operation

The following table lists the packages required for PSA operation. Execute the rpm command to confirm the installation of each package.

The packages that must be installed depend on the CPU architecture (x86/x64).

TABLE B.1 Packages required for PSA operation (RHEL5)

Package	CPU architecture	
	x86	x64
Linux package	gdb-x.x-x.x.i386.rpm lm_sensors-x.x-x.x.i386.rpm net-snmp-x.x.x-x.x.i386.rpm net-snmp-utils-x.x.x-x- x.x.i386.rpm rcs-x.x-x.x.i386.rpm	gdb-x.x-x.x.x86_64.rpm lm_sensors-x.x-x.x.x.i386.rpm lm_sensors-x.x-x-x.x.x86_64.rpm net-snmp-x.x.x-x.x.x86_64.rpm net-snmp-libs-x.x.x-x.x.i386.rpm net-snmp-libs-x.x.x-x.x.x86_64.rpm net-snmp-utils-x.x.x-x.x.x86_64.rpm popt-x.x.x-x.x.i386.rpm rcs-x.x-x.x.x86_64.rpm rpm-libs-x.x.x-x.x.i386.rpm openssl-x.x-x.x.x.i686.rpm openssl-x.x-x.x.x.x86_64.rpm perl-x.x-x.x.x.x86_64.rpm tcp_wrappers-x.x-x.x.x.i386.rpm tcp_wrappers-x.x-x.x.x.x86_64.rpm parted-x.x-x.x.x.i386.rpm parted-x.x-x.x.x.x86_64.rpm
FJSVfefpcl-related packages	Required	Required

TABLE B.2 Packages required for PSA operation (RHEL6)

Package	CPU architecture	
	x86	x64
Linux package	gdb-x.x-x.x.i686 net-snmp-libs-x.x-x.x.i686 net-snmp-x.x-x.x.i686 net-snmp-utils-x.x-x.x.i686 parted-x.x-x.x.i686	gdb-x.x-x.x.x86_64 glibc-x.x-x.x.x.i686 openssl-x.x-x.x.x.i686 net-snmp-libs-x.x-x.x.i686 net-snmp-libs-x.x-x.x.x86_64 net-snmp-x.x-x.x.x86_64 net-snmp-utils-x.x-x.x.x86_64 parted-x.x-x.x.i686
FJSVfefpcl-related packages	Required	Required

TABLE B.3 Packages required for SIRMS operation (RHEL6)

Package	CPU architecture	
	x86	x64
Linux package	Not required	libstdc++-4.4.4-13.el6.i686 or later

Note

The name of the FJSVfefpcl-related package depends on the operating system version.

Syntax

```
/bin/rpm -q <package name>
```

Use the uname command to check the kernel version.

Syntax

```
/bin/uname -r
```

Example of installing the net-snmp package and confirming the installation

```
#!/bin/rpm -q net-snmp  
net-snmp-5.1.2-11
```

If a package has not been installed, install it from the OS installation CD by using the same procedure as that for the RPM package.

Remarks

The FJSVfefpcl package runs together with PSA to enable the functions for stopping Watchdog software and reporting the panic status at the OS panic occurrence time.

Also, a configuration using PCL (PRIMECLUSTER) provides an HBA blocking function to obtain high-speed switching of PCL nodes.

Under a PRIMEQUEST environment, the package must be installed even if PCL (PRIMECLUSTER) is not used.

Confirming the status of the iptables service

Confirm the status of the iptables service.

If the iptables service has stopped, the iptables settings were not made correctly during PSA installation.

Start the iptables service as needed.

Note

If PSA version 2.8.0 or earlier is installed when the iptables service has stopped, the iptables service starts with the settings of the PSA-to-MMB communication LAN written over the existing port settings.

Deal with this problem in the following way.

- To use the iptables service:

Start the iptables service before installing PSA.

- To use a firewall tool other than iptables:
 Stop the iptables service.

B.1.3 Installing PSA

Execute the following command to install the PSA package.

The following explanation is based on the assumption that the PSA package (FJSVpsa-\$VER-\$REL.tar.gz) has been extracted in the work directory (\$WORK_DIR):

Syntax

```
cd $WORK_DIR/FJSVpsa
./INSTALL.sh
```

B.1.4 Automatic configuration during PSA installation

The following table lists settings for PSA operation. The installer automatically adds or updates these settings during PSA installation.

TABLE B.4 Settings automatically added/changed during PSA installation

Target	Action	Remarks
syslog.conf file	Add setting	
snmpd.conf file	Add setting	
snmptrapd.conf file	Add setting	
services files	Add setting	Added port: The installer does not check for duplicate port numbers when adding a setting to the fj-webgate (24450) services file. Change the setting as needed.
snmptrapd start option	Change	
snmpd start option	Change	
Dedicated PSA-to-MMB communication LAN interface	Set IP address	Referring to 6.2.1 Configuring the PSA-to-MMB communication LAN , change settings as needed.
iptables setting	Add setting	Only a chain for PSA-MMB communication is created during manual installation of PSA version 2.6 or later. Referring to Checking the firewall function (opening ports) in B.1.6 Settings after PSA installation , add the jump setting for the chain for PSA-MMB communication to INPUT and OUTPUT chains manually.
SELinux configuration file (/etc/selinux/config)	Change	SELinux is disabled only for RHEL5. If SELinux is disabled, do not change the settings.

Target	Action	Remarks
SELinux setting	Add setting	The policy module is added for RHEL6 or later only.

B.1.5 Restarting the partition

After installing PSA, restart the partition with a reboot.

Syntax

```
/sbin/reboot
```

B.1.6 Settings after PSA installation

This section describes the settings after PSA installation.

[Confirming SELinux function settings](#)

[Checking the firewall function \(opening ports\)](#)

[Setting the destinations of traps from a partition](#)

[Setting the destinations of traps and e-mail via the MMB](#)

[Configuring SNMP to use duplicate disks](#)

Confirming SELinux function settings

For details on how to confirm SELinux function settings, see [6.2.3 Confirming SELinux function settings](#).

Checking the firewall function (opening ports)

[For PSA version 2.5 or earlier]

The required firewall for the PSA-MMB communication LAN is automatically configured.

For details on how to check the firewall function, see [PSA-to-MMB communication LAN interfaces](#) in [6.2.4 Checking the firewall function \(opening ports\)](#).

Also, the settings related to management LAN interfaces are required only for PRIMECLUSTER linkage. For the setting procedure, see [Management LAN interfaces](#) in [6.2.4 Checking the firewall function \(opening ports\)](#).

[For PSA version 2.6 or later]

For the required firewall for the PSA-MMB communication LAN and the management LAN, only a chain is automatically configured.

Since the settings related to PSA-MMB communication LAN interfaces are essential, add the jump setting for the chain for PSA-MMB communication (referred to below as the PSA-MMB_LAN chain) to INPUT and OUTPUT chains in iptables manually. For the setting procedure, see [PSA-to-MMB communication LAN interfaces \(for PSA version 2.6 or later\)](#).

Also, the settings related to management LAN interfaces are required only for PRIMECLUSTER linkage. For the setting procedure, see [Management LAN interfaces](#) in [6.2.4 Checking the firewall function \(opening ports\)](#).

Note

If PSA version 2.8.0 or earlier is installed when the iptables service has stopped, the existing settings are cleared. Deal with this problem in the following way.

- To use the iptables service:

After making the settings to open the ports necessary for the system, open the necessary ports. For details, see [TABLE 6.5 Ports to open for the PSA-to-MMB communication LAN interfaces](#).

- To use a firewall tool other than iptables:

The setting of the PSA-to-MMB communication LAN (PSA-MMB_LAN chain) has been added to iptables. Delete it manually, and then open the necessary ports. For details, see [TABLE 6.5 Ports to open for the PSA-to-MMB communication LAN interfaces](#).

PSA-to-MMB communication LAN interfaces (for PSA version 2.6 or later)

The firewall settings vary depending on the environment. The settings shown in the following procedure are an example of settings for PSA-to-MMB communication.

```
Example: REJECT setting in INPUT and FORWARD
# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     all  --  0.0.0.0/0              0.0.0.0/0    state RELATED,ESTABLISHED
ACCEPT     icmp --  0.0.0.0/0              0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0              0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0              0.0.0.0/0    state NEW tcp dpt:22

REJECT     all  --  0.0.0.0/0              0.0.0.0/0    reject-with icmp-host-
prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
REJECT     all  --  0.0.0.0/0              0.0.0.0/0    reject-with icmp-host-
prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain PSA-MMB_LAN (2 references)
target     prot opt source                destination
ACCEPT     all  --  0.0.0.0/0              0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0              0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0              0.0.0.0/0    icmp type 8
ACCEPT     icmp --  0.0.0.0/0              0.0.0.0/0    icmp type 0
ACCEPT     udp  --  0.0.0.0/0              0.0.0.0/0    udp dpt:161
ACCEPT     udp  --  0.0.0.0/0              0.0.0.0/0    udp spt:161
ACCEPT     tcp  --  0.0.0.0/0              0.0.0.0/0    tcp dpt:24450
ACCEPT     tcp  --  0.0.0.0/0              0.0.0.0/0    tcp spt:24450
ACCEPT     tcp  --  0.0.0.0/0              0.0.0.0/0    tcp spt:5000
```

ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp dpt:5000

1. Confirm that the PSA-MMB_LAN chain has been created.

/sbin/iptables -L

```
# iptables -L Execution result
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     all  --  0.0.0.0/0                0.0.0.0/0    state RELATED,ESTABLISHED
ACCEPT     icmp --  0.0.0.0/0                0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0                0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0                0.0.0.0/0    state NEW tcp dpt:22
REJECT     all  --  0.0.0.0/0                0.0.0.0/0    reject-with icmp-host-
prohibited

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
REJECT     all  --  0.0.0.0/0                0.0.0.0/0    reject-with icmp-host-
prohibited

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain PSA-MMB_LAN (2 references)
target     prot opt source                destination
ACCEPT     all  --  0.0.0.0/0                0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0                0.0.0.0/0
ACCEPT     icmp --  0.0.0.0/0                0.0.0.0/0    icmp type 8
ACCEPT     icmp --  0.0.0.0/0                0.0.0.0/0    icmp type 0
ACCEPT     udp  --  0.0.0.0/0                0.0.0.0/0    udp dpt:161
ACCEPT     udp  --  0.0.0.0/0                0.0.0.0/0    udp spt:161
ACCEPT     tcp  --  0.0.0.0/0                0.0.0.0/0    tcp dpt:24450
ACCEPT     tcp  --  0.0.0.0/0                0.0.0.0/0    tcp spt:24450
```

ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp spt:5000
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp dpt:5000

2. Add the jump setting for the PSA-MMB_LAN chain to INPUT and OUTPUT chains.

Make the setting such that there are no interruptions by an existing REJECT setting in an INPUT or OUTPUT chain or by a user definition chain.

Here, use the following command to add the setting to the fifth INPUT chain (before the REJECT setting) and to the OUTPUT chain. (For details on the iptables option, see the man manual.)

/sbin/iptables -I INPUT 5 -j PSA-MMB_LAN
/sbin/iptables -A OUTPUT -j PSA-MMB_LAN

3. Execute the iptables -L command, and confirm that the PSA-MMB_LAN chains added to the INPUT and OUTPUT chains are not interrupted by the previous REJECT, DROP, or other settings.

Example of settings:					
# iptables -L					
Chain INPUT (policy ACCEPT)					
target	prot	opt	source	destination	
ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0	state
RELATED, ESTABLISHED					
ACCEPT	icmp	--	0.0.0.0/0	0.0.0.0/0	
ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0	
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	state NEW tcp dpt:22
PSA-MMB_LAN	all	--	0.0.0.0/0	0.0.0.0/0	
REJECT	all	--	0.0.0.0/0	0.0.0.0/0	reject-with icmp-host-prohibited
Chain FORWARD (policy ACCEPT)					
target	prot	opt	source	destination	
REJECT	all	--	0.0.0.0/0	0.0.0.0/0	reject-with icmp-host-prohibited
Chain OUTPUT (policy ACCEPT)					
target	prot	opt	source	destination	
PSA-MMB_LAN	all	--	0.0.0.0/0	0.0.0.0/0	
Chain MMLAN (2 references)					
target	prot	opt	source	destination	
ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0	
ACCEPT	all	--	0.0.0.0/0	0.0.0.0/0	

ACCEPT	icmp	--	0.0.0.0/0	0.0.0.0/0	icmp type 8
ACCEPT	icmp	--	0.0.0.0/0	0.0.0.0/0	icmp type 0
ACCEPT	udp	--	0.0.0.0/0	0.0.0.0/0	udp dpt:161
ACCEPT	udp	--	0.0.0.0/0	0.0.0.0/0	udp spt:161
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp dpt:24450
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp spt:24450
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp spt:5000
ACCEPT	tcp	--	0.0.0.0/0	0.0.0.0/0	tcp dpt:5000

4. Log in to the MMB Web-UI, and confirm that the PSA screen appears.

5. Save the firewall configuration.

```
# /sbin/service iptables save
```

Setting the destinations of traps from a partition

For details on how to set the destinations of traps from a partition, see [6.2.5 Setting the destinations of traps from a partition](#).

Setting the destinations of traps and e-mail via the MMB

You can set the destinations of traps and mail sent via the MMB by using the Web-UI.

- For details on MMB trap destinations, see [7.5.2 Configuring SNMP](#).
- For details on e-mail destinations, see [3.3.9 Configuring Alarm E-Mail](#).

Remarks

- Make settings only as needed.
- Operations management software, such as Systemwalker, needs these settings to manage events by partition.

Configuring SNMP to use duplicate disks

For details on how to configure SNMP to use duplicate disks, see [6.2.8 Configuring SNMP to use duplicate disks](#).

B.1.7 Installing a PSA update

For details on how to install a PSA update, see [6.2.9 Installing a PSA update](#).

B.1.8 Uninstalling PSA

For details on how to uninstall PSA, see [6.2.10 Uninstalling PSA](#).

B.2 Manually Installing PSA (Windows Server 2003)

This section describes how to install PSA in Windows Server 2003. You need to log in with Administrator privileges for installation.

Remarks

To operate the PRIMEQUEST 1800E, you need to first install PSA. Otherwise, the following restrictions apply.

- I/O (e.g., PCI Express card, hard disk) failure notification and trap notification to the administrator are disabled.
- Failure notification using symptom detection and trap notification to the administrator are disabled.
 - Threshold exceeded in S.M.A.R.T. monitoring of HDDs
- Operations management software cannot collect information on the partition side.
- Even under an REMCS agreement, no software errors are reported.

B.2.1 Installation flow

For the PSA installation flow, see [CHAPTER 4 Installing the Operating System and Bundled Software](#). For details on how to configure PSA, see [CHAPTER 6 Work after Operating System Installation \(PRIMEQUEST 1800E\)](#).

Remarks

- If you use SVIM to install the operating system, you need not install PSA. However, after installation with SVIM, you need to check and make settings according to [B.2.2 Checks before PSA installation](#) and [B.2.5 Settings after PSA installation](#).
- After installing PSA, execute the SNMP security setting command (setsnmpsec) before you perform the operation in the following situations. For details on the command, see 4.8 SNMP Security Setting Command (setsnmpsec) in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).
 - You will be changing the SNMP Service security setting from [Accept SNMP packets from any host] to [Accept SNMP packets from these hosts].
 - You will be changing the MMB IP address.
- In the initial startup of PSA after installation, the Web-UI may display the error message "E_33077 PSA is Not Active. (01:0000)" in the [PSA] window. This happens because PSA requires extra time to acquire system sensor data only during the initial startup. Wait a few minutes. Then, refresh the display.
- If you change the MMB IP address or the IP address of the PSA-to-MMB communication LAN, you need to then restart PSA. Otherwise, a display error may occur in the [PSA] window of the Web-UI. Moreover, PSA would not be able to post any detected errors.

Notes on configuring Windows Server 2003

- Do not enable [Visual Notification] in the options of Dr. Watson (diagnosis software supplied with Windows). Otherwise, if a PSA error occurs, a message box appears. You cannot restart PSA until you close this box.
- From [Properties] in the Event Viewer, do not change the operation in [When maximum log size is reached] for the system log or application log to [Do not overwrite events (clear log manually)]. Otherwise, after the log reaches the maximum log size, no errors are output to the log, so PSA will be unable to detect any errors.
- Do not stop the Windows Print Spooler service. The information collection function of the operating system uses WMI (Windows Management Instrumentation). If the Print Spooler service is stopped, the function cannot collect the correct configuration information because WMI reports an error.

- If the set value of the following registry key is less than 20000 (20 seconds), the system may hang during operating system shutdown. Be sure to set a value equal to or greater than 20000 (20 seconds). The default is 20000.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control \WaitToKillServiceTimeout

You can use the above registry key to specify the wait time (ms) before the service is terminated in the shutdown sequence.

B.2.2 Checks before PSA installation

This section describes the checks to make before PSA installation.

[Confirming PSA-to-MMB communication LAN settings](#)

[Confirming management LAN settings](#)

[Confirming the services required for PSA operation](#)

Confirming PSA-to-MMB communication LAN settings

For details on how to confirm PSA-to-MMB communication LAN settings, see [6.3.1 Configuring the PSA-to-MMB communication LAN](#).

Confirming management LAN settings

For details on how to confirm management LAN settings, see [6.3.2 Confirming management LAN settings](#).

Confirming the services required for PSA operation

SNMP Service is required for PSA operation. Confirm the installation of SNMP Service by using the following procedure.

Remarks

These operations require the Windows installation DVD.

Operations

1. Select [Control Panel] - [Add or Remove Programs] - [Add/Remove Windows Components].
The Windows Component Wizard appears.
2. Select [Management and Monitoring Tools]. Then, click the [Details] button.
The [Management and Monitoring Tools] dialog box appears.
3. Confirm that the [Simple Network Management Protocol (SNMP)] check box is checked. Then, click the [OK] button.
The screen returns to the Windows Component Wizard.

Remarks

If the check box is not checked, SNMP Service has not been installed. To install SNMP Service, check the check box.

Click the [Next] button in the Windows Component Wizard window. Follow the instructions of the wizard for installation.

B.2.3 Installing PSA

Install the PSA package.

Prepare the ServerView Suite DVD supplied with the main unit.

Operations

1. Execute Tools\General\PSA\fjpsaxxxx.exe (xxxx: Version number).

The following window appears for installation preparations.

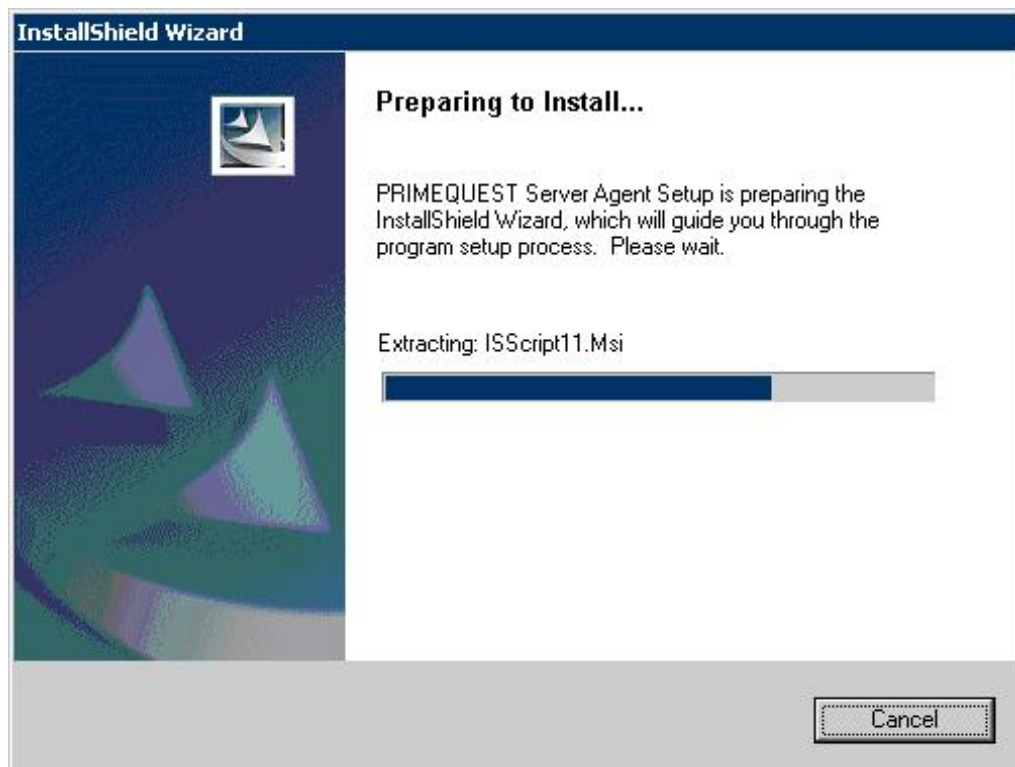


FIGURE B.1 Preparing to Install window

2. After the installation preparations are complete, the following window appears. Click the [Next] button to proceed.

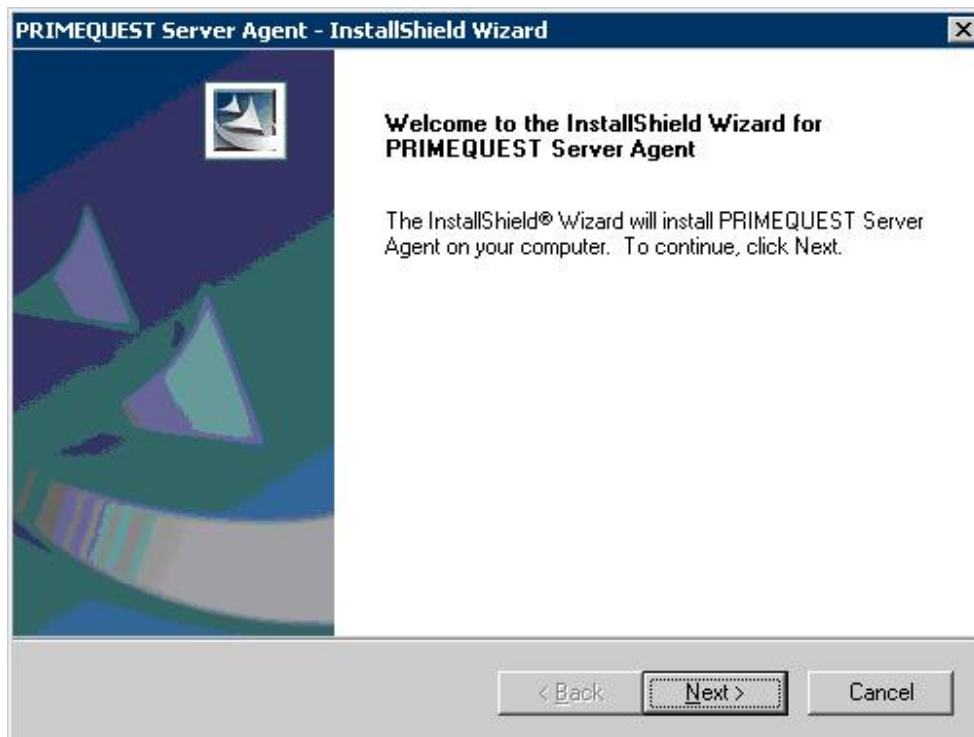


FIGURE B.2 Setup window

3. Specify the installation destination. Then, click the [Next] button.

The default installation path for PSA is Program Files\Fujitsu or Program Files(x86)\Fujitsu. To change the installation destination, click the [Browse] button and specify another installation destination.

