

Areas Covered



Before Reading This Manual	
	This section explains the notes for your safety and conventions used in this manual.
Chapter 1	Overview of ServerView
	This chapter explains the overview of ServerView, its form of management, and the system requirements. Please make sure to read these sections before using ServerView.
Chapter 2	Installing
	This chapter explains how to install ServerView.
Chapter 3	How to Use ServerView
	This chapter explains how to use the various functions that ServerView prepares for monitoring servers.
Chapter 4	Using RemoteControlService
	This chapter explains how to use RemoteControlService.
Chapter 5	Using the Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104)
	This chapter explains how to use the Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104). This is available only for the server on which the Remote Service Board is installed.
Appendix	
	This chapter explains supplementary information such as troubleshooting, a variety of lists, and technical information.

Before Reading This Manual

Remarks

■ Symbols

Symbols used in this manual have the following meanings:

	These sections explain prohibited actions and points to note when using this software. Make sure to read these sections.
	These sections explain information needed to operate the hardware and software properly. Make sure to read these sections.
→	This mark indicates reference pages or manuals.

■ Key Descriptions / Operations

Keys are represented throughout this manual in the following manner:

E.g.: [Ctrl] key, [Enter] key, [→] key, etc.

The following indicate the pressing of several keys at once:

E.g.: [Ctrl] + [F3] key, [Shift] + [↑] key, etc.

■ Entering Commands (Keys)

Command entries are written in the following way:

```
diskcopy a: a:
           ↑ ↑
```

- In the spaces indicated with the "↑" mark, press the [Space] key once.
- In the example above, the command entry is written in lower case, but upper case is also allowed.
- CD-ROM drive names are shown as [CD-ROM drive]. Enter your drive name according to your environment.

```
[CD-ROM drive]:\setup.exe
```

■ Operations for Linux

The mount commands for CD-ROM drive and floppy disk drive differ depending on the version.

Interpret "/mnt/cdrom/", "/media/cdrom/" or "/media/cdrecorder/" and "mnt or media/floppy" in this manual as follows depending on your Linux version.

- For RHEL-AS4(x86)/ES4(x86)/AS4(IPF)
media/cdrecorder, media/floppy
- For RHEL-AS4(EM64T)/ES4(EM64T)
media/cdrom, media/floppy
- For RHEL-AS3(x86)/AS3(IPF)/ES3(x86)
mnt/cdrom, mnt/floppy

■ Screen Shots and Figures

Screen shots and figures are used as visual aids throughout this manual. Windows, screens, and file names may vary depending on the OS, software, or configuration of the server used. Figures in this manual may not show cables that are actually connected for convenience of explanation.

■ Consecutive Operations

Consecutive operations are described by connecting them with arrows (→).

Example: For the operation to click the [Start] button, point to [Programs], and click [Accessories]

↓

Click the [Start] button → [Programs] → [Accessories].

■ Product Names

The following expressions and abbreviations are used throughout this manual.

table: Abbreviations of Product Names

Product name	Expressions and abbreviations
Microsoft® Windows Server™ 2003, Standard Edition Microsoft® Windows Server™ 2003, Enterprise Edition Microsoft® Windows Server™ 2003, Standard x64 Edition Microsoft® Windows Server™ 2003, Enterprise x64 Edition Microsoft® Windows Server™ 2003, Enterprise Edition for Itanium-Based Systems	Windows 2003
Microsoft® Windows® 2000 Server Microsoft® Windows® 2000 Advanced Server	Windows 2000
Microsoft® Windows® Server Network Operating System Version 4.0 Microsoft® Windows NT® Server, Enterprise Edition 4.0	Windows NT
Microsoft® Windows® XP Professional	Windows XP Professional
Windows 2003, Windows 2000, Windows NT	Windows
Microsoft® Windows® 2000 Professional	Windows 2000 Professional
Microsoft® Windows NT® Workstation Operating System 4.0	Windows NT Workstation 4.0
Red Hat® Linux®	Linux
Red Hat Enterprise Linux AS(v.4 for x86)	RHEL-AS4(x86)
Red Hat Enterprise Linux ES(v.4 for x86)	RHEL-ES4(x86)
Red Hat Enterprise Linux AS(v.4 for EM64T)	RHEL-AS4(EM64T)
Red Hat Enterprise Linux ES(v.4 for EM64T)	RHEL-ES4(EM64T)
Red Hat Enterprise Linux AS(v.4 for Itanium)	RHEL-AS4(IPF)
Red Hat Enterprise Linux AS(v.3 for x86)	RHEL-AS3(x86)
Red Hat Enterprise Linux AS(v.3 for Itanium)	RHEL-AS3(IPF)
Red Hat Enterprise Linux ES(v.3 for x86)	RHEL-ES3(x86)

Reference Information

■ Hints.txt

In addition to the descriptions in this manual, ServerView provides the other information and notes to guide you in "Hints.txt". Please read it before using ServerView.

"Hints.txt" is stored in the PRIMERGY Document & Tool CD. Use a text editor to read it.

■ Limitations and Supported OS Associated with Machine Types

Some functions may be restricted depending on your machine type. Limitations for each machine type are described in "Hints.txt". Please make sure to read it before using ServerView.

Some OS described in this manual may not be supported depending on machine types. Please confirm the supported OS for your server in the manuals supplied with each server.

■ Latest Information about ServerView

For the latest information regarding ServerView, refer to the Fujitsu PRIMERGY website (<http://primergy.fujitsu.com>).

Trademarks

VGA and PS/2 are registered trademarks of IBM Corporation.

Microsoft, Windows, MS, MS-DOS, and Windows Server are trademarks or registered trademarks of Microsoft Corporation in the USA and other countries.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the USA and other countries.

Linux is a trademark or registered trademark of Linus Torvalds in the USA and other countries.

Red Hat and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the USA and other countries.

All other hardware and software names used are trademarks or registered trademarks of their respective manufacturers.

Other product names are copyrights of their respective manufacturers.

All Rights Reserved, Copyright© FUJITSU LIMITED 2005

Screen shot(s) reprinted with permission from Microsoft Corporation.

Contents

Chapter 1 Overview of ServerView

1.1 Understanding ServerView	12
1.1.1 Monitoring hardware	14
1.1.2 Abnormality Occurrence Notification/Server Status Check	15
1.1.3 Automatic Reconfiguration & Restart	17
1.1.4 Remote Management	17
1.1.5 Advanced Server Management with Remote Service Board	17
1.2 Hardware Management Mode	18
1.3 System requirements	19

Chapter 2 Installing

2.1 Installation Flow	26
2.2 Checking before Installation	27
2.2.1 Installation of TCP/IP Protocol and SNMP Service	27
2.2.2 Changing Binding Order	31
2.2.3 Service Pack Application	31
2.2.4 Web Server Installation	32
2.2.5 Kernel and RPM Check	33
2.3 Installing	34
2.3.1 [Windows] Installing ServerView Console	34
2.3.2 [Windows] Installing ServerView Agent (Monitored Server)	39
2.3.3 [Linux]Installing ServerView Linux (Monitored Server)	40
2.3.4 [Linux]Installing ServerView Linux (Monitored Server, only ServerView Linux Agent)	48
2.4 Checking after Installation	58
2.4.1 Installing a Web Browser	58
2.4.2 Installing Java™ 2 Runtime Environment Standard Edition	59
2.4.3 Setting an Administrative User	60
2.4.4 Registering the Interrupt Information (MIB) of the Optional Devices	62
2.4.5 Extending the Web Service	64
2.4.6 [Linux]Setting each Service (for Monitored Server)	65
2.4.7 [Linux]Setting each Service (When installing only ServerView Linux Agent on the monitored server)	70
2.4.8 Changing Computer Information after Installation	73

Chapter 3 How to Use ServerView

3.1 Starting and Exiting ServerView S2	76
3.1.1 Starting ServerView S2	76
3.1.2 ServerView S2 Menus (Command List)	79

3.1.3 Registering the Monitored Servers	81
3.1.4 Verifying/Changing the Server Settings	84
3.1.5 Registering MIB (MIB INTEGRATION)	87
3.2 Monitoring Servers	88
3.2.1 Verifying the Server Status	88
3.2.2 Verifying the Server Monitoring Items in Detail	92
3.2.3 Displaying Configuration Information	95
3.2.4 Recovery	100
3.2.5 Displaying Operating System Information	102
3.2.6 Verifying the Status of Mass Storage	103
3.2.7 Verifying the Baseboard Status	108
3.2.8 Verifying the Component Status	112
3.2.9 Version Manager (Inventory)	117
3.2.10 Remote Management	118
3.3 Monitoring Blade Servers	119
3.4 Serious Error Handling (ASR)	123
3.4.1 Setting Procedures	123
3.5 AlarmService	131
3.5.1 Alarm Monitor	132
3.5.2 Alarm Manager	139
3.5.3 Alarm Settings	142
3.6 Performance Manager	171
3.6.1 Starting the Performance Manager	172
3.6.2 Defining/Modifying Thresholds	173
3.6.3 Creating/Editing Set of Thresholds	177
3.6.4 Defining/Modifying Reports	178
3.6.5 Creating/Editing Set of Reports	179
3.6.6 Applying the Settings to Servers	180
3.6.7 Report View	181
3.6.8 Checking/Resolving the Differences	182
3.7 Management of Archive Data	183
3.7.1 Starting the Archive Manager	183
3.7.2 Creating Archive Data	184
3.7.3 Configuring Tasks for Retrieving Archive Data	185
3.7.4 Displaying/Comparing/Deleting Archive Data	187
3.7.5 Archive Data Log	190
3.7.6 Importing Archive Data	191
3.8 Export Manager	192
3.8.1 Acquiring Export Data	192
3.8.2 Configuring Export Data Retrieval	195
3.8.3 Displaying Export Data	200
3.9 ServerView Operation Using the Management Console	202
3.9.1 Starting the Management Console	202
3.9.2 Adding the Monitored Server (Object)	206

3.9.3 Verifying/Changing the Server Information	210
3.9.4 Threshold Manager	211
3.9.5 Report Manager	215
3.9.6 Copying Settings to the Other Servers	218
3.9.7 Monitoring Hardware	219
3.9.8 Verifying the Status of the Blade Servers	235
3.10 Settings for ServerView Agent	237
3.10.1 Modify/Save/Restore Settings (Configuration Tools)	237
3.11 [Linux] How to Use ServerView Linux	241

Chapter 4 Using RemoteControlService

4.1 Overview of RemoteControlService	246
4.1.1 Functions	247
4.1.2 System Requirements	248
4.1.3 Notes	249
4.2 Preparation	252
4.2.1 Configuring RomPilot	252
4.2.2 Configuration for RCM	254
4.2.3 Configuration for IPMI	255
4.2.4 Installing/Uninstalling RemoteControlService/LAN	266
4.2.5 Installing/Uninstalling RemoteControlService/Web	267
4.3 Starting and Exiting	268
4.3.1 Start and Exit for RemoteControlService/LAN	268
4.3.2 Start and Exit for RemoteControlService/Web (For BMC connection)	273
4.3.3 Start and Exit for RemoteControlService/Web (For RSB connection)	276
4.3.4 Start and Exit for RemoteControlService/Web (For ManagementBlade connection)	278
4.4 How to Use	280
4.4.1 Password Management	280
4.4.2 Remote Server Management	282
4.4.3 BIOS Setup	287
4.4.4 Server's Boot Operations	288
4.4.5 Support of the Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104)	291
4.4.6 IPMI Support	299

Chapter 5 Using the Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104)

5.1 Overview	302
5.1.1 Functions	302
5.1.2 Notes	302
5.2 Preparation	303
5.2.1 Setting the LAN Interface	303

5.2.2 Installation and Configuration of the Management Server Application (MSA)	306
5.2.3 Configuring the Directory Service Function	307
5.3 Displaying Each Monitoring Information	310
5.3.1 Starting the Web Interface	310
5.3.2 [Manage] Page	313
5.3.3 [Sensors] Page	331
5.3.4 [Card Config] Page	333
5.3.5 [Server Config] Page	337
5.3.6 [Alarm Config] Page	338
5.3.7 [User Config] Page	340
5.3.8 [Web/SSL Config] Page	343
5.3.9 [DS Config] Page	348

Appendix

A Troubleshooting	352
A.1 Troubleshooting of Installation Script	352
A.2 Troubleshooting of Management Console	355
A.3 Troubleshooting of AlarmService	362
A.4 ServerView S2 Troubleshooting	368
A.5 Other	370
B Uninstallation	376
B.1 Uninstalling ServerView	376
C Icon List	379
C.1 Server List	379
C.2 ServerView menu	380
C.3 Mylex's [Device View] window	381
C.4 [DPT Disk Array Agent] window	381
C.5 Network Interfaces window	381
C.6 Bus and Adaptor window	382
C.7 Alarm Manager window and Alarm Monitor window	382
C.8 Cluster status (unsupported)	383
C.9 Blade server status	386
C.10 Other icons	387
D Trap List	389
E Threshold List	390
E.1 Monitored values	390
E.2 Meaning of each value	390
F Technical Information	396
F.1 Agent and Management Console	396
F.2 Management Information Base	397
F.3 Principles of SNMP	397
F.4 Version Management (Inventory View)	401
F.5 List of Contents to be Exported	402
F.6 How to Change SNMP Settings	404

F.7 Firmware Version of Remote Service Board (RSB)405

Chapter 1

Overview of ServerView

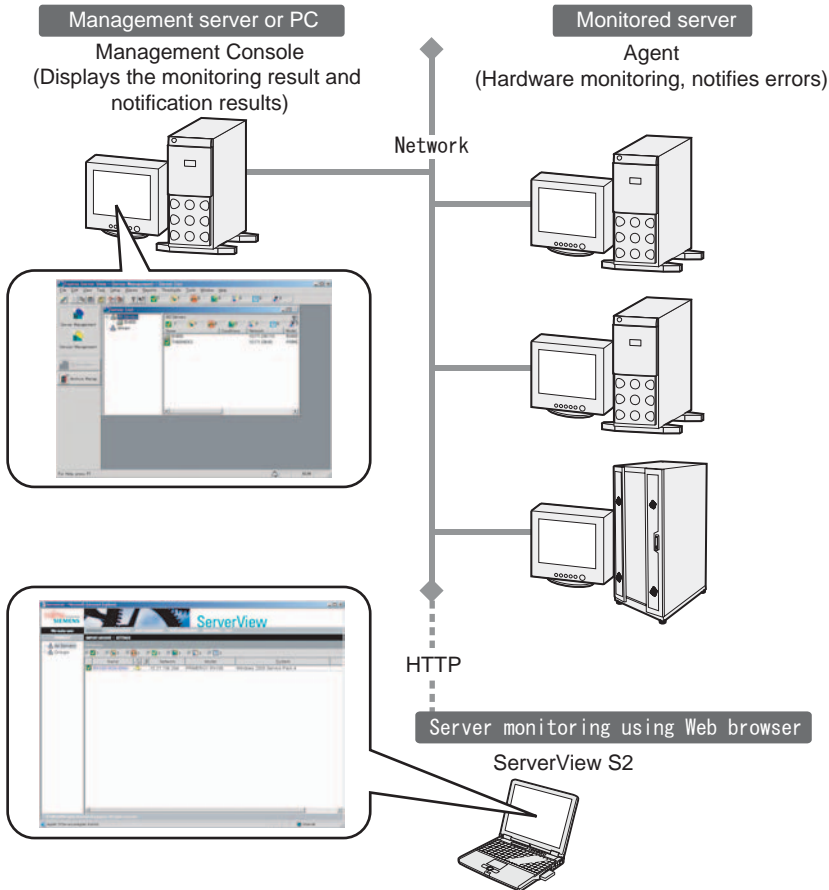
This chapter explains ServerView's functions, management modes, and system requirements.

1.1 Understanding ServerView	12
1.2 Hardware Management Mode	18
1.3 System requirements	19

1.1 Understanding ServerView

ServerView is a software to monitor whether the server hardware is in the proper state via the network. ServerView allows the server to be monitored all the time. If ServerView detects an abnormality, it notifies the server administrator in real-time. This section introduces the functions of ServerView.

The ServerView has several components. The software on the monitored server to actually monitor and notify an abnormality is referred to as "Agent". The software on the management server or PC to browse the monitoring result or control the monitored server is referred to as "Management Console". Also, the ServerView's function "ServerView S2" allows administrator to monitor server with Web browser even if Management Console is not installed on the server or PC. The user can select whether to install both Management Console and Agent or to install them separately depending on the network configuration or the server OS.



■ How to monitor the server

There are two methods for checking server status or setting for server monitoring: using Web browser and using Management Console.

● Server Monitoring with Web browser

ServerView's function "ServerView S2" allows administrator to monitor server with Web browser. The administrator can use ServerView even if Management Console is not installed on the PC outside the office.

For details about how to operate ServerView S2 from Web browser, refer to "3.1 Starting and Exiting ServerView S2" (→pg.76).

● Server Monitoring with Management Console

The administrator can install Management Console into the server or PC that are connected to the network to monitor server.

For details about how to operate Management Console, refer to "3.9 ServerView Operation Using the Management Console" (→pg.202).

■ ServerView's functions

Installing ServerView allows user to utilize the following functions that support reliable server operation.

- Hardware Monitoring (→pg.14)
- Abnormality Occurrence Notification/Server Status Check (→pg.15)
- Automatic Reconfiguration & Restart (→pg.17)
- Remote Management (→pg.17)
- Advanced Server Management with Remote Service Board (→pg.17)

1.1.1 Monitoring hardware

ServerView monitors the hardware components on the server unit and the option devices equipped.

■ Monitorable hardware

The hardware components on the server unit and option devices the ServerView can monitor are listed below.

By installing ServerView agent, monitoring these components and devices starts automatically. The monitored items require no specific setting.

● Hardware components on the server unit

The monitorable hardware components vary depending on the server type. For more details, refer to "Hints.txt" in the PRIMERGY Document & Tool CD.

table: Hardware components

Monitorable components	Monitoring contents
Voltage sensor	Server voltage
Temperature sensor	CPU/chassis temperature
CPU	Display the mounted CPU information, error
Fan	Fans for CPU/chassis interior/power supply
Chassis	Chassis opening/shutting
Memory	Display mounted device information
Power Supply	Failure

● Optional devices

If a MIB file is provided optionally, refer to "2.4.4 Registering the Interrupt Information (MIB) of the Optional Devices" (→pg.62) and register the interrupt information.

table: Optional devices

Monitorable optional devices	Overview of monitoring
Internal hard disk unit mounted on onboard SCSI	Displays the device information
SCSI card	Displays the card information
LAN card	Displays the Internet information Displays the Ethernet MAC statistics
SCSI RAID card	Displays the drive list Displays the card information Displays the device information
IDE-RAID card	Displays the drive list Displays the card information Displays the device information


When SCSI RAID card is monitored:

- ▶ You need to install SCSI-RAIDmanager attached to the SCSI RAID card. Also, the array controller agent meeting each SCSI RAID card must be installed. The table below shows the typical IDE-RAID controller cards and corresponding array controller agents.

table: SCSI RAID cards and corresponding array controller agents

Cards used	SCSI-RAID manager	Array controller agent
PG-140, PG-141, and PG-142	StorageManager	DPT Disk Array Agent
PG-143, PG-144, FC103, and FC105	GAM (Global Array Manager)	Install Mylex dac960 Disk Array Agent

When IDE-RAID card is monitored:

- ▶ You need to install IDE-RAIDmanager attached to the IDE-RAID card. Also, the array controller agent meeting each IDE-RAID card must be installed. Typical IDE-RAID cards and corresponding array controller agents are shown on the table below.

table: IDE-RAID controller cards and corresponding array controller agents

Cards used	IDE-RAIDmanager	Array controller agent
IDE-RAID system	PROMISE Fastrak	Install PROMISE Fastrak IDE Disk Array
PG-1E4B	PAM (PROMISE ARRAY MANAGEMENT) Console	PAM (PROMISE ARRAY MANAGEMENT) Message Server/Message Agent

1.1.2 Abnormality Occurrence Notification/Server Status Check

ServerView provides the means to notify occurrence of the abnormality to Management Console and verify the server status.

The administrator can find out the current server status and the reason for troubles and respond to the trouble promptly.

The contents of the alarm to notify can be set flexibly and in detail to the operation state of the system.

■ Abnormality occurrence notification

When ServerView finds the abnormality in the server hardware, the monitoring program (agent) saves the event to the event log and notifies SNMP trap.

The administrator uses the AlarmService of ServerView to reference, edit, and set the alarm and notification method. For details, refer to "3.5 AlarmService" (→pg.131).

The administrator can customize the monitoring criteria called "threshold" and set ServerView to notify when the threshold is exceeded (regardless of the threshold having been set, monitoring with initial value set for each server type is always performed).

For details about threshold settings, refer to "3.6 Performance Manager" (→pg.171). If you are using the Management Console, refer to "3.9.4 Threshold Manager" (→pg.211).

POINT

- ▶ The event log stored to ServerView Agent is the following:
Log type: application
Source name: ServerView Agents

■ Verifying server status

ServerView has the following functions to find the server status reliably.

- "Version management function" for managing the versions of server hardware and software
- "Archive function" for recording server status
- "Reporting function" for outputting server status

● Version management function

The list of the server hardware components and software can be checked on the Management Console window. By checking their versions, the status of each sever component can be found.

For details about version management function, refer to "3.2.9 Version Manager (Inventory)" (→pg.117).

● Archive function

By using ServerView ArchiveService, the server status can be recorded regularly as an "archive data". By comparing the recorded archived data with the archived data after a trouble, the cause of the trouble can be checked out.

Creating or comparing operation of the archived data is done using "Archive Manager". For more details, refer to "3.7.1 Starting the Archive Manager" (→pg.183).

● Reporting function

For report creation, the values measured regularly for a given period is recorded and displayed in the form of table or graph. This function enables monitoring of server on a long-term basis.

For details, refer to "3.6 Performance Manager" (→pg.171). If you are using the Management Console, "3.9.5 Report Manager" (→pg.215) can be used as well.

■ Copying settings to other server

The values of each setting item for alarm, threshold, and report output above can be copied to other server. Therefore, working hours for setting can be reduced when many servers must be set to the same setting.

For details on how to copy the settings to other servers, refer to "3.9.6 Copying Settings to the Other Servers" (→pg.218).

IMPORTANT

- ▶ When the OS is Linux, reporting function and function for copying settings to other server are not supported.
However, the archive can be obtained from ServerView S2 on Linux.
- ▶ To utilize reporting function and copying setting function, monitoring must be performed from Windows Management Console.

1.1.3 Automatic Reconfiguration & Restart

ServerView provides a function called "ASR (Automatic Server Reconfiguration & Restart)" to automatically restart or shut down the server when an abnormality occurs. Using this function allows you to safely shut down the server in which the abnormality has occurred or continue to operate server by disabling only the abnormal location after restarting.

For details about ASR settings, refer to "3.4 Serious Error Handling (ASR)" (→pg.123).

1.1.4 Remote Management

After installing "RemoteControlService" attached to ServerView and setting server's BIOS extension function, the server administrator can restart, shut down the server, or set up the BIOS from his/her PC. The administrator can manage the server without moving to the server location.

For details about installing RemoteControlService and how to set BIOS, refer to "Chapter 4 Using RemoteControlService" (→pg.245).



- ▶ RemoteControlService allows user to perform important setting related to server operations, such as BIOS set up. The person who has sufficient knowledge, such as a server administrator, should perform this operation.
- ▶ RemoteControlService and LAN are only supported in Windows Management Console.

1.1.5 Advanced Server Management with Remote Service Board

RSB (Remote Service Board) is an optional extension card equipped with dedicated CPU, OS, communication interface and power. This board operates regardless of server status. It monitors or notifies information even when the server shuts down and cannot notify an abnormal condition by itself. The server administrator can grasp the server status through RSB from Management Console on PC or Web browser and perform recovery work such as forced power on or reset.

To use RSB, preparation work such as installing driver has to be done in advance. For more details, refer to "Chapter 5 Using the Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104)" (→pg.301).

1.2 Hardware Management Mode

The server administrator can check the status of the server hardware with Management Console.

The hardware management mode varies depending on the component used.

■ Components of management console and agent

ServerView has the following components:

table: Components of management console and agent

Component name	Supported OS	Description
ServerView Console	<ul style="list-style-type: none"> Windows 2003 Windows 2000 Windows XP Professional 	The Management Console that is installed on the server or PC. The status of all monitored servers can be collectively displayed and multiple servers can be centrally managed. This includes ServerView S2 and AlarmService.
ServerView Agents	<ul style="list-style-type: none"> Windows 2003 Windows 2000 	The Agent that is installed on the monitored server.
ServerView Linux	Linux	
ServerView S2, AlarmService		The web-based management console that is installed on the monitored server.
ServerView Linux Agent		The Agent that is installed on the monitored server.

POINT

- ▶ Management Console can be installed only when the OS is Windows. When the OS is Linux, Management Console is not supported.
- ▶ For details about supported OS, refer to "1.3 System requirements" (→pg.19).

1.3 System requirements

The system requirements for server and PC to use ServerView are as follows:

■ ServerView Agent (Installation to Server)

The system requirements when installing ServerView on the server are as follows:

table: System requirements when installing ServerView Agent

Server system	Operational conditions
Hardware	
Memory used	256MB or more
Hard disk	100MB or more of free space
Monitor	SVGA (800×600) or more of resolution (recommended: 1024×768)
LAN Card	Required (On Board LAN is also possible)
Mouse	Required
Software	
OS	<ul style="list-style-type: none"> • Windows 2003 • Windows 2000 Service Pack 4 or later
Protocol	TCP/IP is required to run
Service	SNMP (service and trap) must be operated.
Account	Privileges equal to administrator must be assigned



- ▶ ServerView Agent is dedicated to PRIMERGY. Do not install it on the servers other than PRIMERGY.

■ ServerView Console (installation to server or PC)

The system requirements when installing ServerView Console on server or PC are as follows:

table: System requirements when installing ServerView Console

PC system	Operational conditions
Hardware	
PC	IBM PC compatible
Processor	Pentium® or higher
Memory used	256MB or more
Hard disk	400MB or more of free space
Monitor	SVGA (800×600) or more of resolution (recommended: 1024×768)
LAN Card	Required (On Board LAN is also possible)
Mouse	Required
Software	
OS	<ul style="list-style-type: none"> • Windows 2003 • Microsoft Windows 2000 Professional Operating System Service Pack 4 or later • Microsoft Windows XP Professional Operating System
Web server	<ul style="list-style-type: none"> • Microsoft Internet Information Server V6.0 (Windows 2003) • Microsoft Internet Information Server V5.0 (Windows 2000) • Microsoft Internet Information Server V5.1 (Windows XP Professional) or <ul style="list-style-type: none"> • ServerView Web-Server (Apache for Win32 based) (Installed automatically when it is selected during the ServerView installation) or <ul style="list-style-type: none"> • Apache2
Protocol	TCP/IP is required to run
Service	SNMP (service and trap) must be operated.
Web browser	<ul style="list-style-type: none"> • Microsoft Internet Explorer 5.5 or later (recommended: 6.0 or later) • Java™ 2 Runtime Environment Standard Edition V1.4.2_08 or later. (It can be installed from PRIMERGY Document & Tool CD.)
Account	Privileges equal to administrator must be assigned



- ▶ Microsoft Virtual Machine is not supported in ServerView V3.40 or later.

■ ServerView Linux Agent (installation to server)

The system requirements when installing ServerView Linux Agent on the server are as follows:

table: System requirements when installing ServerView Linux Agent

PC system	Operational conditions
Hardware	
Memory used	32MB or more
Hard disk	30MB or more of free space (/lib 3MB/var 3MB/etc 3MB/sbin 1MB/usr 20MB)
Monitor	SVGA (800×600) or more of resolution (recommended: 1024×768)
LAN Card	Required (On Board LAN is also possible)
Mouse	Required
Software	
OS	<ul style="list-style-type: none"> • Red Hat Enterprise Linux AS(v.4 for x86) (Abbreviation:RHEL-AS4(x86)) • Red Hat Enterprise Linux ES(v.4 for x86) (Abbreviation:RHEL-ES4(x86)) • Red Hat Enterprise Linux AS(v.4 for EM64T) (Abbreviation:RHEL-AS4 (EM64T)) • Red Hat Enterprise Linux ES(v.4 for EM64T)(Abbreviation:RHEL-ES4 (EM64T)) • Red Hat Enterprise Linux AS(v.3 for x86) (Abbreviation: RHEL-AS3 (x86)) • Red Hat Enterprise Linux AS(v.3 for Itanium) (Abbreviation: RHEL-AS3 (IPF)) • Red Hat Enterprise Linux ES(v.3 for x86) (Abbreviation: RHEL-ES3 (x86))
Protocol	TCP/IP is required to run
Service	SNMP (service and trap) must be operated.
Package (RPM)	<ul style="list-style-type: none"> • net-snmp • net-snmp-utils • compat-libstdc++ • gcc • glibc • glibc-devel • binutils • libstdc++ • make • gawk • rpm • kernel-source(for RHEL-AS3/ES3(x86) / RHEL-AS3(IPF)) • kernel-devel(for RHEL-AS4/ES4(x86) / RHEL-AS4/ES4(EM64T)) • at
Account	Superuser



- ▶ ServerView Linux agent is dedicated for PRIMERGY. Do not install it on the servers other than PRIMERGY.

■ ServerView S2/AlarmService (when OS is Linux)

When installing ServerView S2/AlarmService on the server running Linux OS, the system requirements are the following:

table: System requirements when installing ServerView S2/AlarmService

Server system	Operational conditions
Hardware	
Memory used	128MB or more
Hard disk	70MB or more of free space (/var 60MB/etc 3MB/usr 7MB)
Monitor	Resolution of SVGA (800×600) or more (recommended: 1024×768)
LAN Card	Required (On Board LAN is also possible)
Mouse	Required
Software	
OS	<ul style="list-style-type: none"> • Red Hat Enterprise Linux AS(v.4 for x86) (Abbreviation:RHEL-AS4(x86)) • Red Hat Enterprise Linux ES(v.4 for x86) (Abbreviation:RHEL-ES4(x86)) • Red Hat Enterprise Linux AS(v.4 for EM64T) (Abbreviation:RHEL-AS4 (EM64T)) • Red Hat Enterprise Linux ES(v.4 for EM64T)(Abbreviation:RHEL-ES4 (EM64T)) • Red Hat Enterprise Linux AS(v.3 for x86) (Abbreviation: RHEL-AS3 (x86)) • Red Hat Enterprise Linux AS(v.3 for Itanium) (Abbreviation: RHEL-AS3 (IPF)) • Red Hat Enterprise Linux ES(v.3 for x86) (Abbreviation: RHEL-ES3 (x86))
Web server	Apache (use RPM to install)
Protocol	TCP/IP is required to run
Service	ATD (service) is required to run when Server View S2 and AlarmService are installed
Web browser	<ul style="list-style-type: none"> • Mozilla V1.3 or later • Mozilla FireFox 1.0.4 or later • Java™ 2 Runtime Environment Standard Edition V1.4.2_08 or later (It can be installed from PRIMERGY Document & Tool CD.)
Package (RPM)	<ul style="list-style-type: none"> • net-snmp • net-snmp-utils • compat-libstdc++ • httpd • gnome-libs • rpm • gawk • openssl • mod_ssl • at
Account	Superuser



- ▶ ServerView S2 and AlarmService cannot be used separately. Both must be installed.

■ ServerView S2 Screen-displayed Requirements

When displaying web screen of ServerView S2, the requirements for web browser and Java are the following:

● Web Browser

For Windows: Microsoft Internet Explorer 5.5 or later (recommended: 6.0 or later)

For Linux: Mozilla V1.3 or later, or Mozilla FireFox 1.0.4 or later

● Service

ATD (service) is required to run when ServerView S2 is installed.

● Java

Java™ 2 Runtime Environment Standard Edition V1.4.2_08 or later

(It can be installed from PRIMERGY Document & Tool CD.)



- ▶ Microsoft VirtualMachine is not supported in ServerView V3.40 or later.

Chapter 2

Installing

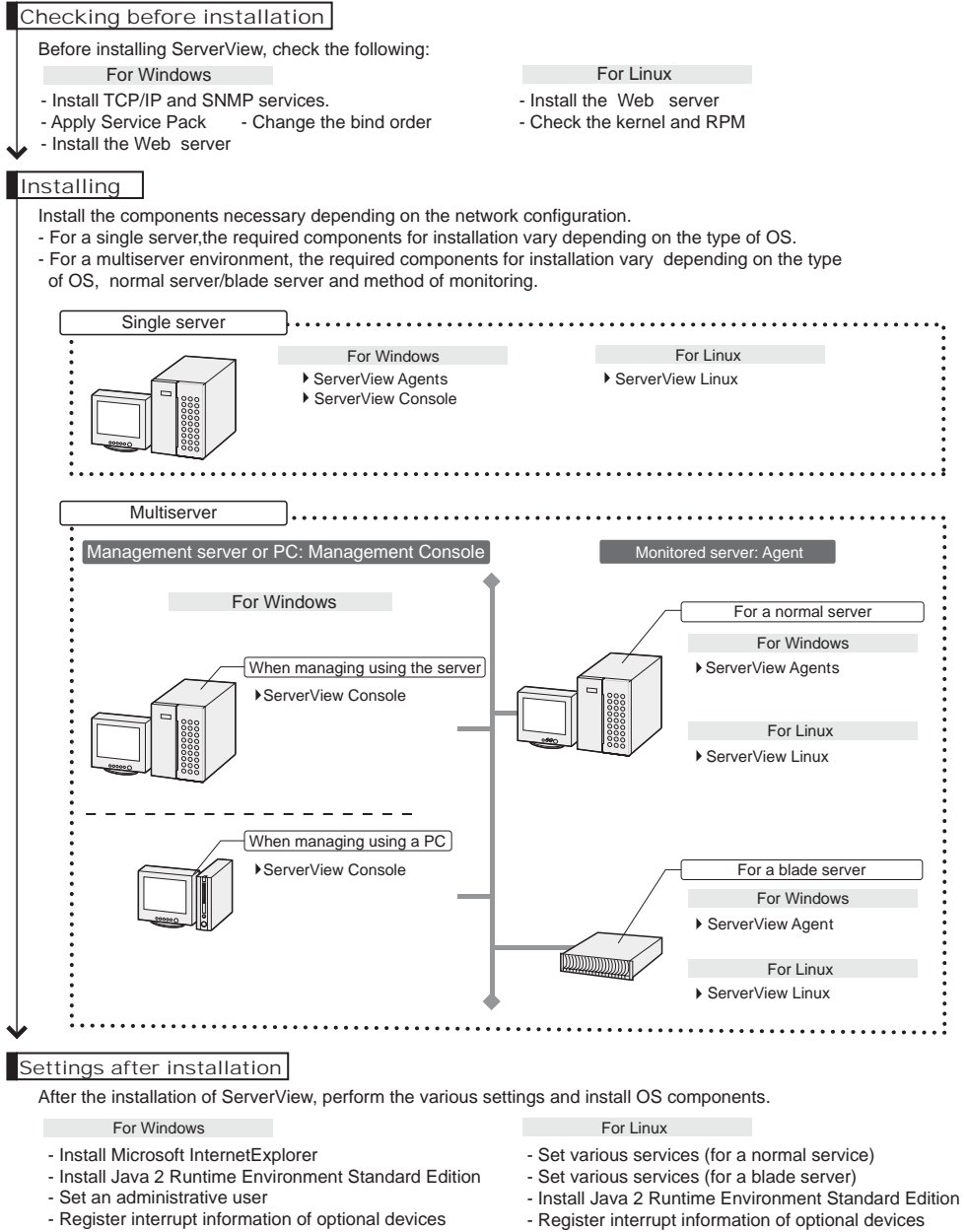
2

This chapter explains how to install ServerView.

2.1	Installation Flow	26
2.2	Checking before Installation	27
2.3	Installing	34
2.4	Checking after Installation	58

2.1 Installation Flow

The installation flow of ServerView is the following:



2.2 Checking before Installation

Before installing ServerView, check the following:

2.2.1 Installation of TCP/IP Protocol and SNMP Service

To make sure that ServerView functions correctly, the TCP/IP protocol and the SNMP service must be installed on the monitored server.

In the description below, the example of the SNMP service community name is written as "public". The community name can be changed when necessary. For details about changing community name, refer to the technical information. "Appendix F Technical Information" (→pg.396)

■ For Windows 2003:

- 1 Start up [Control Panel].
- 2 Double-click [Network Connections].
- 3 Click the [Advanced] menu → [Optional Networking Components].

4 Perform one of the following:

When the [Management and Monitoring Tools] in [Optional Networking Components Wizard] is already checked:

1. Click the [Management and Monitoring Tools] and click [Details], then make sure that the [Simple Network Management Protocol (SNMP)] is checked.
If this check box is already checked, the SNMP service has been already installed. In this case, go to Step 5.

When the [Management and Monitoring Tools] in [Optional Networking Components Wizard] is not checked:

Follow the steps below to install the SNMP service.

1. Check the [Management and Monitoring Tools] in [Optional Networking Components Wizard].
2. Click [Details] and make sure that the [Simple Network Management Protocol (SNMP)] is checked, and then click [OK].
3. In the [Optional Networking Components Wizard], click [Next].

Follow the messages on the window.

- 5 Click [Start] → [Control Panel] → [Administrative Tools].
- 6 Click [Manage Computers].
- 7 On the left tree, click [Services and Applications] → [Services].
- 8 Click [SNMP Service] on the right hand side of the window.

- 9** Click the [Action] menu → [Properties].
- 10** In the [General] tab, make sure that the [Startup Type] is set to [Automatic].
Set it [Automatic] when it is not set [Automatic].
- 11** Click the [Traps] tab.
- 12** If the "public" is already in the [Community name] field, select "public". If not, enter "public" in the [Community name] field and click [Add to list].
- 13** Click [Add] in the [Trap destinations] section.
- 14** Enter the host name and IP address of the server on which ServerView Console is installed and click [Add].
When installing ServerView Console on single server environment, enter its own host name and IP address. When operating multiple ServerView Consoles, enter each host name and IP address.
- 15** Click the [Security] tab.
- 16** Click "public" and [Edit].
- 17** Select [READ WRITE] or [READ CREATE] from [Community rights] and click [OK] ([READ WRITE] is recommended).
When the "public" does not exist in the [Accepted Community Names] list:
Follow the steps below to add the community.
 1. Click [Add].
 2. Select [READ WRITE] or [READ CREATE] from [Community rights] ([READ WRITE] is recommended).
 3. Enter the "public" in the [Community] field and click [Add].
- 18** Configure the hosts from which SNMP packets are accepted.
When accepting SNMP packets from any host:
 1. Click [Accept SNMP packets from any host].
When accepting SNMP packets from the specified hosts:
 1. Click [Accept SNMP Packets from These Hosts].
 2. Click [Add].
 3. Enter the host name and IP address of the server on which ServerView is installed and click [Add].
For the server where ServerView Agent is installed, make sure that the loopback address (127.0.0.1) is included.

19 Click [OK].**POINT**

- ▶ In Windows 2003, the initial setting for the message PopUp (Messenger) is disabled. To perform message PopUp in the ServerView's monitoring function, follow the steps below to set the PopUp.
 1. Click [Start] → [Administrative Tools].
 2. Click [Manage Computers].
 3. On the left tree, click [Services and Applications] → [Services].
 4. Click [Messenger] on the right hand side of the window.
 5. Click the [Action] menu → [Properties].
 6. Click the [General] tab.
 7. Select [Automatic] for [Startup Type] and click [OK].

■ For Windows 2000:

- 1 Start up [Control Panel].
- 2 Double-click the [Network and Dialup Connections] icon.
- 3 Click the [Advanced] menu → [Optional Networking Components].
- 4 Perform one of the following:
 - When the [Management and Monitoring Tools] in [Optional Networking Components Wizard] is already checked:
 1. Click the [Management and Monitoring Tools] and click [Details], then make sure that the [Simple Network Management Protocol (SNMP)] is checked.
If this check box is already checked, the SNMP service has been already installed. In this case, go to Step 5.
 - When the [Management and Monitoring Tools] in [Optional Networking Components Wizard] is not checked:
Follow the steps below to install the SNMP service.
 1. Check the [Management and Monitoring Tools] in [Optional Networking Components Wizard].
 2. Click [Details] and make sure that the [Simple Network Management Protocol (SNMP)] is checked, and then click [OK].
 3. In the [Optional Networking Components Wizard], click [Next].
 4. Follow the messages on the window.
- 5 Double-click the [Administrative Tools] icon in the [Control Panel].
- 6 Double-click the [Manage Computers] icon.
- 7 On the left tree, click [Services and Applications] → [Services].
- 8 Click [SNMP Service] on the right hand side of the window.
- 9 Click the [Action] menu → [Properties].