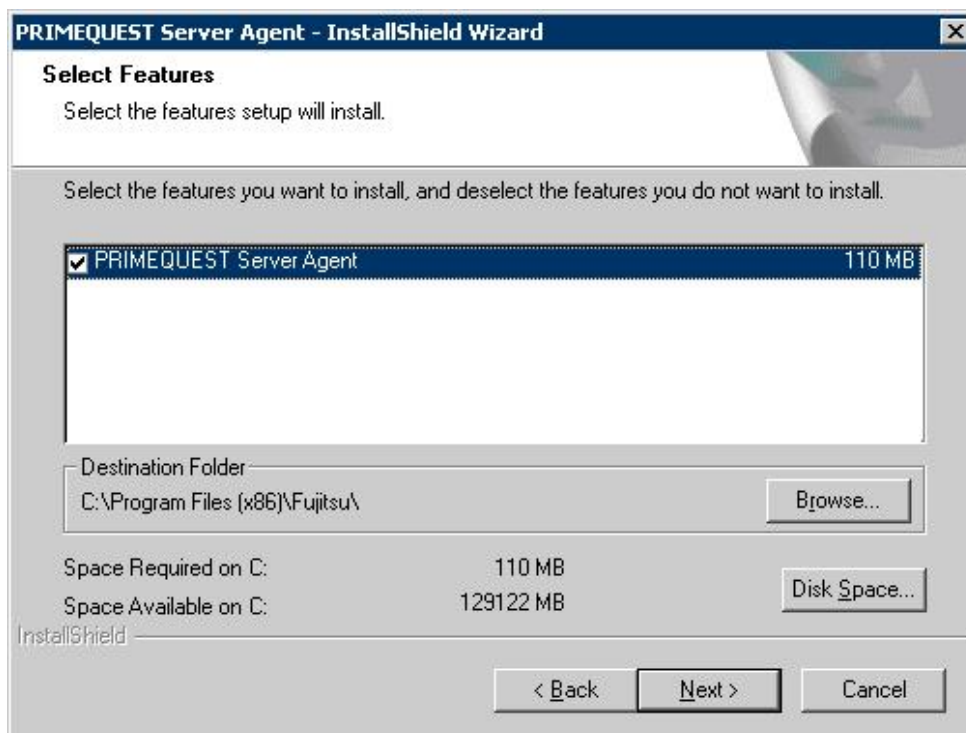


FIGURE B.3 Select Features window

4. After the installation is completed, the following window appears. Click the [Finish] button.

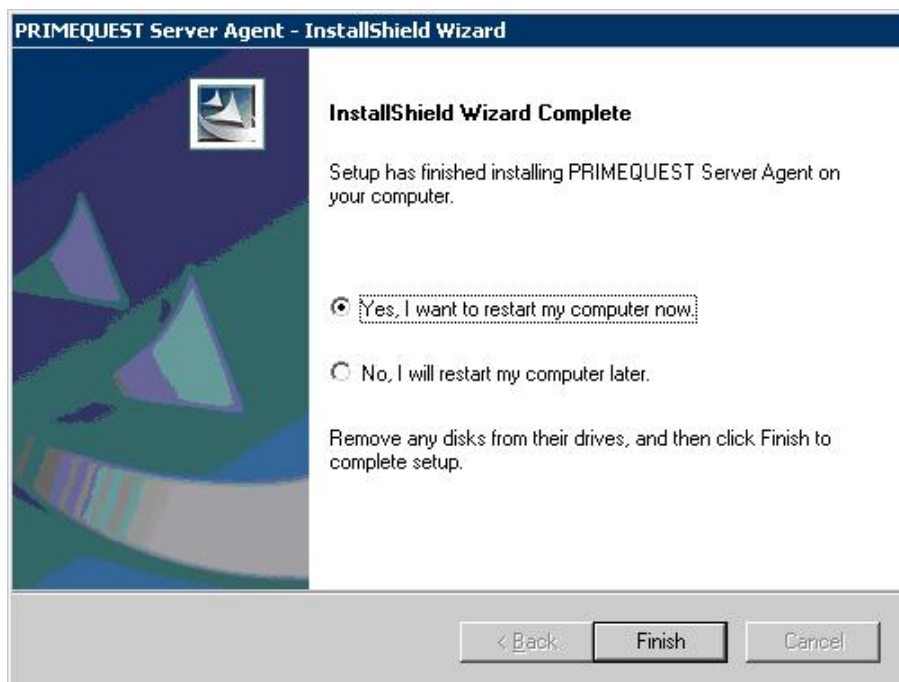


FIGURE B.4 Setup complete window

5. You may need to restart your computer. If so, a confirmation dialog box appears. The dialog box asks whether you want to restart the computer immediately.
Check whether the computer can be restarted at this time. If the computer can be restarted, select the restart option and click the [Finish] button.

B.2.4 Automatic configuration during PSA installation

This section describes the values automatically set for PSA operation during PSA installation.

Service settings

- PRIMEQUEST Server Agent
- PRIMEQUEST PEM Command Service
- PRIMEQUEST PSA Environment Control Service

Environment variable settings

- PATH variables
The values used for PSA are added to existing PATH variables.
- FJSVpsa_INSTALLPATH variable
A new variable is added.

Port setting

The TCP:24450 port is set for use by PSA.

SNMP security settings

Security is set for SNMP Service because PSA needs to accept SNMP packets from the MMB.

The settings depend on the selected items on the [Security] tab in the [SNMP Service Properties] dialog box during PSA installation.

- With [Accept SNMP packets from any host] selected:
SNMP security is not configured.
- With [Accept SNMP packets from these hosts] selected:
If neither the MMB IP address nor localhost is set, SNMP security is configured.

WMI (Windows Management Instrumentation) settings

PSA uses WMI to acquire information on PCI Express cards and SCSI devices. WMI is installed as standard with Windows.

These settings include settings on the size of memory and number of internal handles used by WMI to collect this information. If the system has many LUNs for devices such as RAIDs, it may not have sufficient memory or internal handles. For this reason, the settings are changed to the following values:

- Upper limit on memory used: 536,870,912 bytes
- Upper limit on internal handles: 65,536

B.2.5 Settings after PSA installation

This section describes the settings for items after PSA installation.

[Setting the destinations of traps from a partition](#)

[Setting the destinations of traps and e-mail via the MMB](#)

[Configuring the Windows Firewall](#)

[Setting Watchdog for monitoring after a STOP error \(fatal system error\)](#)

Setting the destinations of traps from a partition

For details on how to set the destinations of traps from a partition, see [6.3.3 Setting the destinations of traps from a partition](#).

Setting the destinations of traps and e-mail via the MMB

For details on how to set the destinations of traps and e-mail via the MMB, see [6.3.4 Setting the destinations of traps and e-mail via the MMB](#).

Configuring the Windows Firewall

For details on how to configure the Windows Firewall, see [6.3.5 Configuring the Windows Firewall](#).

Setting Watchdog for monitoring after a STOP error (fatal system error)

For details on how to set Watchdog for monitoring after a STOP error (fatal system error), see [6.3.6 Setting the Watchdog Timer for monitoring after a STOP error \(fatal system error\)](#).

B.2.6 Installing a PSA update

For details on how to install a PSA update, see [6.3.8 Installing a PSA update](#).

B.2.7 Uninstalling PSA

For details on how to uninstall PSA, see [6.3.9 Uninstalling PSA](#).

B.3 Manually Installing PSA (Windows Server 2008)

This section describes how to install PSA in Windows Server 2008. You need to log in with Administrator privileges for installation. To install the PSA as a non-Administrator user with Administrator privileges, right-click the file, and select [Execute as Administrator] from the menu that appears. Then, install PSA.

Remarks

To operate the PRIMEQUEST 1800E, you need to first install PSA. Otherwise, the following restrictions apply.

- I/O (e.g., PCI Express card, hard disk) failure notification and trap notification to the administrator are disabled.
- Failure notification using symptom detection and trap notification to the administrator are disabled.
 - Threshold exceeded in S.M.A.R.T. monitoring of HDDs
- Operations management software cannot collect information on the partition side.
- Even under an REMCS agreement, no software errors are reported.

B.3.1 Installation flow

For the PSA installation flow, see [CHAPTER 4 Installing the Operating System and Bundled Software](#). For details on how to configure PSA, see [CHAPTER 6 Work after Operating System Installation \(PRIMEQUEST 1800E\)](#).

Remarks

- If you use SVIM to install the operating system, you need not install PSA. However, after installation with SVIM, you need to check and make settings according to [B.3.2 Checks before PSA installation](#) and [B.3.5 Settings after PSA installation](#).
- After installing PSA, execute the SNMP security setting command (setsnmpsec) before you perform the operation in the following situations. For details on the command, see 4.8 SNMP Security Setting Command (setsnmpsec) in the *PRIMEQUEST 1000 Series Tool Reference* (C122-E110EN).
 - You will be changing the SNMP Service security setting from [Accept SNMP packets from any host] to [Accept SNMP packets from these hosts].
 - You will be changing the MMB IP address.
- In the initial startup of PSA after installation, the Web-UI may display the error message "E_33077 PSA is Not Active. (01:0000)" in the [PSA] window. This happens because PSA requires extra time to acquire system sensor data only during the initial startup. Wait a few minutes. Then, refresh the display.
- If you change the MMB IP address or the management LAN IP address on the partition, be sure to then restart PSA. Otherwise, a display error may occur in the [PSA] window of the Web-UI. Moreover, PSA would not be able to post any detected errors.

Notes on configuring Windows Server 2008

- Do not stop the Windows Print Spooler service. The information collection function of the operating system uses WMI (Windows Management Instrumentation). If the Print Spooler service is stopped, the function cannot collect the correct configuration information because WMI reports an error.
- If the set value of the following registry key is less than 20000 (20 seconds), the system may hang during operating system shutdown. Be sure to set a value equal to or greater than 20000 (20 seconds).

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control "WaitToKillServiceTimeout" (Type: REG_DWORD / default; 20000)

You can use the above registry key to specify the wait time (ms) before the service is terminated in the shutdown sequence.

- The event log may have the following message recorded during PSA startup. It does not indicate any operational problem.

"PM child process abnormal end [6:750] (tag) 1:0x00000000"

FJSVpsa Event ID 62

B.3.2 Checks before PSA installation

This section describes the checks to make before PSA installation.

[Confirming PSA-to-MMB communication LAN settings](#)

[Confirming the services required for PSA operation](#)

Confirming PSA-to-MMB communication LAN settings

For details on how to configure the PSA-to-MMB communication LAN, see [6.4.1 Configuring the PSA-to-MMB communication LAN](#)

Confirming the services required for PSA operation

SNMP Service is required for PSA operation. Add SNMP Service by using the following procedure.

Operations

1. Click [Start] - [Administrative Tools] - [Server Manager].
2. Select [Features] - [Add Function] - [SNMP Service] in the [Server Manager] window.
3. Confirm that the [SNMP Service] check box is checked. Then, click the [OK] button.
The screen returns to the Windows Component Wizard.

Remarks

If the check box is not checked, SNMP Service has not been installed. To install SNMP Service, check the check box.

Click the [Next] button in the Windows Component Wizard window. Follow the instructions of the wizard for installation.

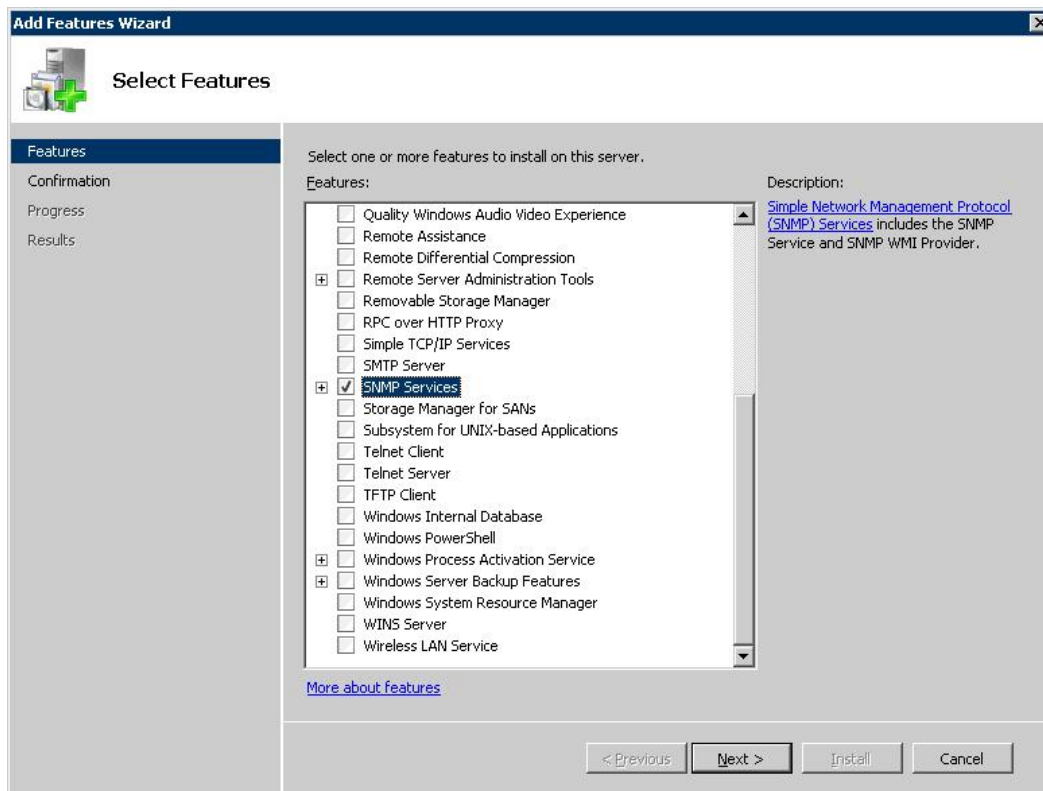


FIGURE B.5 Select Features window

B.3.3 Installing PSA

Install the PSA package.

Prepare the ServerView Suite DVD supplied with the main unit.

Operations

1. Execute Tools\General\PSA\fjpsaxxx.exe (xxxx: Version number).

The following window appears for installation preparations.



FIGURE B.6 Preparing to Install window

2. The following window appears when installation preparations are completed. Click the [Next] button to proceed.

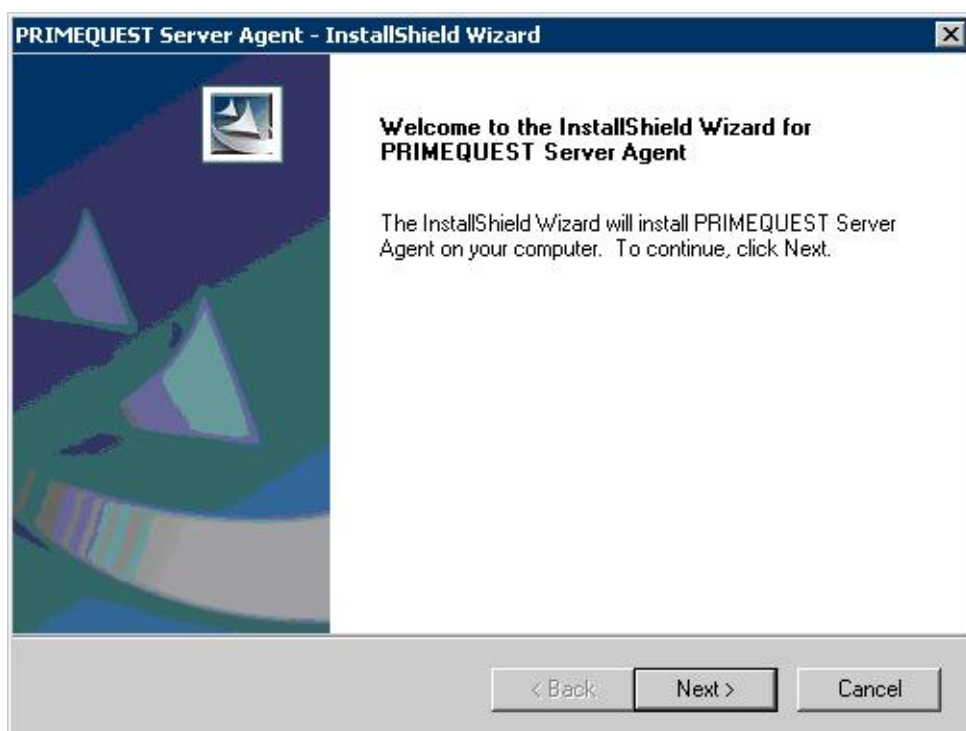


FIGURE B.7 Setup window

3. Specify the installation destination. Then, click the [Next] button.

The default installation path for PSA is Program Files\Fujitsu or Program Files(x86)\Fujitsu. To change the installation destination, click the [Browse] button and specify another installation destination.

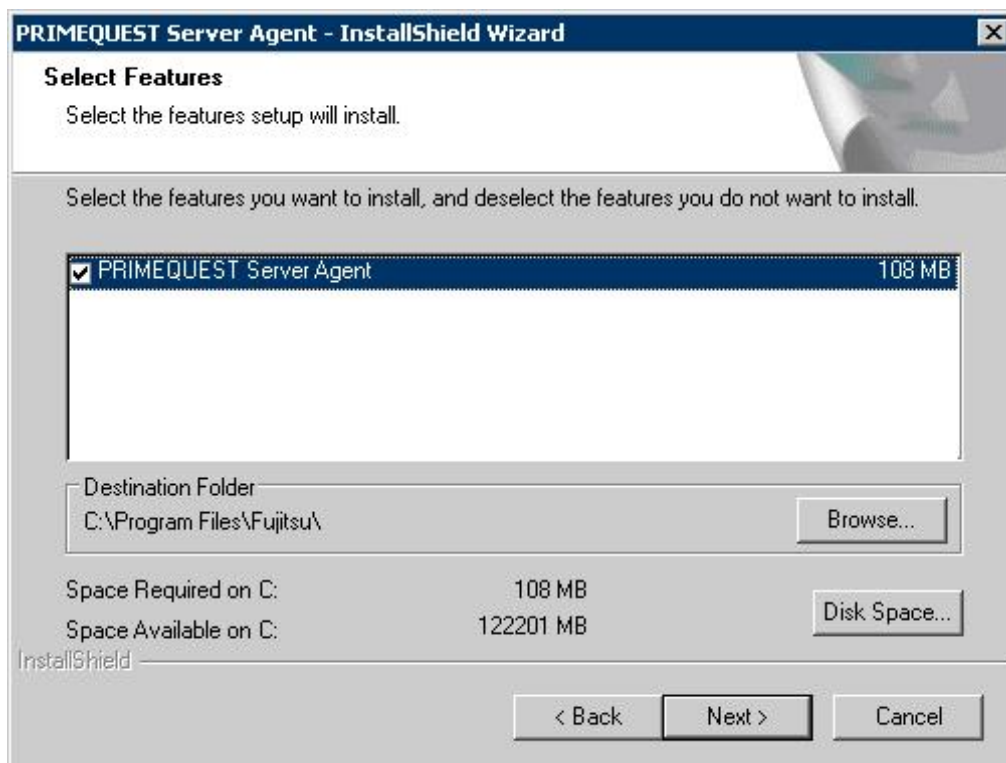


FIGURE B.8 Select Features window

4. After the installation is completed, the following window appears. Click the [Finish] button.
5. You may need to restart your computer. If so, a confirmation dialog box appears. The dialog box asks whether you want to restart the computer immediately.
Check whether the computer can be restarted at this time. If the computer can be restarted, select the restart option and click the [Finish] button.

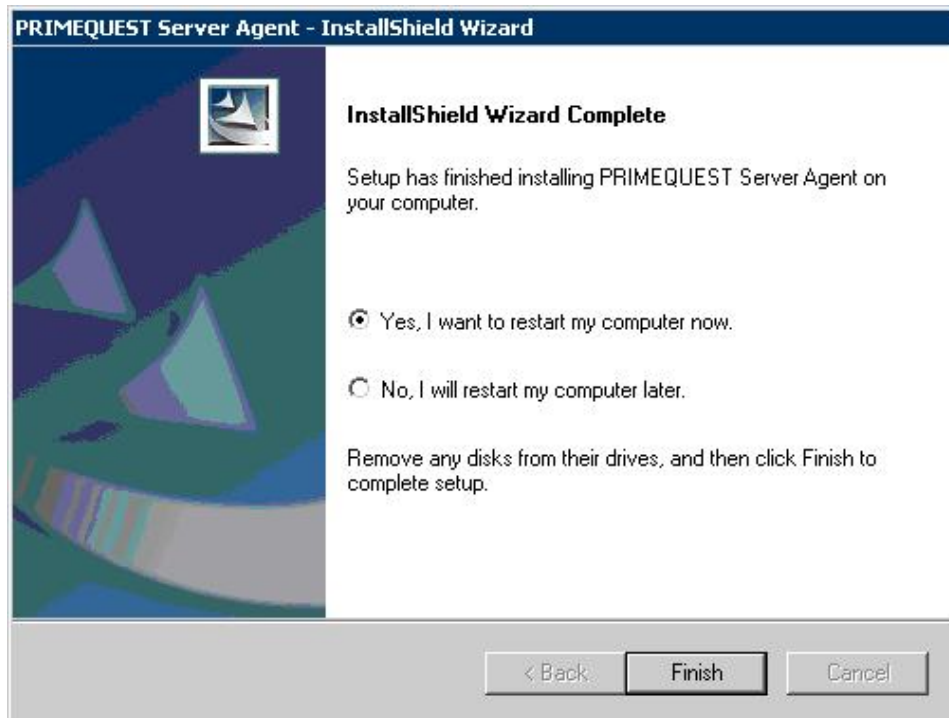


FIGURE B.9 Installation complete window

B.3.4 Automatic configuration during PSA installation

This section describes the values automatically set for PSA operation during PSA installation.

Service settings

- PRIMEQUEST Server Agent
- PRIMEQUEST PEM Command Service
- PRIMEQUEST PSA Environment Control Service

Environment variable settings

- PATH variables
The values used for PSA are added to existing PATH variables.
- FJSVpsa_INSTALLPATH variable
A new variable is added.

Port setting

The TCP:24450 port is set for use by PSA.

SNMP security settings

The PSA installation configures SNMP Service security because PSA needs to accept SNMP packets from the MMB.

The settings depend on the selected items on the [Security] tab in the [SNMP Service Properties] dialog box during PSA installation.

- With [Accept SNMP packets from any host] selected:
SNMP security is not configured.
- With [Accept SNMP packets from these hosts] selected:
If neither the MMB IP address nor localhost is set, SNMP security is configured.

B.3.5 Settings after PSA installation

This section describes the settings for items after PSA installation.

[Setting the destinations of traps from a partition](#)

[Setting the destinations of traps and e-mail via the MMB](#)

[Configuring the Windows Firewall](#)

[Setting Watchdog for monitoring after a STOP error \(fatal system error\)](#)

[Installing the PSBED Plugin driver](#)

Note

From [Properties] in the Event Viewer, do not change the operation in [When maximum log size is reached] for the system log or application log to [Do not overwrite events (clear log manually)]. Otherwise, after the log reaches the maximum log size, no errors are output to the log, so PSA will be unable to detect any errors.

Setting the destinations of traps from a partition

For details on how to set the destinations of traps from a partition, see [6.4.4 Setting the destinations of traps from a partition](#).

Setting the destinations of traps and e-mail via the MMB

For details on how to set the destinations of traps and e-mail via the MMB, see [6.4.5 Setting the destinations of traps and e-mail via the MMB](#).

Configuring the Windows Firewall

For details on how to configure the Windows Firewall, see [6.4.6 Configuring the Windows Firewall](#).

Setting Watchdog for monitoring after a STOP error (fatal system error)

For details on how to set Watchdog for monitoring after a STOP error (fatal system error), see [6.4.7 Setting the Watchdog Timer for monitoring after a STOP error \(fatal system error\)](#).

Installing the PSBED Plugin driver

For details on how to install the PSBED Plugin driver, see [6.4.3 Installing the PSBED Plugin driver](#).

APPENDIX C Software (Links)

For details on the software bundled with the PRIMEQUEST 1000 series hardware, see 3.3 Bundled Software in the *PRIMEQUEST 1000 Series General Description* (C122-B022EN).

C.1 General Description and Types of Bundled Software	
270	

C.1 General Description and Types of Bundled Software

See 3.3 Bundled Software in the *PRIMEQUEST 1000 Series General Description* (C122-B022EN).

APPENDIX D Configuring the SAN Boot Environment

For details on configuring the SAN boot environment, see the
*PRIMEQUEST 1000 Series SAN Boot Environment Configuration
Manual* (C122-E155EN).

APPENDIX E Notes on VMware Installation

This appendix describes how to install VMware vSphere, using a RAID environment configured in built-in hard disks as an example. It also provides notes on installation.

VMware vSphere is referred to below as VMware 4.x, VMware 5.x, or VMware.

E.1 Building a RAID Environment Using VMware 4.x Built-in Disks	273
E.2 Notes on VMware 4.x Installation	274
E.3 Installing VMware 4.x Bundled Software	277
E.4 Settings after VMware 4.x PSA Installation	282
E.5 Settings after VMware 4.x SVMco Installation	292
E.6 Building a RAID Environment Using VMware 5.x Built-in Disks	293
E.7 Installing VMware 5.x Bundled Software	294

E.1 Building a RAID Environment Using VMware 4.x Built-in Disks

The PRIMEQUEST 1000 series supports RAID 0, RAID 1, RAID 1E, RAID 5, RAID 6, and RAID 10 that use built-in hard disks.

For details on building a RAID configuration using built-in hard disks, see the *MegaRAID SAS Software*, the *MegaRAID SAS Device Driver Installation*, and the *Modular RAID Controller Installation Guide*.

E.2 Notes on VMware 4.x Installation

Install VMware 4.x by following the instructions in the *VMware vSphere 4.x Software Handbook*.

For details on the VMware 4.x information and procedures that you need to know for PRIMEQUEST system configuration, contact the distributor where you purchased your product, or your sales representative.

Note the following points during VMware 4.x installation.

- To make the network settings for the PRIMEQUEST 1800E, use the steps in [E.4 Settings after VMware 4.x PSA Installation](#).
- After completing the installation, press the [Alt] + [F1] keys to log in to the ESX Console.

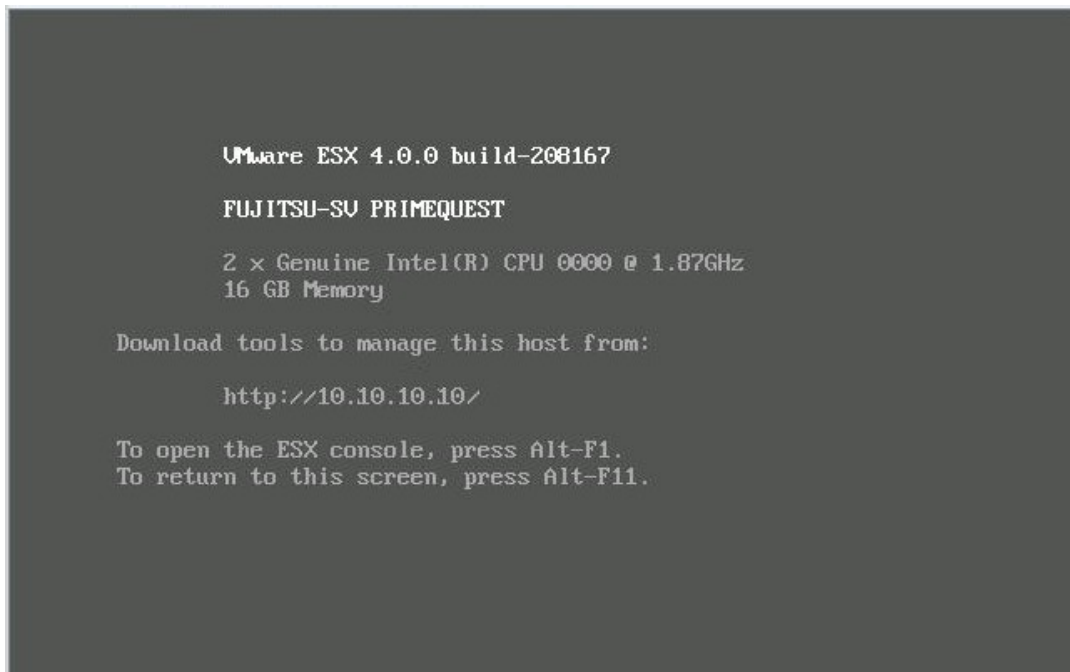


FIGURE E.1 Completion of VMware 4.x installation

- When VMware 4.x is used, fatal system errors such as a panic are not detected automatically. Therefore, perform the following procedures after installation and set the Watchdog Timer for detecting such fatal system errors.
For setting the Watchdog Timer monitoring, use ServerView Operations Manager (V4.92-14 or later).

Note

The setting procedure varies with the version of ServerView Operations Manager (SVOM) being used. Check the version number, and follow the appropriate procedure below.

When using SVOM 4.92

1. Start ServerView Operations Manager.
2. Select [ServerList].
3. Right-click the target partition in the server list on the left side. Select [Maintenance] - [ASR Properties] from the displayed menu.
4. Select [Watchdog] in the displayed window.
5. Specify the following for [Software], and click [Apply].
 - Check the [Active] check box.
 - Select [Continue] for [Action] for cases of abnormal operation.

- Enter a value between 1 and 100 minutes for [Timeout].

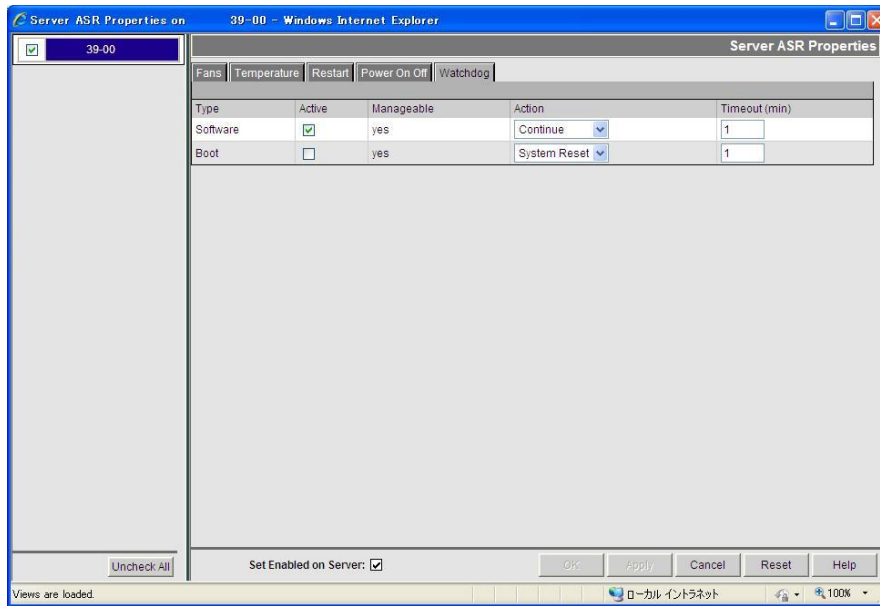


FIGURE E.2 [Watchdog] tab in the VMware 4.x software window

6. Enter your user name and password, and press the [Enter] key.

When using SVOM 5.0 or later

1. Start ServerView Operations Manager.
2. Select [Server Configuration].

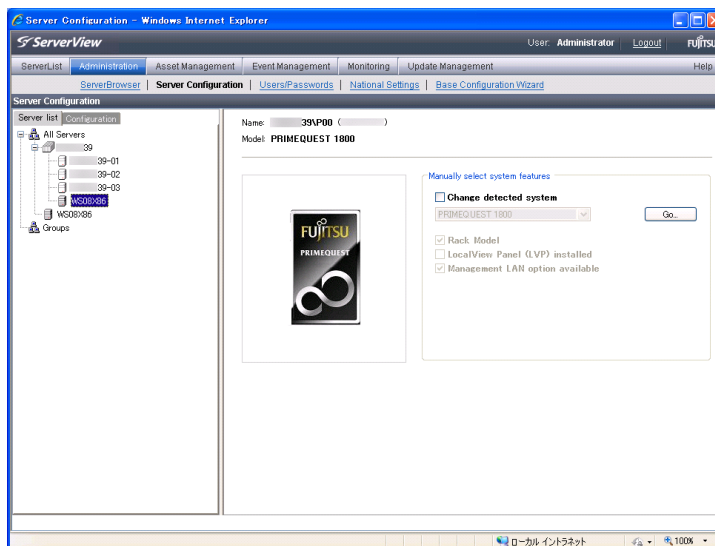


FIGURE E.3 [Server Configuration] window

3. Select the target partition in the server list on the left side. Wait a moment.
When the model name appears, click the [Go] button.
4. Select [Software Watchdog] in the displayed window.
5. Specify the following for [Software Watchdog Setting], and click the [Save Page] button.
 - Check the [Activate] check box.
 - Select [Continue] for [Action].
 - Enter a value between 1 and 100 minutes for [Waiting time], and click the [Save Page] button.

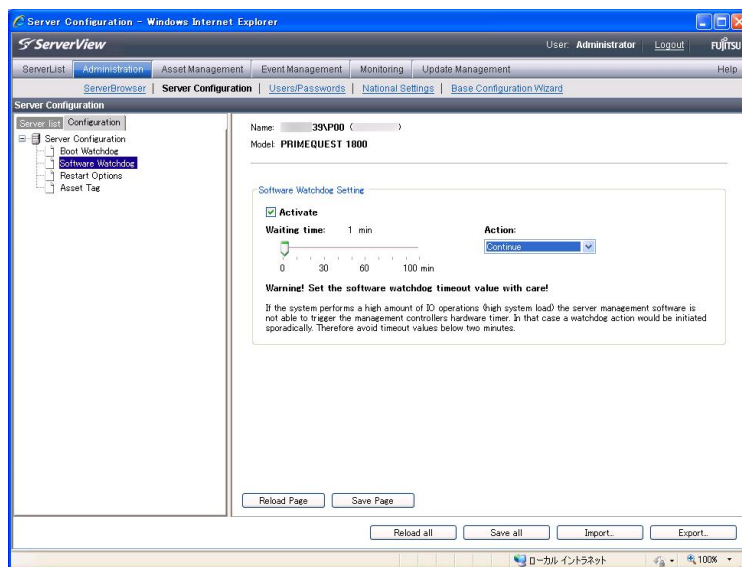


FIGURE E.4 [Software Watchdog] window

E.3 Installing VMware 4.x Bundled Software

The bundled software is stored in ServerView Suite DVD1. Copy the files from ServerView SuiteDVD1 and use them.

E.3.1 Installing ServerView Agent

Install ServerView Agent by referring to the following manuals:

- ServerView Suite

ServerView Operations Manager V4.92

Installation ServerView Agents for Linux

Installation ServerView Agents (SuSE, Red Hat and VMware 4.x)

Installation ServerView Update Agent

Note the following points during the installation.

- Even if ServerView Suite DVD1 is inserted into the drive, the media is not mounted automatically. Execute the mount command.

```
# mount -t udf /dev/cdrom /MNT
```

* MNT is the mount point.

- Use the files for V4.92, which are stored in the following directory:

```
/MNT/SVSSoftware/Software/ServerView/Linux/Agents_V492
```

* MNT is the mount point.

E.3.2 Installing ServerView RAID

This section describes how to install ServerView RAID.

1. Start the terminal with root privileges.
2. Mount ServerView Suite DVD1.
3. Execute the following command.

```
# rpm -ivh /MNT/SVSSoftware \  
/Software/ServerView/Linux/ServerView_RAID/\  
ServerView_RAID-XXX.i686.rpm
```

* MNT is the mount point.

\: This indicates that there is no line feed.

XXX depends on the version or operating system distribution.

E.3.3 Installing RAS Support Service (PRIMEQUEST)

This section describes how to install the RAS Support Service (PRIMEQUEST).

1. Start the terminal with root privileges.
2. Mount ServerView Suite DVD1.
3. Copy the RAS support service module to any directory of the PRIMEQUEST 1000 series, and extract it.

```
# cp MNT/SVSLocalTools/Japanese/RASAssist/Linux/\
LinuxRAS.tgz /tmp
# cd /tmp
# tar xvzf LinuxRAS.tgz
```

*: MNT is the mount point.

\: This indicates that there is no line feed.

In the above example, /tmp is an arbitrary directory.

4. Execute the following commands to install the expansion package (web server).

```
# cd MTEP
# ./install
# cd ..
```

5. Execute the following command to install the RAS support service.

```
# ./rasinstall
```

E.3.4 Installing VMware 4.x HRM/server (PRIMEQUEST)

This section describes how to install HRM/server (PRIMEQUEST)

For PRIMEQUEST 1800E2

1. Start the terminal with root privileges.
2. Mount ServerView Suite DVD1.
3. Copy the HRM/server module to any directory of the PRIMEQUEST 1000 series server. Then, expand the files.

```
# cp MNT/SVSLocalTools/Japanese/HRM/Linux/\FJSVhrm.tgz /tmp
```

MNT is the mount point.

\: This indicates that there is no line feed.

In the above example, the "any directory" is /tmp.

```
# cd /tmp
# tar xvzf FJSVhrmsr.tgz
```


4. Execute the following command.

```
# ./hrm_install_sr.sh
```

5. When the following message appears, press the [N] key.

```
Select HRM Install Mode : Use PRIMEQUEST Server Agent? [Y/N]: N
```

For PRIMEQUEST 1800E

The procedure differs depending on whether ServerView Suite DVD1 has the HRM/SR_Linux/FJSVhrmsr.tgz. See the respective procedure for each of the following:

- HRM/SR_Linux/FJSVhrmsr.tgz is not available
- HRM/SR_Linux/FJSVhrmsr.tgz is not available, and HRM/Linux/FJSVhrm.tgz is available
- HRM/SR_Linux/FJSVhrmsr.tgz is available

1. Start the terminal with root privileges.
2. Mount ServerView Suite DVD1.
3. Copy the HRM/server module to any directory of the PRIMEQUEST 1000 series server. Then, expand the files.

```
# cp MNT/SVSLocalTools/Japanese/HRM/SR_Linux/ \
FJSVhrmsr.tgz /tmp
```

MNT is the mount point.

\: This indicates that there is no line feed.

In the above example, the "any directory" is /tmp.

```
# cd /tmp
# tar xvfz FJSVhrmsr.tgz
```

4. Execute the following command.

```
# ./hrm_install.sh
```

5. When the following message appears, press the [Y] key

```
Select HRM Install Mode : Use PRIMEQUEST Server Agent? [Y/N]: Y
```

- When HRM/SR_Linux/FJSVhrmsr.tgz is not available and HRM/Linux/FJSVhrm.tgz is available

1. Start the terminal with root privileges.

2. Mount ServerView Suite DVD1.

3. Copy the HRM/server module to any directory of the PRIMEQUEST 1000 series server. Then, expand the files.

```
# cp MNT/SVSLocalTools/Japanese/HRM/Linux/ \
FJSVhrm.tgz /tmp
```

MNT is the mount point.

\: This indicates that there is no line feed.

In the above example, the "any directory" is /tmp.

```
# cd /tmp
# tar xvfz FJSVhrmsr.tgz
```

4. Execute the following command.

```
# ./hrm_install.sh
```

5. When the following message appears, press the [Y] key

```
Select HRM Install Mode : Use PRIMEQUEST Server Agent? [Y/N]: Y
```

E.3.5 Installing VMware 4.x PSA

This section describes how to install PSA.