- 10** In the [General] tab, make sure that the [Startup Type] is set to [Automatic].
Set it [Automatic] when it is not set [Automatic].
- 11** Click the [Traps] tab.
- 12** If the "public" is already in the [Community name] field, select "public".
If not, enter "public" in the [Community name] field and click [Add to list].
- 13** Click [Add] in the [Trap destinations] section.
- 14** Enter the host name and IP address of the server on which ServerView Console is installed and click [Add].
When installing ServerView Console on single server environment, enter its own host name and IP address.
When operating multiple ServerView Consoles, enter each host name and IP address.
- 15** Click the [Security] tab.
- 16** Click the "public".
- 17** Click [Edit].
- 18** Select [READ_WRITE] or [READ_CREATE] from [Community rights] and click [OK] ([READ_WRITE] is recommended).
When the "public" does not exist in the [Accepted Community Names] list:
Follow the steps below to add the community.
 1. Click [Add].
 2. Select [READ_WRITE] or [READ_CREATE] from [Community rights] ([READ_WRITE] is recommended).
 3. Enter "public" in the [Community] field.
 4. Click [Add].
- 19** Configure the hosts from which SNMP packets are accepted.
When accepting SNMP packets from any host:
 1. Click [Accept SNMP packets from any host].
When accepting SNMP packets from the specified hosts:
 1. Click [Accept SNMP Packets from These Hosts].
 2. Click [Add].
 3. Enter the host name and IP address of the server on which ServerView is installed and click [Add].
For the server where ServerView Agent is installed, make sure that the loopback address (127.0.0.1) is included.
- 20** Click [OK].

2.2.2 Changing Binding Order

When multiple IP addresses exist in the server due to mounting multiple LAN cards, etc., ServerView searches IP address in the order set for the network bindings.

The binding order should be set so that the adapter that communicates with the Management Console is searched first.

To change the network binding orders, follow the steps below.

- 1 Start up [Control Panel].
- 2 Double-click "Network Connections".
The [Network Connections] window appears.
- 3 In the [Network Connection] window, click [Advanced] in the [Advanced] menu.
The [Advanced] window appears.
- 4 Click the [Adapters and Bindings] tab.
- 5 Click on the connection for which you would like to change and use the arrow buttons on the right side to change the orders.

2.2.3 Service Pack Application

Service Pack must be applied to all servers and PCs on which each component of ServerView is installed. However, the Service Pack installation is not required for Windows 2003.

- For Windows 2000, apply Service Pack 4 or later.



- ▶ Make sure that the Service Pack is applied. If the Service Pack is not applied, the operation cannot be guaranteed.
If the Service Pack has been already applied, it is not required to apply it again.
- ▶ Before applying the Service Pack, make sure that the SNMP service is installed on.

2.2.4 Web Server Installation

The functions such as alarm service (refer to "■ Abnormality occurrence notification" (→pg.15)), archive function (refer to "● Archive function" (→pg.16)), and monitoring servers using the Web browser (refer to "● Server Monitoring with Web browser" (→pg.13)) are used from the Web browser. To use these functions, the Web server software must be installed on the server. The followings are the Web server software that ServerView supports.

- For Windows, use one of the following:
 - ServerView Web-Server (Apache for Win32 based)
 - Microsoft Internet Information Server (IIS)
 - Apache2
- For Linux
 - httpd

POINT

- ▶ If the OS is Linux and ServerView S2/AlarmService is not used, the httpd is not required to install.

■ ServerView Web-Server

The ServerView Web-Server is automatically installed when its installation is selected during the ServerView Console installation.

The ServerView Web-Server is installed at the same time as the ServerView Console when ServerView installation is selected during the set up by ServerStart.

■ Microsoft Internet Information Server (IIS)

To use IIS, it should be installed before the ServerView installation.

The following versions of the IIS are supported for each OS.

table: Supported IIS

OS	Description
Windows 2003	Version 6.0 is supported.
Windows 2000	Version 5.0 is supported.
Windows XP	Version 5.1 is supported.

IMPORTANT

- ▶ Do not change the home directory local path and the SCRIPTS local path. When these settings are changed, the operational warranty will not be applied.

■ Apache2

To use Apache2 independently, it should be installed before the ServerView installation.

■ httpd

If the OS is Linux, RPM for httpd must be installed before the ServerView Linux installation.

2.2.5 Kernel and RPM Check

Insert the PRIMERGY Documents & Tools CD and execute the following command.

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/  
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/  
Linux/ENGLISH  
# ./chkver (for monitored server)  
# ./BR_chkver (when installing only ServerView Linux agent on the  
monitored server)
```

When the error message about the kernel version appears, make sure that the kernel has been properly updated.

When the error message about insufficient RPM package appears, install the package from the Red Hat Linux CD-ROM.

IMPORTANT

- ▶ When the kernel is updated, make sure that the kernel version number matches the kernel-source version number. When they do not match each other, ServerView can not be installed. The kernel version number and the kernel-source version number can be checked by the output results of "uname r". and "rpm -q kernel-source" respectively.

2.3 Installing

This section explains how to install each component of ServerView.

2.3.1 [Windows] Installing ServerView Console

To use the Management Console in Windows, install ServerView Console (Management Console / ServerView S2 / AlarmService).



- ▶ When you want to change or update the Web server (Apache2 or IIS) after the ServerView Console installation, uninstall the ServerView Console and install it again. If ServerView has been automatically installed with ServerStart, the ServerView Web-Server has been selected for the Web server. For information on how to uninstall the ServerView Console, refer to "Appendix B Uninstallation" (→pg.376).
 - ▶ For the system on which the terminal server has been installed, the installation method differs from usual methods. To install ServerView on the terminal server environment, perform the Step 3 below after clicking [Start] → [Control Panel] → [Add/Remove Programs] → [Add Program].
 - ▶ When Java has not been installed before ServerView Console is installed, the following message is displayed.
"No Java Virtual Machine detected. Some functions will not work properly until you install a java Virtual machine from the Support CD."
Click [OK], the installation is continued. Installing Java, after installation ServerView Console.
 - ▶ If you have several different versions of ServerView, install the latest ServerView Console.
- 1 Log in as an administrator or with the name of the user having a privilege equal to the administrator.
 - 2 Close all running applications.

- 3 Insert the PRIMERGY Document & Tool CD and double-click the installer below.

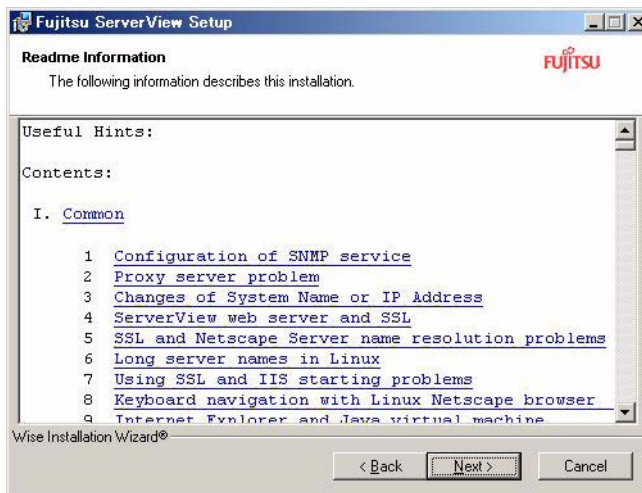
[CD-ROM drive]:\SVMANAGE\ENGLISH\SV_Console.bat

The [Fujitsu ServerView Setup] window appears.



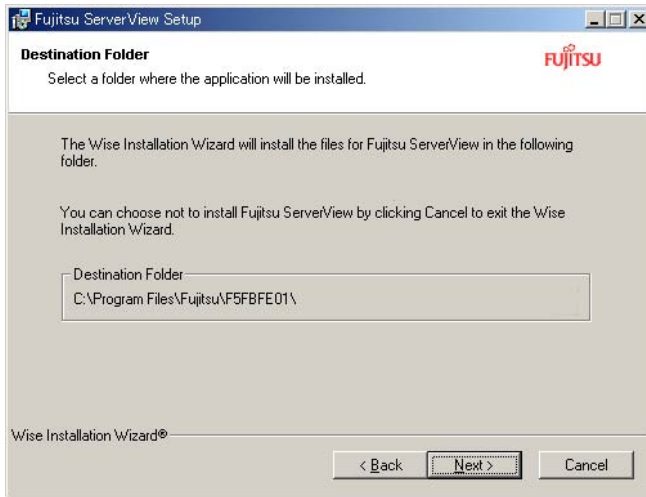
- 4 Click [Next].

The [Readme Information] window appears.



5 Click [Next].

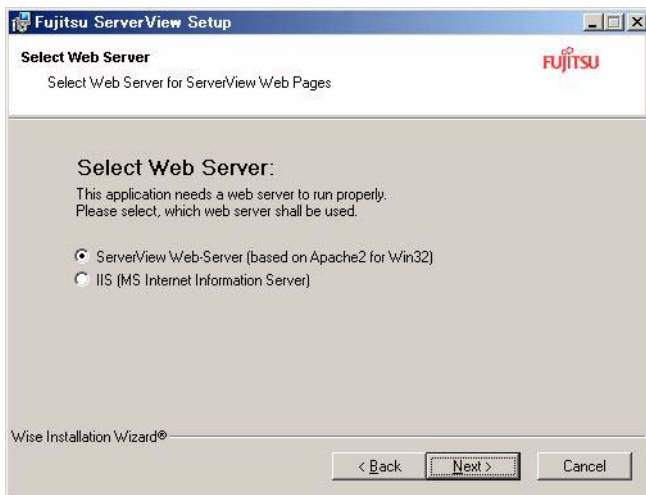
The [Destination Folder] window appears, the destination folder for installing ServerView Console is displayed.



6 Click [Next].

The [Select Web Server] window appears.

Note that if IIS is not installed, the [Select Web Server] window will not appear.



IMPORTANT

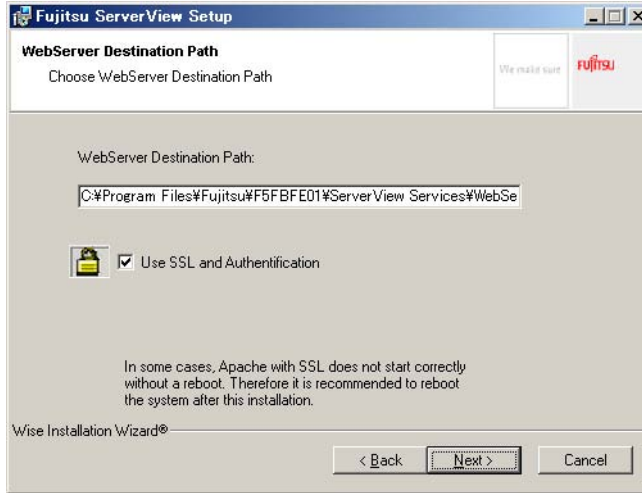
- ▶ When the ServerView Web-Server is selected, the Apache2 for Win32-based Web server is installed with ServerView. And the task with the name "At**(**: task ID)" is added to the Windows Task Scheduler.
- ▶ When the IIS is selected, the installed IIS is used as a Web server.
- ▶ When the Apache2 has been already installed as a Web server, [Apache2 (Installed Apache2 server)] appears instead of [ServerView Web-Server] for the selection item on the [Select Web-Server] window.

7 Select the Web server to use and click [Next].

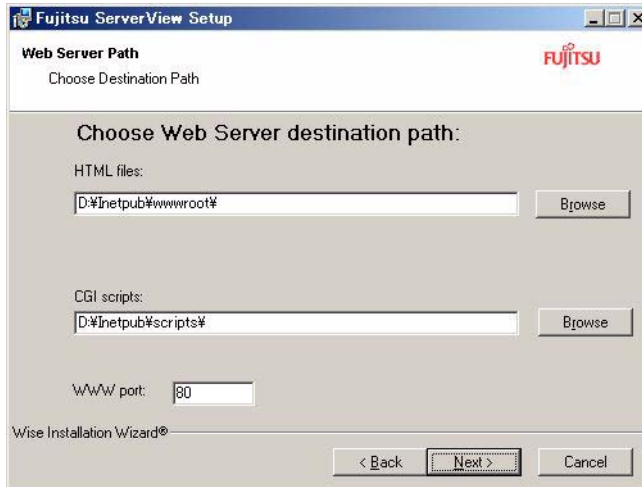
The [WebServer Destination Path] window appears.

The window varies depending on the selected WebServer.

When [ServerView Web-Server] is selected for the Web server:



When [IIS] or [Apache2 (Installed Apache2 server)] is selected for the Web server:



POINT

- ▶ When ServerView Web-Server is selected from the [Select WebServer] window, the [Use SSL and authentication] checkbox appears. If the checkbox is selected, SSL connection is possible when connecting to the Web, and then authentication will be requested when connection is made. When this option is selected, it is recommended to restart the system after the installation.

IMPORTANT

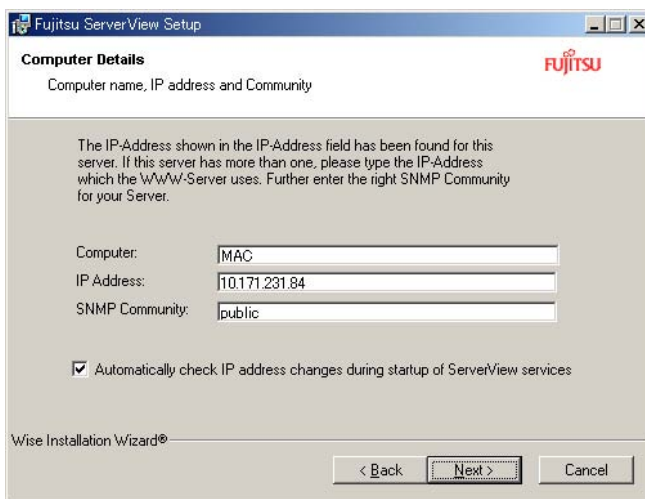
- ▶ Do not change the folder of the location displayed.
- ▶ The IIS port number cannot be acquired automatically. If the IIS port number is changed, enter the changed port number.
- ▶ When ServerView is automatically installed with ServerStart, the use of the SSL and authentication is enabled. To disable them, uninstall ServerView. Then, start the ServerView installer and install ServerView again.

For the user name and password used for authentication, "svuser" is set as the user name and "fsc" is set as the password by default.

For information on how to add or change the user name and password, refer to "● ServerView Web-Server and SSL" (→pg.373).

8 Click [Next].

The [Computer Details] window appears.



9 Click [Next].

The [Ready to Install the Application] window appears.



10 Click [Finish].

Installation starts.

After finishing installation, the [Exit] window will appear.

11 Click [Exit].

Now, the installation has been finished. After the installation has been finished, refer to "2.4 Checking after Installation" (→pg.58) and set the settings required to operate ServerView.

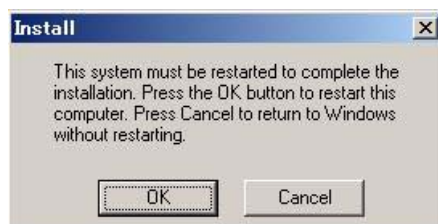
2.3.2 [Windows] Installing ServerView Agent (Monitored Server)

Install "ServerView Agent" on the Windows monitored server.



- ▶ When you want to update ServerView Agent, uninstall the ServerView Agent and install it again. For information on how to uninstall ServerView, refer to "Appendix B Uninstallation" (→pg.376).
- ▶ For the system on which the terminal server has been installed, the installation method differs from usual methods. To install ServerView Agent on the terminal server environment, perform the Step 3 below after clicking [Start] → [Control Panel] → [Add/Remove Programs] → [Add Program].

- 1** Log in as an administrator or with the name of the user having a privilege equal to the administrator.
- 2** Close all running applications.
- 3** Insert the PRIMERGY Document & Tool CD and start the installer below.
[CD-ROM drive]:\SVMANAGE\ENGLISH\Agents_setup.EXE
The [ServerView System Requirements] window appears.
- 4** Click [OK].
The [ServerView Hints] window appears.
- 5** Click [OK].
When the installation has finished, the restart message appears.
- 6** Click [OK] or [Cancel].



After the installation has been finished, refer to "2.4 Checking after Installation" (→pg.58) and set the settings required to operate ServerView.

2.3.3 [Linux]Installing ServerView Linux (Monitored Server)

Install ServerView Linux (ServerView Linux Agent/ServerView S2/AlarmService) on the Linux monitored server.

To install ServerView Linux Agent, ServerView S2, and Linux version of the alarm service at the same time, perform the subsequent steps.

When ServerView S2/AlarmService is installed on a server under the Linux only environment, the status of other servers can be monitored.

There are two ways to install ServerView Linux, Please select the method according to the usage.

- Installation using the install script (→pg.41)
Select this method when performing new installation of ServerView, and performing reinstallation of default setting server, etc.
- Manual installation (→pg.45)
Select this method when installation script cannot be used to install, and performing reinstallation without changing of snmpd.conf setting.

POINT

- ▶ When you want to install only ServerView Linux Agent (without ServerView S2/AlarmService) on the Linux monitored server, refer to "2.3.4 [Linux]Installing ServerView Linux (Monitored Server, only ServerView Linux Agent)" (→pg.48).
If ServerView S2/AlarmService is not used, the httpd , openssl, and mod_ssl are not required to install. Even if ServerView S2/AlarmService are not installed, the monitored server (ServerView Linux Agent) can be monitored from the Windows Management Console.

IMPORTANT

- ▶ When the atd service is stopped, the following message appears. This message must be ignored since it is for RX800.
If the following message appears for RX800, start atd service before installation, and stop atd service after installation.

```
Unable to build the binary module package
srvmagt_mods_bin in the background
Please build the package manually with the fol-
lowing command if necessary:
/etc/init.d/eecd_mods_src makepackage
```

Also, when ServerView S2 and AlarmService are installed, atd service is required to run. Start atd service before installation, and stop atd service after installation.

- ▶ This document describes the ServerView Linux installation from the Document & Tool CD. When you download and install ServerView Linux from our Web page, the specified part of the directory should be changed to the directory to which the files are transmitted and expanded.

- ▶ When “SELINUX” is “Enabled” for RHEL-AS4/ES4(x86) or RHEL-AS4/ES4(EM64T), follow the procedures below to set to “Disabled”.
Change the following value in “/etc/selinux/config” file, and restart the server. After installation, set back this item, and restart the server.
 - (Before edit) SELINUX=enforcing
 - (After edit) SELINUX=disabled

■ Installing ServerView Linux with Installation Script

Using the installation script within the PRIMERGY Document & Tool CD allows you to install ServerView Linux Agent/ServerView S2/AlarmService and edit the SNMP service setting file (/etc/snmp/snmpd.conf).

The SNMP service setting file (/etc/snmp/snmpd.conf) is edited only at the installation for the first time. To update Linux Agent, manual installation is recommended for setting protection.

When the installation script terminates with an error message displayed, refer to "A.1 Troubleshooting of Installation Script" (→pg.352).

POINT

- ▶ The /etc/snmp/snmpd.conf can also be edited manually after the installation of ServerView. After editing manually, execute the "/etc/rc.d/init.d/snmpd restart" command.

IMPORTANT

- ▶ The snmpd.conf may also exist under the /usr/share/snmp directory. The snmpd also reads the settings of the /usr/share/snmp/snmpd.conf. Edit the /usr/share/snmp/snmpd.conf as necessary.

● How to start the installation script

To install with the installation script, log in as superuser and insert the PRIMERGY Document & Tool CD, and then execute the following command.

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
Svmanage/Linux/ENGLISH
# ./inssv
```

■ Entering SNMP trap destination IP address

After the title of installation script is displayed, the SNMP trap destination IP address will be asked to enter. If ServerView Linux Agent has been already installed, you will be asked to enter the SNMP trap destination IP address after the uninstallation is done. Enter the IP address to which you want to send SNMP trap and press the [Enter] key.

It is not necessary to enter the server’s own IP address (127.0.0.1) at this point since it is automatically set. When destination IP address has already been written, it is not added.

If the trap is sent to multiple devices, enter the IP address of each device.

The IP address entered is written into the /etc/snmp/snmpd.conf.

After entering the IP address, press the [e] key. Go to the steps below.

The following is the example of the output result.

```
ServerView install / RPM control script version VX.XLXX
Copyright(C) FUJITSU LIMITED 2005

checking necessary RPMs ...
RPMs check [OK]

available disk space check [OK]
(Uninstallation is performed when ServerView Linux Agent has been
installed already)

Please input IP-addresses to where you want to send SNMPtraps.
(Note : No need to input the IP address of this server, it will be added
automatically by the installer.)

Press "e" key to continue.

>192.168.1.10
>192.168.1.20
>e
```

● Entering the Location

Enter the server location (installation location).

The entered location is written to syslocation item in the `/etc/snmp/snmpd.conf` and will be shown in a property of the server at the ServerView as a "Location".

When the location has already entered by reinstalling, entered location becomes invalid.

Up to 64B of single byte character sets can be entered.

After the location is entered, press the [Enter] key. Go to the step below.

When nothing is entered and the [Enter] key is pressed, the default values will be written.

```
Please input a location of the server.
The specified location will be shown as a property of the server at the
ServerView console.

You can change the location of the server later,
by editing the /etc/snmp/snmpd.conf.
>(Example: computer room L200)
```

● Entering the administrator

Enter the server administrator name.

The entered administrator name is written to `syscontact` item in the `/etc/snmp/snmpd.conf` and will be shown in a property of the server at the ServerView as an "Administrator".

When the administrator name has already entered by reinstalling, entered administrator name becomes invalid.

Up to 64B of single byte character sets can be entered. When the administrator name is entered, press the [Enter] key. Go to the step below. When nothing is entered and the [Enter] key is pressed, the default values will be written.

```
Please input a name of the root user.  
The specified name will be shown as a property of the server at the  
ServerView console.  
  
You can change the name of the root user later,  
by editing the /etc/snmp/snmpd.conf.  
>(Example: Your name)
```

● Executing RPM

The RPMs of ServerView Linux agent and ServerView S2/AlarmService are executed. The output result of each RPM is displayed.

The example below is the normal output result.

```
install srvmagt-mods_src, please wait...
Compiling Server View modules for 2.6.9-11.EL
  Building modules, stage 2.
[ OK ]
Loading Server View modules: smbusr [ OK ]
2712

job 1 at 2004-05-11 21:34

install srvmagt-eeecd, please wait...
Starting eeecd[ OK ]

install srvmagt-agents, please wait...
Stopping snmpd: [ OK ]
Starting snmpd: [ OK ]
Starting agent scagt[ OK ]
Starting agent busagt[ OK ]
Starting agent hdagt[ OK ]
Starting agent mylexagt[ OK ]
Starting agent unixagt[ OK ]
Starting agent etheragt[ OK ]
Starting agent biosagt[ OK ]
Starting agent securagt[ OK ]
Starting agent statusagt[ OK ]
Starting agent invagt[ OK ]
Starting agent vvagt[ OK ]

install Alarm Service, please wait...

install ServerView_S2, please wait...

Restarting eeecd and srvmagt, please wait...
```

● Checking execution result

When ServerView Linux Agent and ServerView S2/AlarmService has been successfully installed, the successful completion message below is shown on the last line.

```
ServerView's RPMs are installed successfully.
```

When the message above is not displayed, refer to "A.1 Troubleshooting of Installation Script" (→pg.352).

When the message above is displayed, execute the following command to unmount the CD and eject the PRIMERGY Document & Tool CD, and then perform the steps shown in "2.4.6 [Linux]Setting each Service (for Monitored Server)" (→pg.65).

```
# cd
# umount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder
```

■ Installing ServerView Linux manually

If you have problems with the installation when using the installation script, if you need to upgrade Linux Agent, or if you need to re-install without modifying the snmpd.conf configuration, log in as a superuser and install ServerView Linux manually according to the following procedure.

1 Check the operation environment.

Refer to "1.3 System requirements" (→pg.19), and check that the system meets the requirements to install ServerView Linux Agent and ServerView S2/AlarmService.

2 Check the installation status of the package (RPM).

To check the requirements for ServerView, insert the PRIMERGY Document & Tool CD and execute the following command.

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
Linux/ENGLISH
# ./chkver
```

If the ServerView within the PRIMERGY Document & Tool CD has been installed, the message below is displayed.

```
RPMs check [OK]
```

If an error message indicating insufficient RPM package is displayed, install the package from the Red Hat Linux CD-ROM.

3 If ServerView Linux Agent has been already installed, uninstall the ServerView.

Execute the following command. The uninstall commands are enclosed with parentheses.

```
rpm -q srvmagt-agents (rpm -e srvmagt-agents)
rpm -q srvmagt-eeed (rpm -e srvmagt-eeed)
rpm -q srvmagt-mods_src (rpm -e srvmagt-mods_src)
```

4 Create the backup file of the /etc/snmp/snmpd.conf.

Execute the following command.

```
# ls /etc/snmp/
snmpd.conf
```

Perform the following command only when the "snmpd.conf.org file" or "snmpd.conf.sv" does not exist.

```
# cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.sv
```

5 Copy the /etc/snmp/snmpd.conf from the PRIMERGY Document & Tool CD.

From the CD-ROM, copy the /etc/snmp/snmpd.conf to which the default values have been set. Execute the following command. Any value can be set as the access right except "user" of snmpd.conf.

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
# cp /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
Linux/snmpd.conf /etc/snmp/snmpd.conf
# chmod 644 /etc/snmp/snmpd.conf
```

6 Edit the /etc/snmp/snmpd.conf.

Edit the following items in the /etc/snmp/snmpd.conf.

For details about the snmpd.conf, refer to the comments in the /etc/snmp/snmpd.conf.

table: Setting Items in the /etc/snmp/snmpd.conf File

Item	Settings
com2sec	Add the setting example below into the com2sec item. Setting example: com2sec svSec default public com2sec svSec localhost public com2sec svSec *** public [Note]: Assign one of the following setting values to "****". default: Allows the accesses from all servers/clients. localhost: Allows the access from own server. <IP address>: Allows the access from the specific server/client. <subnet>/<netmask>: Allows the access from specific network.
trapsink	Add the setting example below into the trapsink item. Setting example: trapsink 127.0.0.1 public trapsink <IP address> public Specify the IP address to which you want to send SNMP trap. It is not necessary to enter the server's own IP address (127.0.0.1) again since it has been set already. If you want to send the trap to multiple devices, enter the different IP addresses with the same form in multiple lines.
syslocation	Add the setting example below into the syslocation item. Setting example: syslocation computer room L200 Enter the server location (installation location) . It will be shown in a property of the server at the ServerView as a "Location".
syscontact	Add the setting example below into the syscontact item. Setting example: syscontact Your name Enter the server administrator name. It will be shown in a property of the server at the ServerView as an "Administrator".



- ▶ To reflect the changes of the `/etc/snmp/snmpd.conf`, it is necessary to execute the `"/etc/rc.d/init.d/snmpd restart"` command.

7 Execute the RPM command.

```
# /etc/rc.d/init.d/snmpd restart
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
Linux/Agent/
# rpm -i srvmagt-mods_src-X.XXXX.redhat.rpm
# rpm -i srvmagt-eeed-X.XXXX.redhat.rpm
# rpm -i srvmagt-agents-X.XXXX.redhat.rpm
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
Linux/ENGLISH/Sv/
# ./InstallAlarmService.sh AlarmServiceStarter-X.X-X.i386.rpm
(When updating: # ./InstallAlarmService.sh -upgrade AlarmServiceS-
tarter-X.X-X.i386.rpm)
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
Linux/ENGLISH/Sv/
# ./InstallServerView_S2.sh ServerView_S2Starter-X.X-X.i386.rpm
(When updating: # ./InstallServerView_S2.sh -upgrade
ServerView_S2Starter-X.X-X.i386.rpm)
(XX means version number.)
```

8 Verify the execution result of the RPM command.

To verify whether the installation has been properly done, execute the following command. When the RPM command has been successfully completed, the version number of the installed RPM package is displayed.

```
# rpm -q srvmagt-mods_src <- command
srvmagt-mods_src-X.XX-XX <- execution result

# rpm -q srvmagt-eeed
srvmagt-eeed-X.XX-XX

# rpm -q srvmagt-agents
srvmagt-agents-X.XX-XX

# rpm -q AlarmService
AlarmService-X.X-X

# rpm -q ServerView_S2n
ServerView_S2-X.X-X
(XX indicates version number.)
```

9 Set the default setting of ServerView Linux Agent.

Execute the following command.

```
# groupadd svuser
# cp /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
Linux/config /etc/srvmagt/config
# chmod 644 /etc/srvmagt/config
# cd /
# /etc/rc.d/init.d/srvmagt stop
# /etc/rc.d/init.d/eecd stop
# /etc/rc.d/init.d/eecd start
# /etc/rc.d/init.d/srvmagt start
```

10 Set the setting for after installation.

Execute the following command.

```
# cd
# umount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder
```

Remove the PRIMERGY Document & Tool CD and execute the steps shown in "2.4.6 [Linux]Setting each Service (for Monitored Server)" (→pg.65).

■ Checking RPM version

The version of the installed RPM package can be checked by executing the following command.

```
# rpm -q srvmagt-mods_src <- command
srvmagt-mods_src-X.XX-XX <- execution result

# rpm -q srvmagt-eecd
srvmagt-eecd-X.XX-XX

# rpm -q srvmagt-agents
srvmagt-agents-X.XX-XX

# rpm -q AlarmService
AlarmService-X.X-X

# rpm -q ServerView_S2
ServerView_S2-X.X-X
(XX indicates version number.)
```

2.3.4 [Linux]Installing ServerView Linux (Monitored Server, only ServerView Linux Agent)

Install ServerView Linux (only ServerView Linux Agent) on the Linux monitored server.

There are two ways to install ServerView Linux:

- Installation using the install script (→pg.41)
- Manual installation (→pg.45)

If you have problems with the installation when using the installation script, or if you need to re-install without modifying the snmpd.conf configuration, install ServerView Linux manually.

POINT

- ▶ This document describes the ServerView Linux installation from Document & Tool CD. When you download and install ServerView Linux from our Web page, the specified part of the directory should be changed to the directory to which the files are transmitted and expanded.
- ▶ If ServerView S2/AlarmService is not used, the `httpd`, `openssl`, and `mod_ssl` are not required to install. Even if ServerView S2/AlarmService are not installed, the monitored server (ServerView Linux Agent) can be monitored from the Windows Management Console.

■ Installing ServerView Linux Agent with installation script

Using the installation script within the PRIMERGY Document & Tool CD allows you to install ServerView Linux Agent and edit the SNMP service setting file (`/etc/snmp/snmpd.conf`).

When the installation script terminates with an error message displayed, refer to "A.1 Troubleshooting of Installation Script" (→pg.352).

POINT

- ▶ The `/etc/snmp/snmpd.conf` can also be edited manually after the installation of ServerView. After editing manually, execute the "`/etc/rc.d/init.d/snmpd restart`" command.

IMPORTANT

- ▶ The `snmpd.conf` may also exist under the `/usr/share/snmp` directory. The `snmpd` also loads the settings of the `/usr/share/snmp/snmpd.conf`. Edit the `/usr/share/snmp/snmpd.conf` as necessary.
- ▶ When "SELINUX" is "Enabled" for RHEL-AS4/ES4(x86) or RHEL-AS4/ES4(EM64T), follow the procedures below to set to "Disabled" before installation. Change the following value in "`/etc/selinux/config`" file, and restart the server.
 - (Before edit) SELINUX=enforcing
 - (After edit) SELINUX=disabled

● How to start the installation script

To install with the installation script, log in as superuser and insert the PRIMERGY Document & Tool CD, and then execute the following command.

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
Svmanage/Linux/ENGLISH
# ./BR_inssv
```

● Entering SNMP trap destination IP address

After the title of installation script is displayed, the SNMP trap destination IP address will be asked to enter. If ServerView Linux Agent has been already installed, the SNMP trap destination IP address will be asked to enter after the uninstallation is done.

Enter the IP address to which you want to send SNMP trap and press the [Enter] key.

It is not necessary to enter the server's own IP address (127.0.0.1) since it is automatically set. If you want to send the trap to multiple devices, enter the IP address for each device. The IP address entered is written into the `/etc/snmp/snmpd.conf`.

After you have entered the IP address, press the [e] key. Go to the steps below.

The following is the example of the output result.

```
ServerView install / RPM control script version VX.XLXXifor BXj
Copyright(C) FUJITSU LIMITED 2005

checking necessary RPMs ...
RPMs check [OK]

available disk space check [OK]
(Uninstallation is performed when ServerView Linux has been
installed already)

Please input IP-addresses to where you want to send SNMP-traps.
(Note : No need to input the IP address of this server,
        it will be added automatically by the installer.)

Press "e" key to continue.

>192.168.1.10
>192.168.1.20
>e
```

● Entering the location

Enter the server location (installation location).

The entered location is written to syslocation item in the `/etc/snmp/snmpd.conf` and will be shown in a property of the ServerView as a "Location".

Up to 64 byte sets can be entered.

After the location is entered, press the [Enter] key. Go to the steps below.

When nothing is entered and the [Enter] key is pressed, the default values are written.

```
Please input a location of the server.
The specified location will be shown as a property of the server at
the ServerView console.
You can change the location of the server later,
by editing the /etc/snmp/snmpd.conf.
>(Example: computer room L200)
```

● Entering the administrator

Enter the server administrator name.

The entered administrator name is written to syscontact item in the `/etc/snmp/snmpd.conf` and will be shown in a property of the ServerView as an "Administrator".

Up to 64 byte sets can be entered.

When the administrator name is entered, press the [Enter] key. Go to the steps below.

When nothing is entered and the [Enter] key is pressed, the default values are written.

```
Please input a name of the root user.
The specified name will be shown as a property of the server at the
ServerView console.

You can change the name of the root user later,
by editing the /etc/snmp/snmpd.conf.
>(Example: Your name)
```

● Executing RPM

The RPM of ServerView Linux agent is executed.

The output result of each RPM is displayed.

The example below is the normal output result.

```
install srvmagt-mods_src, please wait...
Compiling modules for 2.4.21-9.0.1.ELsmp
copa(Ok) cop(Ok) ihpci(Ok) ipmi(Ok) smb(Ok) [ OK ]
Loading modules: ipmi smb [ OK ]

job 2 at 2004-05-11 21:39

install srvmagt-eeecd, please wait...
Starting eeecd [ OK ]

install srvmagt-agents, please wait...
Stopping snmpd: [ OK ]
Starting snmpd: [ OK ]
Starting agent scagt [ OK ]
Starting agent busagt [ OK ]
Starting agent hdagt [ OK ]
Starting agent mylexagt [ OK ]
Starting agent unixagt [ OK ]
Starting agent etheragt [ OK ]
Starting agent biosagt [ OK ]
Starting agent securagt [ OK ]
Starting agent statusagt [ OK ]
Starting agent invagt [ OK ]
Starting agent vvagt [ OK ]
```

● Checking execution result

When ServerView Linux Agent has been successfully installed, the successful completion message below is shown in the last line.

```
ServerView's RPMs are installed successfully.
```

When the message above is not displayed, refer to "A.1 Troubleshooting of Installation Script" (→pg.352).

When the message above is displayed, execute the following command to unmount the PRIMERGY Document & Tool CD, and then perform the steps shown in "2.4.7 [Linux]Setting each Service (When installing only ServerView Linux Agent on the monitored server)" (→pg.70).

```
# cd
# umount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder
```

■ Installing ServerView Linux manually

If you have problems with the installation when using the installation script, or if you need to re-install without modifying the `snmpd.conf` configuration, login as a superuser and install ServerView Linux manually according to the following procedure.

1 Check the operation environment.

Refer to "1.3 System requirements" (→pg.19), and check that the system meets the requirements to install ServerView Linux Agent.

2 Check the installation status of the package (RPM).

To check the requirements for ServerView, insert the PRIMERGY Document & Tool CD and execute the following command.

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
Linux/ENGLISH
# ./BR_chkver
```

If the ServerView within the PRIMERGY Document & Tool CD has been installed, the message below is displayed.

```
RPMs check [OK]
```

The error message about insufficient RPM package is displayed, install the package from the Red Hat Linux CD-ROM.

3 If ServerView Linux Agent has been already installed, uninstall the ServerView.

Execute the following command. The uninstall commands are enclosed with parentheses.

```
rpm -q srvmagt-agents (rpm -e srvmagt-agents)
rpm -q srvmagt-eeed (rpm -e srvmagt-eeed)
rpm -q srvmagt-mods_src (rpm -e srvmagt-mods_src)
```

4 Create the backup file of the `/etc/snmp/snmpd.conf`.

Execute the following command.

```
# ls /etc/snmp/
snmpd.conf
```

Perform the following command only when the `snmpd.conf.org` does not exist.

```
# cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.sv
```

5 Copy the `/etc/snmp/snmpd.conf` from the PRIMERGY Documents & Tools CD.

From the CD-ROM, copy the `/etc/snmp/snmpd.conf` to which the default values have been set. Execute the following commands.

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
# cp /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
Linux/snmpd.conf /etc/snmp/snmpd.conf
# chmod 644 /etc/snmp/snmpd.conf
```

6 Edit the /etc/snmp/snmpd.conf.

Edit the following items in the /etc/snmp/snmpd.conf.

For details about the snmpd.conf, refer to the comments in the /etc/snmp/snmpd.conf.

table: snmpd item

Items	Settings
com2sec	<p>Add the setting example below into the com2sec item.</p> <ul style="list-style-type: none"> • com2sec svSec default public • com2sec svSec default public • com2sec svSec *** public <p>Assign one of the following setting values to ***.</p> <ul style="list-style-type: none"> • default: Allows the accesses from all servers/clients. • localhost: Allows the access from own server. • <IP address>: Allows the access from the specific server/client. • <subnet>/<netmask>: Allows the access from specific network.
trapsink	<p>Add the setting example below into the trapsink item.</p> <ul style="list-style-type: none"> • trapsink 127.0.0.1 public • trapsink <IP address> public <p>Specify the IP address to which you want to send SNMP trap. It is not necessary to enter the server's own IP address (127.0.0.1) again since it has been set already. If you want to send the trap to multiple devices, enter the different IP addresses with the same form in multiple lines.</p>
syslocation	<p>Add the setting example below into the syslocation item.</p> <ul style="list-style-type: none"> • syslocation computer room L200 <p>Enter the server location (installation location). It will be shown in a property of the ServerView as a "Location".</p>
syscontact	<p>Add the setting example below into the syscontact item.</p> <ul style="list-style-type: none"> • syscontact Your name <p>Enter the server administrator name. It will be shown in a property of the ServerView as an "Administrator".</p>



- ▶ To reflect the changes of the /etc/snmp/snmpd.conf, you need to execute the "/etc/rc.d/init.d/snmpd restart" command.

7 Execute the RPM command.

```
# /etc/rc.d/init.d/snmpd restart
#cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
Linux/Agent/
# rpm -i srvmagt-mods_src-X.XXXX.redhat.rpm
# rpm -i srvmagt-eeed-X.XXXX.redhat.rpm
# rpm -i srvmagt-agents-X.XXXX.redhat.rpm
(XX indicates version number.)
```

8 Verify the execution result of the RPM command.

To verify whether the installation has been properly done, execute the following command. When the RPM command has been successfully completed, the version number of the installed RPM package is displayed.

```
# rpm -q srvmagt-mods_src <- command
srvmagt-mods_src-X.XX-XX <- execution result

# rpm -q srvmagt-eeed
srvmagt-eeed-X.XX-XX

# rpm -q srvmagt-agents
srvmagt-agents-X.XX-XX
(XX indicates version number.)
```

9 Set the default setting of ServerView Linux Agent.

Execute the following commands.

```
# groupadd svuser
# cp /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
Linux/config /etc/srvmagt/config
# chmod 644 /etc/srvmagt/config
# cd /
# /etc/rc.d/init.d/srvmagt stop
# /etc/rc.d/init.d/eeed stop
# /etc/rc.d/init.d/eeed start
# /etc/rc.d/init.d/srvmagt start
```

10 Set the setting for after installation.

Execute the following commands.

```
# cd
# umount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder
```

Remove the PRIMERGY Document & Tool CD and execute the steps shown in "2.4.7 [Linux]Setting each Service (When installing only ServerView Linux Agent on the monitored server)" (→pg.70).

■ Checking RPM version

The version of the installed RPM package can be checked by executing the following command.

```
# rpm -q srvmagt-mods_src <- command
srvmagt-eeed-X.XX-XX <- execution result

# rpm -q srvmagt-eeed
srvmagt-eeed-X.XX-XX

# rpm -q srvmagt-agents
srvmagt-agents-X.XX-XX
(XX indicates version number.)
```

■ Installing ServerView S2/AlarmService (Linux)

1 Check the operation environment.

Refer to "1.3 System requirements" (→pg.19), and check that the system meets the requirements for installation.



- ▶ Execute the following command to check that atd servis is running before installation.

```
#/etc/rc.d/init.d/atd status
```

2 Check the installation status of the package (RPM).

Execute the following command to check the installation status of the RPM required for ServerView S2/AlarmService to properly operate.

```
# rpm -q net-snmp
# rpm -q compat-libstdc++
# rpm -q httpd
# rpm -q gnom-libs
# rpm -q rpm
# rpm -q gawk
# rpm -q openssl
# rpm -q mod_ssl
```

If RPM has been installed, "RPM name-XX.XX-XX" will be displayed (XX indicates version number).

If RPM has not been installed, install it from Red Hat Linux CD-ROM.

3 Execute the RPM command.

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
Linux/ENGLISH/Sv/
# ./InstallAlarmService.sh AlarmServiceStarter-X.X-X.i386.rpm
(When updating: # ./InstallAlarmService.sh -upgrade AlarmServiceS-
tarter-X.X-X.i386.rpm)
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
Linux/ENGLISH/ServerView_S2/
# ./InstallServerView_S2.sh ServerView_S2Starter-X.X-X.i386.rpm
(When updating: # ./InstallServerView_S2.sh -upgrade
ServerView_S2Starter-X.X-X.i386.rpm)
(XX indicates version number.)
```

4 Verify the execution result of the RPM command.

To verify whether the installation has been properly done, execute the following command. When the RPM command has been successfully completed, the version number of the installed RPM package is displayed.

```
# rpm -q AlarmService <- command
AlarmService-X.X-X <- execution result

# rpm -q ServerView_S2
ServerView_S2-X.X-X
(XX means version number.)
```

5 Edit the httpd service setting file.

Edit the ServerName directive in the /etc/httpd/conf/httpd.conf (Apache HTTP server setting file).

For details about ServerName directive, refer to Red Hat Linux manuals and comments in the httpd.conf.



- ▶ When ServerView S2/Alarm Service is used in Linux, use the Apache attached to the Red Hat CD-ROM as a Web server and use the default settings of DocumentRoot/ServerRoot. When these settings are changed, operations cannot be guaranteed.

When the server's OS is 64 bit RHEL-AS3 (IPF):

Add the following (underlined text) into the http.conf.

Above step is not required when only ServerView Linux Agent has been installed.

```
# "/var/www/cgi-bin" should be changed to whatever your ScriptAliased
# CGI directory exists, if you have that configured.
#
<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>
#
<Directory "/var/www/cgi-bin/ServerView">
    SetEnv LD_ASSUME KERNEL 2.4.19
</Directory>
#
```


When the Apache (httpd) version is 2 or later:

Change the following line (underlined text).

Above step is not required when only ServerView Linux Agent has been installed.

```
Before change: LanguagePriority en da nl et fr de el it ja kr no pl pt
pt-br ltz ca es sv tw
After change: LanguagePriority ja en da nl et fr de el it kr no pl pt
pt-br ltz ca es sv tw

Before change: AddDefaultCharset ISO-8859-1 or AddDefaultCharset UTF-8
After change: AddDefaultCharset off
```

6 Restart the httpd service.

Enter the following command and restart the httpd service.

```
# /etc/rc.d/init.d/httpd restart
```

7 Set the auto start of the httpd service.

Use the setup command to set the auto start of the httpd service.

For details about the setup command, refer to "■ Auto-start setting of SNMP service/httpd service" (→pg.66).

8 Set the firewall.

Refer to "■ Setting the firewall" (→pg.67).

2.4 Checking after Installation

After the installation of ServerView, perform the following settings to ensure that ServerView properly operates.

The settings vary depending on the OS.

- For Windows:
 - Installing Microsoft Internet Explorer (→pg.58)
 - Installing Java™ 2 Runtime Environment Standard Edition (→pg.59)
 - Setting an administrative user (→pg.60)
 - Registering the interrupt information of the optional devices (→pg.62)
 - Extending Web service (when IIS is selected for the Web server on Windows 2003) (→pg.64)
- For Linux:
 - Installing Mozilla 1.3 or later, or Mozilla FireFox 1.0.4 or later (→pg.58)
 - Installing Java™ 2 Runtime Environment Standard Edition (→pg.59)
 - Registering the interrupt information of the optional devices (→pg.64)
 - Setting each service (for the monitored server) (→pg.65)
 - Setting each service (when installing only ServerView Linux Agent on the monitored server) (→pg.70)

POINT

- ▶ Refer to "2.4.8 Changing Computer Information after Installation" (→pg.73) and set the settings when the computer name or IP address of the server has been changed after the installation.

POINT

- ▶ Microsoft Virtual Machine is not supported in ServerView V3.40 or later.

2.4.1 Installing a Web Browser

Install a Web browser on the server or PC to use ServerView.

■ When the OS on the server or PC is Windows:

Install Microsoft Internet Explorer 6.0 or later on the server and PC shown below.

- Server and PC on which ServerView Console is installed
- Server and PC that show the server monitoring window of ServerView S2
- Server and PC that show the RSB Web interface window

To use ServerView with Windows OS, follow the steps below to perform further settings of the Web site after the installation of the Microsoft Internet Explorer.

- 1 Launch the Microsoft Internet Explorer.
- 2 Select [Internet Options] from the [Tools] menu.
- 3 Click the [Security] tab and select [Intranet] or [Trusted sites].
- 4 Click [Sites] to add the following URL (http:// server IP address) respectively.

When ServerView Console is installed on the server:

- Server's own URL
- The URL of the server on which ServerView S2 (Windows/Linux) is installed

When the server shows the server monitoring window of ServerView S2:

- The URL of the server on which ServerView S2 (Windows/Linux) is installed

When the server shows the RSB Web interface window:

- URL set to RSB

■ When the OS on the Server or PC is Linux:

Install Mozilla 1.3 or later, or Mozilla FireFox 1.0.4 or later, on the server and PC shown below.

- Server on which ServerView Linux is installed
- Server and PC that show the server monitoring window of ServerView S2
- Server and PC that show the RSB Web interface window

2.4.2 Installing Java™ 2 Runtime Environment Standard Edition

Install Java™ 2 Runtime Environment Standard Edition on the server or PC to use ServerView.

The installer of Java™ 2 Runtime Environment Standard Edition has been stored on the PRIMERGY Document & Tool CD. However, the stored Java version may not be compatible with the Web browser depending on the browser version. The following setting method of the plugin for Linux browser (Mozilla) is provided as an example, however, the setting content (Java Plugin directory path) varies depending on the browser version. Please check the adaptive conditions of your browser in advance.

● For Windows

- Server and PC on which ServerView Console is installed
- Server and PC that use Web browser to show the server monitoring window of ServerView S2
- Server and PC that show the RSB Web interface window

● For Linux

- Server on which ServerView Linux is installed
- Server and PC that use Web browser to show the server monitoring window of ServerView S2
- Server and PC that show the RSB Web interface window

■ Installation steps

1 Insert the PRIMERGY Document & Tool CD and start the installer below.

For Windows

[CD-ROM drive]:\SVMANAGE\TOOLS\j2re-x_x_x_xx-windows-i586-p.exe

For Linux

POINT

- ▶ The examples of folder name in "Your browser's folder" are shown below.
 - For Mozilla: /usr/lib/mozilla-x.x.x
 - For firefox: /usr/lib/firefox-x.x.x

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/Linux/
TOOLS
# rpm -iv j2re-x_x_x_xx-linux-i586.rpm
# cd /your browser's folder/plugins
# ls

when the libjavaplugin_oji.so file already exists
# rm -fr /your browser's folder /plugins/libjavaplugin_oji.so
# ln -s /usr/java/j2relx.x.x_xx/plugin/i386/ns610-gcc32/
libjavaplugin_oji.so

# cd
# umount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder
(x.x means version number.)
```

IMPORTANT

- ▶ The java cannot be plugged in to firefox nor mozilla because the java (jre) plug-in for EM64T is not provided.
Use another PC browser to display the ServerView S2 screen or the alarm setting screen of AlarmService.
- ▶ When using Java(TM) 2 Runtime Enviroment Standard Edition V1.4.2_08 on RHEL-AS4(x86)/RHEL-ES4(x86), the displayed characters may be garbled on the ServerView S2 screen or the alarm setting screen of AlarmService.
Copy a file according to the following procedures.

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
# cp /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
Linux/TOOLS/font.properties.ja_JP /usr/java/j2rel.4.2_08/lib
# umount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder
```

2.4.3 Setting an Administrative User

Only the users belonging to a group (FUJITSU SVUSER) that has administrator privileges for ServerView can perform the operation such as changing the monitored server setting and shutting down the server. FUJITSU SVUSER group and the users who belong to it are not created automatically. Create the FUJITSU SVUSER group for each monitored server and add ServerView administrators to the group.

POINT

- ▶ An administrator user in ServerView means the user who belongs to the "FUJITSU SVUSER" group.
- ▶ In Windows 2003, the administrative privilege is not given when the password is not set for the administrative user account. Be sure to set the password.
- ▶ Even when "global" group is added to the FUJITSU SVUSER group, the administrative privilege is not given to the user who belongs to the group added. Add only users to the FUJITSU SVUSER group.
- ▶ When the Remote Service Board is mounted on the server, the user account that has the same user name and password as those registered to the "FUJITSU SVUSER" group on the server system must be created on the Remote Service Board. For details about creating user account for the Remote Service Board, refer to "5.3.7 [User Config] Page" (→pg.340).
- ▶ When the administrative user is set for the groups other than SVUSER, the logon immediately after starting the program may be failed. In this case, click [Cancel] to exit the logon window. Then, set the logon settings again in the [Login] tab of the [Properties] on the server.
- ▶ The ServerView administrative user must belong to the Administrators group.
If the administrative user does not belong to the Administrators group, the user cannot perform Shutdown or ASR setting from ServerView.
Therefore, add the ServerView administrative user to the Administrators group.

■ For Windows

- 1 Open the Control Panel and double-click the [Administrative Tools] icon.
- 2 Double-click the [Computer Management] icon.
The [Computer Management] window appears.
- 3 Select [Local Users and Groups] → [Groups] from the left tree view.
- 4 Click the [Action] menu → [New Group...] in this order.
- 5 Enter [FUJITSU SVUSER] in [Group name] and click [Create].
A new group is created.
Click [Close] to close the [New Group] window.
- 6 Select [Local Users and Groups] → [Users] from the left tree view.
- 7 Click the [Action] menu → [New User...] in this order.
- 8 Set the necessary items and click [Create].
A new group is created.
Click [Close] to close the [New User] window.
- 9 Select the added user and click the [Action] menu → [Properties] in this order.
- 10 Click the [Member of] tab and click [Add].
The [Select Groups] window appears.
- 11 Click [Properties].

- 12 Click [Search Now].
- 13 Select server's "Administrators" and "FUJITSU SVUSER", and click [OK].
Hold down the [Ctrl] key for multiple selections.
The [Select Groups] window appears again.
- 14 Click [OK] to return to the [Properties] window of the user.
Confirm that "Administrators" and "FUJITSU SVUSER" are added to [Member of], and click [OK].
- 15 Click [OK].
Close the [Computer Management] window.

■ For Linux

Refer to "■ Setting to set, shut down, and restart ASR from ServerView Console" (→pg.69) or "■ Setting to set, shut down, and restart ASR from ServerView Console" (→pg.72).

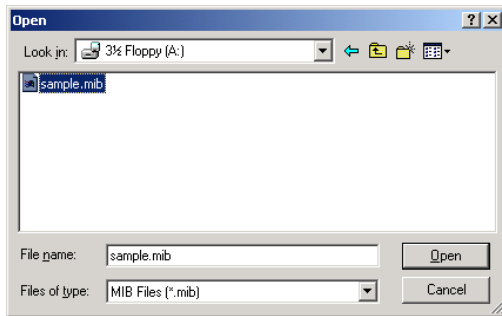
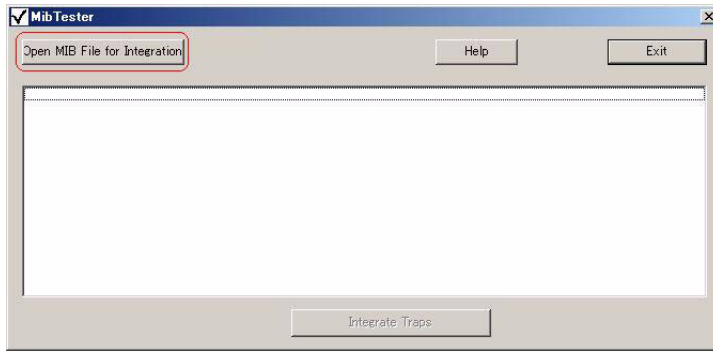
2.4.4 Registering the Interrupt Information (MIB) of the Optional Devices

Register the interrupt information (MIB) of the optional devices on the management server or PC.

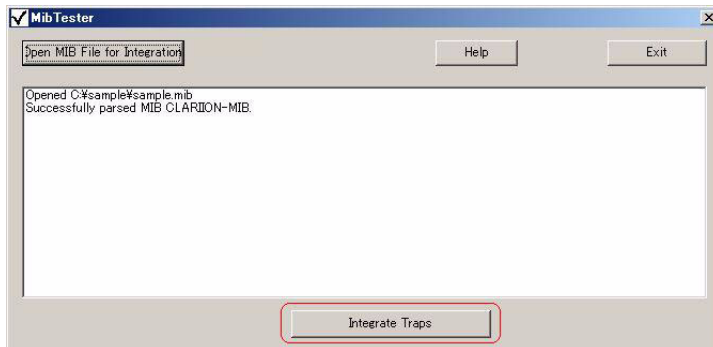
■ For Windows

- 1 Click [Start] → [Programs] → [Fujitsu ServerView] → [MIB Integrator].
The process of interrupt information registration starts, and the [Mib Tester] window will open.

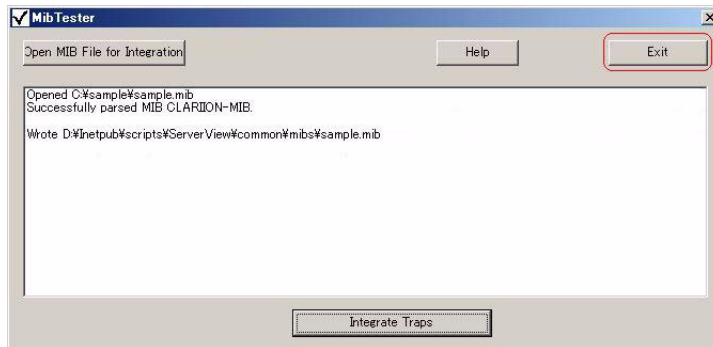
- 2 Click [Open MIB File for Integration] and select the MIB file to register.



- 3 Make sure that the file selected in Step 2 is highlighted and click [Integrate Traps] to process the registration.



- 4 Make sure that the following message is displayed, and click [Exit] to finish the registration.



- 5 Restart Fujitsu ServerView Services.
1. Click [Start] → [Control Panel] → [Administrative Tools] → [Computer Management].
 2. Click [Services] and select [Fujitsu ServerView Services] from the list displayed.
 3. Click [Action] menu → [Restart].

■ For Linux

- 1 Copy the appropriate mib file into the following folder.
/var/www/cgi-bin/ServerView/SnmpTrap/mibs
- 2 Enter the following command and restart the Fujitsu Alarm Service.
#/etc/rc.d/init.d/sv_fwdservice restart

IMPORTANT

- ▶ When replacing the existing mib file registered, pay attention to the difference between upper and lower case of the mib file name. If the file is improperly registered, it would be registered as a new mib file.

■ When using Server View S2

Refer to "3.1.5 Registering MIB (MIB INTEGRATION)" (→pg.87).

IMPORTANT

- ▶ For ServerView S2 running under Linux, MIB registration is not supported.

2.4.5 Extending the Web Service

If ServerView Console has been installed on Windows 2003 and IIS has been selected for the Web server, allow [ALL Unknown CGI Extensions] or perform [Add new Web Service Extensions]. The following steps describe each procedure.

■ Allowing all unknown CGI extensions

- 1 In IIS Manager, expand the local computer and click the [Web Service Extension].
- 2 In the details pane, select the disabled [All Unknown CGI Extensions] and click [Allow].
- 3 Click [OK].

■ Adding new Web service extensions

- 1 In IIS Manager, expand the local computer and click the [Web Service Extension].
- 2 In the details pane, click [Add new Web Service Extensions].
- 3 Type the name of the new Web service extension in the [Extension name] box.
Example: "ServerView"
- 4 Click [Add].
- 5 Type the path into the [Path to file] box or click [Browse] to navigate to any files that the new Web service extension requires, and click [OK].
Add all exe files under the following folders.

```
\Inetpub\scripts\ServerView\SnmpTrap
\Inetpub\scripts\ServerView\SnmpArchive
\Inetpub\scripts\ServerView\common
\Inetpub\scripts\ServerView\SnmpView
```
- 6 After having finished adding all files, click [OK].
- 7 Return to the [Web Service Extension] window and right click on the extension name added in the Step 3 above, and then click [Allow].

2.4.6 [Linux]Setting each Service (for Monitored Server)

■ Editing the httpd service setting file

- 1 Edit the `/etc/httpd/conf/httpd.conf`.
Edit the `ServerName` directive in the `/etc/httpd/conf/httpd.conf` (Apache HTTP server setting file).
For details about `ServerName` directive, refer to Red Hat Linux manuals and comments in the `httpd.conf`.



- ▶ When ServerView S2/Alarm Service is used in Linux, use the Apache attached to the Red Hat CD-ROM as a Web server and use the default settings of DocumentRoot/ServerRoot. When these settings are changed, the operational warranty will not be applied.

When the server's OS is 64 bit RHEL-AS3 (IPF):

Add the following (underlined text) into the http.conf.

Above step is not required when only ServerView Linux Agent has been installed.

```
# "/var/www/cgi-bin" should be changed to whatever your ScriptAliased
# CGI directory exists, if you have that configured.
#
<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>
#
<Directory "/var/www/cgi-bin/ServerView">
    SetEnv LD_ASSUME_KERNEL 2.4.19
</Directory>
#
```

When the Apache (httpd) version is 2 or later:

Change the following line (underlined text).

Above step is not required when only ServerView Linux Agent has been installed.

```
Before change: LanguagePriority en da nl et fr de el it ja kr no pl pt
pt-br ltz ca es sv tw
After change: LanguagePriority ja en da nl et fr de el it kr no pl pt
pt-br ltz ca es sv tw

Before change: AddDefaultCharset ISO-8859-1 or AddDefaultCharset UTF-8
After change: AddDefaultCharset off
```

2 Restart the httpd service.

Enter the following command and restart the httpd service.

```
# /etc/rc.d/init.d/httpd restart
```

■ Auto-start setting of SNMP service/httpd service

Execute the following commands to set auto-start of the services.

```
# /sbin/chkconfig httpd on
# /sbin/chkconfig snmpd on
```

When the setting is correct, the following messages are displayed.

```
#/sbin/chkconfig --list |grep httpd
httpd          0:off 1:off 2:on 3:on 4:on 5:on 6:off
#/sbin/chkconfig --list |grep snmpd
snmpd         0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

■ Setting the firewall

POINT

- ▶ To use a firewall, you need to setup a firewall. If a firewall is not used, the following settings are not required.

Setting the firewall is done when installing Linux or by using the setup command.

This section describes the setting with setup command.

The windows differ between the Linux installation and the setup command execution; however, the setting items are the same. For details about how to set up during the Linux installation, refer to the Red Hat Linux manuals and the following set up method.

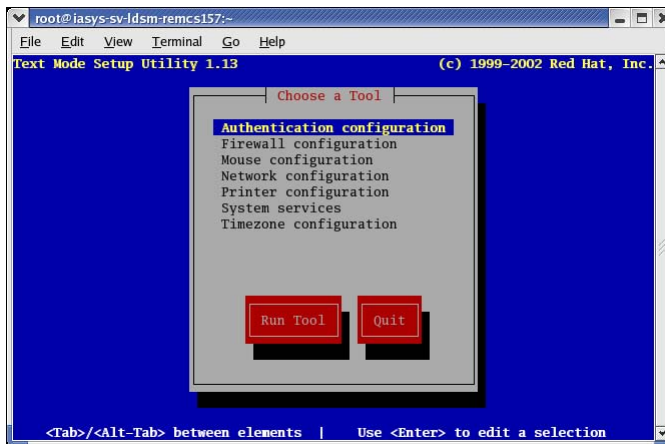
IMPORTANT

- ▶ The firewall setting below is required for ServerView to operate.
For details about the firewall setting, refer to Red Hat Linux manuals.

1 Log in as a superuser and execute the following command.

```
# usr/sbin/setup
```

The menu window appears.



- 2 Select [Firewall configuration] and press the [Enter] key. The [Firewall Configuration] window appears.

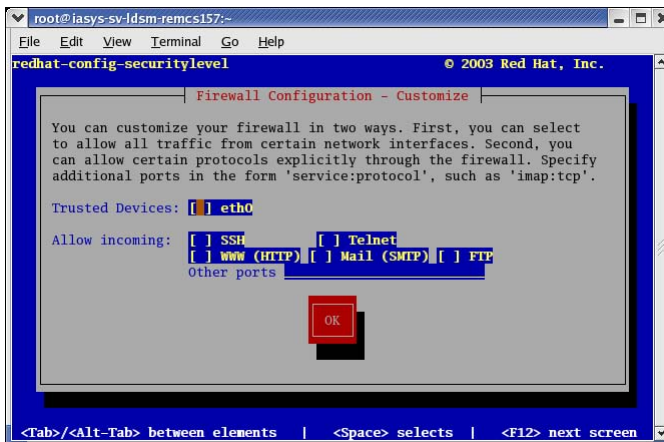


- 3 Add "*" mark to the [Enabled] and use the [Tab] key to position the cursor on the [Customize], and then press the [Enter] key. The [Firewall Configuration – Customize] window appears.



- ▶ When [Disabled] is selected here, the settings below are not required.

- 4 Set the protocols to use.



Set the protocols below.

1. Select "WWW (HTTP)".
Add [*] mark.
2. Enter "snmp:udp https:tcp" into [Other ports].



Protocol Setting

- ▶ "http" and "https" are required to start WebServer.
- ▶ "snmp" is required to start snmp service.

- Use the [Tab] key to position the cursor on the [OK] and press the [Enter] key.

POINT

- To enable other functions, it may be required to set this firewall.

- Use the [Tab] key to position the cursor on the [OK] and press the [Enter] key.
- Select [Stop] and press the [Enter] key.
- Edit the packet filtering setting.

Edit the /etc/sysconfig/iptables.

Add the four lines below.

```
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport
161 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --sport
161 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport
162 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --sport
162 -j ACCEPT
```

- Reflect the packet filtering setting.

Execute the following commands.

```
# /etc/rc.d/init.d/iptables restart
```

■ Setting to set, shut down, and restart ASR from ServerView Console

To perform the ASR (Automatic Server Reconfiguration & Restart) settings, including fan/temperature/restart, or turn the power on/off, the user will be asked to type the user name and the password of the administrative user.

Follow the steps below to set the administrative user.

IMPORTANT

- An administrator user in ServerView means the user who belongs to the "svuser" group. The "svuser" group is automatically created when ServerView is installed with installation script.

- Create a new user as an administrative user.

Log in as a superuser and execute the following command.

```
# useradd -G svuser <user name>
# passwd <user name>
```

- Specify the "svuser" group to the G option of the useradd command. For <user name>, specify the user name of the user to be created.
- Use the passwd command to set the password for the user created. The password must be entered twice for verification. The user name created is enabled when the password is set.
- For details about each command, refer to the useradd (8) and passwd (1) man page.

2 Set the existing user as an administrative user.

Contact with the system administrator to verify whether the existing user to be set belongs to multiple groups and execute the following command.

When the user belongs to only the main group:

```
# usermod -G svuser <user name>
```

When the user belongs to multiple groups:

```
# usermod -G svuser,<affiliation group> <user name>
```

- Specify the "svuser" group to the G option of the usermod command. To specify multiple groups, specify the groups with the comma (,) separator. If the group to which the user previously belonged is not specified, the user is deleted from the group. Specify all groups to which user must belong. For <user name>, specify the user name to be an administrative user. For details about usermod command, refer to the usermod (8) man page.
- You can also directly set the groups by using vigr command or set the groups by using GUI tools. For details, refer to vigr (8) man page or Red Hat Linux manuals.

2.4.7 [Linux]Setting each Service (When installing only ServerView Linux Agent on the monitored server)

■ Auto-start setting of SNMP service

Execute the following commands to set auto-start of the service.

```
# /sbin/chkconfig snmpd on
```

When the setting is correct, the following messages are displayed.

```
#!/sbin/chkconfig --list |grep snmpd
snmpd          0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

■ Setting the firewall

POINT

- ▶ To use a firewall, you need to setup a firewall. If a firewall is not used, the following settings are not required.

Setting the firewall is done when installing Linux or by using the setup command.

This section describes about the setting with setup command.

The windows differ between the Linux installation and the setup command execution; however, the setting items are the same. For details about how to set up during the Linux installation, refer to the Red Hat Linux manuals and the following set up method.

The window for the setup command varies depending on the Red Hat distribution, however, the setting items are the same.

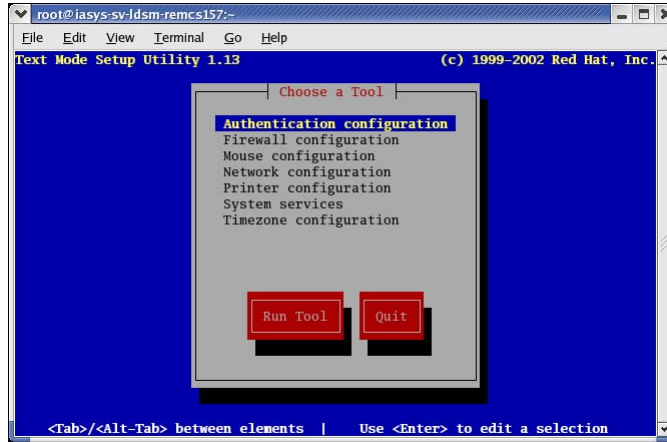


- ▶ The firewall setting below is required for ServerView to operate. For details about the firewall setting, refer to Red Hat Linux manuals.

1 Log in as a superuser and execute the following command.

```
# /usr/sbin/setup
```

The menu window appears.



2 Select [Firewall configuration] and press the [Enter] key.

The [Firewall Configuration] window appears.



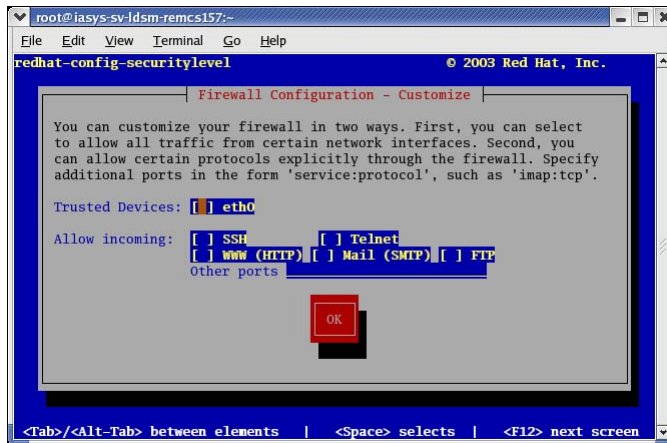
3 Add "*" mark to the [Enabled] and use the [Tab] key to position the cursor on the [Customize], and then press the [Enter] key.

The [Firewall Configuration – Customize] window appears.



- ▶ When [Disabled] is selected here, the settings below are not required.

4 Set the protocols to use.



Set the protocols below.

1. Select "WWW (HTTP)".
Add [*] mark.
2. Enter "snmp:udp https:tcp" into [Other ports].

POINT

Protocol Setting

- ▶ "http" and "https" are required to start WebServer.
- ▶ "snmp" is required to start snmp service.

3. Use the [Tab] key to position the cursor on the [OK] and press the [Enter] key.

POINT

- ▶ To enable other functions, it may be required to set this firewall.

- 5 Use the [Tab] key to position the cursor on the [OK] and press the [Enter] key.

- 6 Select [Stop] and press the [Enter] key.

■ Setting to set, shut down, and restart ASR from ServerView Console

To perform the ASR (Automatic Server Reconfiguration & Restart) settings, including fan/temperature/restart, or turn the power on/off, the user will be asked to type the user name and the password of the administrative user.

Follow the steps below to set the administrative user.

POINT

- ▶ An administrator user in ServerView means the user who belongs to the "svuser" group.
The "svuser" group is automatically created when ServerView is installed with installation script.

1 Create a new user as an administrative user.

Log in as a superuser and execute the following command.

```
# useradd -G svuser <user name>
# passwd <user name>
```

- Specify the "svuser" group to the G option of the useradd command. For <user name>, specify the user name of the user to be created.
- Use the passwd command to set the password for the user created. The password must be entered twice for verification. The user name created is enabled when the password is set.
- For details about each command, refer to the useradd (8) and passwd (1) man page.

2 Set the existing user as an administrative user.

Contact with the system administrator to verify whether the existing user to be set belongs to multiple groups and execute the following command.

When the user belongs to only the main group:

```
# usermod -G svuser <user name>
```

When the user belongs to multiple groups:

```
# usermod -G svuser,<affiliation group> <user name>
```

- Specify the "svuser" group to the G option of the usermod command. To specify multiple groups, specify the groups with the comma (,) separator. If the group to which the user previously belonged is not specified, the user is deleted from the group. Specify all groups to which user must belong. For <user name>, specify the user name to be an administrative user. For details about usermod command, refer to the usermod (8) man page.
- Groups can also be directly set by using vigr command or set the groups by using GUI tools. For details, refer to vigr (8) man page or Red Hat Linux manuals.

2.4.8 Changing Computer Information after Installation

When the name or IP address of the computer that has been installed is changed after the ServerView installation, perform the steps below.

- 1** If ServerView and AlarmService are currently started, exit all applications.
- 2** Click [Start] → [Programs] → [Fujitsu ServerView] → [Change Computer Details].
- 3** Set new computer information.
- 4** Restart the Console.

5 Start ServerView and check the computer name and IP address in the [Server List].

If the name or IP address has not been changed, perform the following settings:

When the IP address has not been changed:

1. Select the target computer from the Server List.
2. Click the [File] menu → [Server Properties].
3. Click the [Server Address] tab and type the IP address changed.
4. Click [OK].

When the computer name has not been changed:

1. Select the target computer from the Server List.
2. Click the [File] menu → [Remove] to remove the server.
3. Click the [File] menu → [New Server] to register the target computer again.

For details about the computer registration, refer to "3.9.2 Adding the Monitored Server (Object)" (→pg.206).

Chapter 3

How to Use ServerView

This chapter explains how to use the ServerView functions.

3

3.1	Starting and Exiting ServerView S2	76
3.2	Monitoring Servers	88
3.3	Monitoring Blade Servers	119
3.4	Serious Error Handling (ASR)	123
3.5	AlarmService	131
3.6	Performance Manager	171
3.7	Management of Archive Data	183
3.8	Export Manager	192
3.9	ServerView Operation Using the Management Console	202
3.10	Settings for ServerView Agent	237
3.11	[Linux] How to Use ServerView Linux	241

3.1 Starting and Exiting ServerView S2

Using ServerView S2, you can monitor the server and configure the settings through your Web browser.

POINT

When using the Management Console

- ▶ You can also start and operate ServerView on the server or PC where the Management Console is installed. See "3.9 ServerView Operation Using the Management Console" (→pg.202).

3.1.1 Starting ServerView S2

- 1 Start the Web browser.

IMPORTANT

- ▶ If you use Windows 2003 Internet Explorer as your Web browser, perform the following procedure after starting the browser to add a Web site.
 1. Select [Internet Options...] from the [Tools] menu.
 2. Click the [Security] tab and select [Local intranet] or [Trusted sites].
 3. Click [Sites...] to add the URL of the server where ServerView S2 was installed.
- ▶ If you use Mozilla or Netscape as your Web browser, perform the following procedure after starting the browser to release the pop-up window blocking.
 1. Select [Preferences] from the [Edit] menu.
 2. Select [Pop-up Window] under [Privacy & Security] from the category list.
 3. Uncheck [Block unrequested pop-up windows].

- 2 Enter one of the following URLs and press the [Enter] key.

When using IIS or Linux

`http://<server name or server IP address>/ServerView/`

`http://<server name or server IP address>/sv_www.html`

When using ServerView Web-Server (normal connection)

`http://<server name or server IP address>:3169/ServerView/`

`http://<server name or server IP address>:3169/sv_www.html`

When using ServerView Web-Server (SSL connection)

https://<server name or server IP address>:3170/ServerView/
https://<server name or server IP address>:3170/sv_www.html

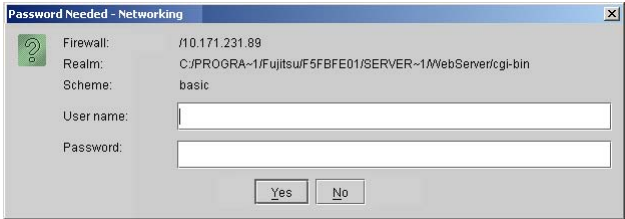
The window of ServerView S2 appears.



POINT

When the user name and password are requested

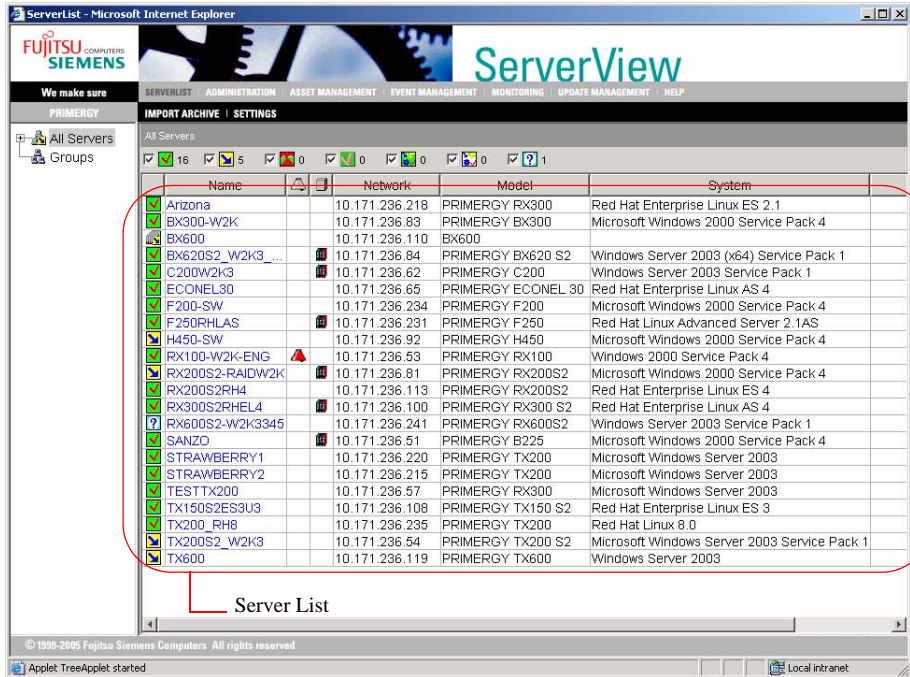
- ▶ When the ServerView Web-Server is selected and Web connection is made using SSL, the following authentication window may be displayed:



The default user name is "svuser" and the password "fsc". Delete this user and add an appropriate user for your security. For the procedure to add users, refer to "● ServerView Web-Server and SSL" (→pg.373).

3 Click [Start].

The [Server List] window appears and all registered servers are displayed in the list.



IMPORTANT

- ▶ When checking monitored servers under Linux using Windows 2000/2003 Internet Explorer as your Web browser, the [Server List] window may not be properly displayed. In this case, perform the following procedure.
 1. Check the httpd service configuration file of the monitored Linux server.
For details, refer to step 5 in "■ Installing ServerView S2/AlarmService (Linux)" (→pg.55).
 2. Select [Internet Options...] from the [Tools] menu of the Web browser (Windows 2000/2003 Internet Explorer).
 3. Click [Delete Files...] under [Temporary Internet files] on the [General] tab.
 4. In the [Delete Files] window, check [Delete all offline content] and click [OK].
 5. Click [OK] in the [Internet Options] window, close the Web browser and restart the server.

3.1.2 ServerView S2 Menus (Command List)

In ServerView S2, commands are executed from the menu bar at the top of the window. For each menu, a submenu is displayed when you point at it with the cursor.

table: ServerView S2 Commands

Menu item	Description
SERVERLIST	
IMPORT ARCHIVE	Imports archive data from other management servers. →"3.7.6 Importing Archive Data" (pg.191)
SETTINGS	Sets the interval for updating the server list. →"■ Setting the Update Interval for the Server List" (pg.91)
ADMINISTRATION	
SERVERBROWSER	Adds servers to be monitored to the server list. →"3.1.3 Registering the Monitored Servers" (pg.81)
MIB INTEGRATION	Adds MIB files. →"3.1.5 Registering MIB (MIB INTEGRATION)" (pg.87)
ASSET MANAGEMENT	
ARCHIVE MANAGER	Retrieves and manages archive data. "3.7.1 Starting the Archive Manager" (→pg.183)
EXPORT MANAGER	Retrieves export data on the servers and saves them on the file. →"3.8 Export Manager" (pg.192)
EVENT MANAGEMENT	
ALARM MONITOR	Displays received alarms. →"3.5.1 Alarm Monitor" (pg.132).
ALARM MANAGER	Manages received alarms. →"3.5.2 Alarm Manager" (pg.139).
ALARM SETTINGS	Configures alarm settings. →"3.5.3 Alarm Settings" (pg.142).
MONITORING	
PERFORMANCE MANAGER	Configures, monitors, and displays threshold values and/or reports. →"3.6 Performance Manager" (pg.171)
HELP	
ABOUT	Displays ServerView S2 version information.
CONTENTS	Displays the help contents.
ON VIEW	Displays the help page for the current screen.

■ Right-click Menu

When the server list view is right-clicked, a menu with the following items appears. The displayed items depend on the location (object) of the right click.