Remarks

PSA is provided only with the PRIMEQUEST 1800E.

1. Start the terminal with root privileges.
2. Mount ServerView Suite DVD1.
3. Copy the PSA module to any directory of the PRIMEQUEST 1000 series server. Then, expand the files.

```
# cp MNT/SVSLocalTools/Japanese/PSA/SR_Linux/\
FJSVpsa-XXXRHEL5.tgz /tmp
```

* MNT is the mount point.

\: This indicates that there is no line feed.

XXX depends on the version.

In the above example, the "any directory" is /tmp.

```
# cd /tmp
# tar xvzf FJSVpsa-XXXRHEL5.tar.gz
```

4. Execute the following command.

```
# cd FJSVpsa
# ./INSTALL.sh -SVIM
```

5. After the installation of PSA, make the required settings. For details on the setting method, see *PSA Setting Procedure for VMware* and [6.2 Configuring PSA \(Linux: Red Hat Enterprise Linux\)](#).

E.3.6 Installing SVMco

For details on installing SVMco, see the SVMco manual.

E.4 Settings after VMware 4.x PSA Installation

The settings after PSA installation for VMware 4.x partly differ from those for RHEL. This section describes only the different parts.

For details on the parts of the setting procedure that are the same as those for RHEL, see the following.

TABLE E.1 Settings after PSA Installation (VMware 4.x)

Settings after PSA installation	For VMware 4.x
Configuring the PSA-to-MMB communication LAN	E.4.1 Configuring the network
Confirming management LAN settings	E.4.1 Configuring the network
Confirming SELinux function settings	(No settings required)
Confirming the firewall function	E.4.2 Configuring the firewall
Setting the destinations of traps from a partition	Same as for RHEL 6.2.5 Setting the destinations of traps from a partition
Setting the destinations of traps and e-mail via the MMB	Same as for RHEL 6.2.6 Setting the destinations of traps and e-mail via the MMB
Setting the management LAN IP address	Same as for RHEL 6.2.7 Setting the management LAN IP address
Configuring SNMP to use duplicate disks	Same as for RHEL 6.2.8 Configuring SNMP to use duplicate disks
Configuring the default gateway	E.4.3 Configuring the default gateway

Remarks

PSA is provided only with the PRIMEQUEST 1800E.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

E.4.1 Configuring the network

This section describes the network settings required to install and operate PSA.

Use the following workflow to perform the work.

[Confirming the PSA-to-MMB communication LAN and management LAN](#)

[Configuring the management LAN](#)

[Configuring the PSA-to-MMB communication LAN](#)

Usually, the network is configured as shown below immediately after the installation of the operating system.

The interface name, BUS number, and other names must be replaced with suitable character strings according to the environment.

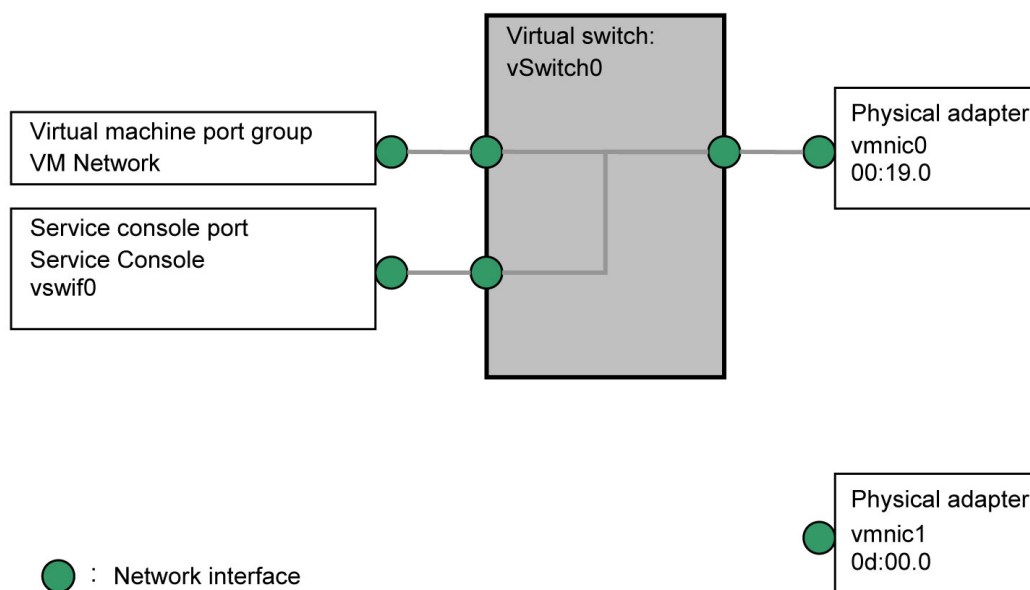


FIGURE E.5 Network configuration immediately after installation of OS

Remark

For details on each command used in the settings below, use `man` for confirmation.

Note

Do not set the host name before setting the IP address of `vswif0`, which exists by default immediately after the installation of the operating system. If you do so, VMware 4.x may change the value of `/etc/hosts` to an unintended value.

The description here is based on the assumption that `vswif0` is used as the management LAN.

Confirming the PSA-to-MMB communication LAN and management LAN

1. The PSA-MMB communication LAN uses the physical adapter assigned BUS number 0000:00:19.0.
 The management LAN uses an arbitrary physical adapter.
 Execute the `esxcfg-nics` command to confirm the physical adapters used for the PSA-to-MMB communication LAN and management LAN.

```
# esxcfg-nics -l
Name   PCI    Driver  Link   Speed  Duplex\
MAC    Address      MTU    Description
vmnic0  00:19.00    e1000e  Up     100Mbps  Half \
00:17:42:de:7c:4b  1500 \
Intel Corporation 82567LF-2 Gigabit Network Connection
vmnic1  0d:00.00    igb     Up     100Mbps  Full \
00:17:42:9b:dc:b4  1500 \
Intel Corporation 82576 Gigabit Network Connection
vmnic2  0d:00.01    igb     Down   0Mbps   Half \
00:17:42:9b:dc:b5  1500 \
Intel Corporation 82576 Gigabit Network Connection
```

\: This indicates that there is no line feed.

In the above example, vmnic0 is used for the PSA-to-MMB communication LAN, and vmnic1 is used for the management LAN.

Configuring the management LAN

1. Use vswif0, which exists by default immediately after the installation of the operating system, for the interface of the management LAN.

Execute the esxcfg-vswif command to confirm the status of vswif0.

```
# esxcfg-vswif -l
Name Port Group/DVPort IP Family IP Address \
Netmask Broadcast Enabled TYPE
vswif0 Service Console IPv4 N/A \
N/A N/A true NONE
```

\: This indicates that there is no line feed.

The above example shows that vswif0 has been set for the Port Group name of "Service Console."

2. Execute the esxcfg-vswitch command to confirm the status of the virtual switch.

```
# esxcfg-vswitch -l
Switch Name Num Ports Used Ports Configured Ports \
MTU Uplinks
vSwitch0 64 2 64 \
1500 vmnic0

PortGroup Name VLAN ID Used Ports Uplinks
VM Network 0 0 vmnic0
Service Console 0 1 vmnic0
```

\: This indicates that there is no line feed.

The above example shows that Service Console exists in vSwitch0, and the physical adapter is vmnic0.

3. Disconnect the physical adapter from vSwitch0, and then connect the physical adapter vmnic1, which is used for the management LAN, to vSwitch0.

```
Execute the esxcfg-vswitch command to disconnect the physical
adapter vmnic0 from vSwitch0.
# esxcfg-vswitch -U vmnic0 vSwitch0
# esxcfg-vswitch -l
Switch Name Num Ports Used Ports Configured Ports \
MTU Uplinks
vSwitch0 64 2 64 \
1500
```

PortGroup Name	VLAN ID	Used Ports	Uplinks
VM Network	0	0	
Service Console	0	1	

Execute the esxcfg-vswitch command to connect the physical adapter vmnic1 to vSwitch0.

```
# esxcfg-vswitch -L vmnic1 vSwitch0
# esxcfg-vswitch -l
Switch Name Num Ports Used Ports Configured Ports \
MTU Uplinks
vSwitch0 64 2 64 \
1500 vmnic1

PortGroup Name VLAN ID Used Ports Uplinks
VM Network 0 0 vmnic1
Service Console 0 1 vmnic1
```

4. Execute the esxcfg-vswif command to assign the IP address (192.168.0.2) to vswif0.

```
# esxcfg-vswif -i 192.168.0.2 -n 255.255.255.0 vswif0
# esxcfg-vswif -l
Name Port Group/DVPort IP Family IP Address \
Netmask Broadcast Enabled TYPE
vswif0 Service Console IPv4 192.168.0.2 \
255.255.255.0 192.168.0.255 true STATIC
```

\: This indicates that there is no line feed.

Configuring the PSA-to-MMB communication LAN

1. Execute the esxcfg-vswitch command to create a virtual switch (vSwitch1).

```
# esxcfg-vswitch -a vSwitch1
# esxcfg-vswitch -l
Switch Name Num Ports Used Ports Configured Ports \
MTU Uplinks
vSwitch0 64 2 64 \
1500 vmnic1

PortGroup Name VLAN ID Used Ports Uplinks
VM Network 0 0 vmnic1
Service Console 0 1 vmnic1

vSwitch1 64 2 64 \
1500
```

PortGroup Name	VLAN ID	Used Ports	Uplinks

\: This indicates that there is no line feed.

2. Execute the esxcfg-vswitch command to connect the physical adapter vmnic0 to the virtual switch.

```
# esxcfg-vswitch -L vmnic0 vSwitch1
# esxcfg-vswitch -l
```

Switch Name	Num Ports	Used Ports	Configured Ports	Uplinks
vSwitch0	64	2	64	\
1500	vmnic1			

PortGroup Name	VLAN ID	Used Ports	Uplinks
VM Network	0	0	vmnic1
Service Console	0	1	vmnic1

Switch Name	Num Ports	Used Ports	Configured Ports	Uplinks
vSwitch1	64	2	64	\
1500	vmnic0			

PortGroup Name	VLAN ID	Used Ports	Uplinks

3. Add the port group (PSA-MMB) to the created switch.

```
# esxcfg-vswitch -A PSA-MMB vSwitch1
# esxcfg-vswitch -l
```

Switch Name	Num Ports	Used Ports	Configured Ports	Uplinks
vSwitch0	64	2	64	\
1500	vmnic1			

PortGroup Name	VLAN ID	Used Ports	Uplinks
VM Network	0	0	vmnic1
Service Console	0	1	vmnic1

Switch Name	Num Ports	Used Ports	Configured Ports	Uplinks
vSwitch1	64	2	64	\
1500	vmnic0			

PortGroup Name	VLAN ID	Used Ports	Uplinks
PSA-MMB	0	0	vmnic0

4. Execute the esxcfg-vswif command to create a virtual port (vswif1).
The IP address to be set depends on the partition number.
Use the values in the table below.

TABLE E.2 IP addresses to be set for virtual ports

Partition number	IP address	Subnet mask
0	172.30.0.2	255.255.255.0
1	172.30.0.3	
2	172.30.0.4	
3	172.30.0.5	

<Example with the partition number of #2 and the PSA-MMB port group of vswif1>

```
# esxcfg-vswif -a vswif1 -i 172.30.0.4 -n 255.255.255.0 \
-p PSA-MMB
# esxcfg-vswif -l
Name Port Group/DVPort IP Family IP Address \
Netmask Broadcast Enabled TYPE
vswif0 Service Console IPv4 192.168.0.2 \
255.255.255.0 192.168.0.255 true STATIC
vswif1 PSA-MMB IPv4 172.30.0.4 \
255.255.255.0 172.30.0.255 true STATIC
```

\: This indicates that there is no line feed.

5. Add the following setting to the PSA-to-MMB communication LAN:

Speed: 100 Mbps

Duplex: full

<Example with the PSA-to-MMB communication LAN of vmnic0>

```
# esxcfg-nics vmnic0 -s 100 -d full
```

6. Set the PSA-to-MMB communication LAN IP addresses in the PSA configuration file.

File storage location : /etc/opt/FJSVpsa/usr/tommbipsetup.conf

Setting values: Enter the IP addresses set in Step 4.

<Setting example>

```
[NETWORK]
TOMMBIP=172.30.0.4
```

The configuration work is completed through the above steps.

In the above configuration example, the network is configured as follows:

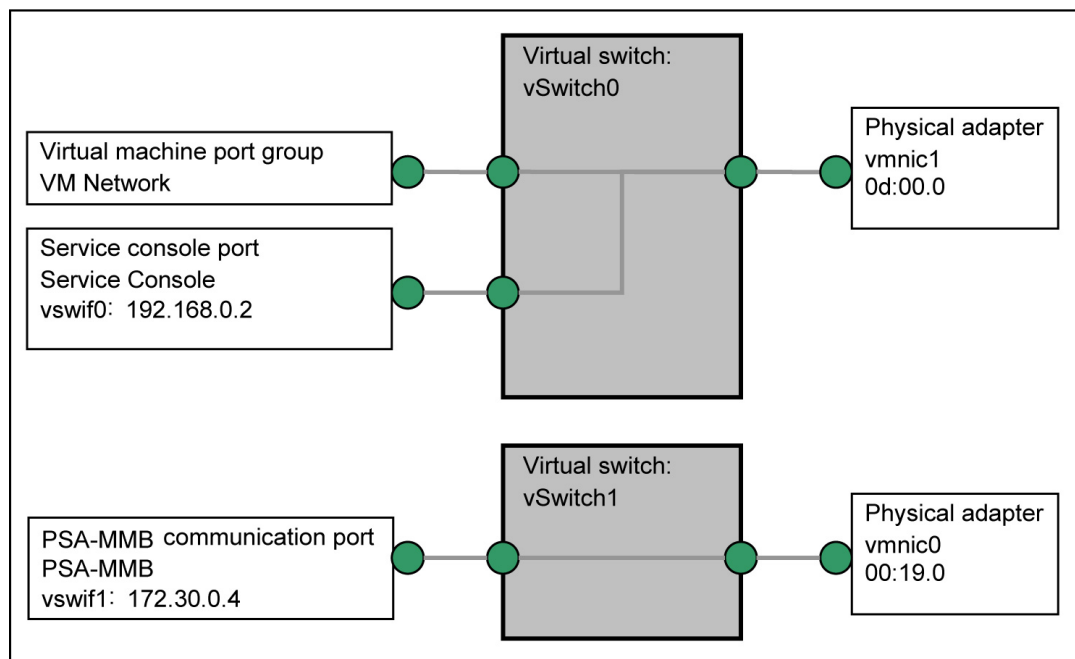


FIGURE E.6 Network configuration after setup

E.4.2 Configuring the firewall

This section describes how to configure the firewall for PSA operation.

For PSA, the following ports must be open.

TABLE E.3 Configuring the firewall for PSA operation

No.	Port	Port number	Description
1	snmp port	udp/snmp or 161	General snmp communication port
2	web-mmb communication port	tcp/fj-webgate or 24450	MMB-PSA port For reporting image information
3	psa-mmb communication port	tcp/5000 on MMB side	MMB-PSA port For reporting events and configuration information

TABLE E.4 Examples of firewall configurations

No.	Implementation example
1	# esxcfg-firewall -o 161,udp,in,SNMP
2	# esxcfg-firewall -o 24450,tcp,in,PSA-WG
3	# esxcfg-firewall -o 5000,tcp,out,PSA-MMB

- Confirming firewall settings

```
#esxcfg-firewall -q
Opened ports:
    SNMP                : port 161 udp.in
    PSA-MMB              : port 5000 tcp.out
```

E.4.3 Configuring the default gateway

Configure the default gateway when installing the operating system.

If the default gateway is not configured for some reason, make this setting.

1. Execute the route command to specify a temporary default gateway.

```
route add default gw <GATEWAY>
```

Example: When specifying 192.168.0.1 as the default gateway

```
# route add default gw 192.168.0.1
```

2. Use VMware vSphere 4.x Client to connect to the service console, and then configure the default gateway from the service console.

1. Start VMware vSphere 4.x Client.
2. Select [Home] - [Inventory] - [Inventory], and then click the [Configuration] tab.
3. Click [DNS and Routing] in the [Software] area in the lower left of the window.
4. Click [Properties] in the upper right of the window displaying the [DNS and Routing] information.

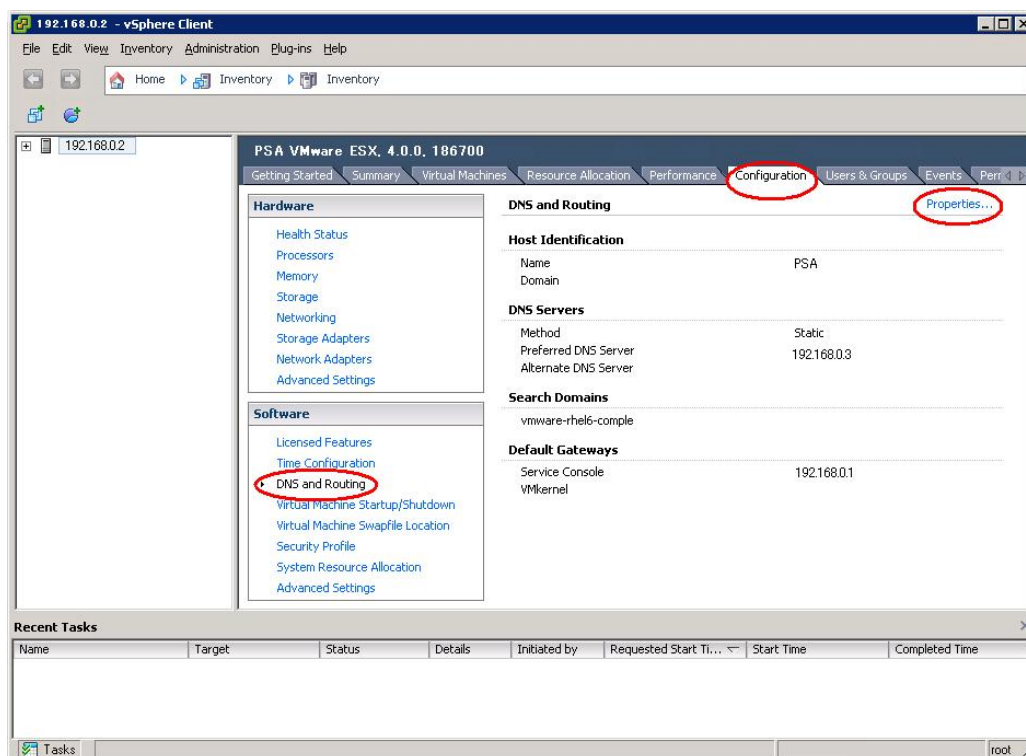


FIGURE E.7 VMware vSphere 4.x Client

5. Click the [Routing] tab, and make the [Default gateway] setting in the [Service Console] area. Then click the [OK] button.

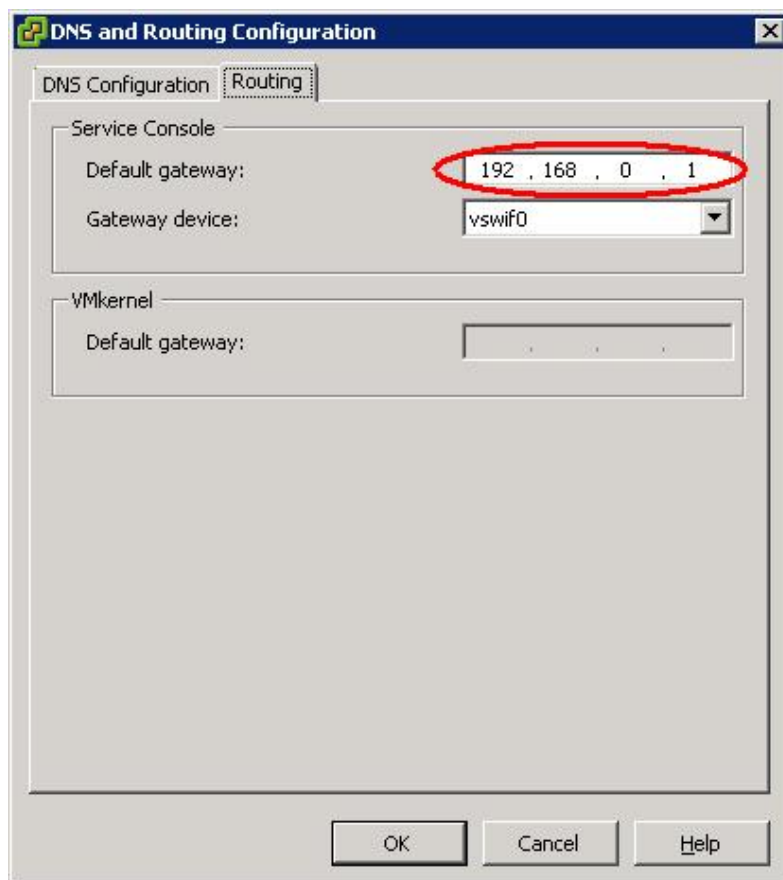


FIGURE E.8 [DNS and Routing Configuration] dialog box

Note

For details on VMware vSphere 4.x Client, see the manual of VMware 4.x.