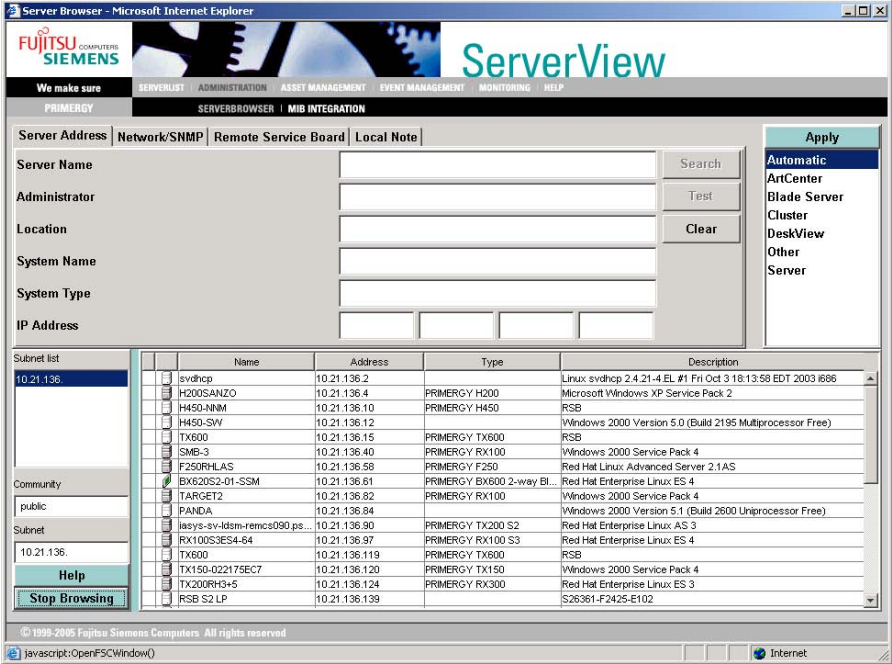
table: Right-click Menu

Menu Item	Description
New Server	Opens the [ServerBrowser] window where you can add servers to monitor. →"3.1.3 Registering the Monitored Servers" (pg.81)
New Group	Creates a new group. A new group will be created under the selected group. You cannot create a group under [all server].
Move to group..	Moves the selected group to another group.
Copy to group..	Registers the selected server in a group.
Rename	Renames the group.
Remove	Deletes the selected server or group.
Server Properties	Displays the property window where you can verify or change the server information. →"3.1.4 Verifying/Changing the Server Settings" (pg.84)
ASR Properties	Displays the ASR window where you can configure responses to failures. →"3.4 Serious Error Handling (ASR)" (pg.123)
Test Connection	Tests the connection to the server. →"■ Verification of Server Connections" (pg.89)
Redetect servers	Redetects the server status. →"■ Redetect Server/Redetect All Servers" (pg.91)
Redetect All Servers	Redetects the status of all servers. →"■ Redetect Server/Redetect All Servers" (pg.91)
Refresh From DB	Refreshes the database.
Accept Alarms	Acknowledges alarms that have not been acknowledged.
Accept All Alarms	Acknowledges alarms that have not been acknowledged from all servers.
Delete Archives	Deletes retrieved archive data. (Displayed only when the archive data exists.)
Obtain Archives Now	Retrieves the archive data for the selected server.

3.1.3 Registering the Monitored Servers

The servers to be monitored on the network need to be registered in the server list in order for ServerView S2 to monitor them. Register servers using the following procedure:

- 1 Click the [ADMINISTRATION] menu → [SERVERBROWSER]. Or, right-click the server list and click [New Server] on the displayed menu. The [SERVER BROWSER] window appears, where the nodes on the network are listed.



3 How to Use ServerView

- 2 Enter the IP address for the server to be registered in the [IP Address] field, and click [Search]. Information for the server, such as the DNS name, is automatically collected and displayed in the other fields. If not displayed, confirm the network configuration for the target server.

POINT

- ▶ Clicking [Test] starts a test of the connection to the server. Clicking [Clear] deletes all the input values.

3 Select a server type from the Server type list.

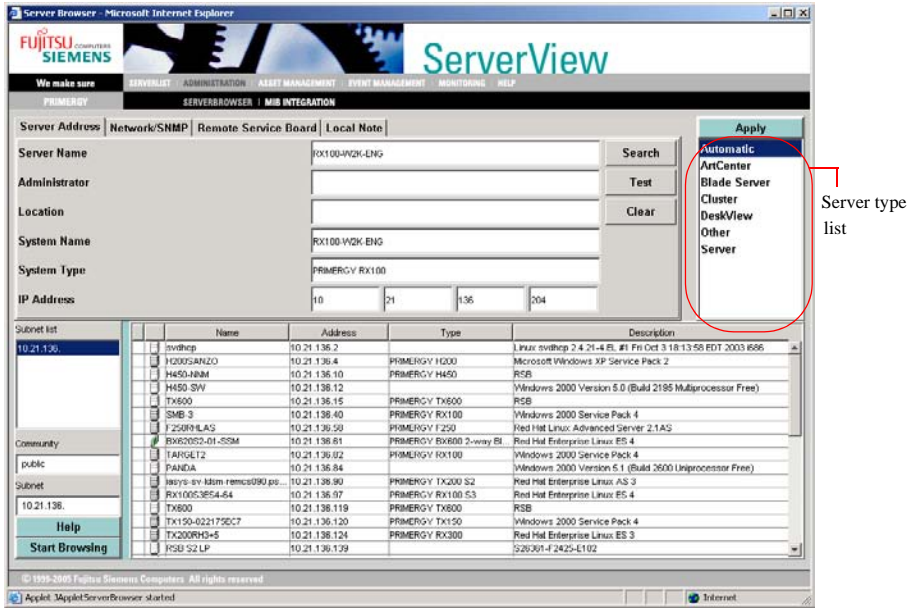
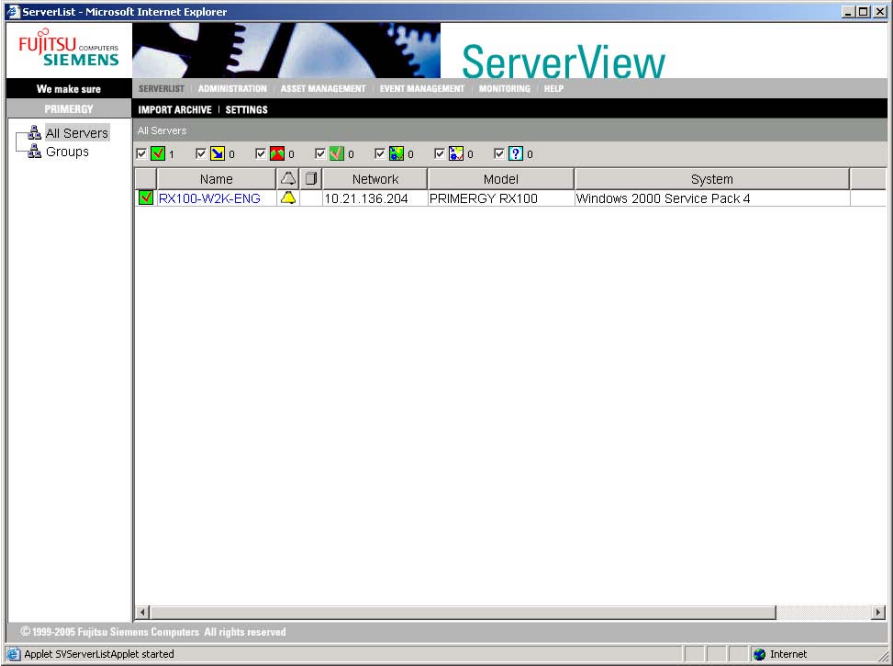


table: Server Types

Type Name	Description
Automatic	Auto-detects the type of the server to be added.
ArtCenter	Not supported.
Blade Server	Adds a blade server.
Cluster	For adding a cluster system, but not supported.
DeskView	For adding a desktop, but not supported.
Other	Select this to add a TCP/IP object other than a server.
Server	Adds a server to be monitored by ServerView Agent.

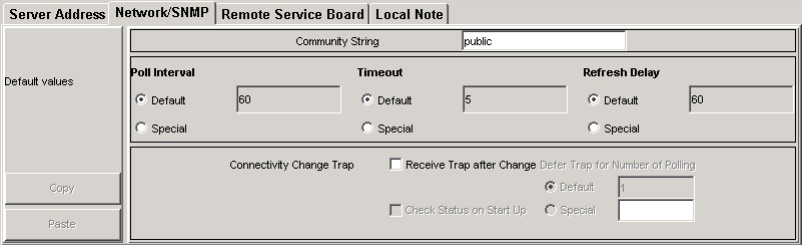
4 Click [Apply].

The server(s) is (are) registered in the server list.

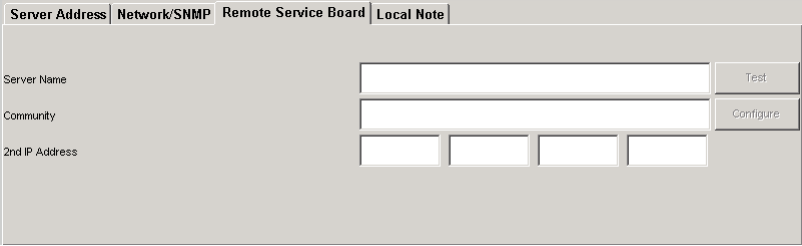


POINT

- ▶ Confirm the settings in each tab window and reconfigure them if necessary.
 - [Network/SNMP] Tab
In the [Network/SNMP] tab, the default values are displayed for [Community String], [Poll Interval], [Timeout], [Refresh Delay] and [Connectivity Change Trap].



- [Remote Service Board] Tab
Displays information about the Remote Service Board installed in the server. Clicking [Test] starts a test of the connection to the Remote Service Board. Clicking [Configure] displays the Web interface for the Remote Service Board.



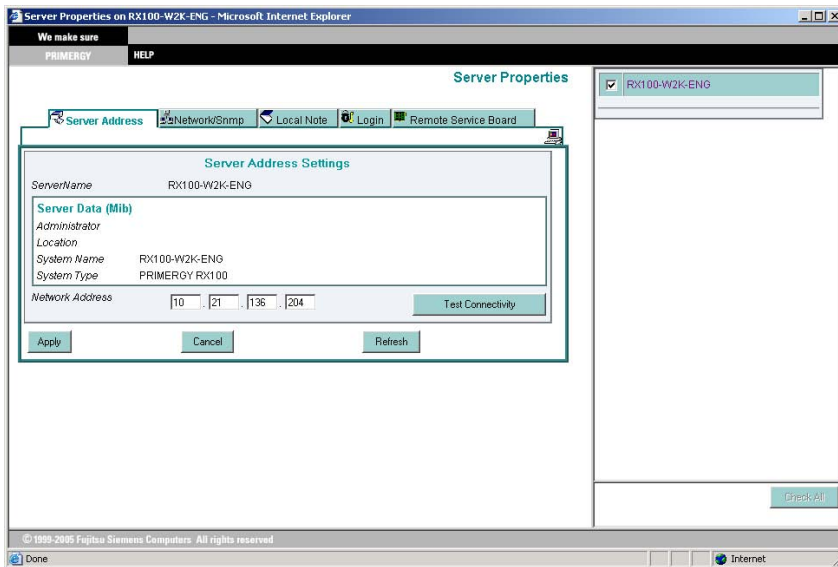
- [Local Note] Tab
Displays the server's local note.
 - ▶ If you select multiple servers from the server list on the ServerView S2 window, [Multiple Selection] will appear in the [Server Name] field. Click [Apply] in this state to register all selected servers on the server list.
You can also select a server by right-clicking it in the server list.
 - Clicking [Select All] selects all servers.
 - Clicking [Select Manageables] selects only manageable servers. Manageable servers are indicated with gray icons.
- You cannot add a server with the same name or network address as an already registered server.

3.1.4 Verifying/Changing the Server Settings

To verify/change the settings for a server, perform the following procedure:

- 1 Select a target server from the server list and click [Server Properties] from the right-click menu.

The [Server Properties] window appears.



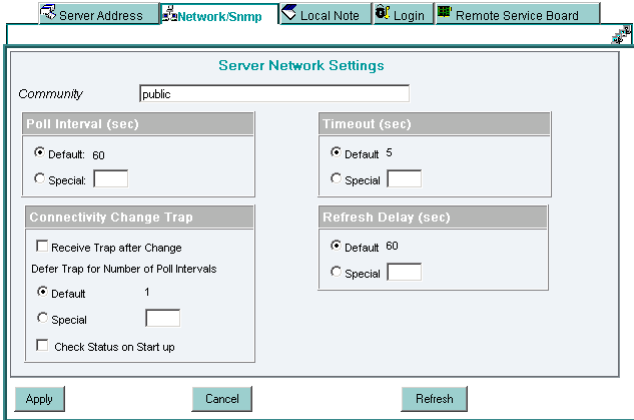
- 2 Verify/change the settings in each tab window.

If you change the settings, make sure to click [Apply] in each tab window before clicking another tab window.

[Server Address] Tab

Here you can verify/change the IP address for the server. If you change the IP address, click [Test Connectivity] to check that the connection works properly.

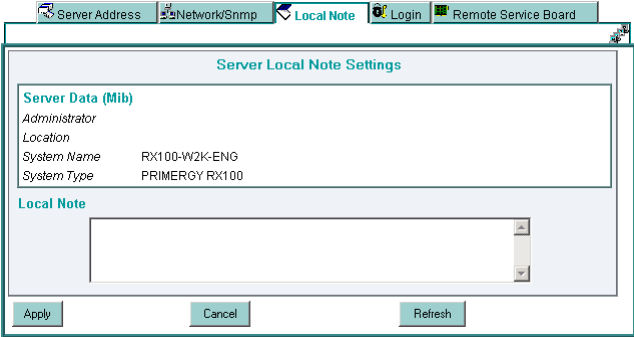
[Network/Snmp] Tab



Here you can verify/change certain network parameters. The items that can be specified are [Community] (name of user community) / [Poll Interval] / [Timeout] / [Connectivity Change Trap] (sending trap after server status changes)/ [Refresh Delay] (refresh delay for opened windows).

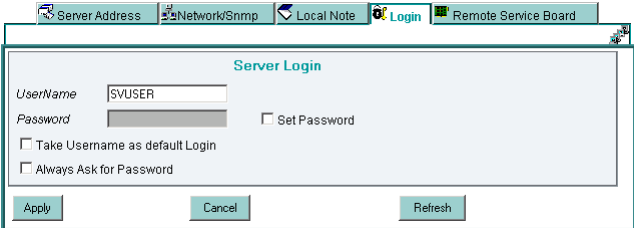
If the load of your network or server is high, it can be improved by changing [Poll Interval], [Timeout], and [Refresh Delay].

[Local Note] Tab



On this tab, you can edit the local note for the server. The local note helps you to find certain servers in the [Server List] window.

[Login] Tab



Specifies the [Username] and [Password] for writing the assigned value to the server. To specify a password, select the [Set Password] checkbox before entering the password. For security reasons, passwords are not stored in any database.

[Remote Service Board] Tab

Here you can verify/change the IP address or community name for the server's secondary channel. By clicking [Test Connectivity], you can check the connection with the remote service board. If you click [Configure], the Web interface to the remote service board starts up and the window for entering the [User ID] and [Password] appears.

For the Web interface, see "5.3.1 Starting the Web Interface" (→pg.310).

[TCP Application] Tab

Here you can configure the Web application settings for a TCP/IP device.

This tab is displayed only when a TCP/IP device is selected as the server type.

- 3 Click [Cancel] to exit the [Server Properties] window.

3.1.5 Registering MIB (MIB INTEGRATION)

This function is used to register a MIB file in ServerView S2.



- ▶ For ServerView S2 running under Linux, MIB registration is not supported.

- 1 Click [ADMINISTRATION] → [MIB INTEGRATION] on the ServerView S2 menu.

The MIB file registration window appears.



- 2 Click [Browse] and specify a MIB file.

- 3 Click [Upload].

The MIB file is registered.

3.2 Monitoring Servers

Here you can verify the server status and the detailed state of each server component.

3.2.1 Verifying the Server Status

■ Server Status Display (Icons)

The status of each server is displayed in the server list with the following icons.

table: Meaning of Icons



























Icon	Meaning
	All components operate properly.
	An error has occurred in one or more components.
	The status for one or more components has deteriorated.
	The server does not respond. It is uncontrollable.
	The server status is under examination.
	The server is inaccessible. Check that the server is connected to the network and that the server is properly specified in ServerView.
	RSB responded through the secondary channel because the server did not respond. It is possible to verify the server status in RSB mode.
	The DiskInfo tool can start. This is not supported.
	The advanced server manager can be activated.
	The Intel LANDesk® Server Manager (LDSM) can be activated.
	ServerView received an alarm from the server.
	Threshold measurement is starting.
	Archive data is created.
	The blade server status (the status of all blades) is normal.
	The blade server status is under investigation.

table: Meaning of Icons

Icon	Meaning
	The blade server status (the status of at least one blade) has deteriorated.
	A blade server status error has occurred (for at least one blade).
	The blade server does not respond. It is uncontrollable.
	The blade server is inaccessible.
	The cluster status is normal.
	The cluster status is in under investigation.
	An error has occurred in one or more components in the cluster.
	All cluster components operate properly.
	The cluster does not respond. It is uncontrollable.
	The cluster is inaccessible. Check that the cluster is connected to the network and that the cluster is properly specified in ServerView.
	The status for one or more components in the cluster has deteriorated.

■ Verification of Server Connections

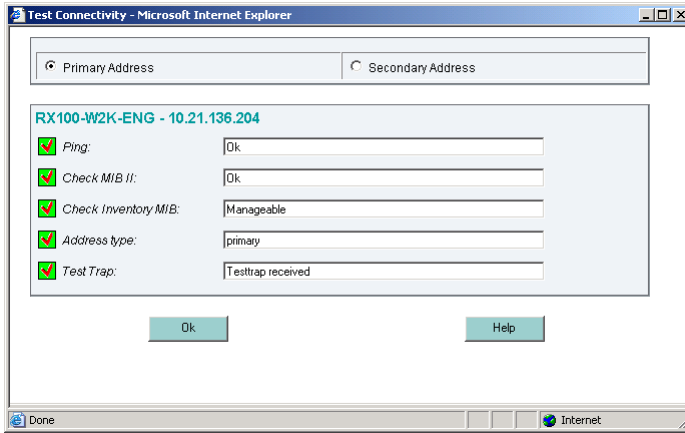
This function is used to test the connections to check that the servers can be properly used in ServerView. This automatically starts the monitoring function and displays the status of the entire system and its subsystems.

IMPORTANT

- ▶ When setting up the server list, it is necessary to confirm that the computer name specified in the server list is available. The computer name is a name assigned to the server during the OS installation. Multiple computer names cannot be assigned to a single IP address simultaneously.

- 1 Check that the server name and the IP address are correctly displayed in the server list.
- 2 Select a server from the server list and click [Test Connectivity] on the right-click menu.

The [Test Connectivity] window appears.



Check that the server responds within the specified timeout period.

The following five tests are executed:

table: Test Connectivity

Test Item	Description
Ping	Checks that servers are connected to the network.
MIB II Check	Checks that the MIB II agent is installed.
Inventory MIB Check	Checks that the inventory MIB for the ServerView agent is installed.
Address Type	Checks if the address type is identified as primary or secondary in the server/RSB.
Test Trap	Checks that traps from the server can be received.

- 3 Execute Step 2 for each server.

■ Redetect Server/Redetect All Servers

To check the status of the current servers, execute [Redetect server] ([Redetect All Servers] for all the servers).

● Redetect Server

- 1 Select the server to verify from the server list and click [Redetect server] on the right-click menu.

The status check starts to check whether the connection status and the current status for each server are normal.

● Redetect All Servers

- 1 Right-click the server list and click [Redetect All Servers] on the menu that appears.

The status check starts for all the servers registered in the server list.

■ Setting the Update Interval for the Server List

Here you can set the interval for updating the server list. The status of the servers registered in the server list is updated with the set interval.

- 1 Click [SERVERLIST] → [SETTINGS] on the ServerView S2 menu.
- 2 Enter the update interval and click [OK].

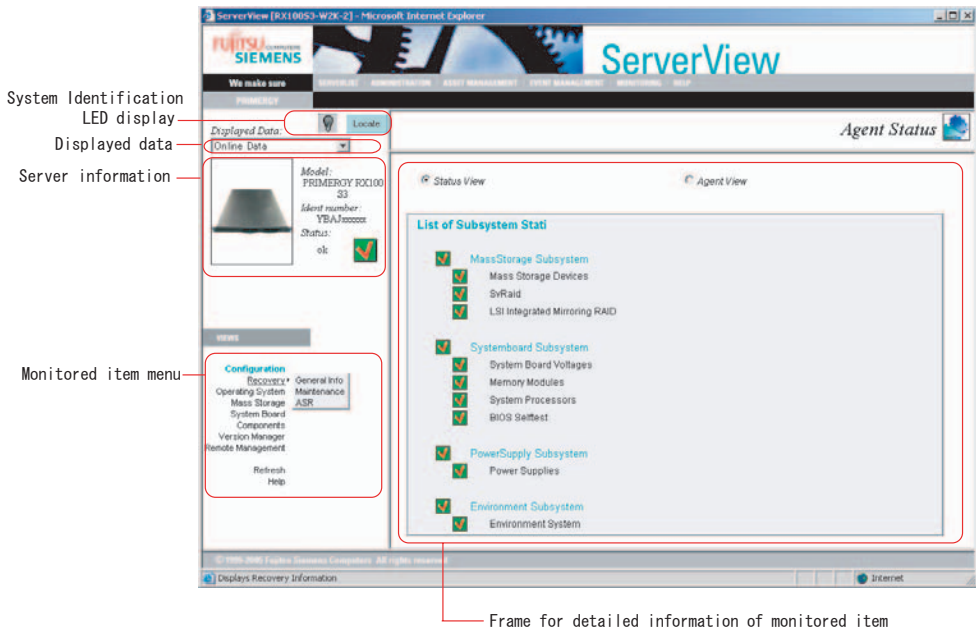


3.2.2 Verifying the Server Monitoring Items in Detail

Here you can verify the server status in detail.

- 1 Click the target server in the server list.

The [ServerView [Server Name]] window appears and the details of the selected server are displayed.



POINT

- ▶ If you select a blade server, the displayed screen will be different, since the monitored objects and monitoring functions are limited. For detailed verification for blade servers, see "3.3 Monitoring Blade Servers" (→pg.119).

● System Identification LED Display

The system identification LED display can be switched. This function is only available for servers that support the system identification LED display. The current status of the system identification LED is displayed with icons.

The following three icons are used.



:LED ON



:LED OFF



:Flashing LED (Indicates a system error)

● Displayed Data

Either Online Data or Archive Data can be specified. Selecting Online Data displays the real-time server information.

Selecting Archive Data displays the server information at the time of the data creation. For archive data, see "3.7.1 Starting the Archive Manager" (→pg.183).

● Server Information

The server model name, ident number and status are displayed. The status is displayed with an icon. For the meaning of the icons, see "■ Server Status Display (Icons)" (→pg.88).

● Monitored Item Menu

For each item, submenu items are displayed when you point at the item with the cursor. When you click the item you want to see, the information is displayed in the frame for detailed information.

table: Monitored Item

Item	Description
Configuration	
Agent Status	Displays the status or agent information. →"■ Agent Status" (pg.95) <ul style="list-style-type: none"> • Status View The subsystem status is displayed. This is linked to each of the subsystems. • Agent View The ServerView agent version, MIB revision, and SNMP agent configuration are displayed.
System Info	Displays system information. →"■ System Information" (pg.96)
Mass Storage	Displays the Mass Storage connected to the server and their file systems. →"■ Mass Storage" (pg.97)
Network Interfaces	Displays the Network Interface installed in the server. →"■ Network Interfaces" (pg.97)
Expansion Boards	Displays the server buses and Expansion Boards. →"■ Expansion Boards" (pg.98)
Recovery	Displays information about the server operation, such as the event log and the error log. →"■ Recovery" (pg.98)
Others	Displays information about fans and temperature sensors. →"■ Others" (pg.99)
MB II	Displays MIB II. →"■ MIB- II " (pg.99)
Recovery	
General Info	Displays error messages and boot options. If you configure the restart option here, you can shut down or restart the server. →"■ Recovery" (pg.100)
Maintenance	Displays the usage time for the internal CMOS battery and information about the fans. →"■ Maintenance" (pg.102)
ASR	You can configure the Automatic Server Reconfiguration & Restart (ASR) function. →"3.4 Serious Error Handling (ASR)" (pg.123)

table: Monitored Item

Item	Description
Operating System	Displays information about the OS installed in the server. →"3.2.5 Displaying Operating System Information" (pg.102)
Mass Storage	
Controller View	Displays information about the adaptors installed in the server and the Mass Storage connected to the adaptors. →"3.2.6 Verifying the Status of Mass Storage" (pg.103)
Logical View	Displays information about the file systems on the server's logical drives.
Partition View	Displays information about the partitions.
System Board	
General Info	Displays information related to the baseboard, such as processors, memory modules, and power voltage. →"3.2.7 Verifying the Baseboard Status" (pg.108)
Busses and Adapters	Displays the adaptors connected to the server bus in a tree view. You can verify the detailed information about the adaptor and the functions for the adaptor selected in the tree view.
Memory Modules	Displays information about the memory modules installed in the server.
Voltages	Displays information about the voltage at certain points of the baseboard.
Components	
Environment	Displays the server temperature and the fan status. →"■ Environment" (pg.112)
Power Supply	Displays the configuration and status of the server's power supply. →"■ Power Supply" (pg.113)
Network Interfaces	Lists the I/F, Status, Type, and Description for the Network Interfaces installed in the server. →"■ Network Interfaces" (pg.115)
Resources	Displays the system resources. →"■ Resources" (pg.116)
Version Manager	
Inventory View	Displays the server Inventory information (the hardware and software configuration information). →"3.2.9 Version Manager (Inventory)" (pg.117)
Remote Management	Displays the remote management information. →"3.2.10 Remote Management" (pg.118)
Refresh	
Server Status	Refreshes the Server Status information.
View	Refreshes the window that is currently displayed on the frame for detailed information.
Help	
Version Information	Displays the version information of ServerView S2.
Contents	Displays the ServerView S2 help contents.
View	Displays the help contents for the window that is currently displayed on the frame for detailed information.

3.2.3 Displaying Configuration Information

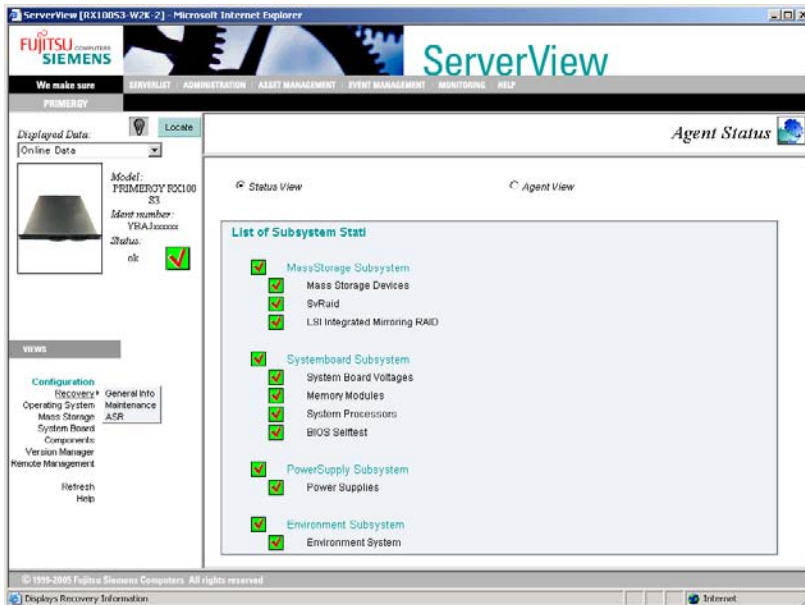
Here, various information about the server configuration is displayed.

■ Agent Status

By selecting [Status View] or [Agent View], you can toggle between the screens.

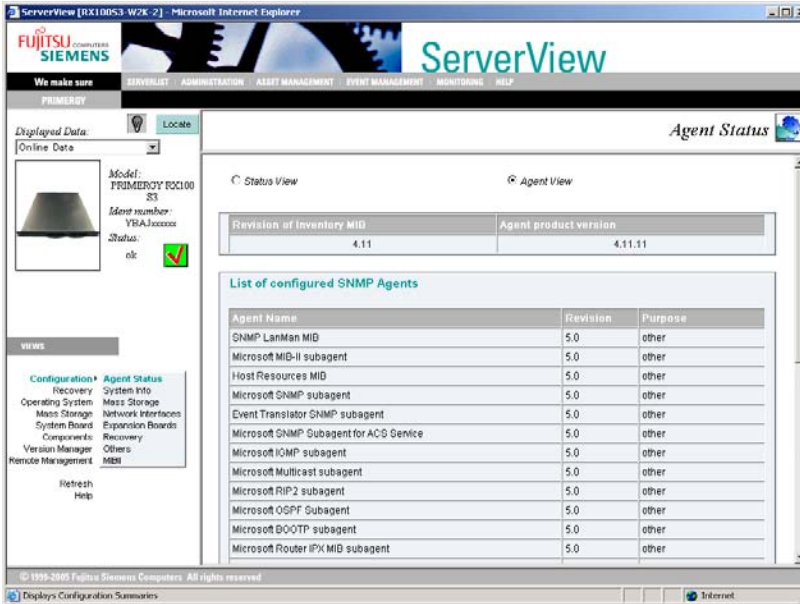
● Status View

The subsystem status is displayed. This is linked to each of the subsystems.



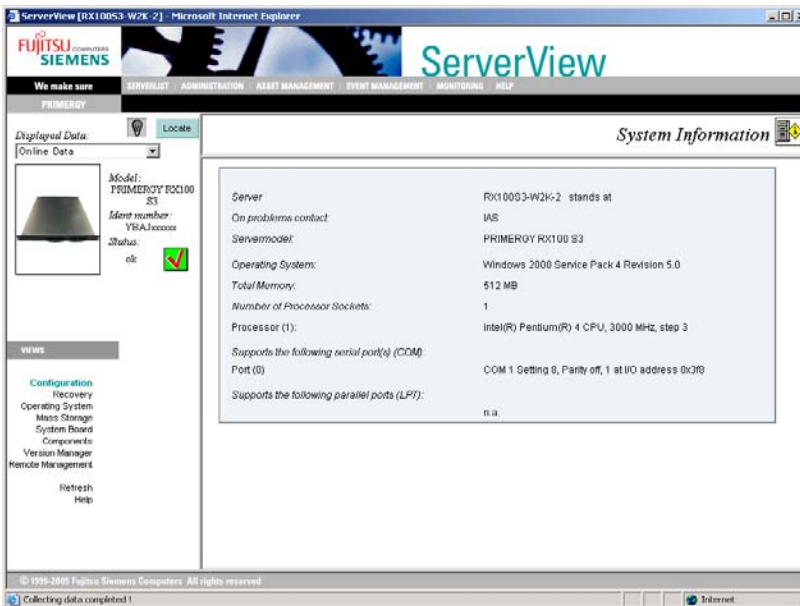
● **Agent View**

The ServerView agent version, MIB revision, and SNMP agent configuration are displayed.



■ **System Information**

Displays system information.



■ Mass Storage

Displays the Mass Storage connected to the server and information about their file systems.

The screenshot shows the ServerView interface for a server. The main content area displays the following information:

Mass Storage

Device Name	Capacity
MITSUMI CD-ROM SR244W T02B (MITSUMI CD-ROM SR244W)	0 MB
LSILOGIC1030 IM1000 (1030 IM)	34695 MB

File Systems

Name	Total Blocks	Sectors	File System Type(s)
W2k (mounted)	2560351	0	NTFS.
NO NAME FOUND (mounted)	0	0	.
NO NAME FOUND (mounted)	3504495	0	NTFS.
W2kx64 (mounted)	2735050	0	NTFS.

■ Network Interfaces

Displays information about the Network Interfaces installed in the server.

The screenshot shows the ServerView interface for a server. The main content area displays the following information:

Network Interfaces

MS TCP Loopback interface

Network Type	softwareLoopback
Physical Address	n.a.
Network Speed (Mbps)	10
Operation Status	up

Broadcom NetXtreme Gigabit Ethernet Driver

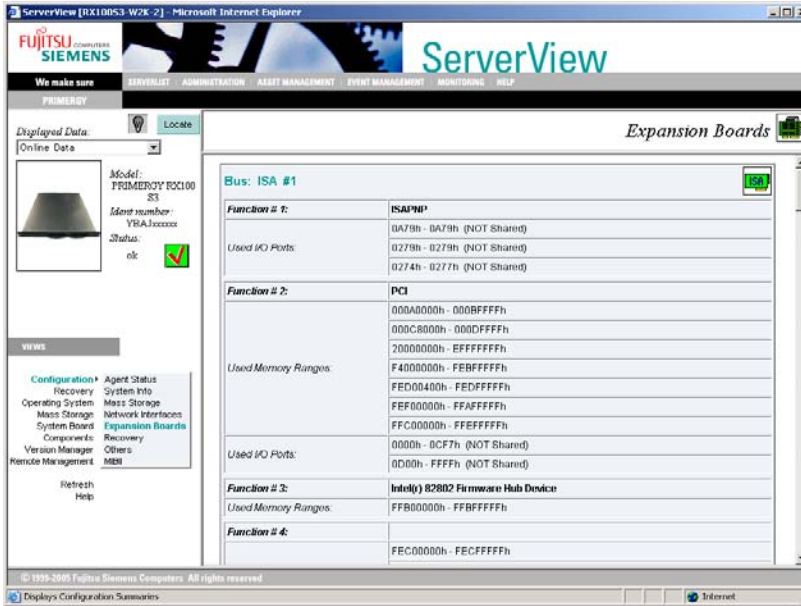
Network Type	ethernet-csmacd
Physical Address	000AE41471E2
Network Speed (Mbps)	100
Operation Status	up
Interrupt	#17 (NOT Shared)
Shared Memory	FC400000 - FC40FFFF

Broadcom NetXtreme Gigabit Ethernet Driver

Network Type	ethernet-csmacd
Physical Address	000AE41471E1
Network Speed (Mbps)	1000
Operation Status	down
Interrupt	#16 (NOT Shared)

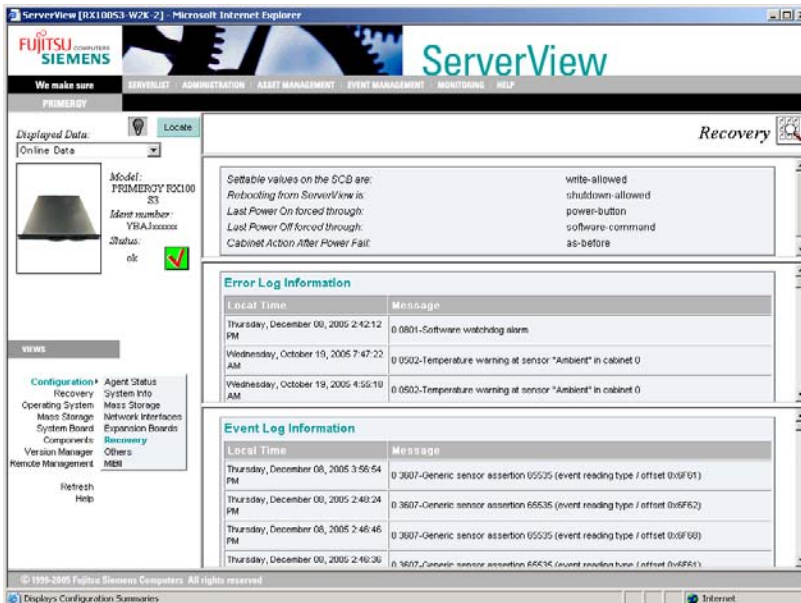
■ Expansion Boards

Displays information about the buses and expansion boards installed in the server.



■ Recovery

Displays information such as the event log and the error log.




Others

Displays information about fans and temperature sensors.

The screenshot shows the ServerView interface for a server. The main content area is titled 'Others' and displays the following information:

Server RX100S3-W2K-2 is configured to have 1 Cabinet
1 cabinet is present.
RX100S3-W2K-2 is configured to be a standalone-server.

Server: RX100S3-W2K-2
Cabinet Id: 0
Location: 
Type: PRIMERGY RX100 S3
Firmware Version: 4.08.04190048
IdentNumber: YBAJxxxxxx
BoardId: S20361-C2004-U10

Temperature Sensors			Fans		
Sensor Number	Sensor Purpose	Critical Reaction	Fan Number	Fan Purpose	Fan Fail Reaction
0	Systemboard	continue	1	FAN SYS1	continue
1	CPU	continue	2	FAN SYS2	continue
2	Ambient	continue	3	FAN SYS3	continue
3	PSU	continue	4	FAN SYS4	continue
			5	FAN SYS5	continue
			6	FAN1 PSU	continue
			8	FAN2 PSU	continue

MIB- II

Displays MIB II information.

The screenshot shows the ServerView interface for a server. The main content area is titled 'General Information' and displays the following information:

System Information

System Name: RX100S3-W2K-2
Description: Hardware: x86 Family 15 Model 4 Stepping 3 ATAT COMPATIBLE - Software: Windows 2000 Version 5.0 (Build 2195 Multiprocessor Free)
Location:
Contact: IAS
Up Time: up 0 days, 21:59:41
Enterprise: .1.3.6.1.4.1.311.1.1.3.1.2
Services: internet,end-to-end,applications

Network Interface Information

MB TCP Loopback interface

Network Type: software_loopback
Physical Address: n/a
Network Speed (Mbps): 10
Operation Status: up
IP Address: 127.0.0.1
Subnet Mask: 255.0.0.0

Broadcom NetXtreme Gigabit Ethernet Driver

Network Type: ethernet_comacd

3.2.4 Recovery

In [Recovery], there are three menu items: "■ Recovery" (→pg.100), "■ Maintenance" (→pg.102) and "3.4 Serious Error Handling (ASR)" (→pg.123).

■ Recovery

When you click [General Info] in the [Recovery] item, the [Recovery] window appears.

The screenshot shows the ServerView Recovery window for a Fujitsu/Siemens server. The window is titled "ServerView [RX10053-W2K-2] - Microsoft Internet Explorer". The main content area is divided into several sections:

- Boot Options:** Displays error halt settings (halt-on-any-error, os-running, power-button, software-command), current boot status, last power-on reason, and last power-off reason.
- Restart Options:** Includes radio buttons for Standard Boot and Boot Diagnostic System, a Shutdown Delay field, and buttons for Restart, Shutdown & Off, and Abort Shutdown.
- Contents of Error Message Buffers:** Includes radio buttons for GMT and Local time, and checkboxes for Critical Errors (°C) and Non-critical Errors.
- Error Message Table:** A table with columns for Date / Time, Cabinet / Error, and Message. The messages listed are "Software watchdog alarm" and "Temperature warning at sensor 'Ambient' in cabinet 0".

On the left side, there is a "Displayed Data" section showing the server model (PRIMERGY RX100 S3), identity number (YBA1xxxxx), and status (ok). Below this is a "VIEWS" menu with options like Configuration, Recovery (selected), General Info, Operating System, Maintenance, Mass Storage, System Board, Components, Version Manager, Remote Management, Refresh, and Help.

● Boot Options

Information about the boot process is displayed under Boot Options. ServerView displays the following information corresponding to the server BIOS settings.

- Error Halt Settings
Settings such as whether a system should stop or not if an error occurs are displayed.
- Current Boot Status
The Current Boot Status is displayed.
- Last PowerOn Reason
The power-on reason is displayed.
- Last PowerOff Reason
The power-off reason is displayed.

● Restart Options

By specifying an option here and clicking the function button, you can shut down or restart the server. When you click each button, the login window appears for security reasons. The user name and password must have ServerView administrator privileges.

- The [Restart] button
Restarts the server. Specify the time required until the server restarts.
- The [Shutdown & Off] button
This button shuts down the server and turns off the power. Specify the time required until the server is shut down or the power turned off.
- The [Abort Shutdown] button
This button aborts any shutdown that is started by clicking [Restart] or [Shutdown & Off]. However, if the restart or shutdown has already started, it cannot be aborted.

POINT

- ▶ When [Change of a default user] is executed in the login window, the default user is temporarily modified. However once ServerView shuts down, this information is lost. To change the default login user, start [Server Properties] and specify it in the [Login] tab window. For this procedure, refer to "3.1.4 Verifying/Changing the Server Settings" (→pg.84).
- ▶ [Boot Diagnostic System] is not supported. Do not select this option.