E.4.4 Retrieving VMware 4.x PSA maintenance information

When a problem regarding PSA occurs, execute the PSA troubleshooting information collection command (getopsa), and then execute the vm-support command.

1. getopsa command

```
# /opt/FJSVpsa/sh/getopsa <file name>
```

2. vm-support command

<Execution example>

```
# vm-support
```

Remarks

In VMware 4.x, the core file is output in /var/core, and is not automatically deleted. After executing the vm-support command, we recommend deleting the core file as required.

E.4.5 Notes on VMware 4.x PSA

Note the following points on PSA in VMware 4.x.

- PSA can run only on the console operating system. It manages the configuration of devices in the console operating system and detects device problems. It cannot run in the guest operating system, and must not be installed in the guest operating system.
- It may take time (at least five minutes) to start PSA after starting the operating system.

E.5 Settings after VMware 4.x SVMco Installation

The settings are required for SVMco operation.

For details on the SVMco settings, see the *ServerView Mission Critical Option user manual*.

Contact your sales representative for inquiries about the ServerView manuals.

E.6 Building a RAID Environment Using VMware 5.x Built-in Disks

The PRIMEQUEST 1000 series supports RAID 0, RAID 1, RAID 1E, RAID 5, RAID 6, and RAID 10 that use built-in hard disks.

For details on building a RAID configuration using built-in hard disks, see the *MegaRAID SAS Software*, the *MegaRAID SAS Device Driver Installation*, and the *Modular RAID Controller Installation Guide*.

E.7 Installing VMware 5.x Bundled Software

The bundled software is stored in ServerView Suite DVD1. Copy the files from ServerView SuiteDVD1 and use them.

The bundled software required for VMware vSphere 5 comprises the following.

TABLE E.5 VMware 5.x bundled software and its installation destination

Bundled software	Installation destination
ServerView ESXi CIM Provider	VMware ESXi
ServerView RAID Manager (ServerView RAID)	Guest OS (*1)
ServerView Mission Critical Option for VM (SVMcovm)	Guest OS (*1)(*2)

*1 ServerView is installed in only one guest OS. There is no need to install it in all guest OSs.

Also, select a guest OS that will not be migrated to another partition by using vMotion, vSphereHA, etc.

If the relevant OS is migrated to another partition, it may no longer be able to correctly report events.

*2 SVMcovm applies to all models of the PRIMEQUEST1000 Series in VMware5.x.

TABLE E.6 VMware 5.x setting procedure and setting destination

Setting procedure	Setting destination
BBU life monitoring (Setting procedure using standard OS functions)	Guest OS (*)

* ServerView is installed in only one guest OS. There is no need to install it in all guest OSs.

E.7.1 Installing ServerView RAID

For details on installing ServerView RAID, contact the distributor where you purchased your product, or your sales representative.

E.7.2 Configuring BBU service life monitoring

For details on configuring BBU service life monitoring, contact the distributor where you purchased your product, or your sales representative.

E.7.3 Installing and setting SVMcovm

For details on installing and setting SVMcovm, see the *ServerView Mission Critical Option User Manual*. Contact your sales representative for inquiries about the ServerView manuals.

APPENDIX F Setting up the NTP Server (Windows)

This appendix describes how to specify and set of an NTP server for a specific Windows operating system.

This appendix is not needed for Active Directory member servers.

Active Directory member servers automatically synchronize the system clock with the domain controller.

F.1 Overview of NTP Client Settings	296
F.2 NTP Settings in Windows Server 2003	298
F.3 NTP Settings in Windows Server 2008	301
F.4 NTP Settings in Windows Server 2008 R2	307
F.5 NTP Settings in Windows Server 2012	315

F.1 Overview of NTP Client Settings

This appendix describes procedures for settings synchronizing the system clock with an NTP server for operating systems consisting of the following:

- Windows Server 2003/Windows Server 2003 R2

The setup steps do not distinguish between Windows Server 2003 and Windows Server 2003 R2. Windows Server 2003 and Windows Server 2003 R2 are both called "Windows Server 2003" in this manual.

- Windows Server 2008

- Windows Server 2008 R2

- Windows Server 2012/Windows Server 2012 R2

The setup steps do not distinguish between Windows Server 2012 and Windows Server 2012 R2. Windows Server 2012 and Windows Server 2012 R2 are both called "Windows Server 2012" in this manual.

Remarks

This appendix is not needed for Active Directory member servers. Active Directory member servers automatically synchronize the system clock with the domain controller.

In the PRIMEQUEST 1000 series, the system time of a partition is kept in the Home SB. Therefore, if the Home SB of a partition is replaced during maintenance or switched by the reserved SB function, the system time of the partition may become incorrect.

The system clock synchronizes with an NTP server once a week in the default configuration of the Workgroup environment of Windows.

Before Windows Server 2008, the system clock is synchronized at system startup. However, in Windows Server 2008 R2 or later, it is not synchronized.

Use the following procedures to set the system to synchronize with the system clock.

TABLE F.1 Settings for system clock synchronization

Task name	Task description	Target OS
Specifying an NTP Server	Specify an NTP server in [Control Panel] - [Date and Time].	Windows Server 2003 Windows Server 2008 Windows Server 2008 R2 Windows Server 2012
Synchronization Interval Setting	Set the following registry value with the Registry Editor to set a synchronization interval of 15 minutes: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient *There is no line feed in the above registry key. name: SpecialPollInterval type: REG_DWORD value: 900 (decimal)	Windows Server 2003 Windows Server 2008 Windows Server 2008 R2 Windows Server 2012

Task name	Task description	Target OS
Startup Settings of NTP Service	Set the Windows Time service to start automatically in [Computer Management] - [Services and Applications] - [Services] (only Windows Server 2008 R2).	Windows Server 2008 R2 Windows Server 2012
Event Task Settings	Register the following in Task Scheduler to synchronize with the System time when the time can be acquired from an NTP server: Log: "System", Source: "Time-Service", ID:37 The "w32tm /resync" command will run.	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012

For detailed procedures, see following chapter:

- [F.2 NTP Settings in Windows Server 2003](#)
- [F.3 NTP Settings in Windows Server 2008](#)
- [F.5 NTP Settings in Windows Server 2012](#)
- [F.5 NTP Settings in Windows Server 2012](#)

F.2 NTP Settings in Windows Server 2003

The procedures in this chapter require Administrator privileges.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

F.2.1 Specifying an NTP Server

1. Select [Control Panel] - [Date and Time]. The [Date and Time Properties] dialog box appears.

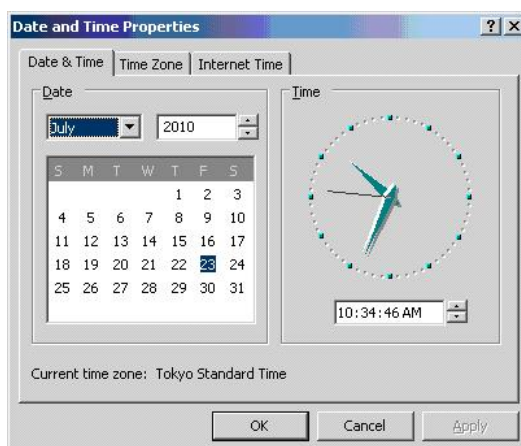


FIGURE F.1 [Date and Time Properties] window (1)

2. Click the [Internet Time] tab. Set the following parameters.
 - [Automatically synchronize with an Internet time server]: Check the check box.
 - [Server]: Enter an NTP server name.

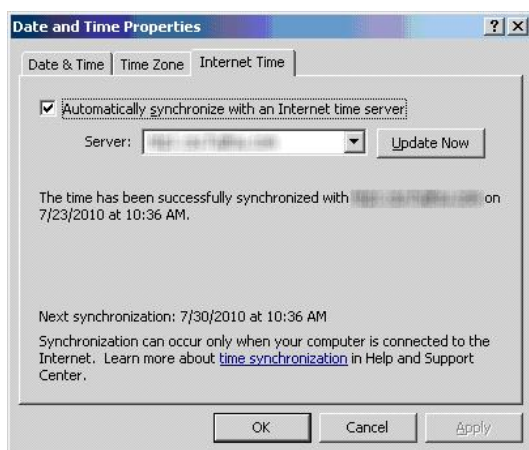


FIGURE F.2 [Date and Time Properties] window (2)

3. Click the [OK] button to close the [Date and Time Properties] dialog box.

F.2.2 Synchronization Interval Setting

1. Select [Start] - [Run]. Enter "regedit.exe" in the dialog box, and click the [OK] button.
The Registry Editor appears.

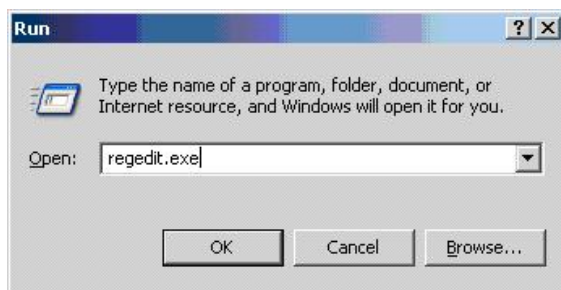


FIGURE F.3 [Run] window

2. Open the following key, and set 900 for the SpecialPollInterval value.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time  
\TimeProviders\NtpClient  
"SpetcialPollInterval" Type: REG_DWORD, Data: 900 (decimal)
```

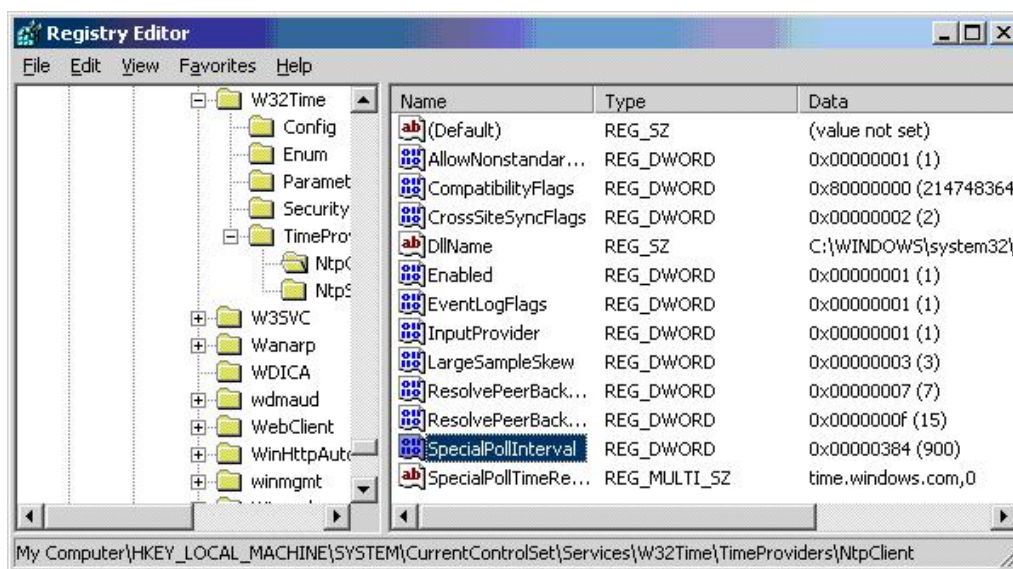


FIGURE F.4 [Registry Editor] window

3. Close the Registry Editor.
4. Open [Start] - [Administrative Tools] - [Services].

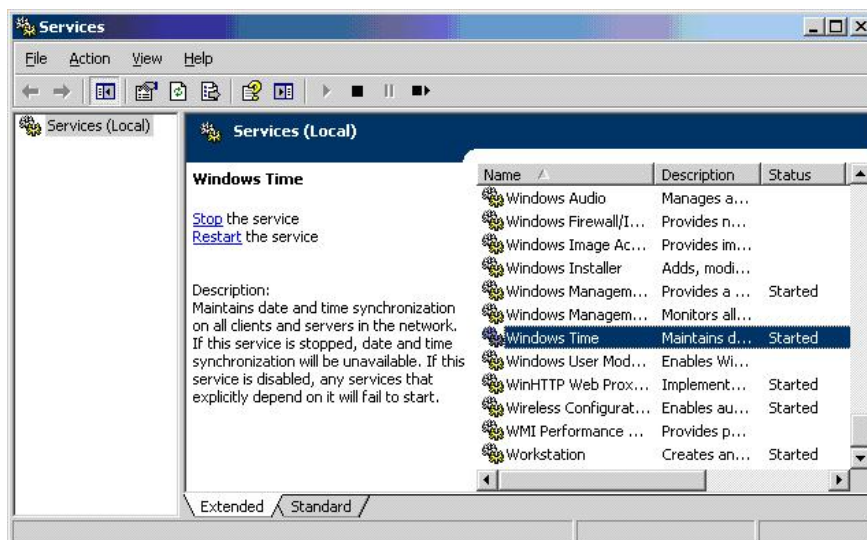


FIGURE F.5 [Services] window

5. Right-click the Windows Time service. Select [Restart] from the context menu.

F.3 NTP Settings in Windows Server 2008

The procedures in this chapter require Administrator privileges.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

F.3.1 Specifying an NTP Server

1. Select [Control Panel] - [Date and Time]. The [Date and Time] dialog box appears.

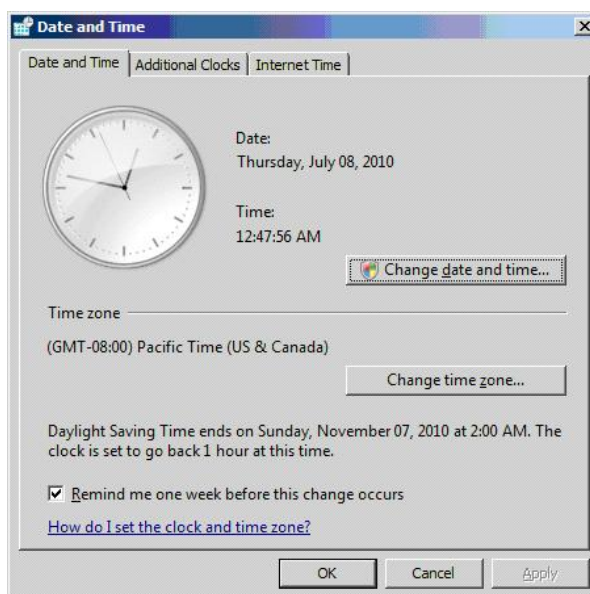


FIGURE F.6 [Date and Time] window (1)

2. Click the [Change settings] button on the [Internet Time] tab.



FIGURE F.7 [Date and Time] window (2)

3. Set the following parameters in the [Internet Time Settings] dialog box.
 - [Synchronize with an Internet time server]: Check the check box.
 - [Server]: Enter an NTP server name.

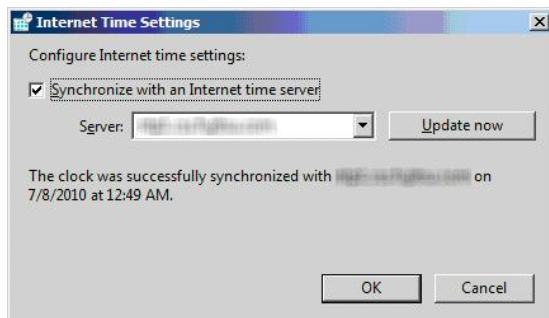


FIGURE F.8 [Internet Time Settings] window

4. Click the [OK] button to close the [Internet Time Settings] dialog box.
5. Click the [OK] button to close the [Date and Time] dialog box.

F.3.2 Synchronization Interval Setting

1. Select [Start] - [Run]. Enter "regedit.exe" in the dialog box, and click the [OK] button.

The Registry Editor appears.

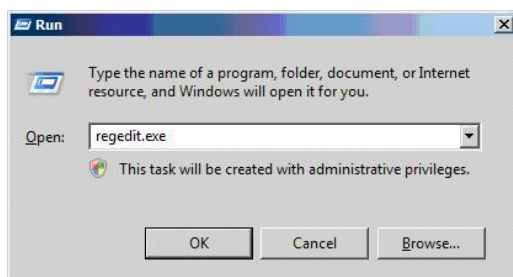


FIGURE F.9 [Run] window

2. Open the following key, and set 900 for the SpecialPollInterval value.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time
\TimeProviders\NtpClient
"SpetcialPollInterval" Type: REG_DWORD, Data: 900 (decimal)
```

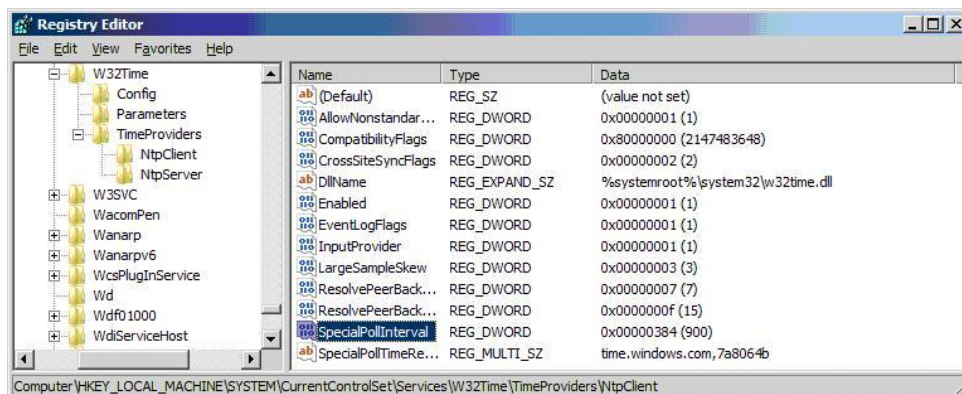


FIGURE F.10 [Registry Editor] window

3. Close the Registry Editor.

4. Open [Start] - [Administrative Tools] - [Services].

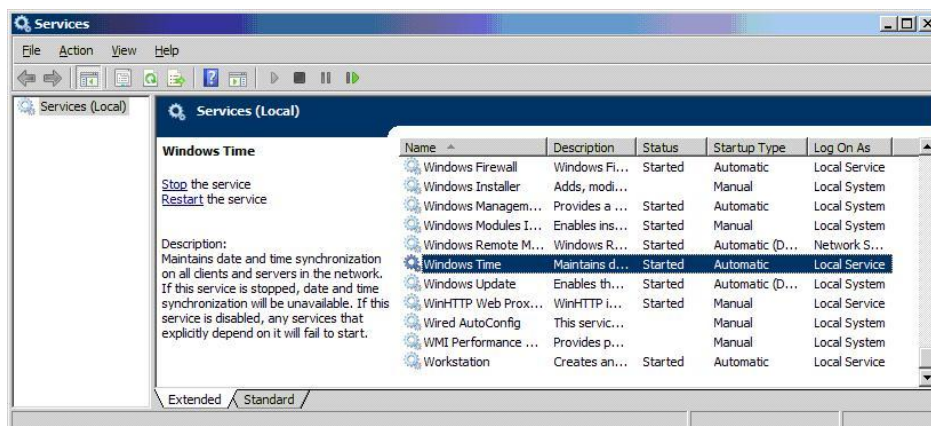


FIGURE F.11 [Services] window

5. Right-click the Windows Time service. Select [Restart] from the context menu.

F.3.3 Event Task Settings

1. Open [Start] - [Administrative Tools] - [Task Scheduler].

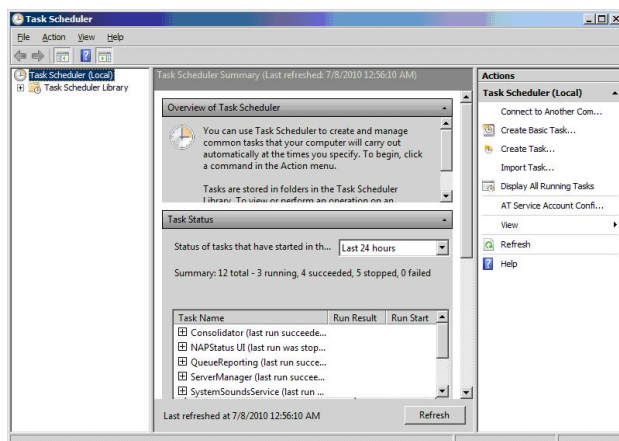


FIGURE F.12 [Task Scheduler] window

2. Select [Create Basic Task] at the right of the window. [Create Basic Task Wizard] appears.
3. Enter a chosen task name in [Name] on the [Create a Basic Task] screen, and click the [Next] button.
Example: On the screen below, "ntp-sync" is an arbitrary task name.