● Contents of Error Message Buffers

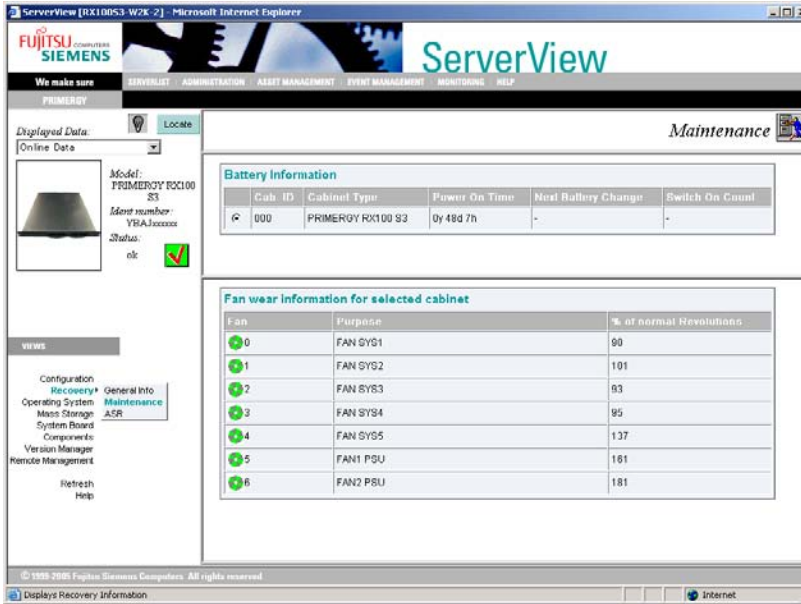
The list is sorted in the order of date/time with the latest entry at the top. Each message consists of five parts: "C" (when the message level is critical), "Date/Time", "Cabinet/Error", and "Message". Select whether to display the time in Greenwich Mean Time or local time.

The contents that appear in the Error Message Buffers depend on whether a remote service board exists or not.

- When there is a remote service board
The SEL information that the remote service board has acquired and the errors that it has detected appear in the Error Message Buffers.
- When there is no remote service board
The SEL contents for the server itself appear in the Error Message Buffers.

Maintenance

When you click [Maintenance] in the [Recovery] item, the following window appears, where the usage time for the internal CMOS battery and information about the fans are displayed.



3.2.5 Displaying Operating System Information

When you click [Operating System], information about the OS installed on the server is displayed. Data for the currently running process as well as the OS name, version, language, and system run time are displayed.



3.2.6 Verifying the Status of Mass Storage

For Mass Storage, you can verify the following states:

- Verifying the device controllers and device status. → "Controller View" (P.103)
- Verifying information about the system files in the logical drives. → "Logical View" (P.107)
- Verifying detailed information about the partitions. → "Partition View" (P.107)

■ Controller View

When you click [Controller View] in the [Mass Storage] item, detailed information appears about hard disks and controllers.

The screenshot shows the ServerView web interface for a PRIMERGY RX100 S3 server. The main content area is titled "Controller View" and contains a table of controllers and a "Details of the Selected Controller" section.

No.	Status	Type	Adapter Name
1	OK	PCI	82801 G (ICH7 Family) IDE Controller
2	OK	ISA	Primary IDE Channel
3	OK	ISA	Secondary IDE Channel
4	OK	PCI	LSI 1020A SCSI Controller

Details of the Selected Controller

Driver Name: pciide
 Adapter Model: 82801 G (ICH7 Family) IDE Controller
 Agent Type: IDE controller
 Bus Type & No.: PCI 1
 Slot: onboard

IRQ: n.a. DMA Channel: n.a.
 Device Number: 31 I/O Range: 3400h - 340fh
 No. Attached Dev.: 0 Function: 2 Memory Range: n.a.

● Controller List

The data for the controllers connected to the server are listed. "No.", "Status" (OK or FAIL), "Type" (EISA, PCI, ISA), and "Adapter Name" are displayed.


● Details of the Selected Controller

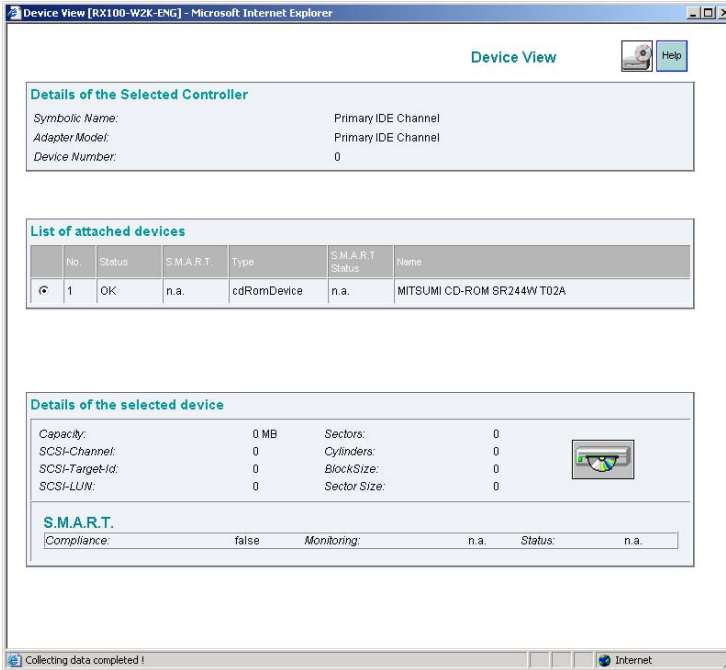
Detailed information about the controller selected in the controller list is displayed. The links to [MULTIPATH VIEW] and [DEVICE VIEW] are displayed to the right. When you click these links, a detailed information window opens. (→ "Device View" (P.104)) The links shown here and the detailed information window vary depending on the type of the selected controller.

POINT

- ▶ Make sure to select a controller for which you want detailed information to be displayed. If you do not select any controller, unrelated information may be displayed.

● Device View

When you click [DEVICE VIEW , the [Device View] window opens and detailed information about the devices connected to the controller is displayed.



- **Details of the Selected Controller**
Detailed information about the selected controller is displayed.
- **List of attached devices**
A list of the connected devices is displayed. Select the device for which you want to verify the detailed information.
- **Details of the selected device**
Detailed information about the device selected in the [List of attached devices] is displayed.
- **[View RAID]**
If the [View RAID] button is displayed at the bottom and you click this button, the logical drive list and the physical devices on the RAID card are displayed so that you can verify them in detail. → "MYLEX Devise View (View RAID)" (P.105)

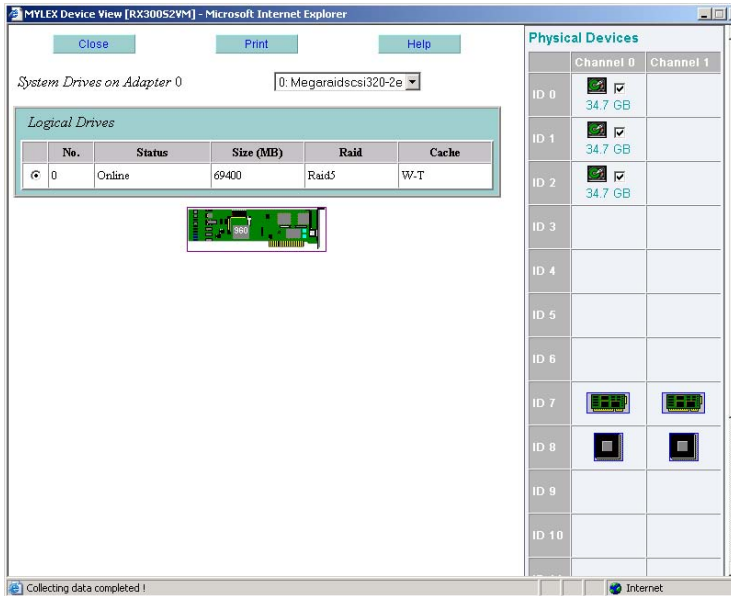
POINT

- ▶ The information displayed in the Self Monitoring and Reporting Technology (S.M.A.R.T.) column is returned from the S.M.A.R.T. procedure. S.M.A.R.T. is a technology used to detect hard device errors at an early stage (PDA = Prefailure Detection and Analysis). SCSI and ATA hard disk drives are supported.

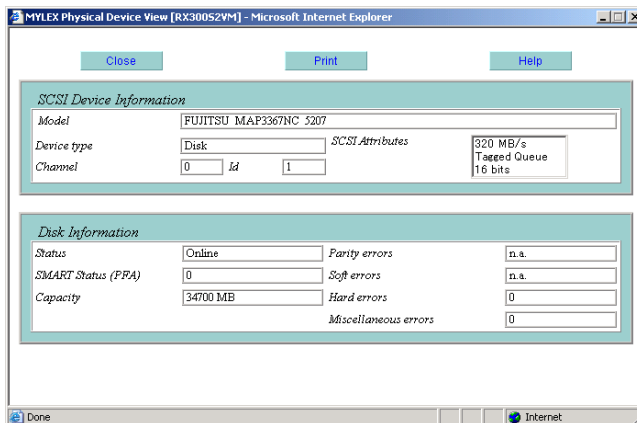
● MYLEX Device View (View RAID)

If the [View RAID] button is displayed in the [Devis View] window and you click this button, the following window appears.

When you click [DEVICE VIEW], the [Devis View] window opens and detailed information about the devices connected to the controller is displayed. Also, when you click [View RAID] that may be displayed at the bottom of the [Devis View] window, the following window is displayed.

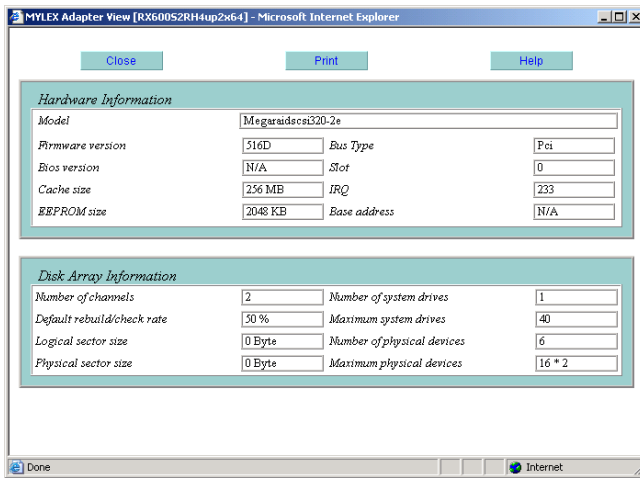


- Logical Drives
A list of the logical drives on the RAID card is displayed.
- Physical Devices
The physical drives on the RAID card are displayed. When you select a drive number from the [Logical Drives] list, a check mark appears in the [Physical Devices] list for the physical device that corresponds to the selected logical drive.
When you click a link in the [Physical Devices] list, the Physical Device View appears, where you can verify the SCSI device information and disk drive information.



- Controller Icon

When you click a controller icon, the Adapter View window appears, where you can verify the hard disk drive information and the disk array information.



POINT

- ▶ In order to monitor and display the RAID card, make sure to install the management tool supplied with the card. The Management Console can be notified of information about detected errors.

IMPORTANT

- ▶ The SCSI array controller card/IDE-RAID controller card information may be incorrectly displayed depending on the version numbers of ServerView and the RAID manager/IDE-RAID manager. Therefore verify the status using RAID management tools such as the RAID manager/IDE-RAID manager.
- ▶ For the settings of the Global Array Manager (GAM), see below.
When using the Linux installation proxy service bundle type, refer to the release notes supplied with the server. In addition, when using a SCSI type or diskless type Linux distribution, obtain the "Driver Kit" for the corresponding machine type from [Download Search] on the following home page, and then refer to the "Installation Guide" contained in the "Driver Kit".
 - The Fujitsu PRIMERGY website
(<http://primergy.fujitsu.com>)

■ Logical View

When you click [Logical View] in the [Mass Storage] item, the [Logical View] window appears, where the file systems for the server's logical drives are listed. The details for the file system selected in the list are displayed. You can verify the file system size, mount status, file system type, and the utilization.

The screenshot shows the ServerView interface in Microsoft Internet Explorer. The main content area is titled "Logical View" and contains a table of logical drives and a "Selected File System Info" section.

No	Name
1	W2K
2	NO NAME FOUND
3	NO NAME FOUND
4	W2K3R64

Selected File System Info

Size: 10001 MB
 Mounted: yes
 File System Types: NTFS

Utilization: Used 44.1%, Free 55.9%

■ Partition View

When you click [Partition View] in the [Mass Storage] item, the [Partition View] window appears, where you can verify the detailed information about the server partitions.

The screenshot shows the ServerView interface in Microsoft Internet Explorer. The main content area is titled "Partition View" and contains a table of partitions and detailed information about the associated controller and device.

No	Status	Type	Name	Offset	Size
1	ok	7	NTFS Partition	0 MB	10001 MB
2	ok	7	NTFS Partition	10001 MB	14001 MB
3	ok	7	NTFS Partition	24003 MB	10683 MB

Details of the Associated Controller

Symbolic Name: LSI 1020A SCSI Controller
 Adapter Model: LSI 1020A SCSI Controller
 Bus Type & No.: PCI 3 Device Number: 5 Function: 1

Details of the Associated Device

Type: directAccessDevice No.: 2
 Name: LSI_LOGIC1030 IM1000

By selecting a partition number in partition list, you can verify the following detailed information for the selected partition.

- Details of the Associated Controller
Symbolic Name, Adapter Model, Bus Type & No., Device Number, and Function of the controller for that partition are displayed.
- Details of the Associated Device
The type, number, and name of the device, where the partition is created, are displayed.

3.2.7 Verifying the Baseboard Status

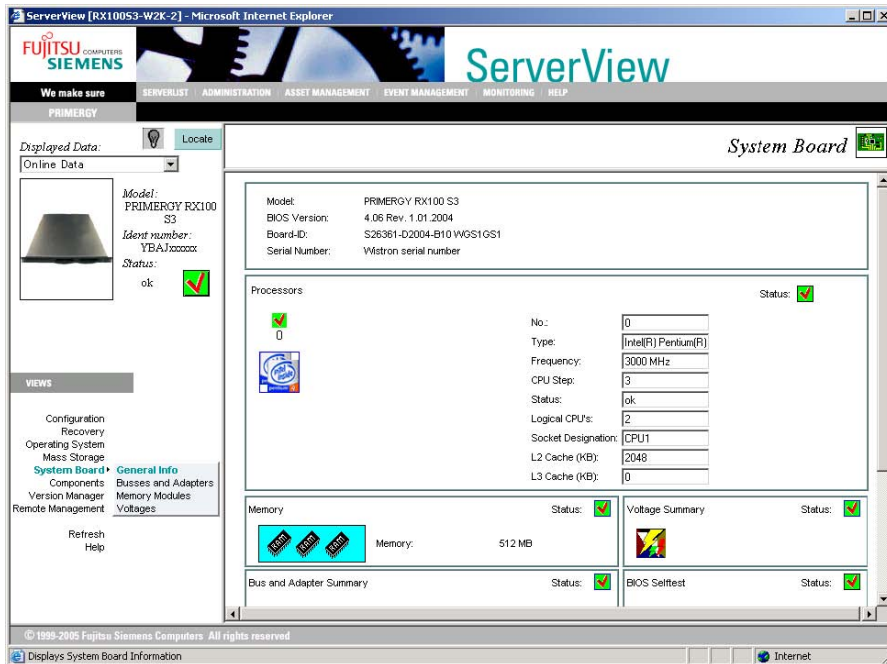
You can verify the following states for the baseboard:

- Verifying the baseboard status. → "System Board" (P.108)
- Verifying information about the adaptors connected to the server bus. → "Busses and Adapters" (P.110)
- Verifying the status of the memory modules installed in the server. → "Memory Modules" (P.110)
- Verifying the voltage states at certain points of the baseboard. → "Voltages" (P.111)

■ System Board

When you click [General Info] in the [System Board] item, the [System Board] window appears, where the baseboard information (the model, BIOS version, board ID, and serial number) is displayed.

The serial number may not be displayed depending on the model.



● Processors

Information about the installed processors is displayed.

When you click a processor icon, the number, type, frequency, CPU step, status, number of logical CPUs, socket type, L2 cache (KB) and L3 cache (KB) of the clicked processor are displayed.

● Memory

The total memory size and status are displayed. When you click the status icon, the [Memory Modules (→ P.110)] window appears.

● Voltage Summary

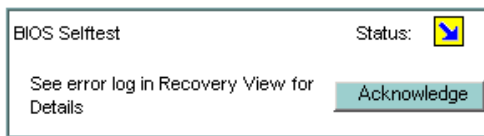
The voltage status is displayed. When you click the status icon, the [Voltages (→ P.111)] window appears.

● Bus and Adapter Summary

The supported bus types and status are displayed. When you click the status icon, the [Busses and Adapters (→ P.110)] window appears.

● BIOS Selftest

The result of the BIOS self-test at the server power-on is displayed.



If the [degraded] icon is displayed as the status, you can revert the icon to [OK] by clicking [Acknowledge]. Verify the detailed [degraded] information in the [Contents of Error Message Buffers] in the [Recovery (→ P.100)] window.

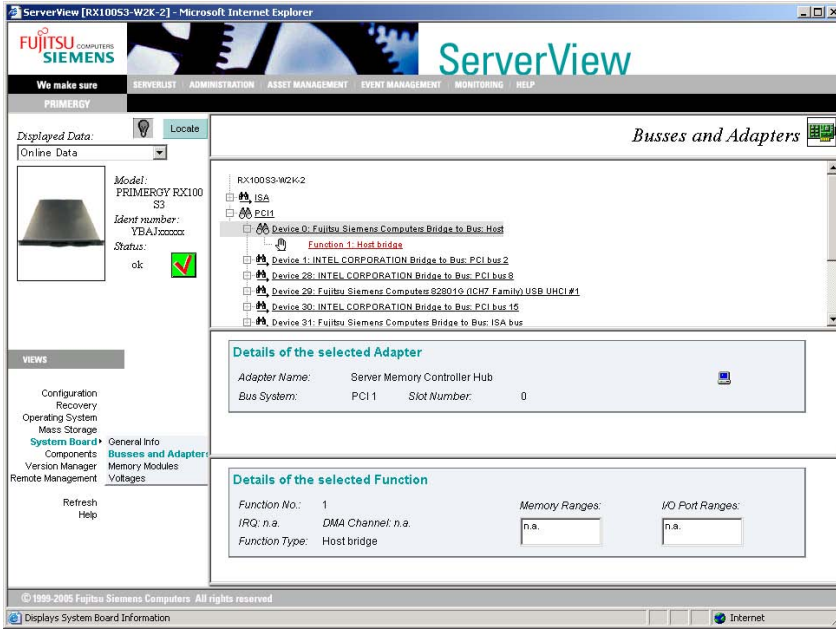
However, if the BIOS (version) does not have a self-test notification function, the BIOS self-test information is not displayed.

POINT

- ▶ If you re-install the ServerView Agent after reverting the icon to [OK] by clicking [Acknowledge], the icon may go back to [degraded] (a trap may also occur). In that case, click [Acknowledge] again to revert the icon to [OK].

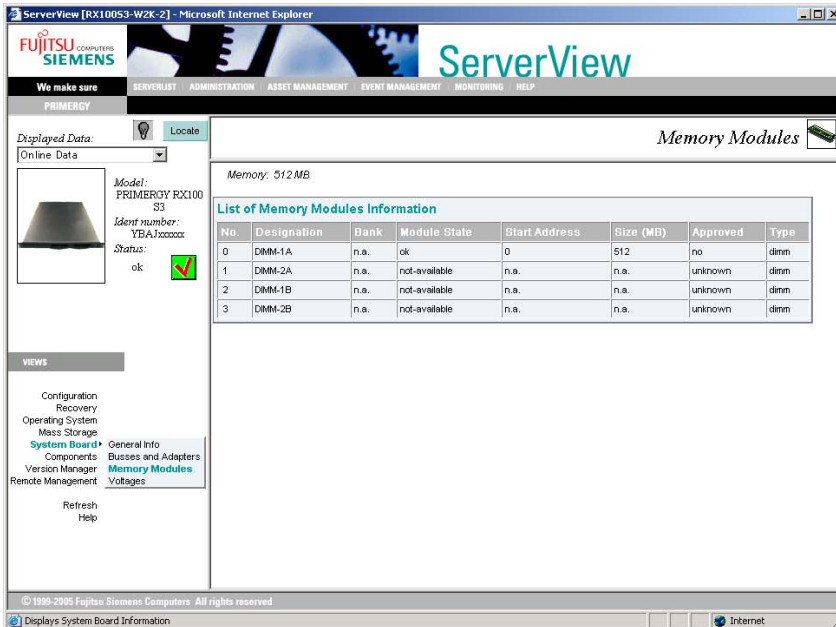
■ Busses and Adapters

When you click [Busses and Adapters] in the [System Board] item, the [Busses and Adapters] window appears. The adaptors connected to the server busses are displayed in a tree view. You can verify the detailed information about the adaptor and the functions for the adaptor selected in the tree view.



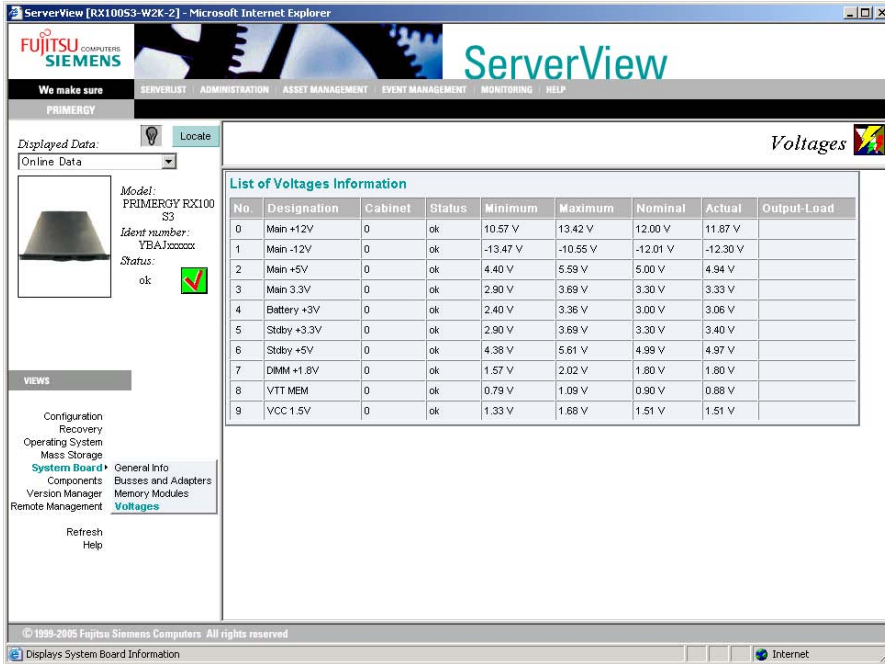
■ Memory Modules

When you click [Memory Modules] in the [System Board] item, the [Memory Modules] window appears, where detailed information about the memory modules installed in the server is installed.



■ Voltages

When you click [Voltages] in the [System Board] item, the [Voltages] window appears, where you can verify the detailed information about the voltage at certain points on the baseboard.



The screenshot shows the ServerView web interface for a Fujitsu Siemens server. The main content area displays the 'Voltages' window, which contains a table of voltage information. The table lists various voltage points, their designations, cabinet numbers, status, and measured values.

No.	Designation	Cabinet	Status	Minimum	Maximum	Nominal	Actual	Output-Load
0	Main +12V	0	ok	10.57 V	13.42 V	12.00 V	11.87 V	
1	Main -12V	0	ok	-13.47 V	-10.55 V	-12.01 V	-12.30 V	
2	Main +5V	0	ok	4.40 V	5.59 V	5.00 V	4.94 V	
3	Main 3.3V	0	ok	2.90 V	3.69 V	3.30 V	3.33 V	
4	Battery +3V	0	ok	2.40 V	3.36 V	3.00 V	3.06 V	
5	Stabby +3.3V	0	ok	2.90 V	3.69 V	3.30 V	3.40 V	
6	Stabby +5V	0	ok	4.38 V	5.61 V	4.99 V	4.97 V	
7	DRAM +1.8V	0	ok	1.57 V	2.02 V	1.80 V	1.80 V	
8	VTT MEM	0	ok	0.79 V	1.09 V	0.90 V	0.88 V	
9	VCC 1.5V	0	ok	1.33 V	1.68 V	1.51 V	1.51 V	

3.2.8 Verifying the Component Status

For the components, you can verify the following states:

- Verifying the server temperature and the fan status. → "Verifying the Environment Status" (P.234)
- Verifying the server power supply information. → "Verifying the Power Supply Status" (P.232)
- Verifying information about the Network Interfaces installed in the server. → "Network Interfaces" (P.115)
- Verifying the system resources. → "Resources" (P.116)

■ Environment

When you click [Environment] in the [Components] item, the [Environment] window appears.

The screenshot shows the ServerView interface for a Fujitsu/Siemens server. The main content area displays the 'Environment' view for a 'PRIMERGY RX100 S3' system. A server icon is shown with green status indicators. A table titled 'Temp. Sensors' provides the following data:

No.	Purpose	State	Value
	Systemboard		41
1	CPU		43
2	Ambient		26
3	PSU		59

The interface also includes a left sidebar with navigation options like 'Configuration', 'Recovery', and 'Environment', and a top navigation bar with 'SERVERLIST', 'ADMINISTRATION', 'ASSET MANAGEMENT', 'EVENT MANAGEMENT', 'MONITORING', and 'HELP'.

● Server Icon Display

The server icon indicates the server door or housing is open or closed. If the server icon is green, it means that the server door or housing is closed. A yellow icon means that it is open.

However, the server door/housing open/closed status indication may not be supported depending on the server model.

● Fan and Temperature Status Display

When you point at a fan icon with the cursor, the name of the fan is displayed. For redundant fans, cascaded fan icons are displayed.

When you click the temperature sensor status icon, the basic threshold for the temperature and the current temperature are displayed in the figure.



- ▶ The basic threshold stored in the server (hardware) is used to determine the status. This value is unrelated to the threshold value set in the Performance Manager.

The colors of the fan and temperature sensor icons indicate the following states:

table: Fan and Temperature Status

	Shutdown	Danger	OK	Sensor Failure	Cannot Verify
Temperature	Red	Yellow	Green	Blue	Gray
Fan	Red	Yellow	Green	---	Gray

● Summary

When you select an extension storage device, its status is displayed just like the server status.

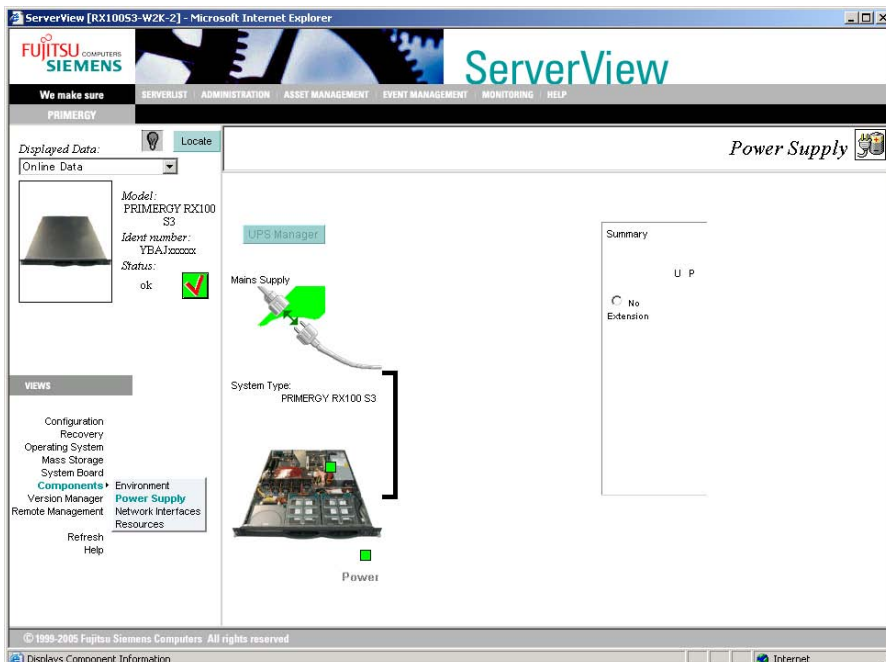
■ Power Supply

When you click [Power Supply] in the [Components] item, the [Power Supply] window appears.

When you point at the status with the cursor, the name of the Power Supply is displayed.

If the Power Supply operates properly, a green rectangle is displayed on the corresponding Power Supply.

For redundant Power Supply, two cascaded rectangles are displayed.



● **Mains Supply**

The status of the connection between the server and the Mains Supply is displayed. If any extension storage device is connected to the server, its Mains Supply is also displayed.

A Mains Supply failure for the server and the extension storage devices is indicated with a yellow or red rectangle.

Usually, the power status is updated every 60 seconds.

● **System Type**

The overall status of the server power supply is indicated with a green, yellow or red rectangle.

● **Expansion Disk Devices**

Existing extension storage devices are displayed. BBU installation can also be detected. The overall status of the power supply for extension storage devices is indicated with a green or red rectangle.

● **Summary**

When you select an extension storage device, its status is displayed just like the server status.

● **UPS Manager**

Unsupported.

When the UPS management software is installed and the settings for interaction with the UPS management software are assigned, the [UPS Manager] button is enabled.

■ Network Interfaces

When you click [Network Interfaces] in the [Components] item, the [Network Interfaces] window appears, where the Network Interfaces installed in the server are listed. The detailed information about the selected Network Interfaces and the overall statistic information are displayed. When you click [Refresh], the displayed statistics are updated.

The screenshot shows the ServerView application window with the 'Network Interfaces' section active. The interface displays a table of network interfaces, details for the selected interface, and global statistics.

IF	Status	Type	Description
1	up	softwareLoopback	MS TCP Loopback interface
16777219	up	ethernet-csmacd	Broadcom NetBtreme Gigabit Ethernet Driver
16777220	down	ethernet-csmacd	Broadcom NetBtreme Gigabit Ethernet Driver

Details of the Selected Interface

Description: Broadcom NetBtreme Gigabit Ethernet Driver
 Adapter Model: Broadcom NetBtreme Gigabit Ethernet
 Type: ethernet-csmacd

MAC Statistics

Phys. Address: 000E41471E2 Slot Number: 0
 IPX Network: n.a. Function: 1
 Speed: 100 Mb/Sec IRQ: 17
 IP Address: 10.21.136.238 DMA Channel: n.a.
 IP Subnet Mask: 255.255.255.0 I/O Addr. Range: n.a.
 Bus Type & No.: pci 12 MEM Addr. Range: FC400000 - FC40FFFF

Global Statistic

IP Pkts. In:	398340	IPX Pkts. In:	n.a.	Refresh
Out:	389415	Out:	n.a.	

■ Resources

When you click [Resources] in the [Components] item, the [Resources] window appears, where the Resources in the system are displayed. For each IRQ, I/O-Port, DMA, and Memory, the bus, type, device name and vendor name are displayed.

The screenshot shows the ServerView interface with the 'Resources' window open. The window displays a table of system resources, including IRQ, I/O Port, DMA, and Memory. The table has columns for IRQ, Bus, Type, DeviceName, and VendorName. The resources listed include System timer, Standard keyboard, Communications Port (COM1), Standard floppy disk controller, System CMOS/real time clock, CSDB USB, Intel(R) 82540EM based Network Connection, PS/2 Compatible Mouse, Numeric data processor, Primary IDE Channel, Secondary IDE Channel, FASITRAK 100LP ATA RAID controller, Intel(R) PRO100 S Server Adapter, and ATI RADE XL PCI.

IRQ	Bus	Type	DeviceName	VendorName
00	0	isa	System timer	(Standard system devices)
01	0	isa	Standard 101/1102-Key or Microsoft Natural PS/2 Keyboard	(Standard keyboards)
04	0	isa	Communications Port (COM1)	(Standard port types)
06	0	isa	Standard floppy disk controller	(Standard floppy disk controllers)
08	0	isa	System CMOS/real time clock	(Standard system devices)
09	0	pci	CSDB USB	Reliance Computer Corporation/ServerWorks
10	0	pci	Intel(R) 82540EM based Network Connection	Fujitsu Siemens Computers
12	0	isa	PS/2 Compatible Mouse	Microsoft
13	0	isa	Numeric data processor	(Standard system devices)
14	0	isa	Primary IDE Channel	(Standard IDE ATA/ATAPI controllers)
15	0	isa	Secondary IDE Channel	(Standard IDE ATA/ATAPI controllers)
20	0	pci	FASITRAK 100LP ATA RAID controller	PROMISE TECHNOLOGY
22	0	pci	Intel(R) PRO100 S Server Adapter	Fujitsu Siemens Computers
23	0	pci	ATI RADE XL PCI	Visionet Corporation

3.2.9 Version Manager (Inventory)

When you click [Inventory] in the [Version Manager] item, the [Inventory] window appears, where the server Inventory information (the hardware/software configuration information) is displayed. For each object, the Name, Vendor, Version, Serial Number, and Component Type are displayed.

The screenshot shows the 'Inventory' window in the ServerView application. The window title is 'ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer'. The interface includes a navigation menu on the left with options like 'Configuration', 'Recovery', 'Operating System', 'Mass Storage', 'System Board', 'Components', 'Version Manager', and 'Remote Management'. The 'Inventory View' is selected. The main area displays a table of hardware components:

Name	Vendor	Version	Serial Number	Component Type
GEM318	SDR	0		SCSI Device
RX100S3 SDR ID-0125	FSC	04.10		SDRVersion
LSI 1020A SCSI CONTROLLER	Fujitsu Siemens Computers	05.13.08.00		BIOS
82801G (ICH7 Family) IDE Controller	Fujitsu Siemens Computers	1		SCSI Controller
82801GB/GR (ICH7 Family) LPC Interface Bridge	Fujitsu Siemens Computers	1		Bridge Device
82801G (ICH7 Family) USB UHCI #4	Fujitsu Siemens Computers	1		I/O
82801G (ICH7 Family) USB2 EHCI Controller	Fujitsu Siemens Computers	1		I/O
82801G (ICH7 Family) PCI Express Port 1	INTEL CORPORATION	1		Bridge Device
82801GR/GH/GHM (ICH7 Family) PCI Express Port 5	INTEL CORPORATION	1		Bridge Device
82801GR/GH/GHM (ICH7 Family) PCI Express Port 6	INTEL CORPORATION	1		Bridge Device
82801G (ICH7 Family) USB UHCI #2	Fujitsu Siemens Computers	1		I/O
82801G (ICH7 Family) USB UHCI #3	Fujitsu Siemens Computers	1		I/O
82801G (ICH7 Family)	Fujitsu Siemens	1		I/O

POINT

When starting from the Management Console

- ▶ When you select a server in the [Version Management] mode and click [Inventory View], the [Inventory View] window appears.

The screenshot shows the 'Inventory View' window for a PRIMERGY T1600 server. The window title is 'Fujitsu Server View - Version Management - Inventory View [TX600W2K3] - Inventory View [TX600W2K3]'. The interface includes a navigation menu on the left with options like 'Server Management', 'Version Management', 'Inventory View', 'Archive Manag...', 'Export Manag...', and 'Global CleanUp...'. The main area displays a table of hardware components:

Name	Vendor	Version	Serial Num.	Component Type
BIOS	FSC	4.06 Rev. 1.0.		BIOS
CDIB-10 PCI Bridge	Reliance Computer Cor.	5		Bridge Device
CDIB-10 PCI Bridge	Reliance Computer Cor.	5		Bridge Device
CDIB-10 PCI Bridge	Reliance Computer Cor.	5		Bridge Device
CDIB-10 PCI Bridge	Reliance Computer Cor.	5		Bridge Device
CMO-1E A2.0	Reliance Computer Cor.	0		Bridge Device
CMO-1E A2.0	Reliance Computer Cor.	0		Bridge Device
CMO-1E A2.0	Reliance Computer Cor.	50		Bridge Device
CSB8	Reliance Computer Cor.	160		Bridge Device
CSB8 ISA Bridge	Reliance Computer Cor.	0		Bridge Device
PRIMERGY T1600	FSC	0501	Prototyp48	Cabinet
T1600R	FSC	0501	Prototyp48	Chassis
TX600W2K3	FSC	N/A		Complete System
Mem. MP 2552 MHz	Intel	Step 5		CPU
acpi.sys	Microsoft Corporation	5.2.2790.1830		Device driver
adpu320.sys	Adaptec, Inc.	7.0.00.000 IN.		Device driver
afd.sys	Microsoft Corporation	5.2.2790.1830		Device driver
afmp.sys	Microsoft Corporation	5.2.2790.1830		Device driver
atapi.sys	ATI Technologies, Inc.	5.10.3665.6003.		Device driver
audbus.sys	Microsoft Corporation	5.2.2790.1830		Device driver
b57xp32.sys	Broadcom Corporation	0.34.0.0 built b.		Device driver
beep.sys	Microsoft Corporation	5.2.2790.0		Device driver
cdrom.sys	Microsoft Corporation	5.2.2790.1830		Device driver
cdrom.sys	Microsoft Corporation	5.2.2790.1830		Device driver
classpnp.sys	Microsoft Corporation	5.2.2790.1830		Device driver
cordisk.sys	Microsoft Corporation	5.2.2790.1830		Device driver
dfs.sys	Microsoft Corporation	5.2.2790.1830		Device driver
disk.sys	Microsoft Corporation	5.2.2790.1830		Device driver
dmio.sys	Microsoft Corporation	5.2.2790.1830		Device driver
dmload.sys	Microsoft Corporation	5.2.2790.0		Device driver
dmapi.sys	Microsoft Corporation	5.2.2790.0		Device driver
dm.sys	Microsoft Corporation	5.2.2790.1830		Device driver
dmq.sys	Microsoft Corporation	5.2.2790.1830		Device driver
dmq.sys	Microsoft Corporation	5.2.2790.1830		Device driver
dm.sys	Microsoft Corporation	5.2.2790.1830		Device driver

3.2.10 Remote Management

When you click [Remote Management], the following [Remote Management] window appears. The contents of this window vary depending on the server model, configuration, and settings.

The screenshot shows the ServerView Remote Management window for a PRIMERGY RX330 server. The interface includes a navigation menu on the left with options like Configuration, Recovery, and Remote Management. The main content area is titled 'Remote Management' and shows the 'Last Known Configuration' for the server. The configuration is divided into three sections, each with a table of network details and associated action buttons.

Controller Type	IP Address	Address Type	MacAddress
System LAN	10.21.136.124	primary	00300546569E
System LAN	10.21.136.202	primary	00300546569F
RSB	10.21.136.14	secondary	003005711E93
Baseboard Management Controller	10.21.136.16	baseboard-controller	00300546569E

For details, see "4.3.2 Start and Exit for RemoteControlService/Web (For BMC connection)" (→pg.273) or "4.3.3 Start and Exit for RemoteControlService/Web (For RSB connection)" (→pg.276).

3.3 Monitoring Blade Servers

This is used to verify the blade server status.

When you click a blade server in the server list, the [Blade Server View [Server Name]] window appears, where detailed information about the selected blade server is displayed.



● System Identification LED Display

The system identification LED display can be switched. This function is only available for servers that support the system identification LED display. The current status of the system identification LED is displayed with icons.

The following three icons are used.

 :LED ON  : LED OFF

 :Flashing LED (Indicates a system error)

● Blade Server Information

The Status, model name and ident number for the blade server are displayed.

The status is indicated with an icon. For the meaning of the icons, see "■ Server Status Display (Icons)" (→pg.88).

For the model name, the name of the blade server system that is configured as the management blade is displayed.









For the Ident number, the ID number for the blade server system is displayed.

● Displayed Data

Either Online Data or Archive Data can be specified. Selecting Online Data displays the real-time server information. Selecting Archive Data displays the server information at the time of the data creation.

● Blade List

The table for all the blades in the blade server system is displayed. For the Type/ID, the blade ID and blade type are indicated with icons.