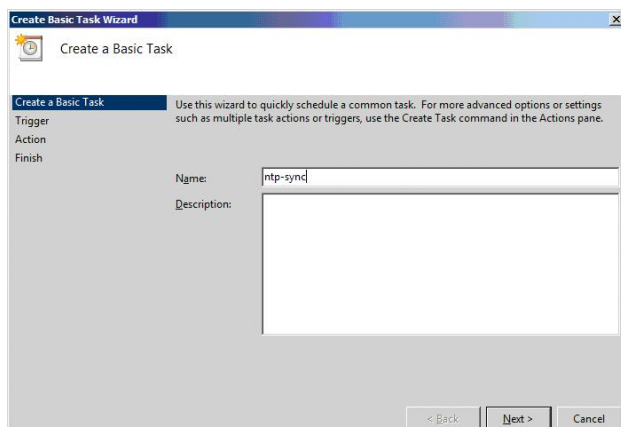


FIGURE F.13 [Create Basic Task Wizard] window (Create a Basic Task)

4. Select "When a specific event is logged" on the [Task Trigger] screen. Click the [Next] button.

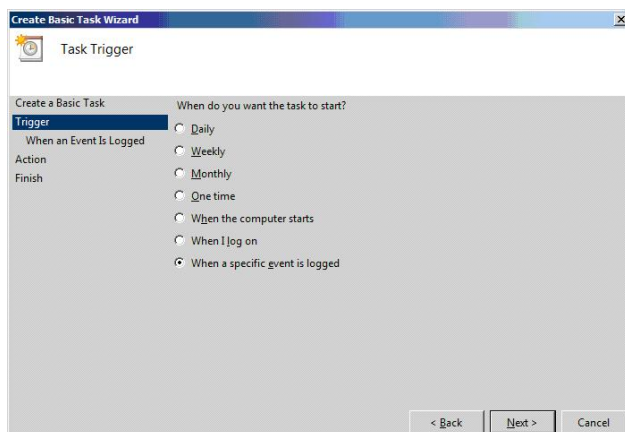


FIGURE F.14 [Create Basic Task Wizard] window (Task Trigger)

5. [When a Specific Event Is Logged] screen appears. Set the following parameters.
- [Log]: System
 - [Source]: Time-Service
 - [Event ID]: 37

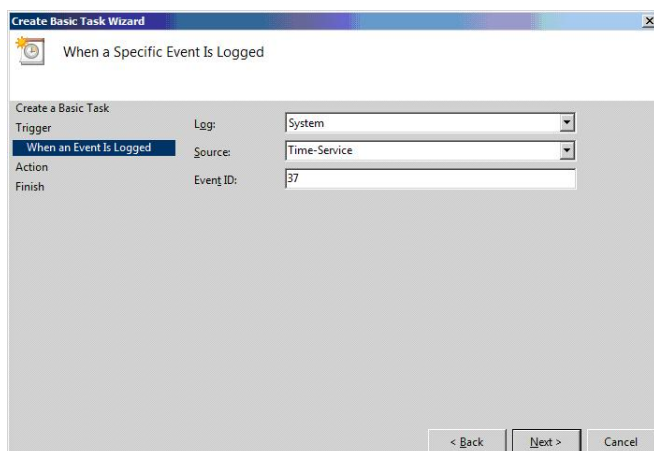


FIGURE F.15 [Create Basic Task Wizard] window (When a Specific Event Is Logged)
Click the [Next] button.

6. Select "Start a program" on the [Action] screen. Click the [Next] button.

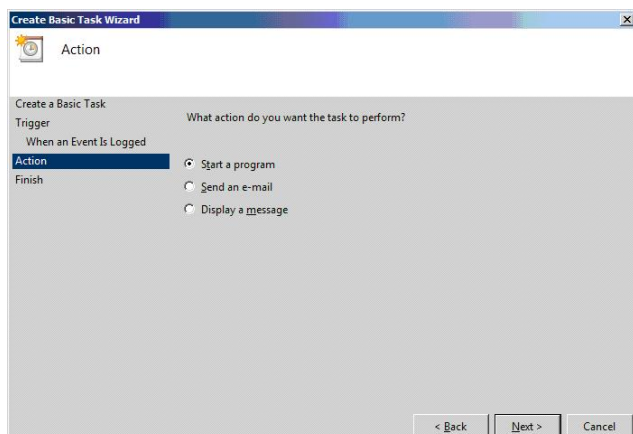


FIGURE F.16 [Create Basic Task Wizard] window (Action)

7. Set the following parameters on the [Start a Program] screen.
- [Program/script]: %SystemRoot%\System32\w32tm.exe
 - [Add arguments] (optional): /resync

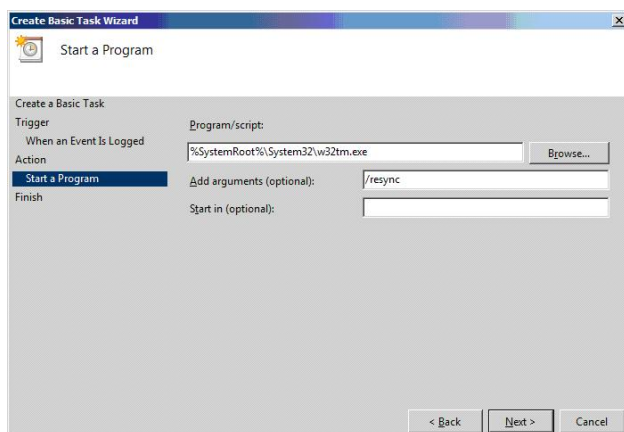


FIGURE F.17 [Create Basic Task Wizard] window (Start a Program)

Click the [Next] button.

8. Check the [Open the Properties dialog for this task when I click Finish] check box on the [Summary] screen.

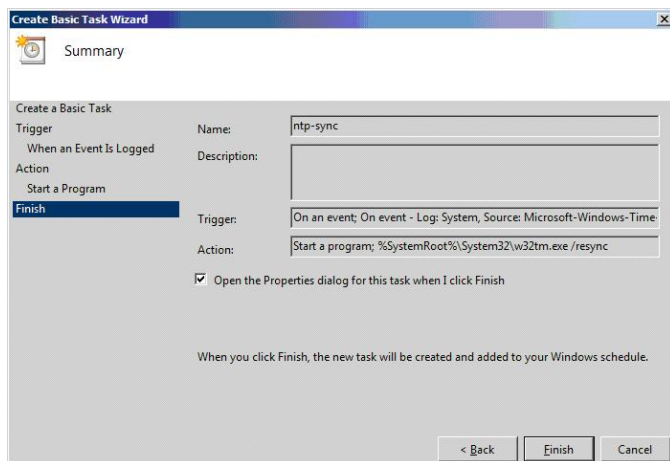


FIGURE F.18 [Create Basic Task Wizard] window (Summary)

Click the [Finish] button.

9. Click the [Change User or Group] button in the [Properties] dialog box.

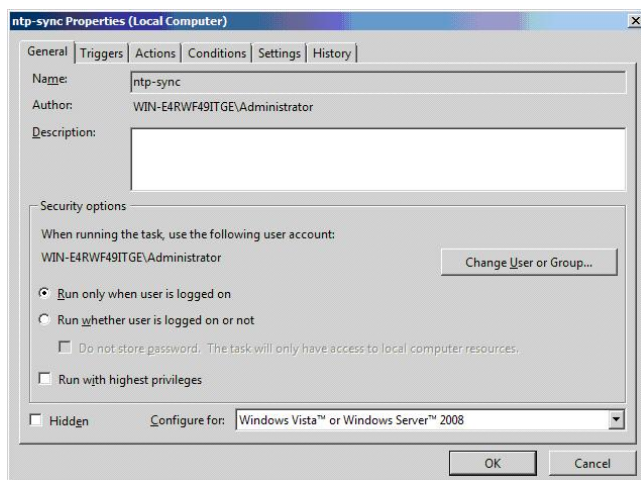


FIGURE F.19 [Properties] dialog box

10. [Select User or Group] dialog box appears.

Set the following parameter.

- [Enter the object name to select]: System

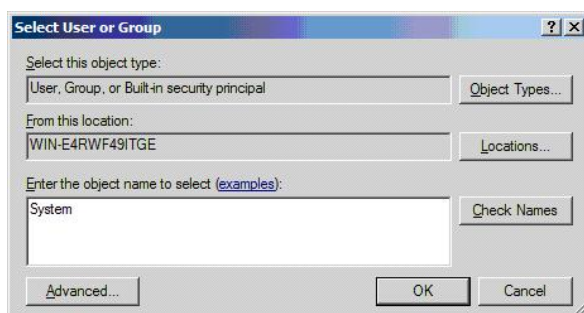


FIGURE F.20 [Select User or Group] window

Click the [OK] button.

11. Click the [OK] button to close the [Properties] dialog box.

F.4 NTP Settings in Windows Server 2008 R2

The procedures in this chapter require Administrator privileges.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

F.4.1 Specifying an NTP Server

1. Select [Control Panel] - [Set the time and date]. The [Date and Time] dialog box appears.

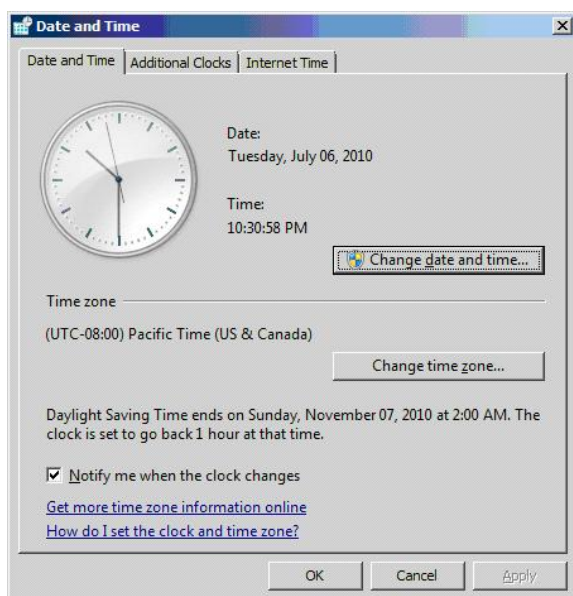


FIGURE F.21 [Date and Time] window (1)

2. Click the [Change settings] button on the [Internet Time] tab.

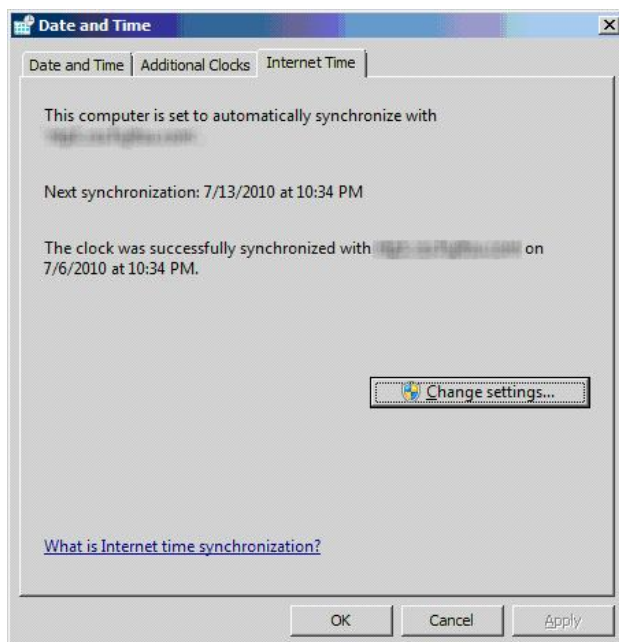


FIGURE F.22 [Date and Time] window (2)

3. Set the following parameters in the [Internet Time Settings] dialog box.
 - [Synchronize with an Internet time server]: Check the check box.

- [Server]: Enter an NTP server name.

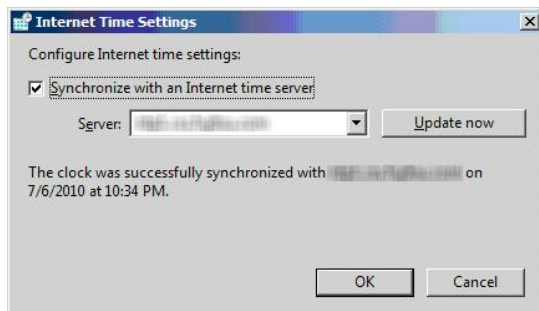


FIGURE F.23 [Internet Time Settings] window

4. Click the [OK] button to close the [Internet Time Settings] dialog box.
5. Click the [OK] button to close the [Date and Time] dialog box.

F.4.2 Synchronization Interval and Startup Settings of NTP Service

1. Select [Start] - [Run]. Enter "regedit.exe" in the dialog box, and click the [OK] button.

The Registry Editor appears.

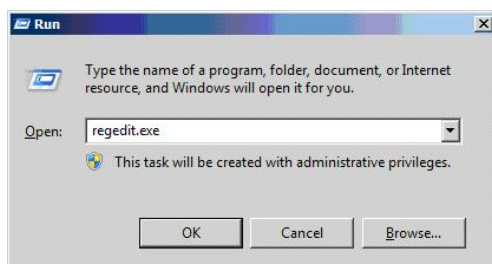


FIGURE F.24 [Run] window

2. Open the following key, and set 900 for the SpecialPollInterval value.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time
 \TimeProviders\NtpClient
 "SpetcialPollInterval" Type: REG_DWORD, Data: 900 (decimal)

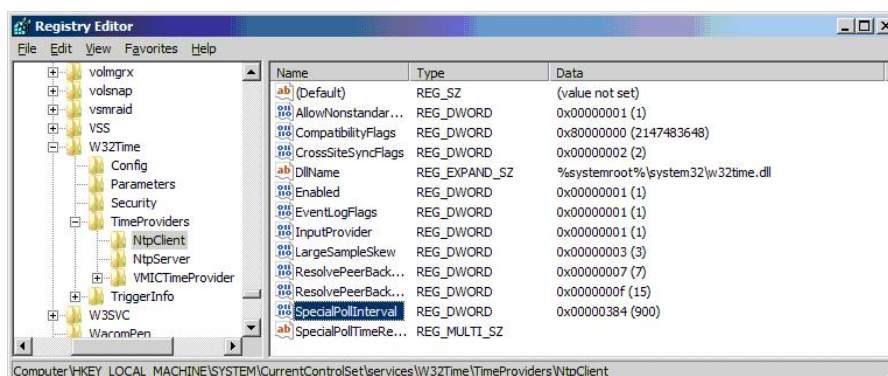


FIGURE F.25 [Registry Editor] window

3. Close the Registry Editor.

4. Open [Start] - [Administrative Tools] - [Services].

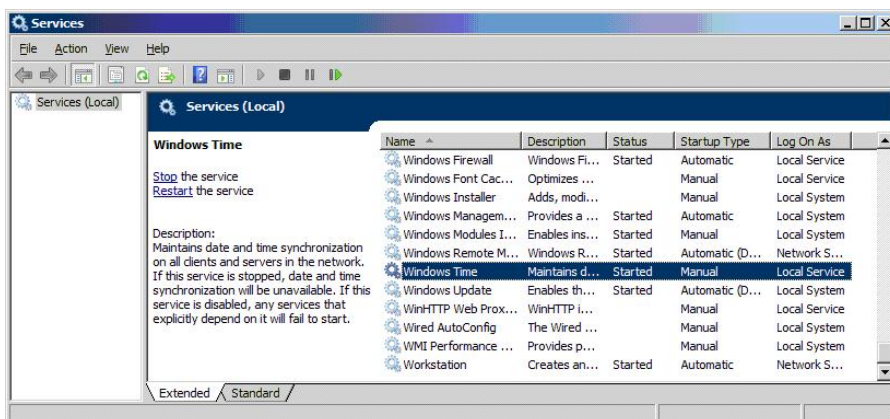


FIGURE F.26 [Services] window

5. Right-click the Windows Time service. Select [Properties] from the context menu.
6. Set "Automatic (Delayed Start)" in [Startup Type] in the [Windows Time Properties] dialog box.

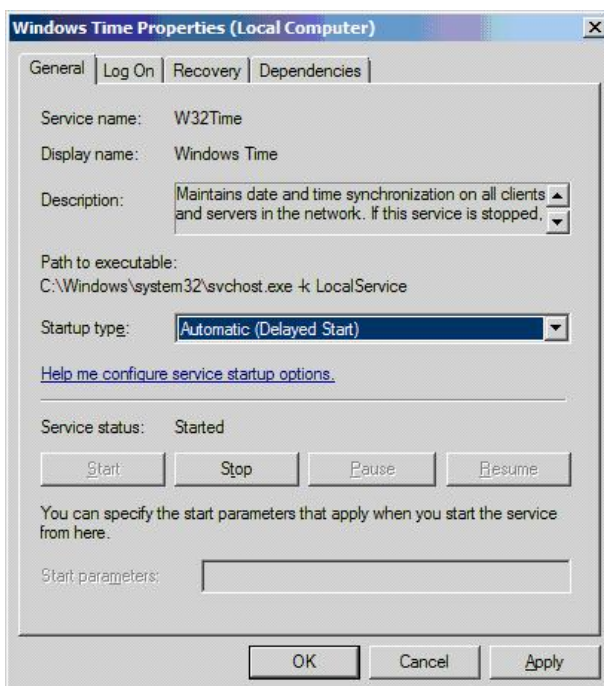


FIGURE F.27 [Windows Time Properties] window

7. If the W32Time service is stopped, click the [Start] button.
If the W32Time service is running, click the [Stop] button to pause the service, and then click the [Start] button.
8. Click the [OK] button to close the [Windows Time Properties] dialog box.

F.4.3 Event Task Settings

1. Open [Start] - [Administrative Tools] - [Task Scheduler].

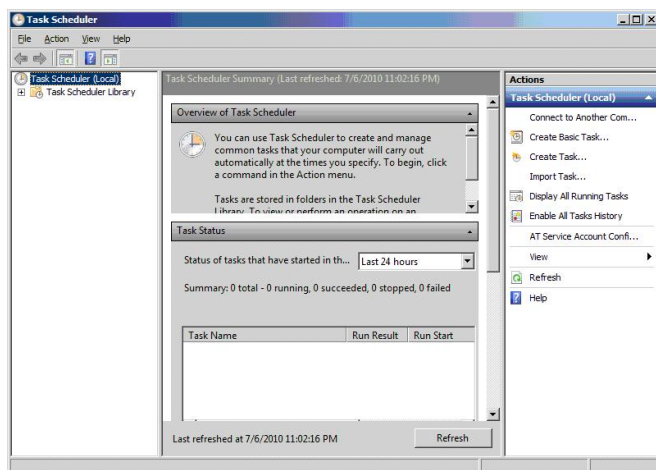


FIGURE F.28 [Task Scheduler] window

2. Select [Create Basic Task] at the right of the window. [Create Basic Task Wizard] appears.
3. Enter a chosen task name in [Name] on the [Create a Basic Task] screen, and click the [Next] button.
Example: On the screen below, "ntp-sync" is an arbitrary task name.

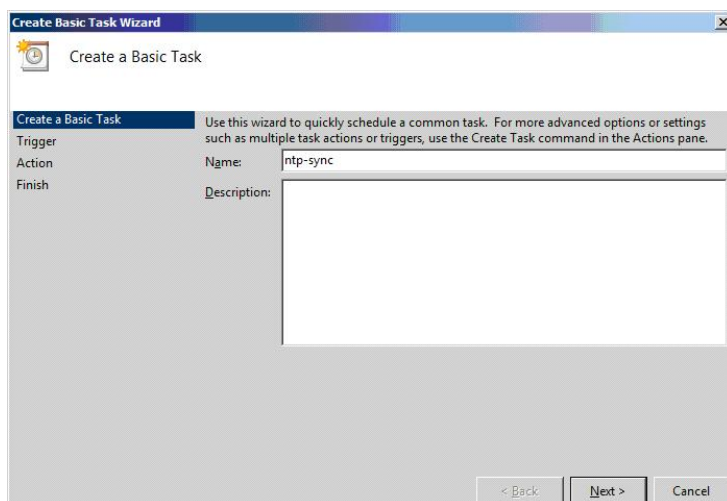


FIGURE F.29 [Create Basic Task Wizard] window (Create a Basic Task)

4. Select "When a specific event is logged" on the [Task Trigger] screen. Click the [Next] button.

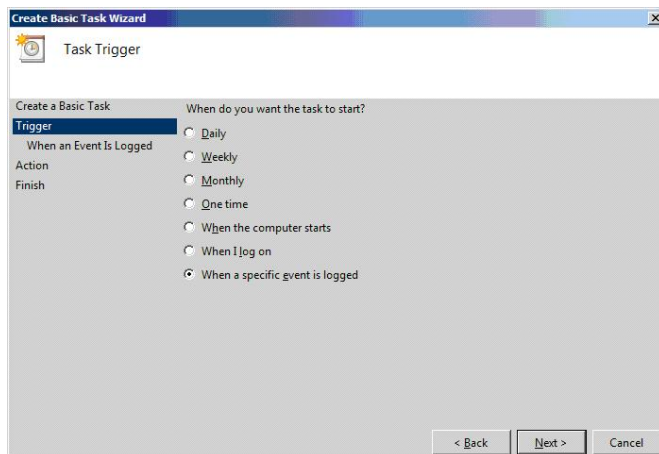


FIGURE F.30 [Create Basic Task Wizard] window (Task Trigger)

5. [When a Specific Event Is Logged] screen appears. Set the following parameters.

- [Log]: System
- [Source]: Time-Service
- [Event ID]: 37

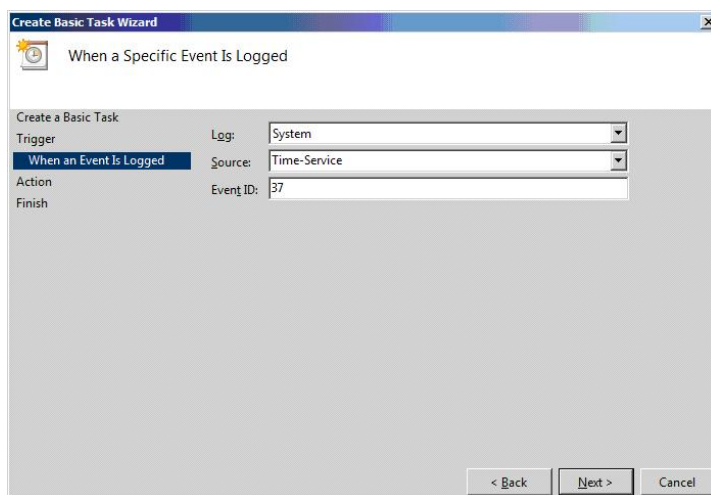


FIGURE F.31 [Create Basic Task Wizard] window (When a Specific Event Is Logged)

Click the [Next] button.

6. Select "Start a program" on the [Action] screen. Click the [Next] button.

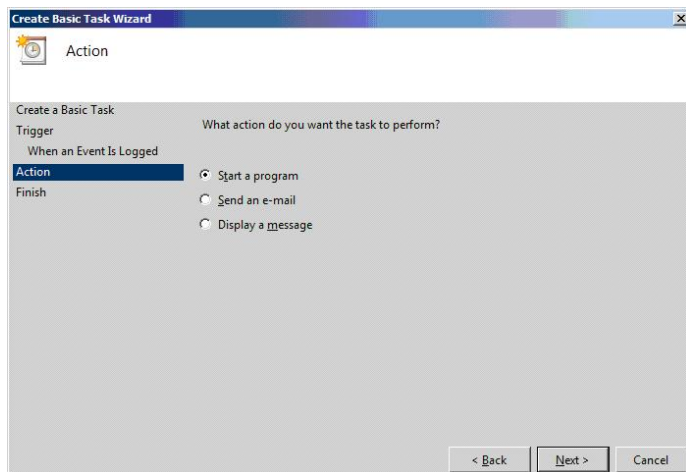


FIGURE F.32 [Create Basic Task Wizard] window (Action)

7. Set the following parameters on the [Start a Program] screen.
 - [Program/script]: %SystemRoot%\System32\w32tm.exe
 - [Add arguments] (optional): /resync

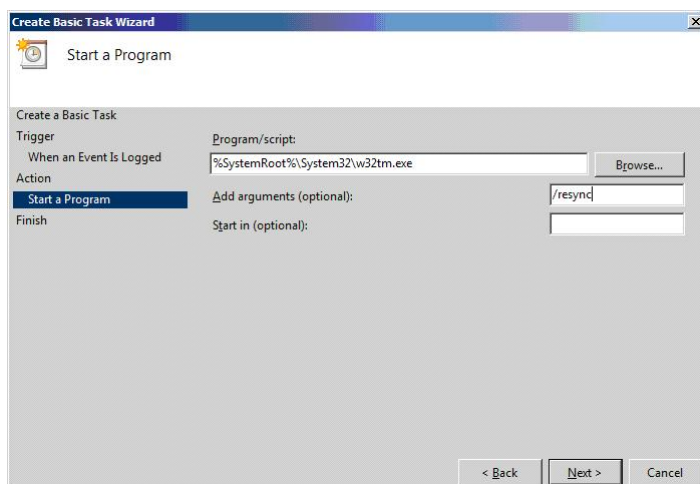


FIGURE F.33 [Create Basic Task Wizard] window (Start a Program)

Click the [Next] button.

8. Check the [Open the Properties dialog for this task when I click Finish] check box on the [Summary] screen.

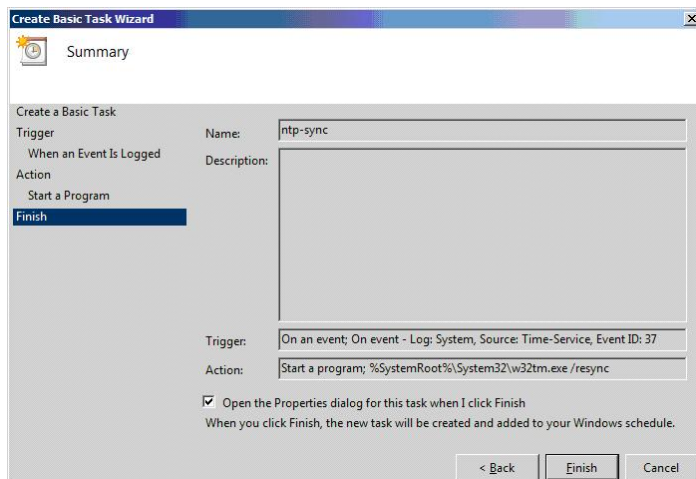


FIGURE F.34 [Create Basic Task Wizard] window (Summary)
Click the [Finish] button.

9. Click the [Change User or Group] button in the [Properties] dialog box.

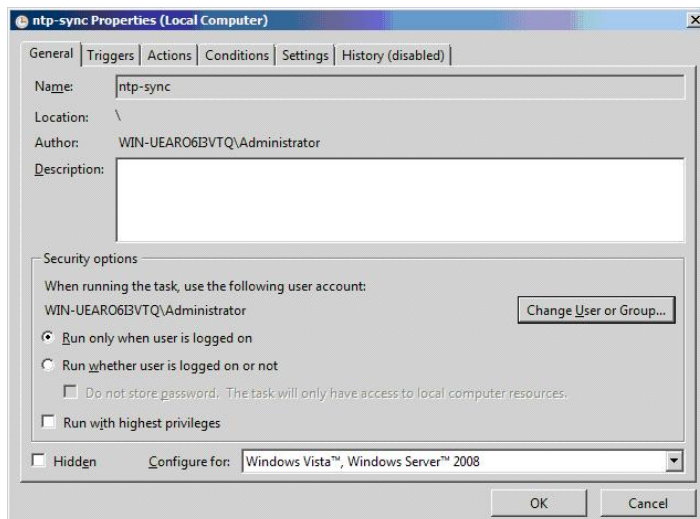


FIGURE F.35 [Properties] dialog box

10. [Select User or Group] dialog box appears.

Set the following parameter.

- [Enter the object name to select]: System

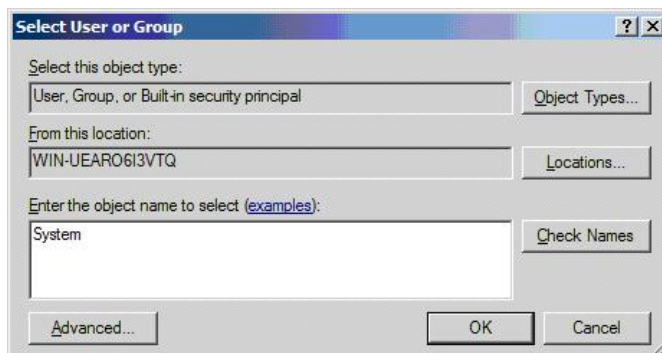


FIGURE F.36 [Select User or Group] window
Click the [OK] button.

11. Click the [OK] button to close the [Properties] dialog box.

F.5 NTP Settings in Windows Server 2012

The procedures in this chapter require Administrator privileges.

All screenshots are display examples, and the actually displayed contents vary depending on the system configuration and other factors.

F.5.1 Specifying an NTP Server

1. Select [Control Panel] - [Set the time and date]. The [Date and Time] dialog box appears.

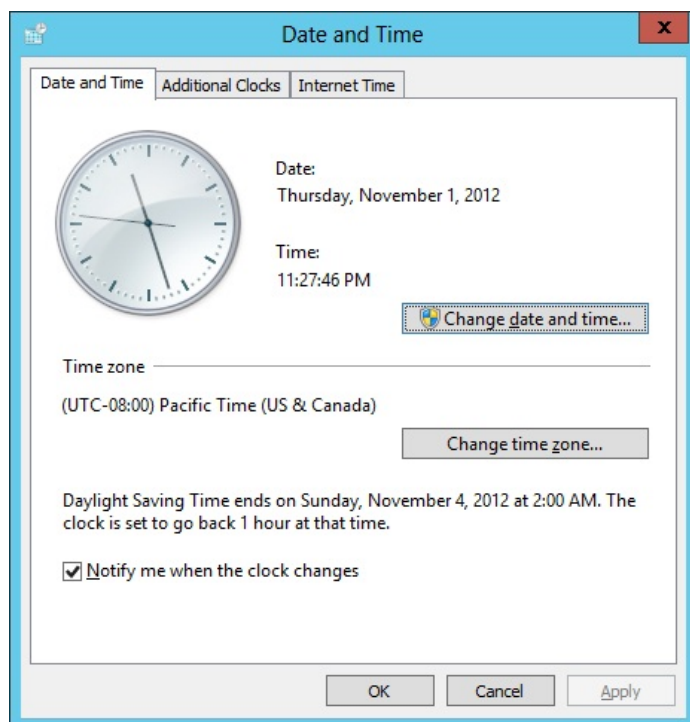


FIGURE F.37 [Date and Time] window (1)

2. Click the [Change settings] button on the [Internet Time] tab.

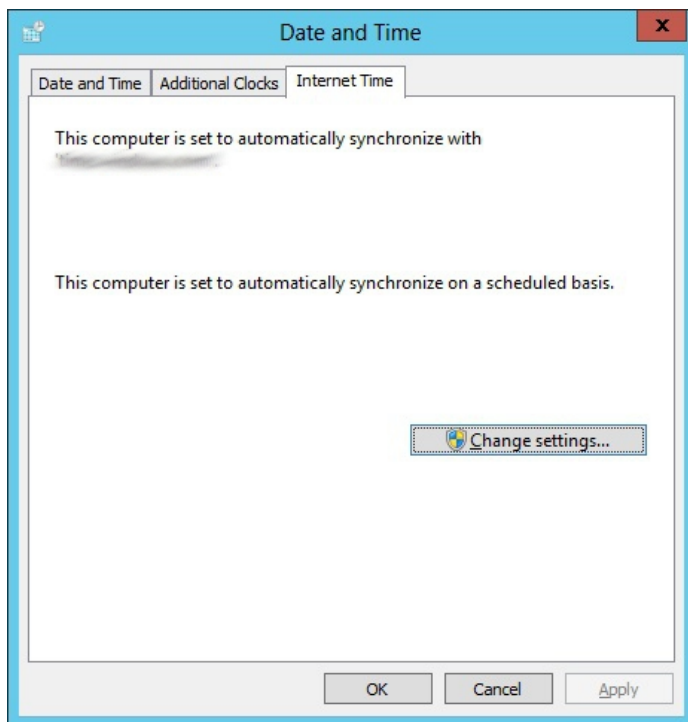


FIGURE F.38 [Date and Time] window (2)

3. Set the following parameters in the [Internet Time Settings] dialog box.
 - [Synchronize with an Internet time server]: Check the check box.
 - [Server]: Enter an NTP server name.

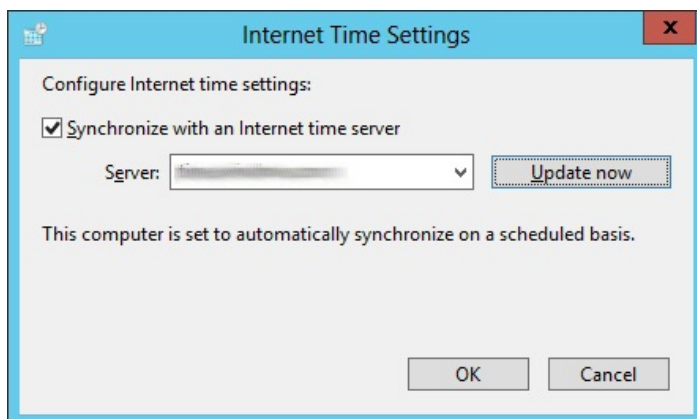


FIGURE F.39 [Internet Time Settings] window

4. Click the [OK] button to close the [Internet Time Settings] dialog box.
5. Click the [OK] button to close the [Date and Time] dialog box.

F.5.2 Synchronization Interval and Startup Settings of NTP Service

1. Enter "regedit" in [Search] to start the Registry Editor.

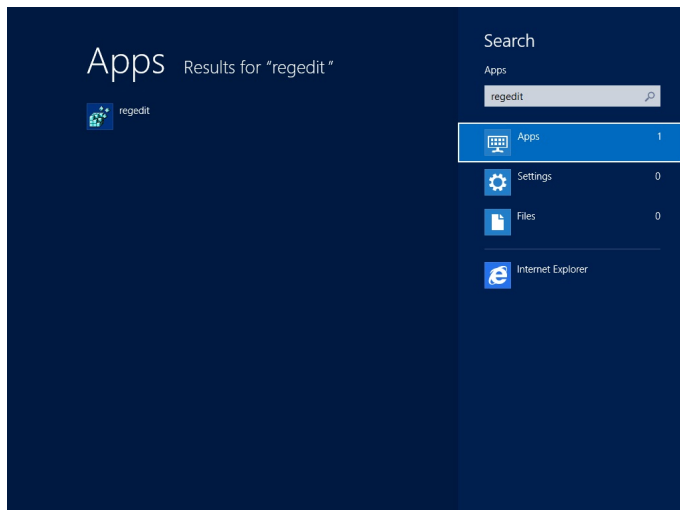


FIGURE F.40 [Registry Editor] selection window

2. Open the following key, and set 900 for the SpecialPollInterval value.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time
\TimeProviders\NtpClient
"SpetcialPollInterval" Type: REG_DWORD, Data: 900 (decimal)

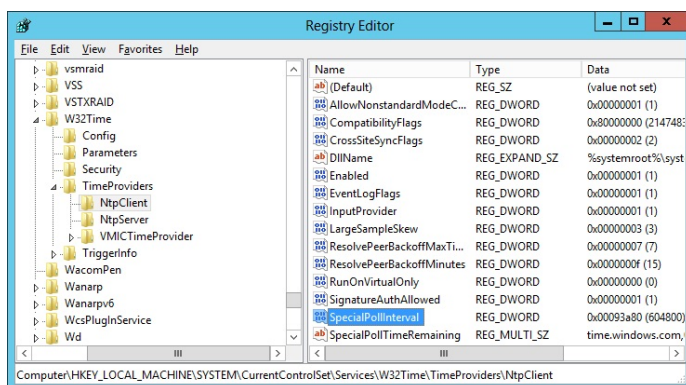


FIGURE F.41 [Registry Editor] window

3. Close the Registry Editor.
4. Open [Start] - [Administrative Tools] - [Services].

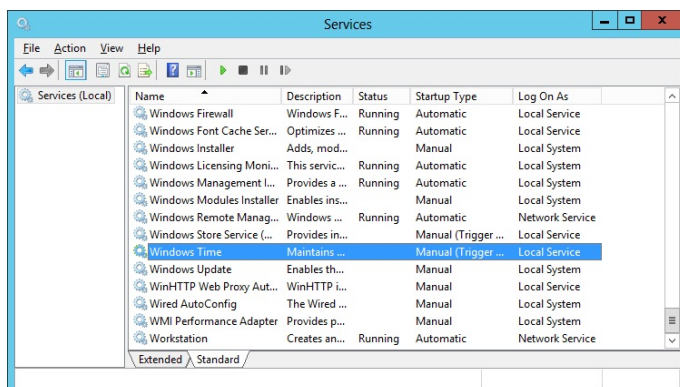


FIGURE F.42 [Services] window

5. Right-click the Windows Time service. Select [Properties] from the context menu.
6. Set "Automatic (Delayed Start)" in [Startup type] in the [Windows Time Properties] dialog box.

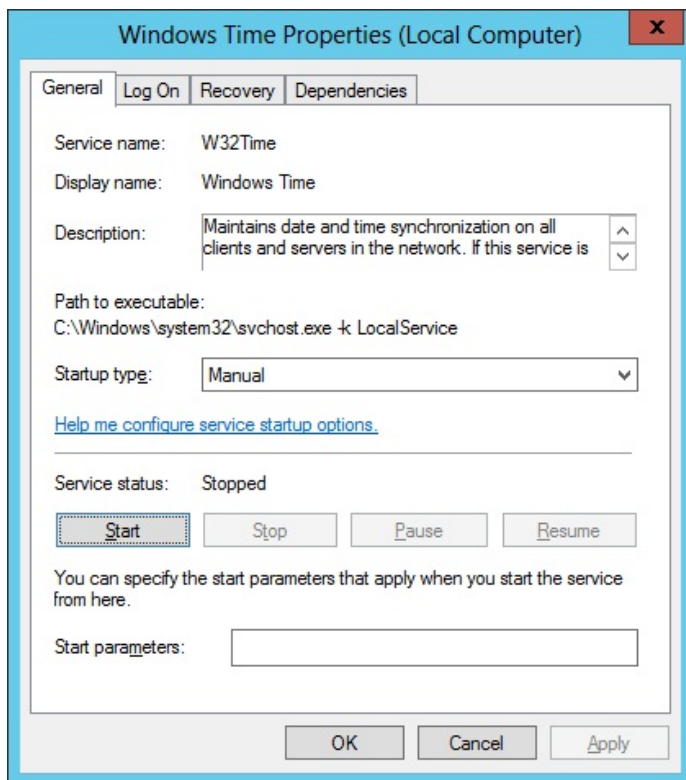


FIGURE F.43 [Windows Time Properties] window

7. If the W32Time service is stopped, click the [Start] button.
If the W32Time service is running, click the [Stop] button to pause the service, and then click the [Start] button.
8. Click the [OK] button to close the [Windows Time Properties] dialog box.

F.5.3 Event Task Settings

1. Open [Start] - [Administrative Tools] - [Task Scheduler].

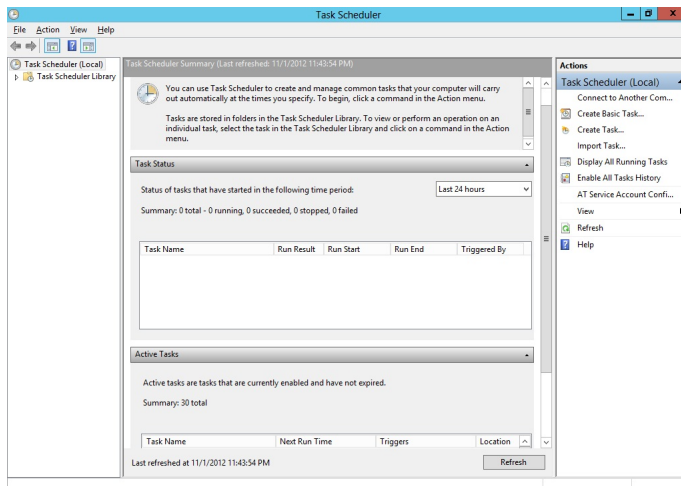


FIGURE F.44 [Task Scheduler] window

2. Select [Create Basic Task] at the right of the window. [Create Basic Task Wizard] appears.
3. Enter a chosen task name in [Name] on the [Create a Basic Task] screen, and click the [Next] button.
Example: On the screen below, "ntp-sync" is an arbitrary task name.