-  : Management blade (master)
-  : Management blade (slave)
-  : Switch blade
-  : fiber channel path through blade
-  : LAN path through blade
-  : KVM blade
-  : fiber channel switch blade
-  : Server blade

● Function Buttons

The following function buttons are available for verifying status of each component:



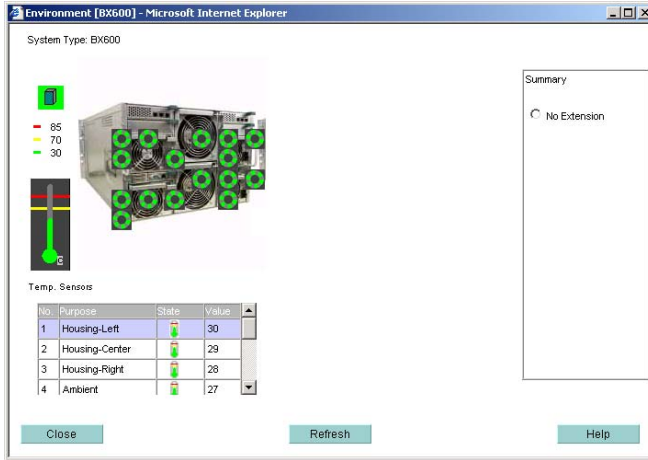
- ▶ If the security for the management blade is enabled, the user must log in before operating the function buttons. The user name and password can be configured by accessing the management blade via the Telnet or Web interface.

table: Blade Server Status

Item	Description
Environment	The status for environmental subsystems (fans, temperature) is displayed. → "Verifying the Blade Server's Environmental Status" (P.121)
Power Supply	The status for power supply subsystems is displayed. → "Verifying the Blade Server's Power Status" (P.122)
RemoteView	The [RemoteConsoleService/Web] window appears. "4.3.4 Start and Exit for RemoteControleService/Web (For ManagementBlade connection)" (→pg.278)
Refresh	Updates the information that is displayed in the window to the most recent information.
Configure	When you select the management blade or switch blade and click [Configure], the configuration window for the blade appears. For details about each blade setting window, refer to the manual for the management blade or switch blade. When the server blade is selected, you cannot select this button.
ServerView	When you select a server blade and click [ServerView], the [Server Management] window appears. For details about the [Server Management] window, see "3.2.2 Verifying the Server Monitoring Items in Detail" (→pg.92). When a management blade or switch blade is selected, this button is disabled.
Help	Displays help for each item.

■ Verifying the Blade Server's Environmental Status

When you click [Environment], the window for environment status appears.



● Server Icon Display

The server icon indicates whether the server door or housing is open or closed. If the server icon is green, it means that the server door or housing is closed. A yellow icon means that it is open.

However, the server door/housing open/closed status indication may not be supported depending on the server model.

● Fan and Temperature Status Display

When you point at a fan icon with the cursor, the name of the fan is displayed. For redundant fans, cascaded fan icons are displayed.

When you click the temperature sensor status icon, the basic threshold for the temperature and the current temperature are displayed in the figure.



- ▶ The basic threshold stored in the server (hardware) is used to determine the status. This is unrelated to the threshold value set in the Performance Manager.

The colors of the fan and temperature sensor icons indicate the following states:

table: Fan and Temperature Status

Item	Shutdown	Danger	OK	Sensor Failure	Cannot Verify
Temperature	Red	Yellow	Green	Blue	Gray
Fan	Red	Yellow	Green	---	Gray

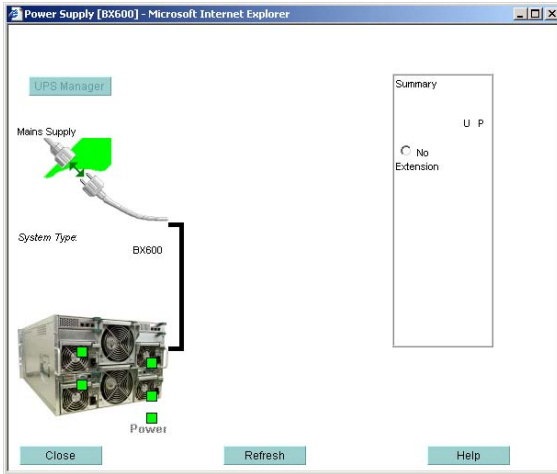
■ Verifying the Blade Server's Power Status

When you click [Power Supply], the window for power status appears.

When you point at the status with the cursor, the name of the Power Supply is displayed.

If the Power Supply operates properly, a green rectangle is displayed on the corresponding Power Supply.

For redundant Power Supply, two cascaded rectangles are displayed.



● Mains Supply

The status of the connection between the server and the Mains Supply is displayed. If any extension storage device is connected to the server, its Mains Supply is also displayed.

A Mains Supply failure for the server and the extension storage devices is indicated with a yellow or red rectangle.

Usually, the power status is updated every 60 seconds.

● System Type

The overall status of the server power supply is indicated with a green, yellow or red rectangle.

3.4 Serious Error Handling (ASR)

ASR (Automatic Server Reconfiguration & Restart) is a function that the server deals with serious problems automatically. The following items can be set.

- Fan error policy
- Overheat error policy
- Server reboot policy
- Boot monitoring (BOOT Watchdog) and Agent monitoring (Software Watchdog) policy
- Scheduling setting for Power ON/OFF

POINT

ASR Examples

- ▶ A server can be specified to automatically shut down when it overheats and automatically restart after a specific period of time (measures at abnormal temperature).
- ▶ It allows the settings for a system to automatically restart when it failed to start successfully, in case of a temporary failure in a SCSI cable or device (boot monitoring settings - measures at the occurrence of faults from system booting till ServerView Agent is activated), for example.

3.4.1 Setting Procedures

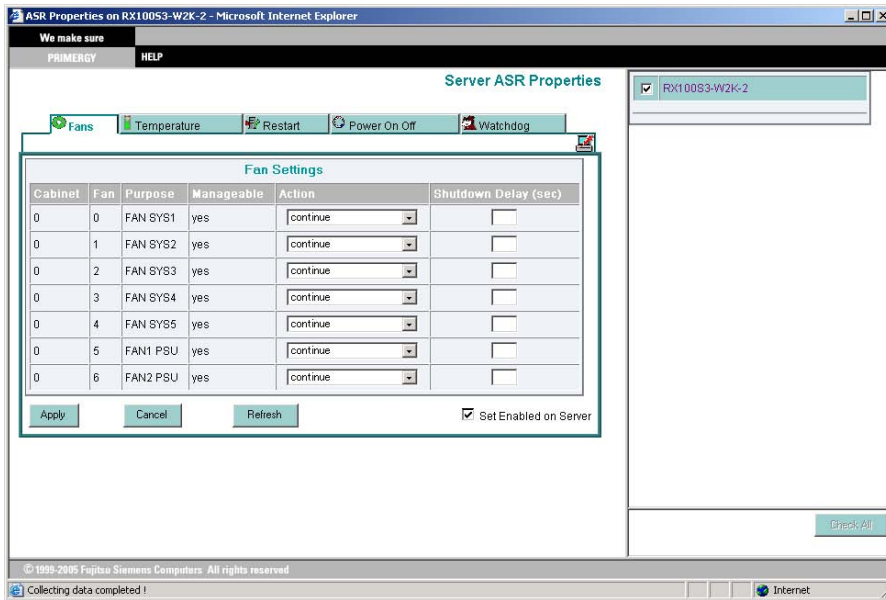
Although the functions are the same between ServerView S2 and Management Console, there are some differences in the item names on the screen. The following describes the screens displayed when operating ServerView S2.

IMPORTANT

- ▶ All settings are not supported in all servers. When one or more fields are certainly set "N/A" for the selected server, these parameters are not supported.
- ▶ The settings of the ASR function are written to BIOS of the server.
The wrong settings may cause the system to fail in starting. Please make sure to specify them carefully.
- ▶ Please make sure that the server may be shut down for any unexpected reason when ServerView is uninstalled with the changed BIOS settings.
- ▶ The status of the fan/temperature sensor becomes abnormal when the value exceeds the basic threshold stored in the server hardware. The basic threshold is independent of the [Threshold] set in the Performanse Manager or Threshold Manager.

- 1 Right-click on the server to specify and click [ASR Properties] within the pop-up menu.

The [ASR Properties] window appears.

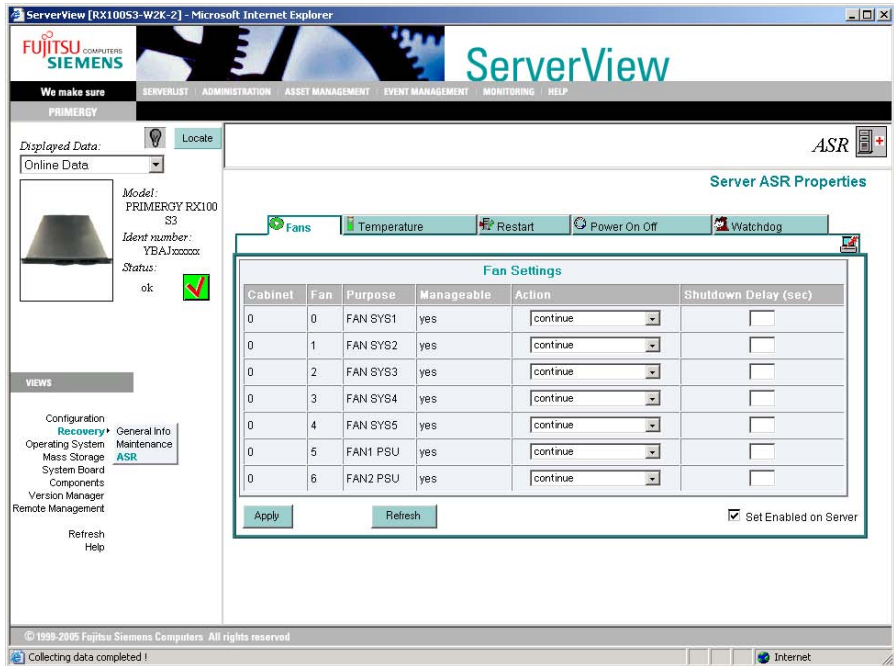


POINT

- ▶ The [Set Enabled on Server] checkbox exists in the lower right corner of the window. When the settings of the server can be modified, this checkbox is selected. When the checkbox is not selected, it indicates that the server cannot be modified.

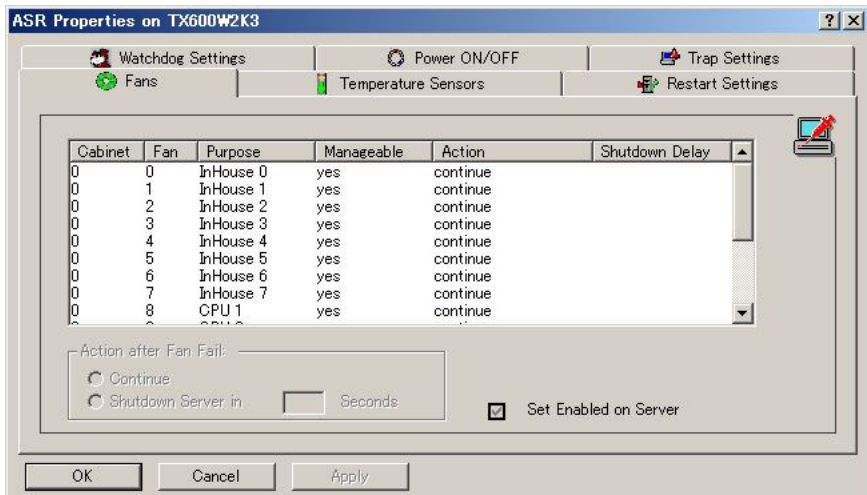
ServerView S2

Clicking [Action] → [ASR] from the server management window of ServerView S2. The following window appears.



Management Console

Right-click the server in management console and click [ASR Properties] from the displayed menu. The following window appears.



2 Click the tab to specify and assign each item.

The tabs include the types below. For details about the items to specify in each tab, refer to the following sections respectively:

- [Fans] tab (→pg.126)
- [Temperature] tab / [Temperature Sensors] tab (→pg.127)
- [Restart] tab / [Restart Settings] tab (→pg.128)
- [Power On Off] tab / [Power ON/OFF] tab (→pg.129)
- [Watchdog] tab / [Watchdog Settings] tab (→pg.129)
- [Trap Settings] tab (→pg.130)

POINT

- ▶ When ASR detects the serious state (CPU error, memory error, and OS hanging) in the server operation status or storage media, the system is restarted and the hardware component with a trouble turns unavailable in restarting.

■ [Fans] Tab (ServerView S2/Management Console)

Specify the measures to perform at fan failure.

Specify [Actions after Fan Fail] for each fan.

table: [Fans] Tab

Item	Description
Continue	The server continues to run after fan failure detection.
Shutdown server in _seconds	The server shuts down after a specific delay. Specify the delay in second.

IMPORTANT

- ▶ When any of the expansion disk devices are connected, [Shut down server in _seconds] may be selected in the fan information within the expansion disk that is shown. In this case, the system cannot automatically shut down.

■ [Temperature] Tab (ServerView S2) / [Temperature Sensors] Tab (Management Console)

Specifies the measures at abnormally high temperature.

Specify [Action] for each temperature sensor monitored.

Cabinet	Sensor Number	Purpose	Action
0	0	Systemboard	continue
0	1	CPU	continue
0	2	Ambient	continue
0	3	PSU	continue

Apply Cancel Refresh Set Enabled on Server

table: [Temperature Sensors] Tab

Item	Description
Continue	The server continues to run after abnormal high temperature detection.
Shut down the server now	The server shuts down immediately when temperature reaches the critical value.



- ▶ When any expansion disk devices are connected, [Shut down the server now] may be selected in the temperature sensor information within the expansion disk that is shown. In this case, the system cannot automatically shut down.

■ [Restart] Tab (ServerView S2) / [Restart Settings] Tab (Management Console)

Specify the operation after power failure and for server restarting.

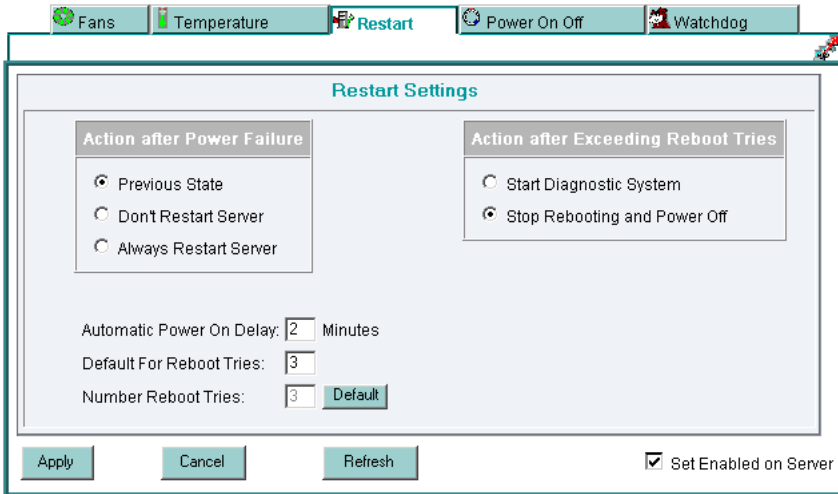


table: [Restart Settings] Tab

Item	Description
Action after Power Failure	Select one of the following items to set restart action after power failure. <ul style="list-style-type: none"> • Previous State • Don't Restart Server • Always Restart Server
Actions after Exceeding Reboot Tries	[Stop Rebooting and Power Off] is selected for handling at the time when the maximum retry number is exceeded. [Start Diagnostic System] is not supported.
Automatic Power On Delay	Specify 1 to 30 minutes.
Default For Reboot Tries	Specify 0 to 7.
Number Reboot Tries	Current number of retry is displayed. If you click [Default], the value specified in [Default Number of Retry to Restart] is assigned.



- ▶ Do not select the [Start the diagnosis system] item in [Actions at Excess of Retry Number to Restart].

■ [Power On Off] Tab (ServerView S2) / [Power ON/OFF] Tab (Management Console)

This allows you to specify the server starting time/exiting time for each day.

For example, you can shut down a server on weekends and restart it on Monday. However it may not be specified depending on the server machine types.

Weekday	OnTime		OffTime	
	Enabled	Time	Enabled	Time
Sunday	<input checked="" type="checkbox"/>	23 : 59 hh:mm	<input checked="" type="checkbox"/>	02 : 00 hh:mm
Monday	<input type="checkbox"/>	: hh:mm	<input type="checkbox"/>	: hh:mm
Tuesday	<input type="checkbox"/>	: hh:mm	<input type="checkbox"/>	: hh:mm
Wednesday	<input type="checkbox"/>	: hh:mm	<input type="checkbox"/>	: hh:mm
Thursday	<input type="checkbox"/>	: hh:mm	<input type="checkbox"/>	: hh:mm
Friday	<input type="checkbox"/>	: hh:mm	<input type="checkbox"/>	: hh:mm
Saturday	<input type="checkbox"/>	: hh:mm	<input type="checkbox"/>	: hh:mm

Shutdown allowed on Server
 Set Enabled on Server

IMPORTANT

- ▶ The settings are written to BIOS of the scheduled server. Make sure to disable scheduling before ServerView is uninstalled from the server.

When ServerView is uninstalled with the scheduling enabled, the server may be shut down at an unexpected time.

■ [Watchdog] Tab (ServerView S2) / [Watchdog Settings] Tab (Management Console)

Specify Software Watchdog monitoring and Boot Watchdog monitoring. You can set the functions whose [Manageable] is "yes".

Type	Active	Manageable	Action	Timeout (min)
Software	<input checked="" type="checkbox"/>	yes	Power Cycle	1
Boot	<input type="checkbox"/>	yes	System Reset	1

Set Enabled on Server

● Software Watchdog (Agent monitoring)

Software Watchdog monitors the status of ServerView Agent.

When the interval without response from ServerView Agent exceeds the specified timeout period, the designated action is executed.

To enable the monitoring with Software Watchdog, check [Active] of the [Software] item and assign the waiting time till timeout in [Timeout(min)] to 1 to 120 minutes.

Also, select the [Action] at the time when the waiting time exceeds from the following items:

- Continue to run
- Restart
- Power off/on

POINT

- ▶ If you stop ServerView Agent manually for any reason or if you uninstall ServerView, this setting needs to be released.

● BOOT Watchdog (Boot monitoring)

Boot Watchdog monitors the server's boot phase. When the interval between the server power-on and the normal response from ServerView Agent exceeds the specified timeout period, the designated action is executed.

To enable the monitoring with BOOT Watchdog, check [Active] of the [BOOT] item and assign the waiting time till timeout in [Timeout(min)] to 1 to 120 minutes.

Also, select the [Action] at the time when the waiting time exceeds from the following items:

- Continue to run
- Restart
- Power off/on

POINT

- ▶ Before configuring this setting, you need to know how long it usually takes for the system to finish the boot process.

■ [Trap Settings] Tab (Management Console only)

This allows traps to be set to enabled/disabled for the specified server. For the enabled trap, when a server detects some errors in the system and any trap is defined for this error, the trap is sent from the server to the management console. The disabled trap is not sent.

IMPORTANT

- ▶ Traps are listed in this tab only when the monitored server runs Windows.

3.5 AlarmService

The AlarmService receives alarms (SNMP traps) that are transmitted when ServerView Agent detects exceptional states, and notifies the administrator in real time in the predefined manner.

The AlarmService consists of the [Alarm Monitor], [Alarm Manager], and [Alarm Actions (settings)] functions.

■ Alarms

ServerView Agent transmits an alarm to ServerView S2 for each server event. Alarms vary widely from "a critical impact on server operation" to "mere server information".

For each alarm, the severity is used as a management criterion. The object of this function is to promptly respond to events significant for the server management without overlooking any such events. Here are some examples:

- When a predefined event occurs, a message automatically pops up or is sent by mail to notify the administrator, and let the administrator respond to the event.
- When a predefined event occurs, the specified program is automatically executed on the server.

The AlarmService receives SNMP traps from the server monitoring program or the OS. The corresponding data can be stored in the event log, displayed as a pop-up message, or forwarded to another server or client. By configuring the various functions of the AlarmService, the program can notify the system administrator in an efficient way when exceptional events occur.

■ Starting the AlarmService

- 1 Start the Web browser.
- 2 Enter one of the following URLs and press the [Enter] key.

When IIS or Linux is used

`http://<server name or server IP address>/AlarmService.htm`

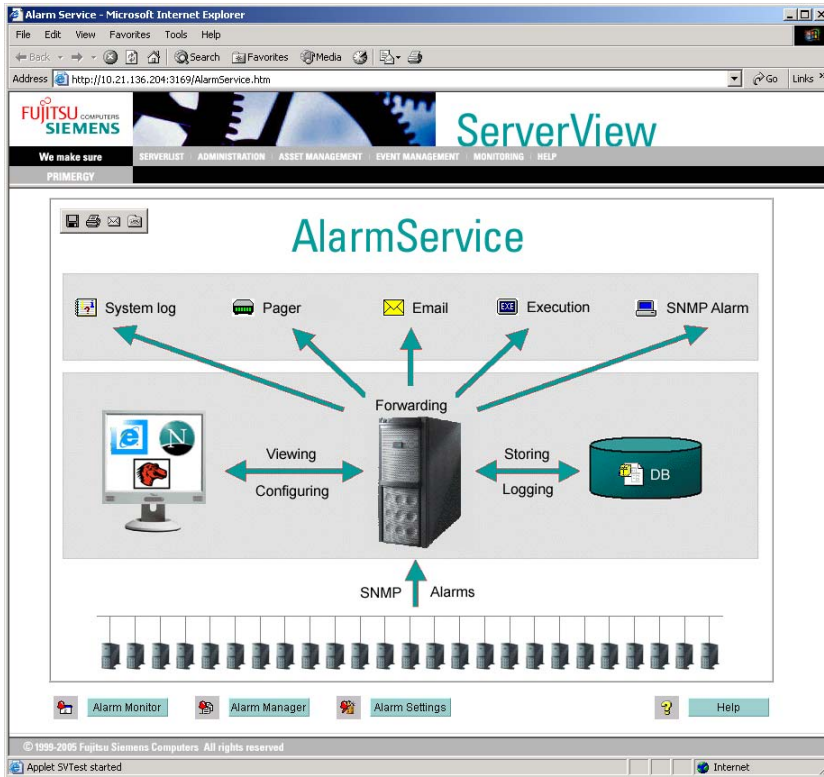
When using ServerView Web-Server (normal connection)

`http://<server name or server IP address>:3169/AlarmService.htm`

When using ServerView Web-Server (SSL connection)

`https://<server name or server IP address>:3170/AlarmService.htm`

The window of AlarmService appears.



3.5.1 Alarm Monitor

The alarm monitor displays received alarms (SNMP traps) in the order of reception.

- 1 Click [EVENT MANAGEMENT] → [ALARM MONITOR] from the ServerView S2 menu.

When starting the alarm monitor from Management Console

Click the [Alarm] menu → [Monitor].

If ServerView is not running

Click the [Start] button → [Programs] → [Fujitsu ServerView] → [Alarm Service] to display the [Alarm Service] window. Then, click [EVENT MANAGEMENT] → [ALARM MONITOR].

The [Alarm Monitor] window appears.

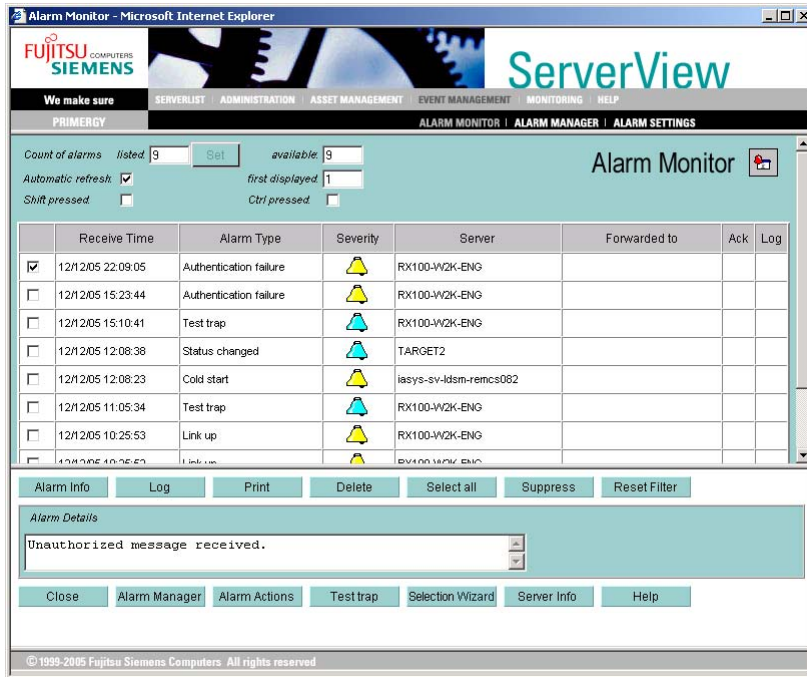


table: Description of the Alarm Monitor Window






Item	Description
Count of alarms	The number of alarms listed in the alarm monitor window is displayed. You can click [Set] to specify the number of alarms listed in each page. The default number is "30" and the minimum number is "10". If "all" is selected, all received alarms are displayed.
available	The number of alarms that Alarm Monitor has received is displayed.
Automatic refresh	When this option is checked, the alarm monitor window is automatically updated when a new alarm is received. If not checked, the window will not be updated automatically. Only the [available] value is updated.
Shift Pressed	Select this checkbox when you want to select a range of alarms. Perform the following procedure: Click the start of the range, check [Shift Pressed], and then click the end of the range.
Ctrl Pressed	When this option is checked, multiple alarms can be selected.
Receive Time	The time when the alarm was received is displayed.
Alarm Type	The type of alarm is displayed.
Severity	The severity of the alarm is indicated with the alarm reception icons below.  (Red): Danger  (Pink): High level  (Yellow): Low level  (Blue): Information  (White): Unknown
Server	The server name is displayed.
Forwarded to	The action at the time when the alarm is received is displayed. Actions are specified in the [Set / Edit Destination] window within [ALARM SETTINGS].

table: Description of the Alarm Monitor Window

Item	Description
Ack	When an alarm is accepted, an icon is displayed.
Log	When an alarm is logged into Alarm Manager, an icon is displayed.
Alarm Details	A detailed message for the selected alarm is displayed.

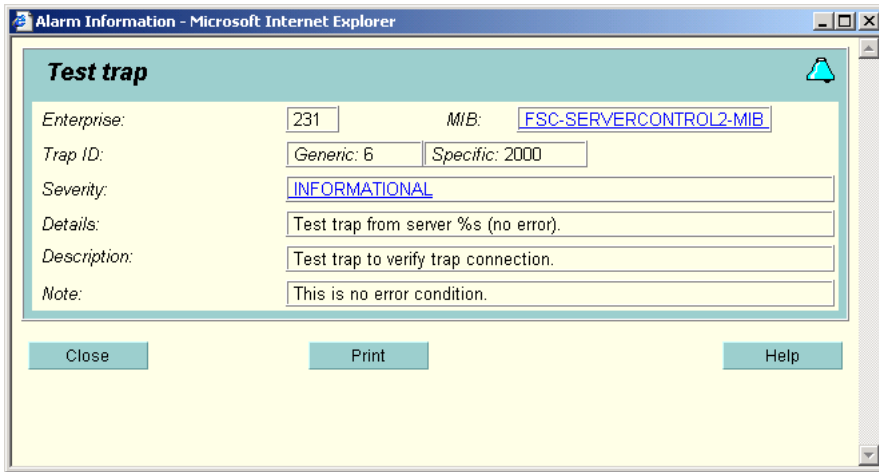
2 After checking the target alarm, select an operation among the following:

table: Alarm Operations

Function Button	Description
Alarm Info	Displays detailed information about the alarm. For details, see "■ The [Alarm Info] Button" (→pg.135).
Log	The selected alarm is logged into Alarm Manager. For details, see "■ The [Log] Button" (→pg.135).
Print	Prints the selected alarm.
Delete	Deletes the selected alarm from the alarm list.
Select All	Selects all alarms.
Suppress	Suppresses the selected alarm from the server. The alarm selected for exclusion is deleted from the list and incoming alarms are not added to the list. This function is useful when there is a server that does not work properly and the list overflows with alarms. For details, see "■ The [Suppress] Button/[Reset Filter] Button" (→pg.135).
Reset Filter	The excluded alarms are listed. It is also possible to release excluded alarms. For details, see "■ The [Suppress] Button/[Reset Filter] Button" (→pg.135)..
Alarm Manager	Starts the alarm manager. For details, see "3.5.2 Alarm Manager" (→pg.139).
Close	Closes the [Alarm Monitor] window.
Alarm Actions	The [Overall Settings] window appears. In this window you can edit the alarm actions. For details, see "3.5.3 Alarm Settings" (→pg.142).
Test trap	Tests transmission of traps. For details, see "■ The [Test trap] Button" (→pg.136).
Selection Wizard	When the same alarm monitor manages the alarms from multiple servers, this wizard is used to set the extraction conditions for alarms to verify/select among a large volume of alarms. For details, see "■ The [Selection Wizard] Button" (→pg.138).
Server Info	Displays an information window for the selected server where you can verify the server information.
Help	Displays help for the alarm monitor.



■ The [Alarm Info] Button

When you select an alarm from the list and click [Alarm Info], the [Alarm Information] window appears. This window lists the Alarm names, Enterprise, MIB, Trap ID, Severity, Note, and Details. The MIB field is linked to the Severity field, and these fields show "the alarms listed of the MIB" and "the Help of severity" respectively.



■ The [Log] Button

When you select an alarm from the list and click [Log], the alarm is added to the [Alarm Manager] regardless of its severity. (With the default settings, only alarms with the severity "Danger" are automatically added to the [Alarm Manager].)

For alarms that have been added to the [Alarm Manager], the  icon is displayed in the [Log] field. If alarms are accepted using the [Ack Alarm] button in the [Alarm Manager], the  icon is added. The [Ack Alarm] icon also appears in the [Ack] field of the [Alarm Monitor].

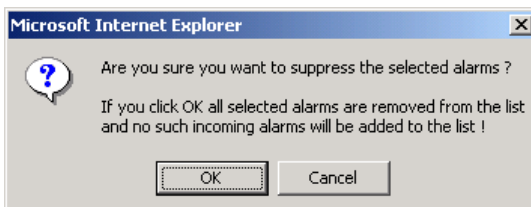
POINT

- ▶ Logging and acceptance of alarms is assumed to be performed as follows:
The administrator needs to make some sort of response to the alarm that is logged into Alarm Manager. The administrator "accepts" the alarm in acknowledgment of the response. The acceptance is also reflected in the Alarm Monitor to avoid duplicate responses.

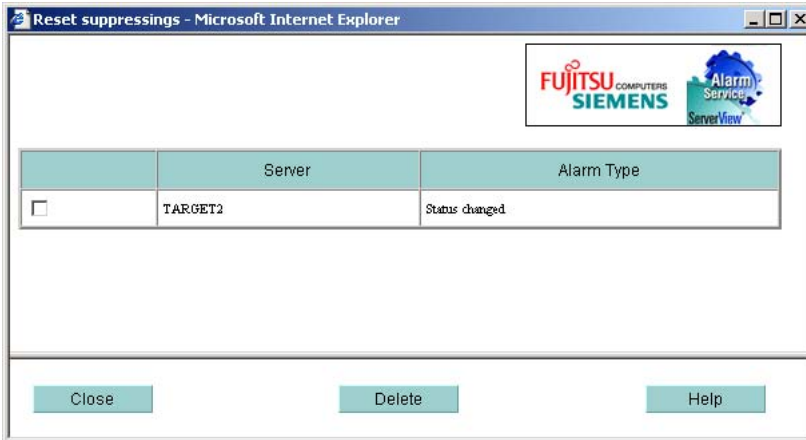
■ The [Suppress] Button/[Reset Filter] Button

When you select an alarm from the list and click [Suppress], the confirmation window for deleting the selected alarm is displayed.

When you click [OK], the selected alarm is excluded from the [Alarm Monitor].



The excluded alarms (of the same type from the same server) are deleted from the list and further alarms of the same kind will be not added to the list until the exclusion is released. This function is useful when there is a server that does not work properly and the list overflows with alarms. The excluded alarms are registered in the [Reset Filter] as follows. The [Reset Filter] is displayed by clicking [Reset Filter].



The excluded alarms are managed according to the [Server] and the [Alarm Type]. Alarms matching these two criteria are deleted from the [Alarm Monitor], and subsequent matching alarms will also not be displayed. By selecting an alarm from the [Reset Filter] and clicking [Delete], the exclusion of that alarm is released.

POINT

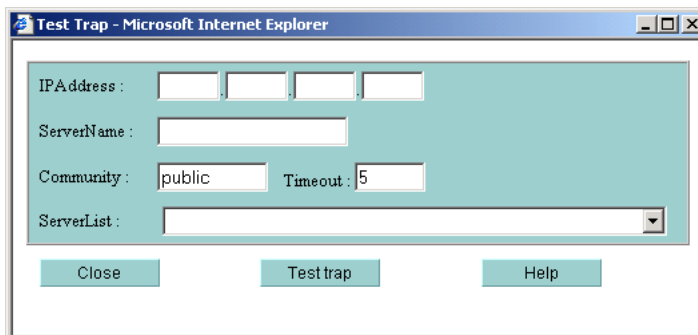
- ▶ When the server is starting up, a RAID manager, an Ethernet card, etc. may issue an alarm (SNMP trap) as the start-up notification (e.g. RFC1157LinkUP). To suppress this kind of alarms, configure the alarm exclusion. This blocking function must be specified for each server. If multiple servers are monitored, configure this setting for each server using the alarm function.

■ The [Test trap] Button

Sends a test trap to the server to confirm whether alarms from the server are sent and received properly.

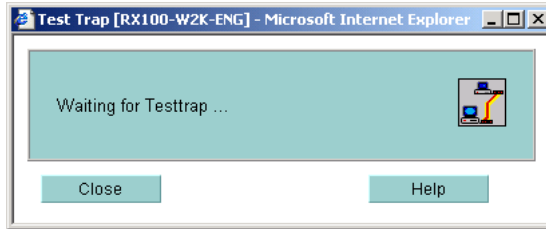
1 Click [Test trap].

The [Test trap] window appears.



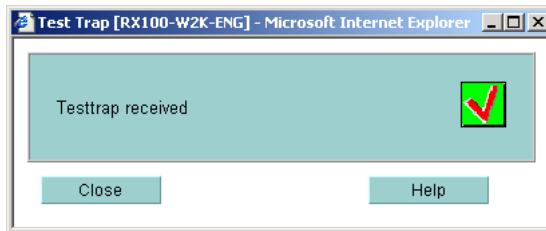
- 2 Select a server from the [Server List] or enter the server's IP address to execute the test trap.

The test trap is executed and the following window appears.



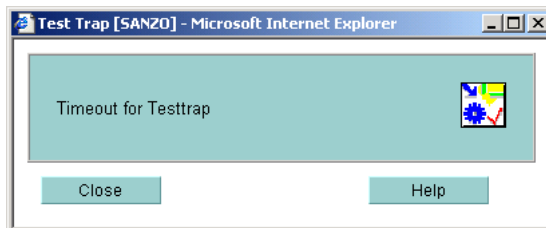
If the transmission/reception succeeds

If the test trap is sent and received successfully, the following information is displayed:



If the transmission/reception fails

If for some reason the test trap is not sent or received successfully, the following information is displayed:

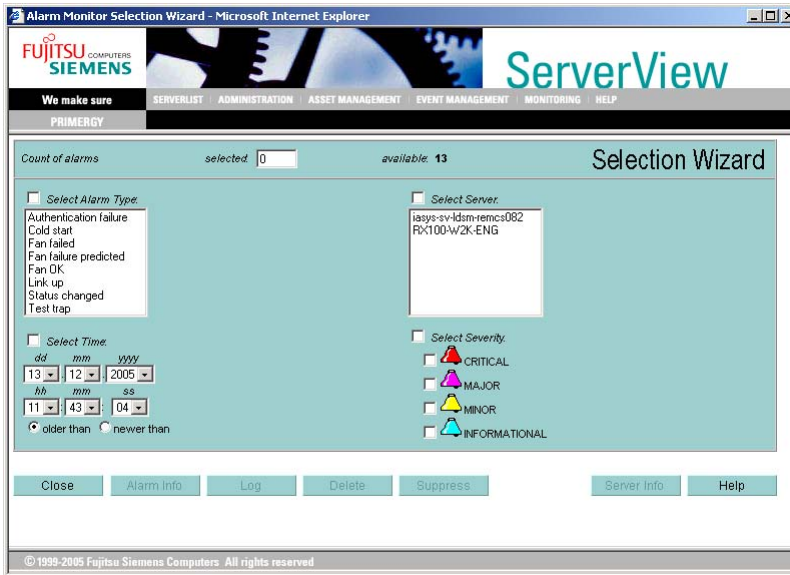


If the transmission/reception is unsuccessful, check the following points:

- Does the SNMP community name among the server-side SNMP settings (the SNMP service properties for Windows, or /etc/snmp/snmpd.conf for Linux) match the name among the console-side settings (ServerView S2)?
- Is the console-side IP address (or DNS name) specified as destination among the server-side SNMP settings?
- Do the console-side SNMP settings allow reception from the server-side IP address?

■ The [Selection Wizard] Button

When the same alarm monitor manages the alarms from multiple servers, this wizard is useful for searching for alarms to verify/select among a large volume of alarms.



Alarms are extracted using a combination of four criteria; alarm type, time, server, and alarm Severity. The number of alarms matching these factors is displayed in [selected]. For the selected alarms, you can use the function buttons [Alarm Info], [Log], [Delete], and [Suppress].

3.5.2 Alarm Manager

You can edit and manage alarms.

- 1 Click [EVENT MANAGEMENT] → [ALARM MANAGER] on the ServerView S2 menu.

When starting from the Management Console

Click the [Alarm] menu → [Manager].

If ServerView is not running

Click the [Start] button → [Programs] → [Fujitsu ServerView] → [Alarm Service] to display the [Alarm Service] window. Then, click [EVENT MANAGEMENT] → [ALARM MANAGER].

The [Alarm Manager] window appears.

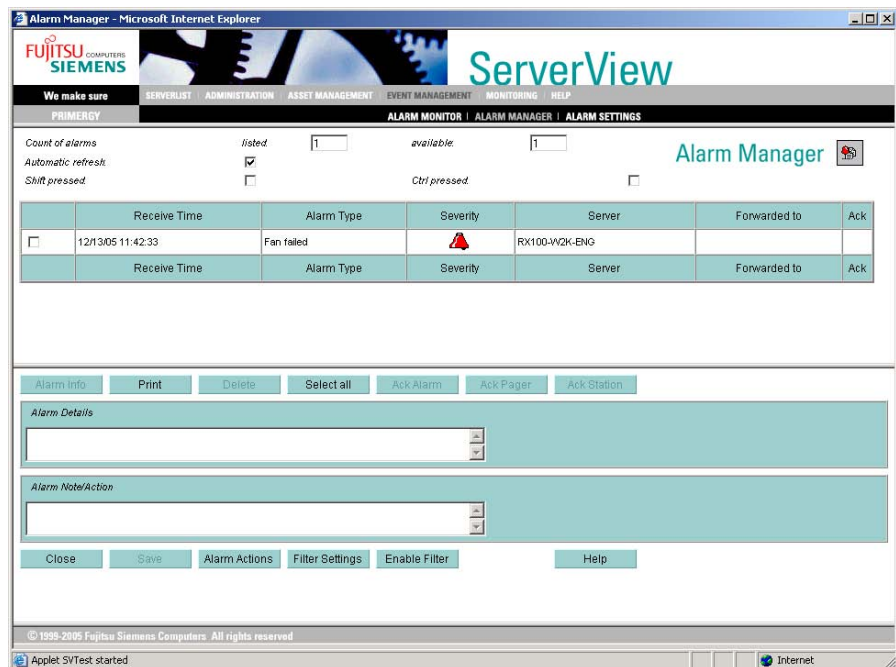







table: Description of the Alarm Manager Window

Item	Description
Count of alarms listed	The number of alarms listed in the alarm manager window is displayed.
available	The number of alarms that are recorded in the alarm log database is displayed.
Automatic refresh	When this item is checked, the alarm manager window is automatically updated when a new alarm is received. Otherwise the window is not automatically updated. Only the [available] value is updated.
Shift Pressed	This item is used to select a range of alarms. Click the start of the range, check [Shift Pressed], and then click the end of the range.
Ctrl Pressed	When this is checked, multiple alarms can be selected.
Receive Time	The time when the alarm was received is displayed.
AlarmType	The type of alarm is displayed.
Severity	The severity of the alarm is indicated with the alarm reception icons below.  (Red): Danger  (Pink): High level  (Yellow): Low level  (Blue): Information  (White): Unknown
Server	The server name is displayed.
Forwarded to	The action taken when the alarm was received is displayed. Actions are specified in the [Set / Edit Destination] window within [ALARM SETTINGS].
Ack	When an alarm is accepted, an icon is displayed.
Alarm Details	A detailed message for the selected alarm is displayed.
Alarm Note/Action	Here you can enter an explanatory note, such as details of the selected alarm.

2 After checking the target alarm, select an operation among the following:

table: Alarm Operations

Function Button	Description
Alarm Info	Displays details about the alarm(s).
Print	Prints the selected alarm(s).
Delete	Deletes all selected alarms among the accepted alarms.
Select All	Selects all the alarms.
Ack Alarm	Accepts the selected alarm(s). When an alarm is accepted, the acceptance icon is displayed in the alarm list.
Ack Pager	Not supported.
Ack Station	Accepts the selected station transfer action. When the action is accepted, the acceptance icon is displayed in the alarm list.
Save	Saves the information entered in the [Alarm Note/Action] field.
Alarm Actions	The [Overall Settings] window appears where you can verify/change the alarm settings.

table: Alarm Operations

Function Button	Description
Filter settings	You can filter the alarms to be displayed for convenience of management. For details, see 「The [Filter settings] Button」 (→ P.141) .
Enable Filter	Enables/disables the alarm filtering settings.
Help	Displays the help for the alarm manager.
Close	Closes the [Alarm Manager] window.

■ The [Filter settings] Button

Clicking [Filter settings] opens the following [Setup Alarm Filter] window.

You can define the Filter settings using a combination of five factors: server, alarm severity, action execution status, time, and station forwarding.

3.5.3 Alarm Settings

Here you can configure the general settings for alarms, such as creating/editing the "alarm group" and "alarm action".



- ▶ When configuring the alarm settings for a blade server, each individual blade needs to be registered as a unique server in the server list.

■ Starting the Alarm Settings

- 1 Click [EVENT MANAGEMENT] → [ALARM SETTINGS] on the ServerView S2 menu.

When starting from Management Console

Click the [Alarm] menu → [Settings].

If ServerView is not running

Click the [Start] button → [Programs] → [Fujitsu ServerView] → [Alarm Service] to display the [Alarm Service] window. Then, click [EVENT MANAGEMENT] → [ALARM SETTINGS]. The [Start Alarm Settings] window appears.



2 Configure the Alarm Settings.

The [ALARM SETTINGS] consists of five settings: "■ Overall Settings" (→pg.143), "■ Filter Server" (→pg.147), "■ Edit / New Alarmgroup" (→pg.147), "■ Set / Edit Destination" (→pg.150), and "■ Overview" (→pg.163).

When you use the wizard, the pages for the five settings are shown in turn.

You can also go to each settings page directly by selecting the name of the settings from [Go directly to] and clicking [Next]. Each page has the following function buttons:

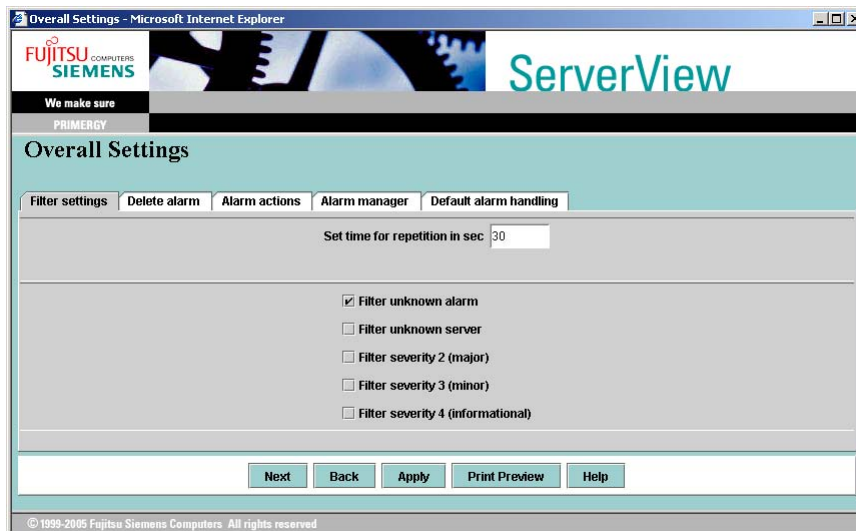
table: Description of the Buttons

Button	Description
Next	Moves to the next settings page. If the settings of the current page have not been applied, a warning message is displayed.
Back	Moves back to the previous settings page. If the settings of the current page have not been applied, a warning message is displayed.
Apply	Applies the settings of the current page.
Delete	Deletes the alarm group or action.
Finish	Exits the configuration and goes back to the initial page of the Alarm Settings. If the settings of the current page have not been applied, a warning message is displayed. Click [Finish] on the initial page to exit the Alarm Settings.
Print Preview	Displays the Print Preview window.
Help	Displays the help for the Alarm Settings.

■ Overall Settings

The [Overall Settings] window has five tabs: [Filter settings], [Delete alarm], [Alarm actions], [Alarm manager], and [Default alarm handling].

● The [Filter settings] Tab



Configures the filter for Filter settings to be received.

table: Description of Each Item

Item	Description
Set time for repetition in sec	The purpose of this filter is to suppress "the same kind of alarms rushing in". This filter is effective when the same kind of alarms are sent from the same server multiple times and the interval between them is equal to or shorter than the value set here. The lower the severity is, the longer the interval becomes: the Set time for repetition in sec for each severity level = the set value for "the Set time for repetition in sec" x "the Severity". The value "0" means unlimited (no interval filtering).
Filter unknown alarm	If this is checked, unknown alarms cannot pass through the filter.
Filter unknown server	If this is checked, alarms from unknown servers cannot pass through the filter.
Filter severity 2 (major)	If this is checked, alarms with severity 2 cannot pass through the filter.
Filter severity 3 (minor)	If this is checked, alarms with severity 3 cannot pass through the filter.
Filter severity 4 (informational)	If this is checked, alarms with severity 4 cannot pass through the filter.

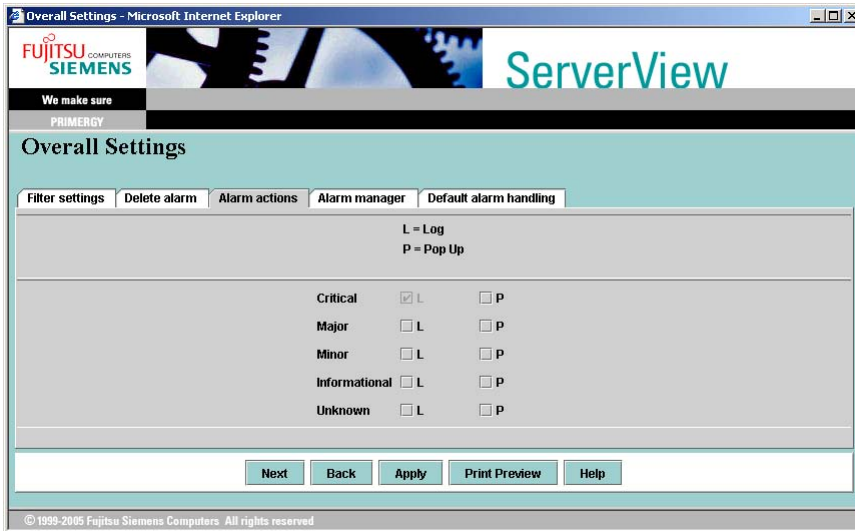
● The [Delete alarm] Tab



Alarms that exceed the specified limit are deleted.

If the set number of days has passed after alarms were logged or if the number of entries reaches the specified number, the alarms are deleted in order from the oldest entry.

● The [Alarm actions] Tab



Specifies the action to be executed when receiving an alarm.

In [Overall Settings], [Log] and [Pop Up] can be set as the action for each alarm severity. Each time an alarm is received, its severity is determined and the corresponding action is executed.

table: Description of Each Item

Item	Description
Log	Logs the entry in the alarm log database (alarm manager).
Pop Up	Automatically makes the [Alarm Monitor] window the active window.

● The [Alarm manager] Tab

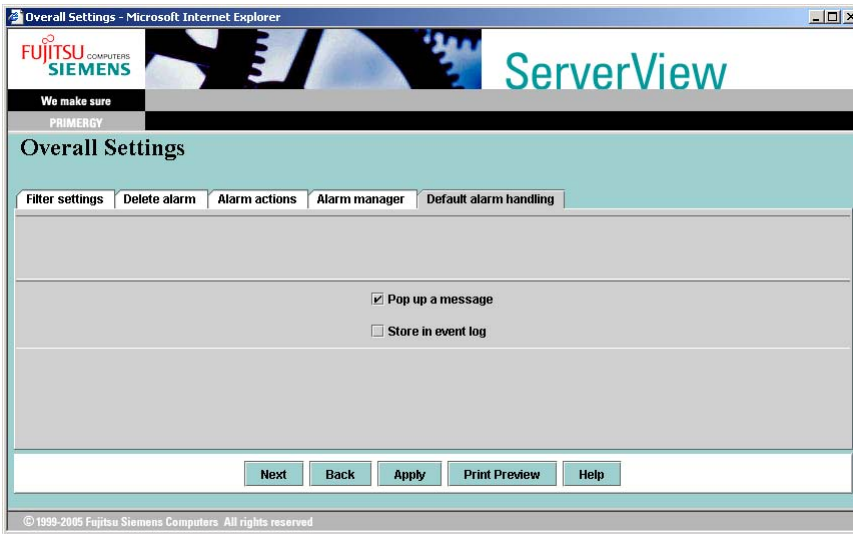


Configures the alarm log database (= Alarm manager).

Table: Alarm Manager

Item	Description
Maximum number of log entries	Specifies the maximum number of logs to be stored.
Action on exceed	Specifies the action when the number of logged entries exceeds the [Maximum number of log entries]. <ul style="list-style-type: none"> • Pop up warning Displays a message to warn the user. • Wrap around Deletes the entries from the oldest one.

● The [Default alarm handling] Tab



Configures the default action. The action is always executed when an alarm is issued, regardless of the settings for the alarm group.

table: Description of Each Item

Item	Description
Pop up a message	Displays all the alarms as pop-up messages.
Store in event log	Forwards all alarms to the event log.

■ Filter Server

The [Filter Server] window appears.



Excludes alarms from certain servers/groups.

The alarms from the excluded servers are not displayed. The [All Servers] and [Groups] items on the left side are the same as the ones in the [Server list] window. On the right side, the servers from which alarms are excluded are displayed.

To add servers to be excluded, select target servers from the left hand side list and click [>>>]. To remove excluded servers, select target servers from the right hand side list and click [<<<]. By clicking [Info], you can confirm the information for each server.

■ Edit / New Alarmgroup

You can create, edit, or delete alarm groups.

● Alarm Group

An alarm group is a set of alarms, defined by the server and kind of the alarm. An "action" can be set for each alarm group. Using the combination of the "alarm group" and the "action", a "predefined action" can be executed automatically when a "predefined alarm" is sent from the "predefined server".

● Creating an Alarm Group

- 1 Enter an alarm group name and click [Apply].

In the example below, the group is called "test".



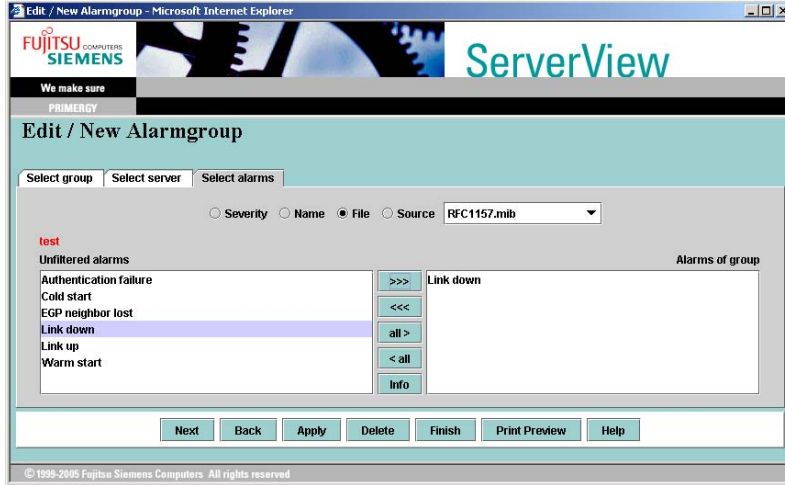
- 2 Click the [Select server] tab and select a server to be added to the alarm group.

In the example below, "TESTSERVER" is selected.



- 3 Click the [Select alarms] tab and select an alarm to be added to the alarm group.

For example, to add the alarm "LinkDown" included in the MIB file "RFC1157.Mib", click [File], select [RFC1157.Mib] from the combo box, select [LinkDown], and click [>>>].



- 4 Click [Apply].

The alarm group is created.

The alarm group "test", which was created in this example, contains only the alarm "LinkDown" from the server "TESTSERVER".

POINT

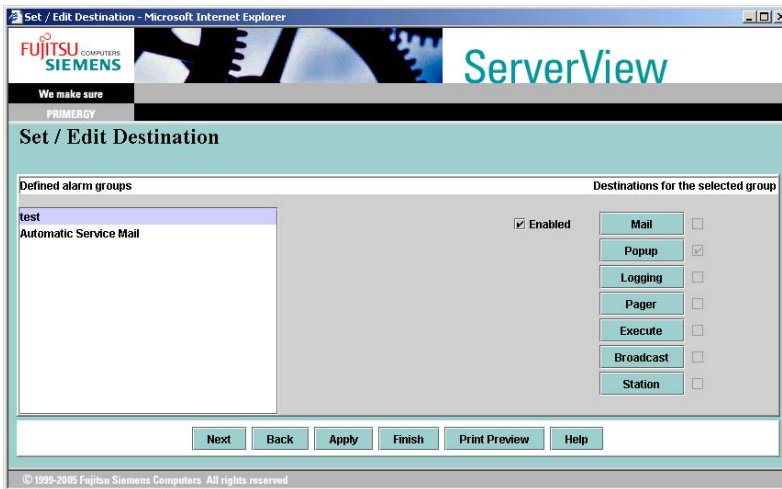
- ▶ To delete an alarm group, perform the following procedure:
 1. Select an alarm group from listbox.
 2. Click [Delete].

IMPORTANT

- ▶ If you change the IP address or host name for a monitored server that belongs to an alarm group, changes of the server are not reflected to the alarm group. Edit the alarm group first, and then register the server again.
- ▶ The alarm group "Automatic Service Mail", which is created by default, cannot be used. Please create a new alarm group.

■ Set / Edit Destination

The [Set / Edit Destination] window is displayed where you can configure the action for the alarm group.



On the left side, the existing alarm groups are listed.

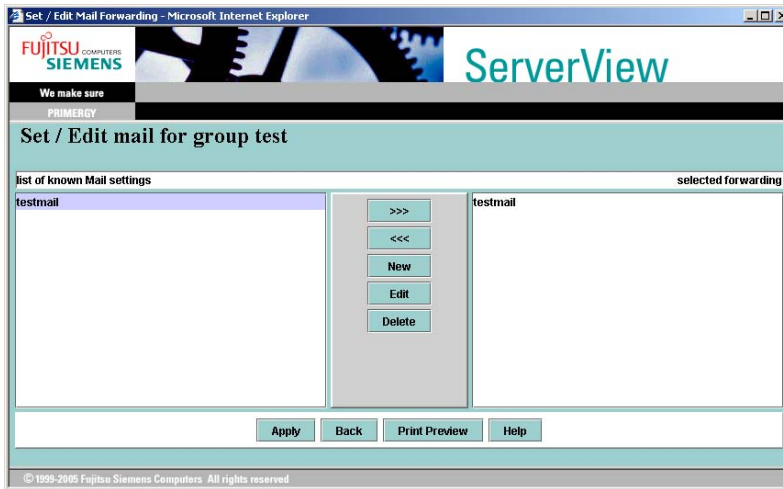
You can set an action for the selected alarm group by clicking an action setting button on the right side.

The following actions can be set:

- Send an e-mail →pg.151
- Display a message →pg.154
- Write in the log →pg.156
- Execute a command →pg.157
- Broadcast a notification →pg.159
- Send to the station →pg.161

- **Mail**

When you click [Mail], the [Set / Edit mail for group test] window appears.



The existing mail settings are displayed in the list. In the initial settings, no mail settings are registered. Create a new setting.

If you have made any changes, do not forget to click [Apply]. When you click [Back], the display returns to the [Set / Edit Destination] window.

Applying the Mail Settings

Select the name of a setting from the [list of known Mail settings] list to the left and click [>>>]. The setting appears in the [selected forwarding] list to the right.

To release a setting, select the name of the setting from the [selected forwarding] list to the right and click [<<<].

Modifying Settings

Select the name of the setting you want to modify from the [list of known Mail settings] list to the left and click [Edit]. Modify the settings as required. The window for changing the settings is the same as the one for creating new settings. See "Creating New Mail Settings" (→pg.152).

Removing Settings

Select the name of the setting you want to remove from the [list of known Mail settings] list to the left and click [Delete].

Creating New Mail Settings

1 Click [New].


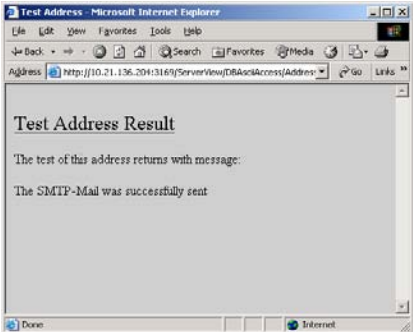
The [Mail Settings] window appears.

2 Configure each of the items.

table: [Mail Settings] Window

Item	Description
Description	Enter the name of the mail settings.
Subject	Enter the subject for the outgoing mail.
Mail to	Enter the destination address of the mail.
Cc	Enter the CC address of the mail.
Time Model	Select the time to execute the action from the predefined Time Model. Click [TM Setting] to configure the Time Model.
Additional Message	Enter additional text for the mail message. The following macros can be used to add the server information. \$_SRV : server name \$_TRP : trap text \$_IPA : IP address of the server \$_IPX : IPX address of the server \$_CTY : server community \$_SEV : trap severity (critical, major, minor, informational, unknown)
[SMTP] button	If this button is clicked, the caption changes to "MAPI", but MAPI mail is not supported. Do not change this setting. Keep the setting as "SMTP".

table: [Mail Settings] Window

Item	Description
[Properties] button	<p>The [Mail Properties (SMTP)] window appears.</p>  <p>Configure [From], [SMTP Server] and [Port], and click [OK].</p>
[Test Address] button	<p>This button becomes enabled if you click the [Properties] and configure the SMTP server settings. Click this button to test whether mails can be sent properly. The following message appears when a mail is sent properly.</p> 
[TM Setting] button	<p>Set the time to execute the action. Clicking [TM Setting] displays the [TM Setting] window. The timetable for the week is displayed, and the time to execute the action is displayed in black. The Time Models [always] and [never] cannot be removed or changed.</p>

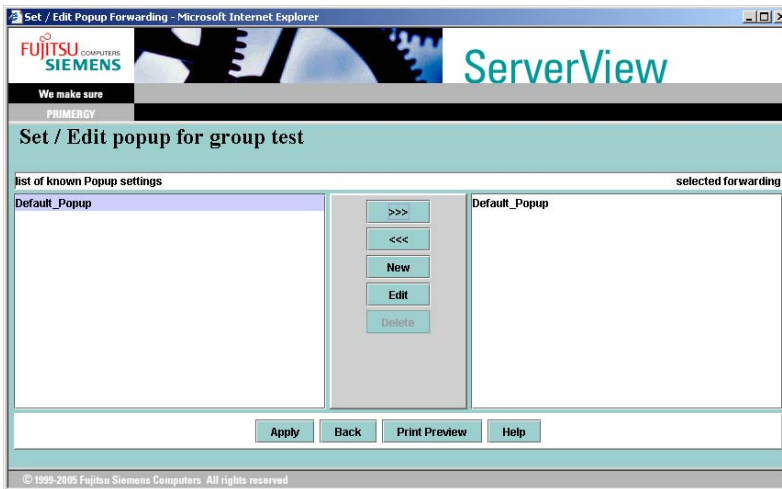
3 Confirm the settings, and click [OK].

The display returns to the [Set / Edit mail for group test] window.

The newly created mail setting is displayed in the [list of known Mail settings].

● Popup

When you click [Popup], the [Set / Edit popup for group test] window appears.



The existing pop-up settings are displayed in the list. If you have made any changes, do not forget to click [Apply]. When you click [Back], the display returns to the [Set / Edit Destination] window.

Applying the Pop-up Settings

Select the name of a setting from the [list of known Popup settings] list to the left and click [>>>]. The setting appears in the [selected forwarding] list to the right.

To release a setting, select the name of the setting from the [selected forwarding] list to the right and click [<<<].

Modifying Settings

Select the name of the setting you want to modify from the [list of known Popup settings] list to the left and click [Edit]. Modify the settings as required. The window for changing the settings is the same as the one for creating new settings. See "Creating New Pop-up Settings" (→pg.155).

Removing Settings

Select the name of the setting you want to remove from the [list of known Popup settings] list to the left and click [Delete].

Creating New Pop-up Settings

1 Click [New].

The [Popup Settings] window appears.

2 Configure each of the items.

table: [Popup Settings] Window

Item	Description
Description	Enter the name of the pop-up setting.
Time Model	Select the time to execute the action from the predefined Time Model. Click [TM Setting] to configure the Time Model.
Additional Message	Enter additional text for the pop-up message.
[TM Setting] button	Set the time to execute the action. Clicking [TM Setting] displays the [TM Setting] window. The timetable for the week is displayed, and the time to execute the action is displayed in black. The Time Models [always] and [never] cannot be removed or changed.

3 Confirm the settings, and click [OK].

The display returns to the [Set / Edit popup for group test] window.

The newly created pop-up setting is displayed in the [list of known Popup settings].

● Logging

When you click [Logging], the [Set / Edit Logging for group test] window appears.



The existing logging settings are displayed in the list. If you have made any changes, do not forget to click [Apply]. When you click [Back], the display returns to the [Set / Edit Destination] window.

You cannot create new logging settings. It is only possible to apply the existing settings.

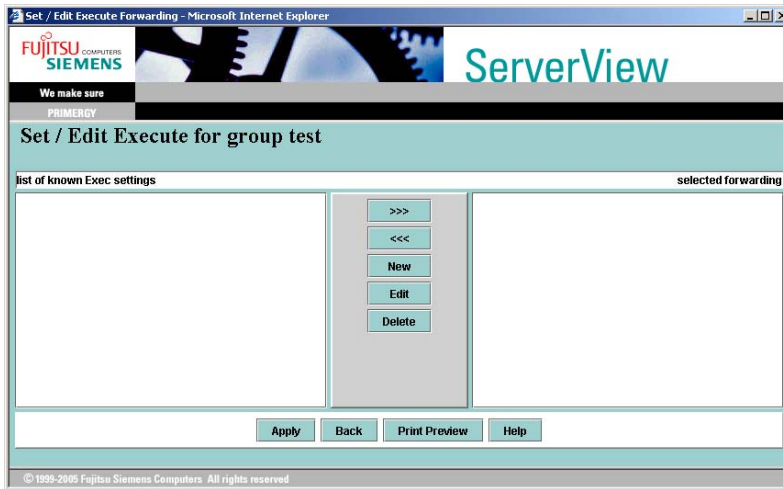
Applying the Logging Settings

Select the name of a setting from the [list of known Logging settings] list to the left and click [>>>]. The setting appears in the [selected forwarding] list to the right.

To release a setting, select the name of the setting from the [selected forwarding] list to the right and click [<<<].

● Execute

When you click [Execute], the [Set / Edit Execute for group test] window appears.



The existing Execute settings are displayed in the list. If you have made any changes, do not forget to click [Apply]. When you click [Back], the display returns to the [Set / Edit Destination] window.

Applying the Command Settings

Select the name of the setting from the [list of known Exec settings] list to the left and click [>>>]. The setting appears in the [selected forwarding] list to the right.

To release a setting, select the name of the setting from the [selected forwarding] list to the right and click [<<<].

Modifying Settings

Select the name of the setting you want to modify from the [list of known Exec settings] list to the left and click [Edit]. Modify the settings as required. The window for changing the settings is the same as the one for creating new settings. See "Creating New Command Executing" (→pg.158).

Removing Settings

Select the name of the setting you want to remove from the [list of known Exec settings] list to the left and click [Delete].

Creating New Command Executing

1 Click [New].

The [Exec Settings] window appears.



2 Configure each of the items.

table: [Exec Settings] Window

Item	Description
Description	Enter the name of the Execute setting.
Command	Enter the command to execute.
Work Directory	Enter the directory where the command to execute exists.
Time Model	Select the time to execute the action from the predefined Time Model. Click [TM Setting] to configure the Time Model.
[TM Setting] button	Set the time to execute the action. Clicking [TM Setting] displays the [TM Setting] window. The timetable for the week is displayed, and the time to execute the action is displayed in black. The Time Models [always] and [never] cannot be removed or changed.

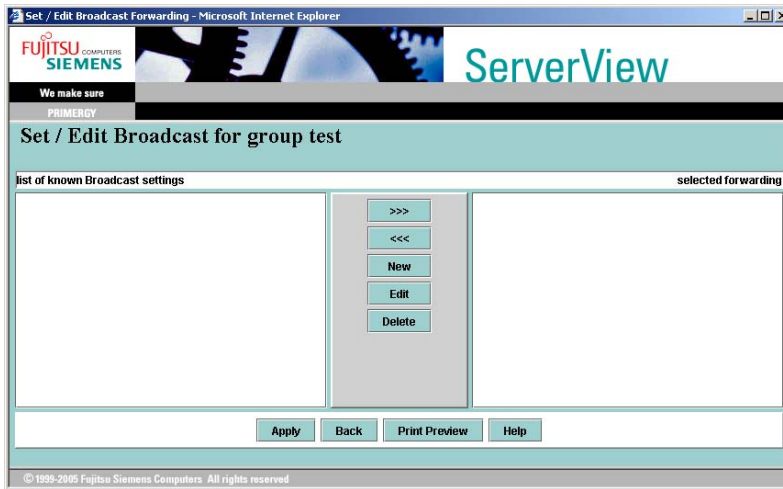
3 Confirm the settings, and click [OK].

The display returns to the [Set / Edit Execute for group test] window.

The newly created Execute setting is displayed in the [list of known Exec settings].

● Broadcast

When you click [Broadcast], the [Set / Edit Broadcast for group test] window appears.



The existing broadcasting settings are displayed in the list. If you have made any changes, do not forget to click [Apply]. When you click [Back], the display returns to the [Set / Edit Destination] window.

Applying the Broadcasting Settings

Select the name of a setting from the [list of known Broadcast settings] list to the left and click [>>>]. The setting appears in the [selected forwarding] list to the right.

To release a setting, select the name of the setting from the [selected forwarding] list to the right and click [<<<].

Modifying Settings

Select the name of the setting you want to modify from the [list of known Broadcast settings] list to the left and click [Edit]. Modify the settings as required. The window for changing the settings is the same as the one for creating new settings. See "Creating New Broadcasting Settings" (→pg.160).

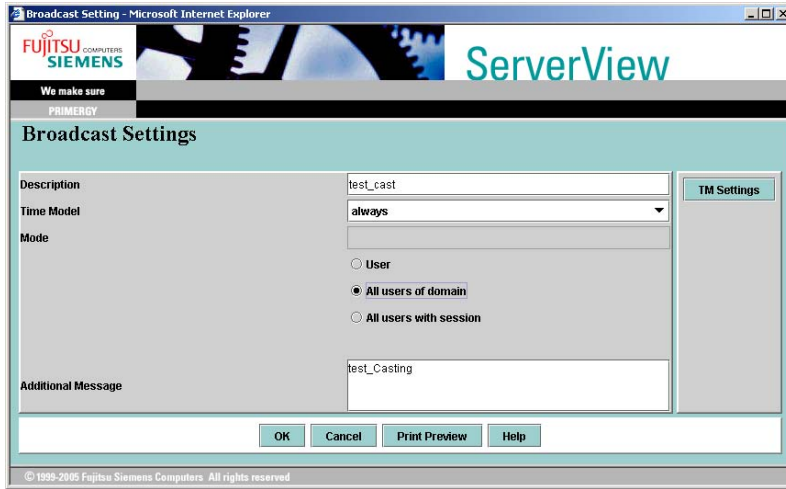
Removing Settings

Select the name of the setting you want to remove from the [list of known Broadcast settings] list to the left and click [Delete].

Creating New Broadcasting Settings

1 Click [New].

The [Broadcast Settings] window appears.



2 Configure each of the items.

table: [Broadcast Settings] Window

Item	Description
Description	Enter the name of the broadcasting setting.
Time Model	Select the time to execute the action from the predefined Time Model. Click [TM Setting] to configure the Time Model.
Mode	Select the broadcasting mode. <ul style="list-style-type: none"> • User Only a single specified user is notified of the information. Enter a user name in the field next to [Mode]. • All users of domain (only when using Windows) All users in the same domain as the forwarding destination are notified. • All users with session All users connected via the forwarding session are notified.
Additional Message	Enter additional text for the message.
[TM Setting] button	Set the time to execute the action. Clicking [TM Setting] displays the [TM Setting] window. The timetable for the week is displayed, and the time to execute the action is displayed in black. The Time Models [always] and [never] cannot be removed or changed.

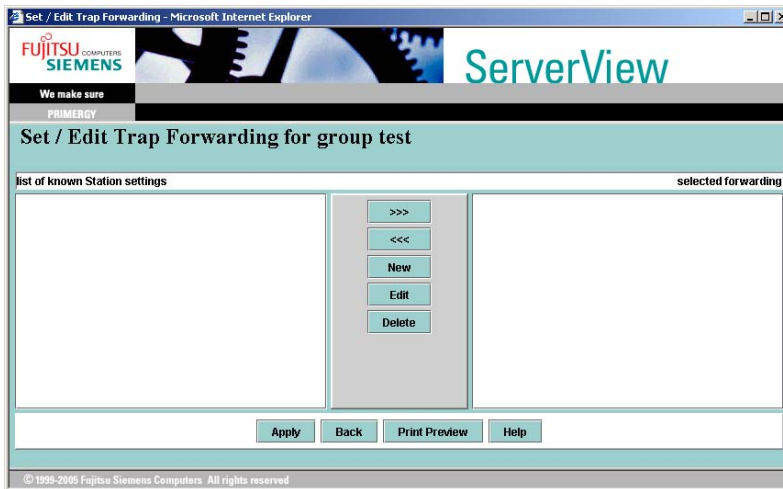
3 Confirm the settings, and click [OK].

The display returns to the [Set / Edit Broadcast for group test] window.

The newly created broadcasting setting is displayed in the [list of known Broadcast settings].

● Station

When you click [Station], the [Set / Edit Trap Forwarding for group test] window appears.



The existing station settings are displayed in the list. If you have made any changes, do not forget to click [Apply]. When you click [Back], the display returns to the [Set / Edit Destination] window.

Applying the Station Settings

Select the name of a setting from the [list of known Station settings] list to the left and click [>>>]. The setting appears in the [selected forwarding] list to the right.

To release a setting, select the name of the setting from the [selected forwarding] list to the right and click [<<<].

Modifying Settings

Select the name of the setting you want to modify from the [list of known Station settings] list to the left and click [Edit]. Modify the settings as required. The window for changing the settings is the same as the one for creating new settings. See "Creating New Station Settings" (→pg.162).

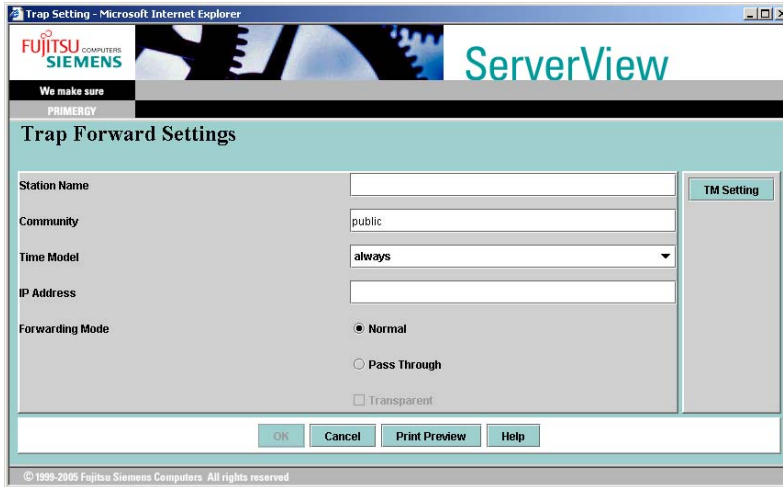
Removing Settings

Select the name of the setting you want to remove from the [list of known Station settings] list to the left and click [Delete].

Creating New Station Settings

1 Click [New].

The [Trap Forward Settings] window appears.



2 Configure each of the items.

table: [Trap Forward Settings] Window

Item	Description
Station Name	Enter the name of the station setting.
Community	Enter the community of the forwarding destination station. When a new setting is created, "public" is set as the default value.
Time Model	Select the time to execute the action from the predefined Time Model. Click [TM Setting] to configure the Time Model.
IP Address	Enter the IP address of the forwarding destination.
Forwarding Mode	Selects the forwarding mode.
[TM Setting] button	Set the time to execute the action. Clicking [TM Setting] displays the [TM Setting] window. The timetable for the week is displayed, and the time to execute the action is displayed in black. The Time Models [always] and [never] cannot be removed or changed.

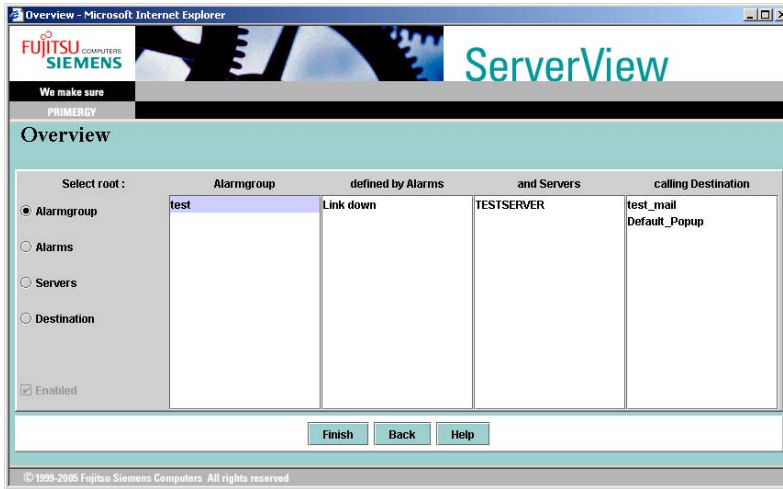
3 Confirm the settings, and click [OK].

The display returns to the [Set / Edit Trap Forwarding for group test] window.

The newly created execute setting is displayed in the [list of known Station settings].

■ Overview

All alarm groups and the specified associated alarms/servers/actions are displayed in list view.



If [Select root] is set to [Alarmgroup], you can confirm the associated values by selecting each of the defined alarm groups. You can confirm each setting by changing [Select root].

■ Setting Example

Here is a typical setting example using Alarm Settings:

● Purpose

When an event with severity 1 (Critical) occurs on the server "ALARMTEST", a mail must be sent to the administrator (admin@test.co.jp).

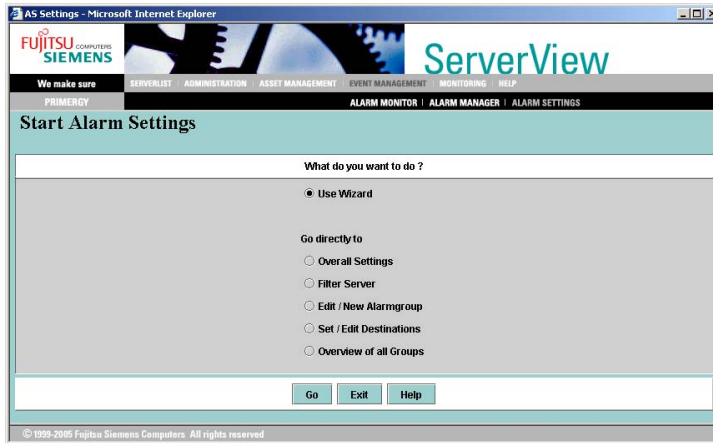
● Premises

- ServerView Agent is running on the server, and the server is registered as a management target in ServerView S2 on the same network.
- Test traps from ServerView Agent to ServerView S2 function normally.
- ServerView S2 can access to the SMTP server (192.168.1.20) while it is in operation.

● Setting Procedure

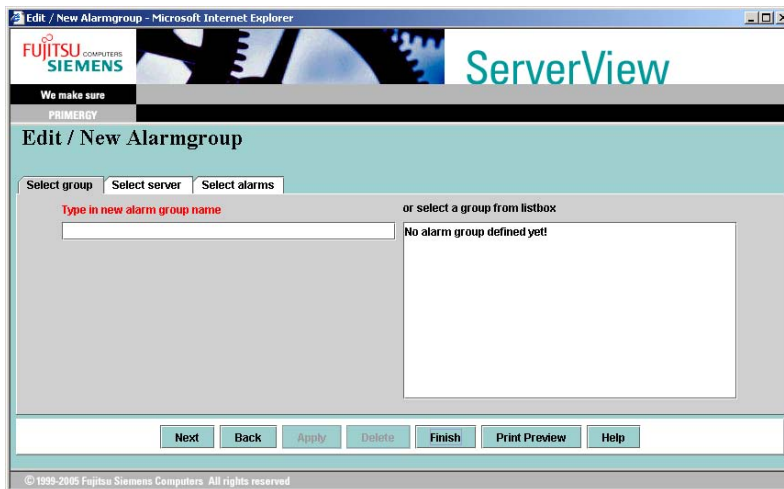
- 1 Start ServerView S2 and select [EVENT MANAGEMENT] and [ALARM SETTINGS] from the menu.

The [Start Alarm Settings] window appears.

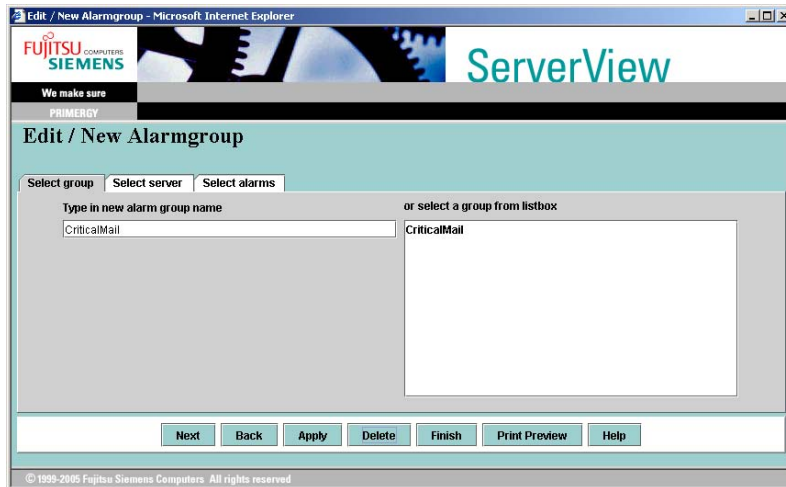


- 2 Select [Set / New Alarmgroup] and click [Next].

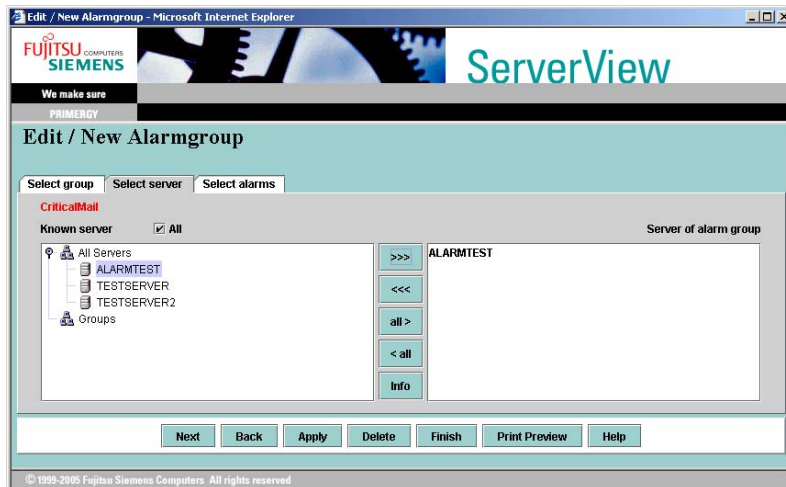
The [Set / New Alarmgroup] window appears.