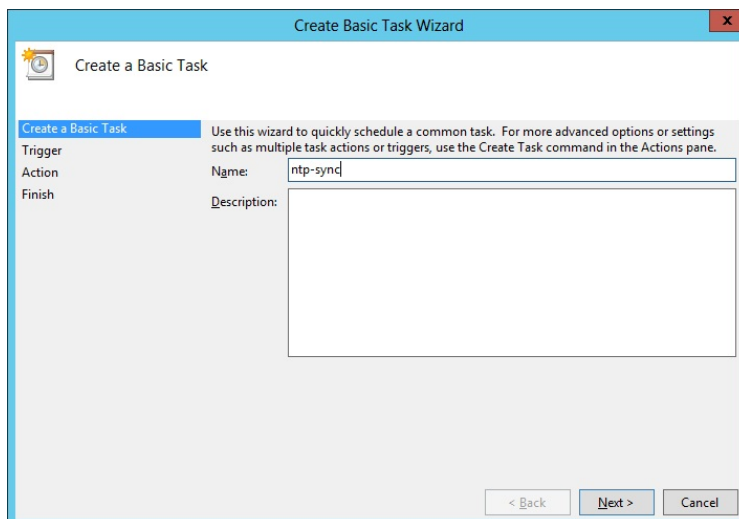


FIGURE F.45 [Create Basic Task Wizard] window (Create a Basic Task)

4. Select "When a specific event is logged" on the [Task Trigger] screen. Click the [Next] button.

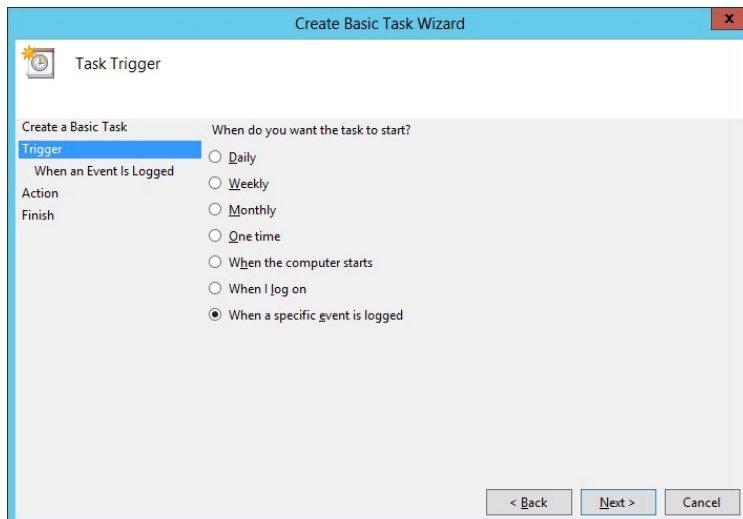


FIGURE F.46 [Create Basic Task Wizard] window (Task Trigger)

5. [When a Specific Event Is Logged] screen appears. Set the following parameters.
- [Log]: System
 - [Source]: Time-Service
 - [Event ID]: 37

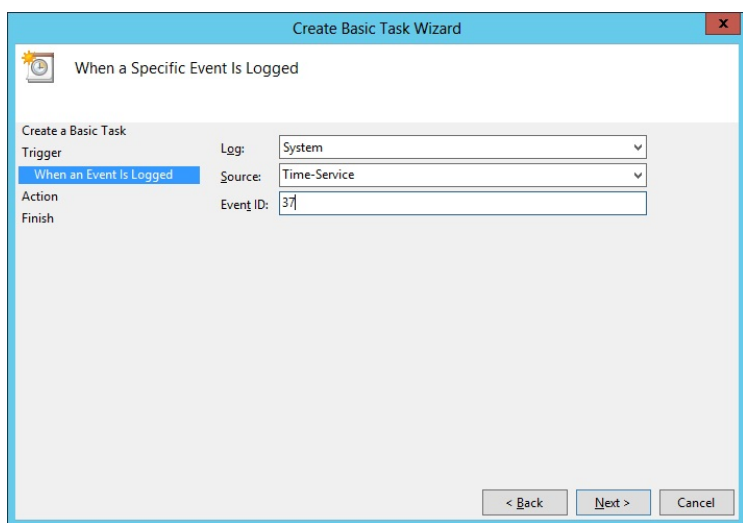


FIGURE F.47 [Create Basic Task Wizard] window (When a Specific Event Is Logged)
Click the [Next] button.

6. Select "Start a program" on the [Action] screen. Click the [Next] button.

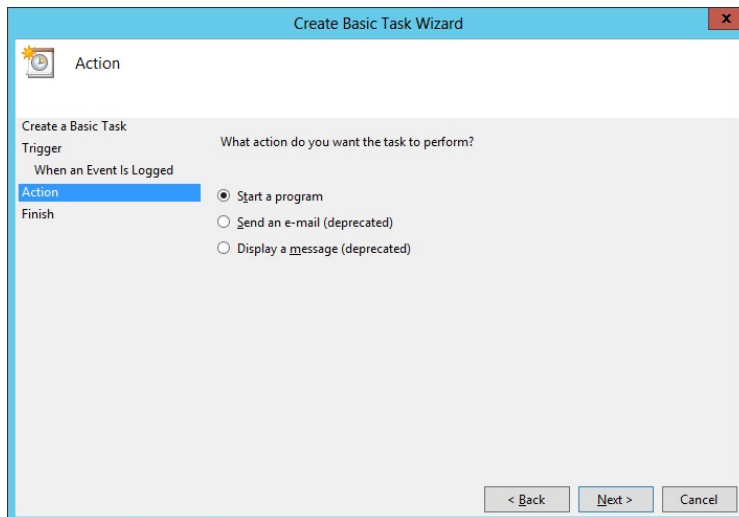


FIGURE F.48 [Create Basic Task Wizard] window (Action)

7. Set the following parameters on the [Start a Program] screen.
 - [Program/script]: %SystemRoot%\w32tm.exe
 - [Add arguments] (optional): /resync

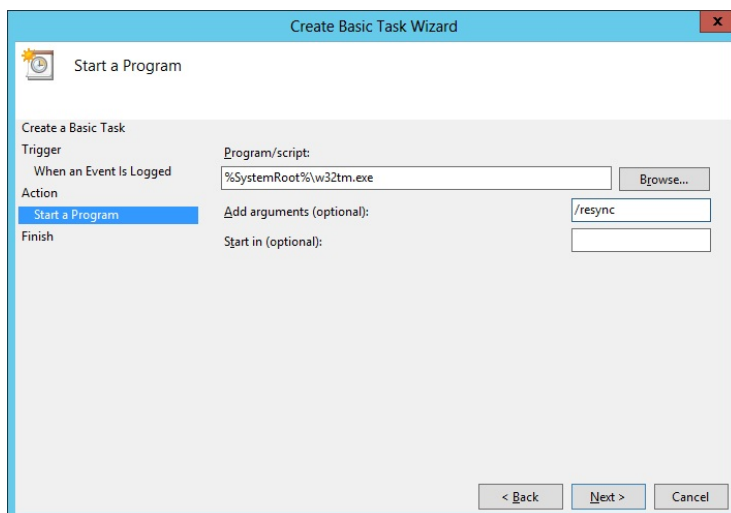


FIGURE F.49 [Create Basic Task Wizard] window (Start a Program)

Click the [Next] button.

8. Check the [Open the Properties dialog for this task when I click Finish] check box on the [Summary] screen.

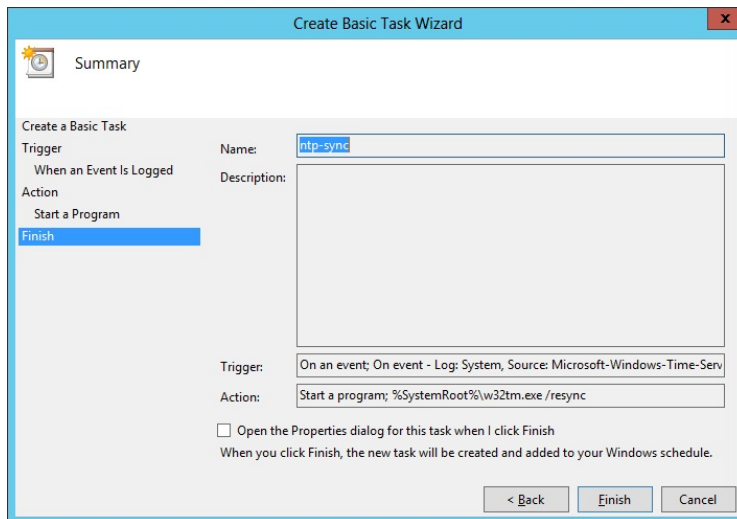


FIGURE F.50 [Create Basic Task Wizard] window (Summary)
Click the [Finish] button.

9. Click the [Change User or Group] button in the [Properties] dialog box.

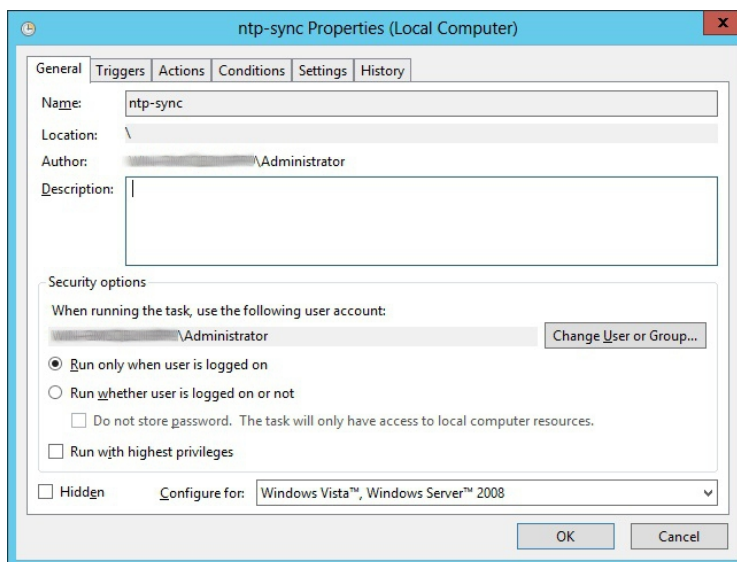


FIGURE F.51 [Properties] dialog box

10. [Select User or Group] dialog box appears.
Set the following parameter.
 - [Enter the object name to select]: System

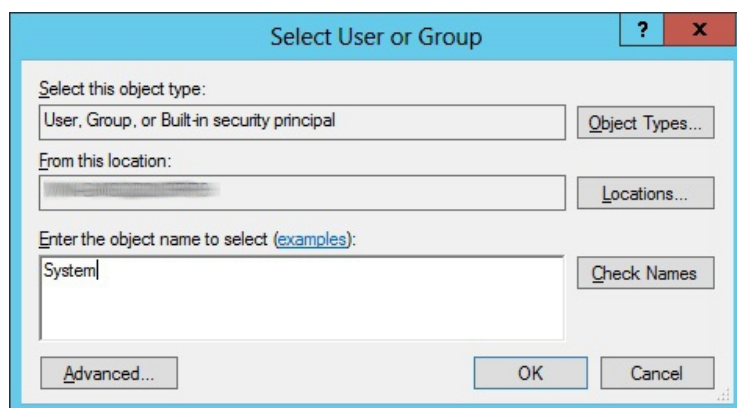


FIGURE F.52 [Select User or Group] window
Click the [OK] button.

11. Click the [OK] button to close the [Properties] dialog box.

Index

- [A]
- [Access Control] window (example)..... 226
 - Accessories required in main unit installation..... 11
 - [Add a Port] dialog box (PSA)..... 168
 - [Add a Port] dialog box (SNMP)..... 169
 - [Add Filter] window (example)..... 227
 - [Add SB/IOB/GSPB to Partition] window (example).... 44
 - [Add User] window (example)..... 38
 - [Alarm E-Mail Filtering Condition] window (example).... 37
 - [Alarm E-Mail] window (example)..... 36
- [B]
- Backup/Restore MMB Configuration window (example).... 57
 - [Backup/Restore MMB Configuration] window (example)... 133 , 209
 - [Backup BIOS Configuration] window (example).... 134 , 210
 - Before Installing the Main Unit..... 7
 - Before Starting Setup..... 18
 - BlueScreenTimeout setting ([Configuration] tab)..... 50
 - BlueScreenTimeout setting ([Misc] settings)..... 51
 - BMC Settings..... 243
 - Building a RAID Environment Using VMware 4.x Built-in Disks..... 273
 - Building a RAID Environment Using VMware 5.x Built-in Disks..... 293
 - Buttons in the title area..... 31
- [C]
- Checking Environmental Conditions..... 8
 - Checking the Installation Site..... 10
 - Completion of VMware 4.x installation..... 274
 - Configuring a DNS Server..... 223
 - Configuring a Partition..... 43
 - Configuring NTP..... 219
 - Configuring PSA (Linux: Red Hat Enterprise Linux).... 141
 - Configuring PSA (Windows Server 2003)..... 161
 - Configuring PSA (Windows Server 2008)..... 175
 - Configuring Security..... 225
 - Configuring Service Life Monitoring by RAS Support Service..... 135 , 211
 - Configuring SMTP..... 224
 - Configuring SVS (SVagent/SVmco)..... 117
 - Configuring the firewall for PSA operation..... 288
 - Configuring the NTP Client..... 132 , 205
 - Configuring the SAN Boot Environment..... 271
 - Confirmation message dialog box..... 173 , 201
 - Confirmation of the required settings for PSA operation, and corresponding features about the settings.... 141 , 161 , 175
 - Confirming the Supplied Parts..... 12
 - Connecting and Configuring the MMB..... 20
 - Connecting the Power Cables..... 14
 - [Console Redirection Setup] window (example)..... 55
 - Content area..... 30
 - [Create Basic Task Wizard] window (Action).... 305 , 312 , 321
 - [Create Basic Task Wizard] window (Create a Basic Task)... 304 , 310 , 319
 - [Create Basic Task Wizard] window (Start a Program).... 305 , 312 , 321
 - [Create Basic Task Wizard] window (Summary).... 305 , 313 , 322
 - [Create Basic Task Wizard] window (Task Trigger).... 304 , 311 , 320
 - [Create Basic Task Wizard] window (When a Specific Event Is Logged)..... 304 , 311 , 320
- [D]
- [Date/Time] window (example)..... 41 , 221
 - [Date and Time Properties] window (1)..... 298
 - [Date and Time Properties] window (2)..... 298
 - [Date and Time] window (1)..... 301 , 307 , 315
 - [Date and Time] window (2)..... 301 , 307 , 316
 - Default user account and password..... 26
 - [DNS and Routing Configuration] dialog box..... 290
 - Dump device configuration menu..... 122 , 124
 - Dump device list menu..... 125
 - Dump device maintenance menu..... 121 , 124 , 126
 - Dump device selection menu..... 122 , 123
 - Dump device setting menu..... 125
 - Dump Device Setting Menu..... 126
 - Duplicate Network Adapter Configuration..... 218
- [E]
- [Edit User] window (example)..... 39
 - Event Task Settings..... 303 , 309 , 318
 - Example of display of the [Change Boot Order] menu.... 63 , 69 , 75 , 84 , 99 , 103 , 107 , 112
 - Example of the Device Manager menu..... 119
 - Examples of firewall configurations..... 288
 - [Export List] window (example)..... 207
 - [Export] window (example)..... 208
 - External interfaces of the MMB..... 21
 - External network configuration..... 218
- [G]
- General Description and Types of Bundled Software.... 270
 - [General] tab in [SNMP Service (UDP In) Properties].... 182
- [I]
- If the folder contains one file..... 79 , 88
 - If the folder contains two files..... 79 , 88
 - Information displayed in the window..... 27
 - [Information] window (example)..... 56
 - Installation complete window..... 266
 - Installation Overview..... 1
 - Installation Procedure for the Operating System and Bundled Software..... 60

Installing the Operating System and Bundled Software....	59
Installing VMware 4.x Bundled Software.....	277
Installing VMware 5.x Bundled Software.....	294
[Install Windows] window.....	77 , 86
[Internet Time Settings] window.....	302 , 308 , 316
[IP Address] dialog box.....	184
IP addresses to be set for virtual ports.....	287
[L]	
Lists of Settings (Links).....	239
[M]	
Main menu (sadump).....	119 , 121 , 127
Maintenance status display.....	28
[Management LAN Port Configuration] window (example)	42
Manually Installing PSA (Linux: Red Hat Enterprise Linux)	246
Manually Installing PSA (Windows Server 2003).....	255
Manually Installing PSA (Windows Server 2008).....	261
Manual PSA Installation and Uninstallation.....	245
Message for advance notification of replacement and replacement notification message (RAID card)....	135 , 211
Message for advance notification of replacement and replacement notification message (UPS).....	137 , 213
MMB connection and configuration flow.....	20
MMB Settings.....	240
MMB USER port location.....	23
MMB Web-UI login window.....	26
[Mode] window (example).....	54 , 76 , 85
Mounting location and external interfaces of the MMB....	21
Mounting the Main Unit in a 19-inch Rack.....	13
[N]	
Network configuration after setup.....	288
Network configuration and IP addresses of the management LAN.....	24
Network configuration immediately after installation of OS	283
[Network Interface] window (example).....	33 , 35
[Network Protocols] window (example)....	34 , 228 , 232 , 233
New Inbound Rule Wizard - Action.....	189
New Inbound Rule Wizard - Name.....	191
New Inbound Rule Wizard - Profile.....	190
New Inbound Rule Wizard - Program.....	186
New Inbound Rule Wizard - Protocol and Ports.....	187
New Inbound Rule Wizard - Rule Type.....	185
New Inbound Rule Wizard - Scope.....	188
New Outbound Rule Wizard - Protocol and Ports....	192 , 194
Notes on VMware 4.x Installation.....	274
Notes on VMware Installation.....	272
NTP Settings in Windows Server 2003.....	298
NTP Settings in Windows Server 2008.....	301
NTP Settings in Windows Server 2008 R2.....	307

NTP Settings in Windows Server 2012.....	315
[O]	
Operating system installation by SVIM....	62 , 68 , 74 , 83 , 98 , 102 , 106 , 110
Operation with external NTP servers (three NTP servers)....	220
Overview of NTP Client Settings.....	296
[P]	
Packages required for PSA operation (RHEL5).....	247
Packages required for PSA operation (RHEL6).....	247
Packages required for SIRMS operation (RHEL6).....	248
[Partition Configuration] window (example)....	43 , 45 , 52
[Partition Home] window (example).....	47
Ports to open for the management LAN interfaces.....	147
Ports to open for the PSA-to-MMB communication LAN interface.....	108 , 113
Ports to open for the PSA-to-MMB communication LAN interfaces.....	151
Power cable socket locations (PCI_Box).....	15
Power cable socket locations (PRIMEQUEST 1800E2/1800E).....	15
[Power Control] window (example).....	236 , 238
Powering On and Off a Partition.....	235 , 236
Preparing for Main Unit Installation.....	5
Preparing the Power Supply Equipment.....	9
Preparing to Install the Main Unit.....	11
Preparing to Install window.....	171 , 197 , 201 , 257 , 264
[Program and Features] window.....	200
Program removal window.....	199
[Properties] dialog box.....	306 , 313 , 322
[Protocol and Ports] setting items.....	186 , 192
PSA Settings.....	241
[R]	
RAS Support Service screens (move to another partition)....	136 , 212
RAS Support Service screens (no BBU).....	135 , 212
Recommended Write Policy Setting for SAS Disk RAID Units.....	214
Recovery Procedure after the Execution of the Simple Setup Tool (editconf.sh).....	215
[Registry Editor] selection window.....	317
[Registry Editor] window.....	299 , 302 , 308 , 317
[Remove SB/IOB/GSPB from Partition] window (example)	46
Required settings for external LAN connections.....	24
[Reserved SB Configuration] window (example).....	48
RHEL Installation Procedures on the SAN Storage Unit....	61
[Run] window.....	299 , 302 , 308
[S]	
sadump setup menu.....	120
Safety Precautions.....	6
Saving Configuration Information.....	57
Saving Management and Configuration Information....	133 , 206

Scheduled Operations.....	234
[Scope] setting items.....	187 , 192 , 194
[Scope] tab in [SNMP Service (UDP In) Properties].....	183
secLevel settings.....	154
Select Features window.....	258 , 263 , 265
[Select User or Group] window.....	306 , 313 , 323
[Server Configuration] window.....	275
[Services] window.....	300 , 303 , 309 , 317
Setting of sadump.....	118
Settings after PSA Installation (VMware 4.x).....	282
Settings after VMware 4.x PSA Installation.....	282
Settings after VMware 4.x SVMco Installation.....	292
Settings automatically added/changed during PSA installation.....	142 , 162 , 176 , 249
Settings for system clock synchronization.....	296
Settings for terminal software.....	21
Setting Up the Dump Environment (Linux).....	129 , 204
Setting Up the Dump Environment (Windows)....	128 , 203
Setting up the NTP Server (Windows).....	295
Setting various modes.....	52
Setup complete window.....	259
Setup window.....	258 , 264
Setup Workflow.....	2
[SNMP Community] window (example).....	229
[SNMP Trap] window (example).....	230
[SNMP v3 Configuration] window (example).....	231
Software (Links).....	269
[Software Watchdog] window.....	276
Specifying an NTP Server.....	298 , 301 , 307 , 315
Starting the System.....	19
Status indicator types.....	31
Submenu area.....	29
SUSE Linux Enterprise Server 11 Service Pack 2 Installation Procedures on the Built-in HDD.....	110
SUSE Linux Enterprise Server 11 Service Pack 2 Installation Procedures on the SAN Storage Unit.....	105
Synchronization Interval and Startup Settings of NTP Service	308 , 316
Synchronization Interval Setting.....	298 , 302
[System Information] window (example).....	40
System status indicators.....	28

[T]

[Task Scheduler] window.....	303 , 310 , 319
Types of Work.....	116 , 140
Types of work.....	116 , 140

[U]

UEFI Settings.....	242
Uninstall Complete window.....	174 , 202
Update installation complete window.....	173 , 198
Update installation window.....	172 , 197
URL to enter for login.....	26
[User List] window (example).....	38

[V]

VMware 5.x bundled software and its installation destination	294

VMware 5.x setting procedure and setting destination....	294
VMware vSphere 4.x Client.....	289

[W]

[Watchdog] tab in the VMware 4.x software window....	275
Windows Firewall window.....	181
[Windows Time Properties] window.....	309 , 318
Work after Installation.....	217
Work after Operating System Installation (PRIMEQUEST 1800E).....	139
Work after Operating System Installation (PRIMEQUEST 1800E2).....	115
Work before Operating System Installation.....	17
Work performed by the user.....	2

FUJITSU