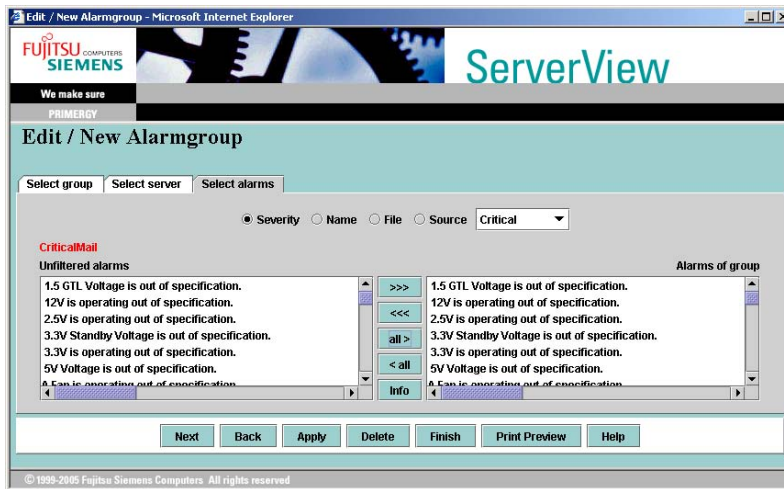
- 3 Enter "CriticalMail" as the alarm group name and click [Apply].



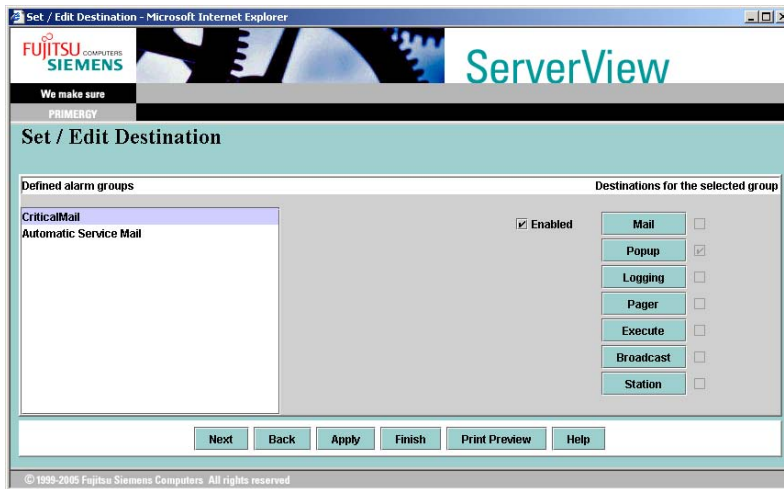
- 4 Click the [Select server] tab, select "ALARMTEST" from the server list, and click [>>>] to add the server to the alarm group.



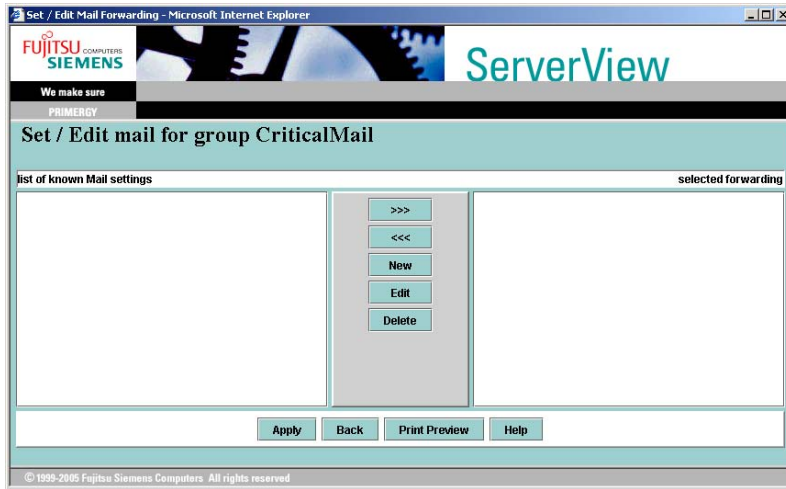
- Click the [Select alarms] tab, select [Critical] in [Severity], and click [all>] to add all the displayed alarms to the alarm group.



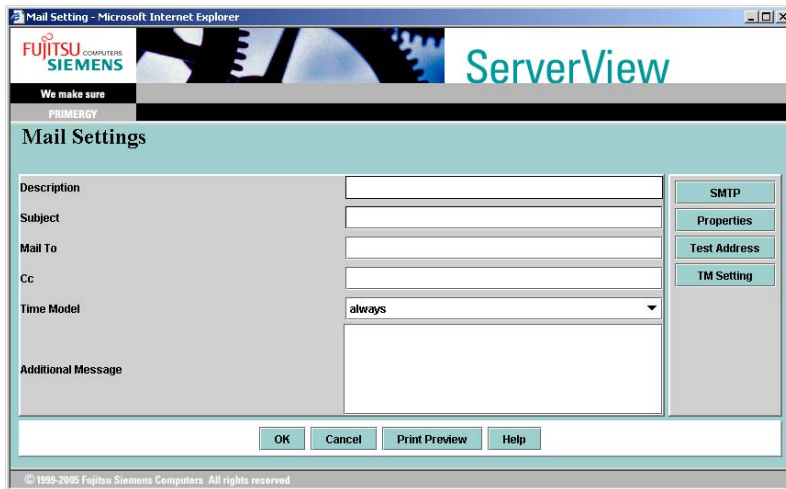
- Click [Apply], and then [Next].



- 7 Verify that the newly created "CriticalMail" is selected in the alarm group list and click [Mail].



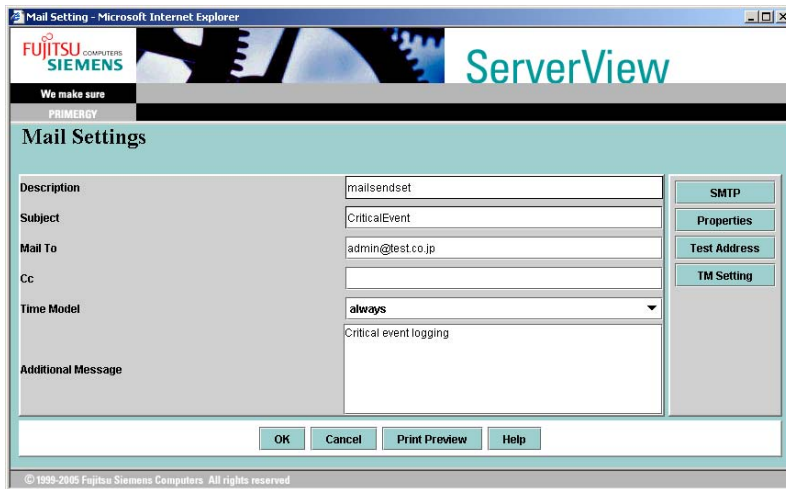
- 8 Click [New].



- 9 Click [Properties] and enter the required value in each field.



- 10 Click [OK] to return to the [Mail Settings] window and enter the required value in each field.

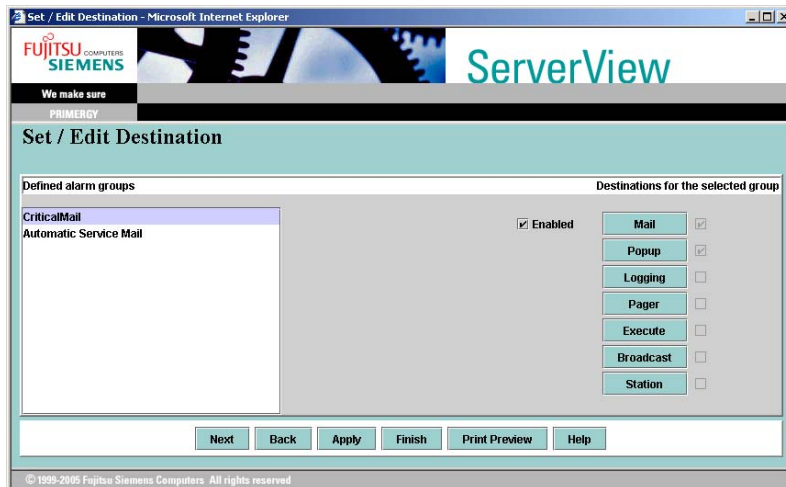


- 11 Click [OK] to return to the [Set / Edit mail for group Critical Mail] window, click [Apply] and then [Back].

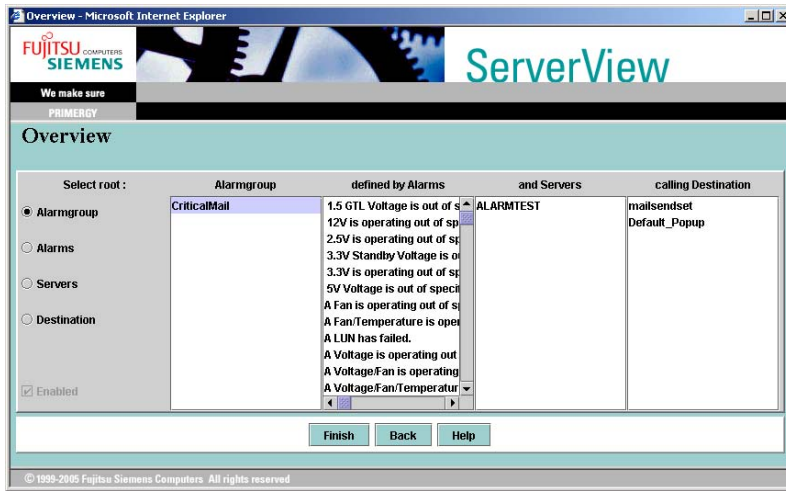


The display returns to the [Set / Edit Destination] window. Since the mail settings have been configured, [Mail] has a check mark.

- 12 Click [Next].



13 Confirm the configuration, and click [Finish] to exit.



3.6 Performance Manager

The performance manager enables settings, application, and management of threshold values and reports on the servers or the server groups.

● Threshold

An optional value may be specified for some parameters. This is called the threshold and an upper/lower limit, a relative threshold value, and poll intervals can be assigned.

● Reports

Creating reports helps monitor servers on a long-term basis.

The values selected in the Set of Reports are regularly measured and recorded for a specific period.

POINT

Resources Available for the Set of Thresholds and Reports

- ▶ The resource is either an SNMP object or a CIM object, registered by default. These objects have a normal object and a table object. Only one column can be used from a table object (e.g. the CPU idle time can be used from the CPU table).

IMPORTANT

- ▶ It requires NT Agent V4.00.05 (or later) to be installed on the server side to use the Performance Manager's function. See Agent View in "■ Agent Status" (→pg.95) to check the Agent version.
- ▶ As for the Linux Agent, the function has not been available.

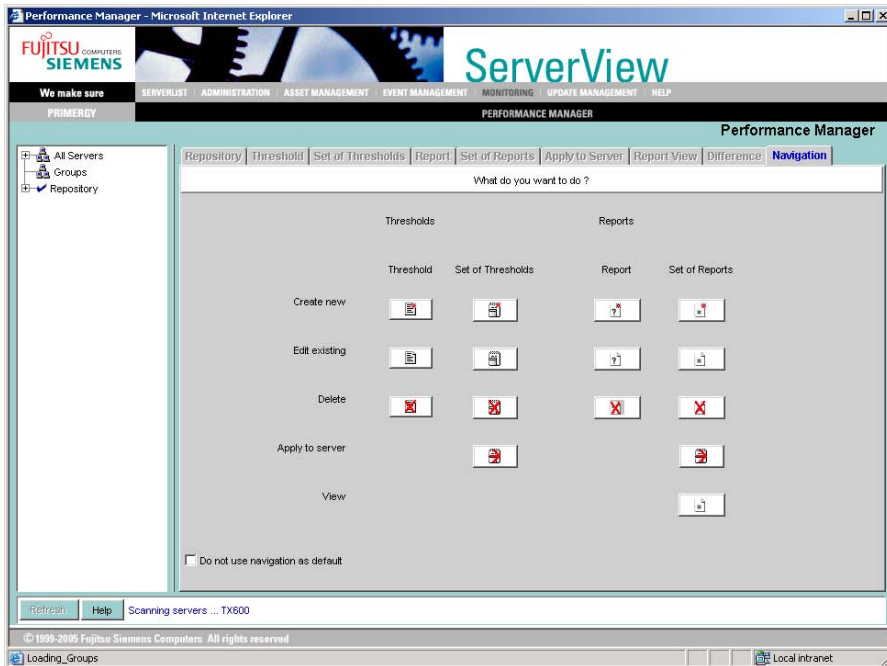
3.6.1 Starting the Performance Manager

- 1 Click [MONITORING] from the ServerView S2 menu and select [PERFORMANCE].

When starting from Management Console

Click [Performance Manager] from the [Tool] menu.

The [Performance Manager] window appears.



On the left frame, servers, server groups and repositories are displayed in a tree view.

At the startup, "Repository" is highlighted in the tree.

On the right frame, the [Navigation] tab is displayed as default. You can select any functions you want in this tab.

table: Functions on Each Tab

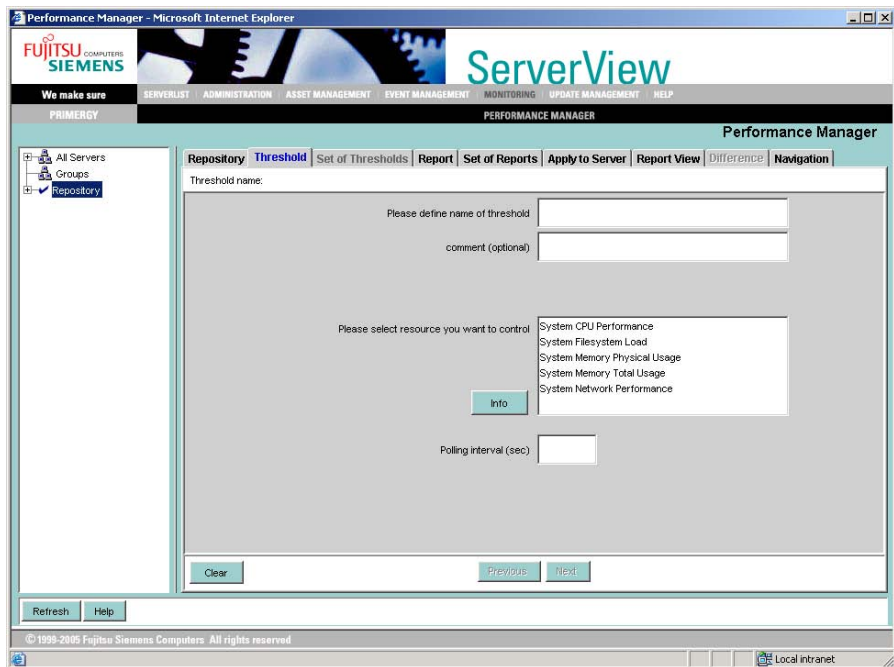
Tab	Function Overview
Overview Tab	When you select an item for which you want to view the detailed information from the left-side tree view, the tab title changes to the item's name, and the detailed information is displayed. Depending on the item selected, the tab title and the displayed contents vary.
[Threshold] Tab	Creates/edits "thresholds".
[Set of Thresholds] Tab	Creates/edits "Set of Thresholds".
[Report] Tab	Creates/edits "reports".
[Set of Reports] Tab	Creates/edits "Set of Reports".
[Apply to Server] Tab	Applies the "Set of Thresholds" and "Set of Reports" to the server.

table: Functions on Each Tab

Tab	Function Overview
[Report View] Tab	Displays report contents.
[Differences] Tab	When there are differences between the settings on the server and the settings on the repository, this tab becomes enabled and the differences can be checked.
[Navigation] Tab	The required functions can be selected.

3.6.2 Defining/Modifying Thresholds

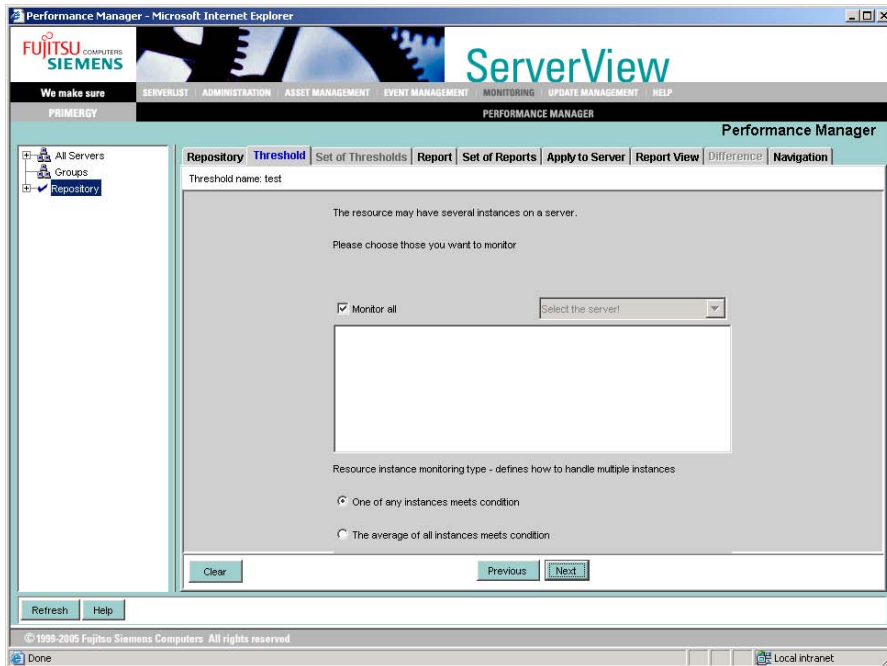
- 1 Click the [Threshold] tab in the [Performance Manager] window.
A screen to define Thresholds appears.



- 2 Enter the threshold name and set the observed resource and poll interval.
If an existing threshold name is selected from the left-frame tree view, you can edit the threshold.
Enter a "comment" if desired.
By clicking the [Info] for the resource, the detailed information for the resource can be confirmed.

3 Click [Next].

If the selected resource has multiple instances, a screen to select the observed target appears.

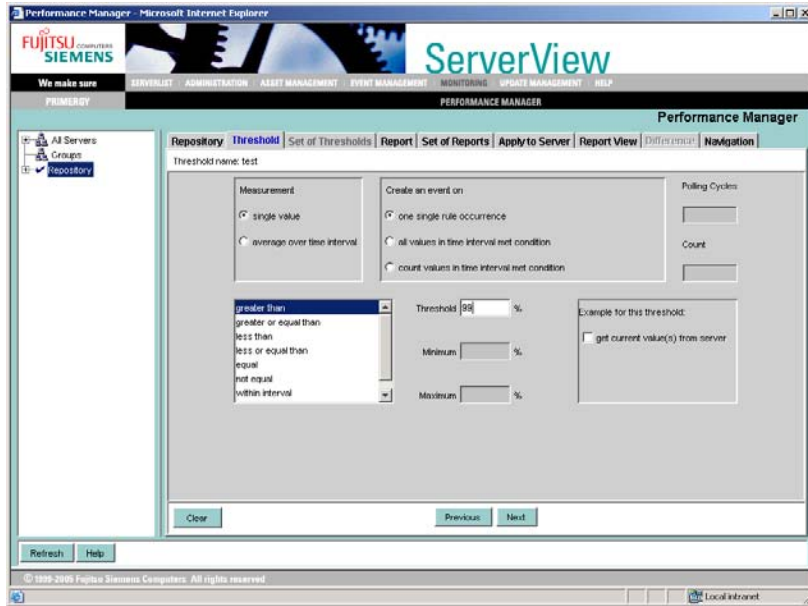


Usually, [Monitor all] is checked in order to observe all resources.

If only certain resources need to be observed, uncheck [Monitor all], select a server from the combo box, and select a resource from the displayed list. Also, select monitoring method for multiple instance (the average of the instance or any instance value).

4 Click [Next].

A screen to set the conditions appears.

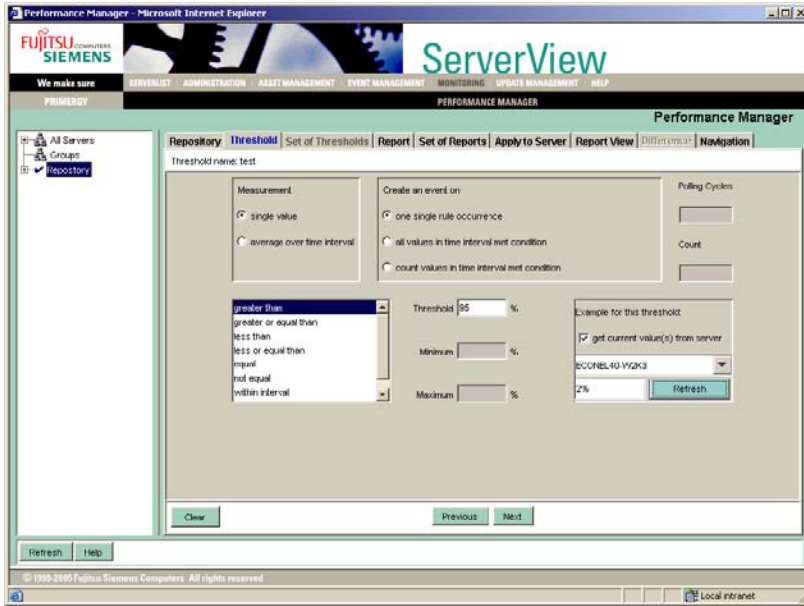


Set the conditions.

table: Condition Settings

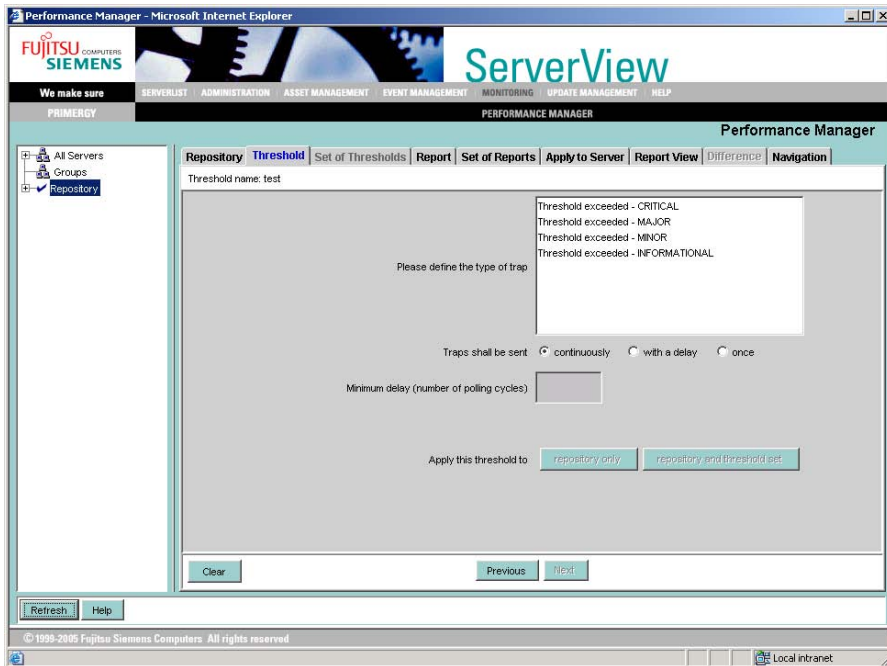
Item	Description
Measurement	Defines what kind of values are measured.
single value	Values are checked if they satisfy the condition each time.
average over time interval	The average value is checked if they satisfy the condition.
Create an event on	Specifies the condition for creating an event.
one single rule occurrence	An event is created if the threshold condition is met once.
all values in time interval met condition	An event is created if the threshold condition is met within the period of time.
count values in time interval met condition	An event is triggered if the specified number of values within the period of time satisfy the condition.
Polling Cycles	Specifies the Polling Cycles by the second to calculate condition for creating an event.
Count	Specifies the count condition for creating an event.
Condition list	Specifies the condition to be applied to the threshold. The condition can be selected from [greater than], [greater or equal than], [less than], [less or equal than], [equal], [not equal], [within interval], or [without interval].
Threshold	Specifies threshold.
Minimum/Maximum	Specifies the minimum/maximum value of threshold.
get current value(s) from server	Current resource value of the server is displayed to draw upon setting the thresholds. Selects the server displaying current value. Click [Refresh] to update current value of the selected server.

The following example is for managing the CPU usage.
 If the server's effective value is displayed, the value is updated when clicking [Refresh].



5 Click [Next].

A screen to select the trap type appears.

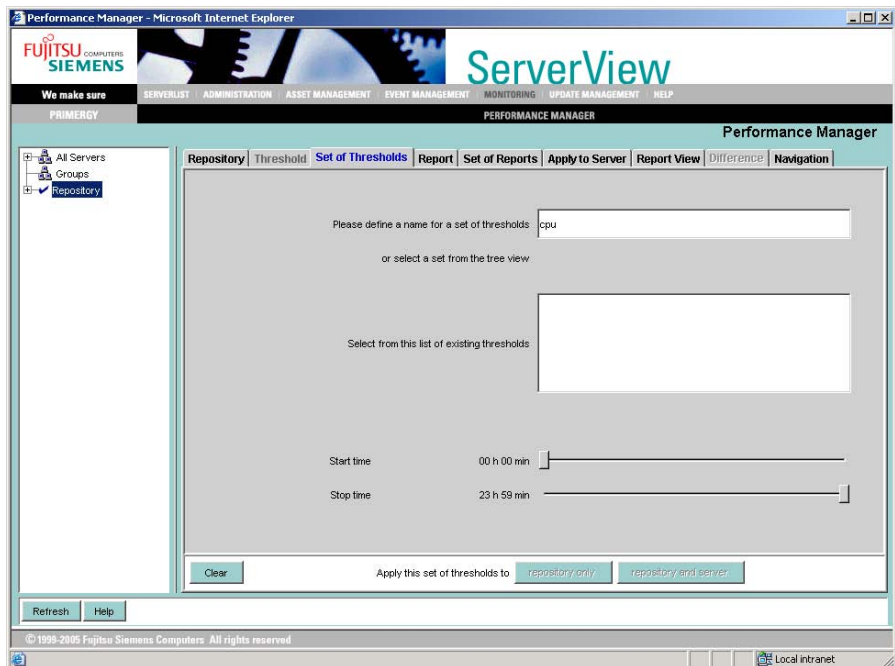


- 6 Select the trap type from the list and choose the sending option from [continuously], [with a delay], and [once].
If you select [with a delay], enter a number in [Minimum delay].
- 7 Store the threshold.
[repository only]: The threshold is stored in the repository.
[repository and threshold set]: The threshold is stored in the repository and the [Set of Thresholds] tab appears.

3.6.3 Creating/Editing Set of Thresholds

You can create and edit the Set of Thresholds.

- 1 Click the [Set of Thresholds] tab in the [Performance Manager] window.
The [Set of Thresholds] window appears.



The Set of Thresholds is a collection of thresholds. Only one Set of Thresholds is effective in the same period though two or more can be applied to one server. The Set of Thresholds is defined of the name, the threshold (multiple selection), and start/stop time.

- 2 Enter the name of the Set of Thresholds and select the thresholds to register on the Set of Thresholds.
- 3 Specify the monitoring time (Start time/Stop time) for the Set of Thresholds.

4 Store the Set of Thresholds.

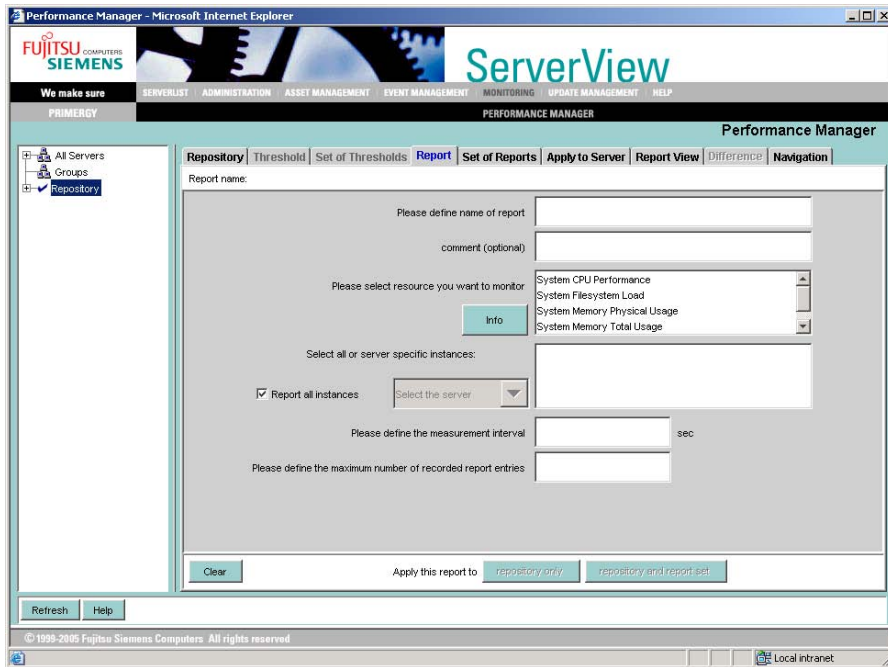
[repository only]: The Set of Thresholds is stored in the repository.

[repository and server]: The Set of Thresholds is stored in the repository and the [Apply to Server] tab appears.

3.6.4 Defining/Modifying Reports

1 Click the [Report] tab in the [Performance Manager] window.

A window to set the report contents appears.



2 Enter the report name and set the observed resource and poll interval.

table: Setting Items for the Report Definition

Item	Description
Please define name of report	Enter the report name here.
comment (optional)	Enter a comment for the report here. This item is optional.
Please select resource you want to monitor	Select one or more resources to be observed. If the selected resource has multiple instances, select a server from the combo box and select a resource from the displayed list. If all instances are selected, the average of all instances is reported.
Please define the measurement interval	Specifies the interval between two reports in seconds.
Please define the maximum number of recorded report entries	Sets the maximum number of report entries. When the number of reports reaches the maximum number, entries are deleted from the oldest one.



- ▶ If the [Please define the maximum number of recorded report entries] is not set, no entries are deleted. The size of the report entries grows unlimitedly.

3 Store the reports.

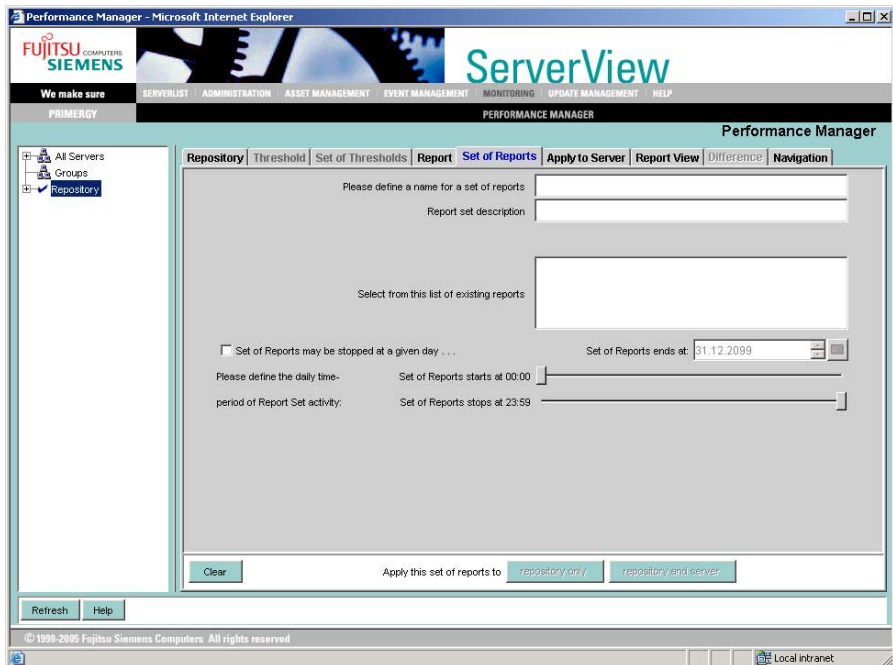
[repository only]: The report is stored in the repository.

[repository and report set]: The report is stored in the repository and the [Set of Reports] tab appears.

3.6.5 Creating/Editing Set of Reports

1 Click the [Set of Reports] tab in the [Performance Manager] window.

The [Set of Reports] window appears.



2 Set or change the Set of Reports.

You can select any reports from the list to add to the Set of Reports. Optionally, you can specify the date of expiring the Set of Reports. You can also set a daily execution period for the Set of Reports. The data is acquired only during the specified period of time.

3 Store the Set of Reports.

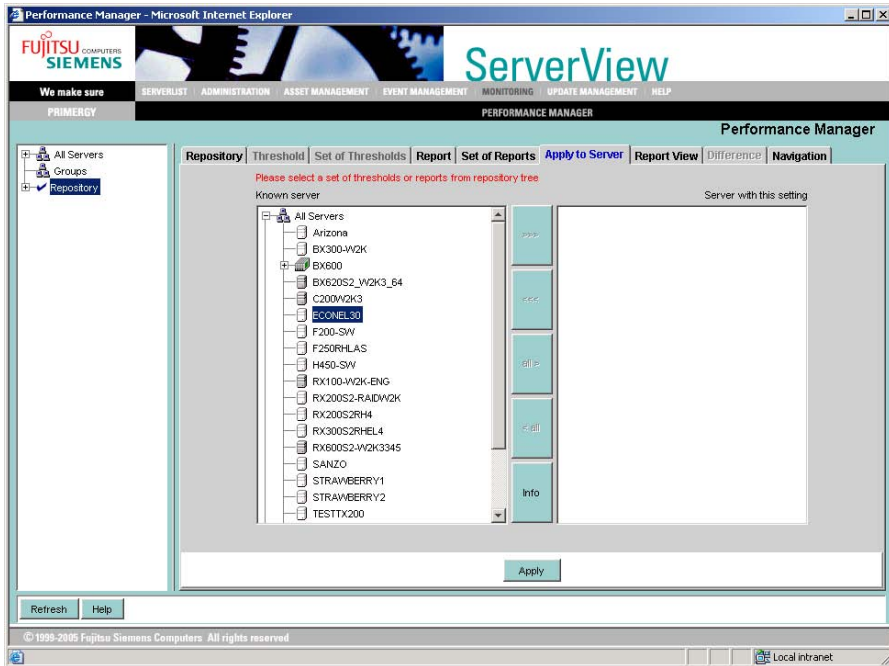
[repository only]: The Set of Reports is stored in the repository.

[repository and server]: The Set of Reports is stored in the repository and [Apply to Server] tab appears.

3.6.6 Applying the Settings to Servers

Applies the Set of Thresholds or the Set of Reports to servers.

- 1 Click the [Apply to Server] tab in the [Performance Manager] window. The [Apply to Server] window appears.



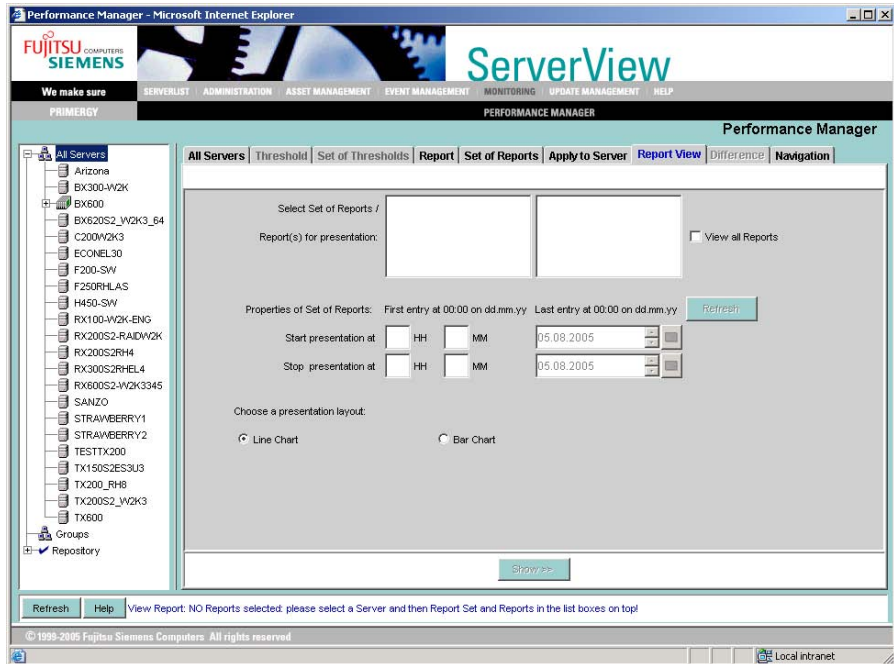
The [Known servers] list on the left side shows the server tree view. The [Server with this setting] list on the right side shows the servers to which the selected threshold/report settings have already been applied.

- 2 Using the [>>>] and [<<<] buttons, set the servers to be applied. Using the [all>] and [<all] buttons, you can set all servers at once.
- 3 Click [Apply]. The settings are applied to the servers.

3.6.7 Report View

By checking the report contents, you can confirm the server performance status.

- 1 Select a server for which you want to see the report from the left-frame server tree view.
- 2 Click the [Report View] tab.
The report window appears.



If [View all Reports] is checked, all configured report information is displayed. If it is not checked, you can select the report to be displayed.

The starting date/time and the ending date/time can be specified with the time sliders and the date field. The dates can be selected from the calendar that is displayed when clicking the [Calendar] button.

- 3 Select the presentation layout and click [Show>>].
As the presentation layout, select either [Line Chart] or [Bar Chart].
The report data is displayed.

3.6.8 Checking/Resolving the Differences

When there are differences between the configured threshold and the configured value on the server, the [Differences] tab is enabled. If the [Differences] tab becomes enabled, resolve the differences.

- 1 Click the [Differences] tab in the [Performance Manager] window.

The [Differences] window appears.

If there are multiple types of differences, only the severest type of difference is displayed. The types of differences are: New resource, new thresholds/reports, missing thresholds/reports, different thresholds/reports, new set of thresholds/reports, missing set of thresholds/reports, different set of thresholds/reports, enable/disable, and timestamp.

- 2 To make the repository settings effective, click [Take DB values].

To make the server values effective, click [Take server values].

The difference is resolved. If another difference is shown, repeat the procedure above. Repeat this procedure until no differences are displayed.

3.7 Management of Archive Data

This section explains how to create and manage archive data.

3.7.1 Starting the Archive Manager

The archive manager is used to create, display, compare and delete archive data of a server.

POINT

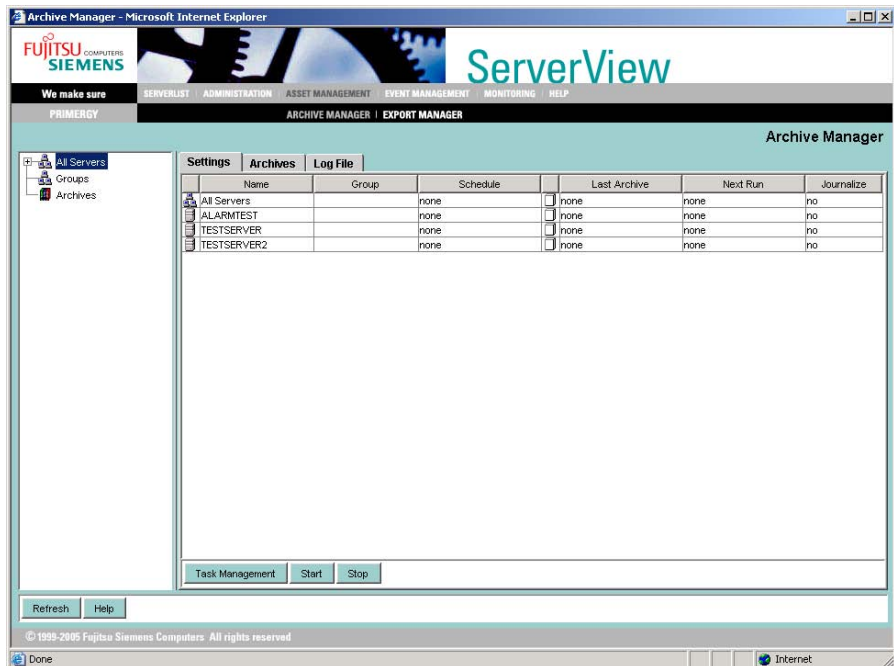
- ▶ For details about the archive manager, refer to online help topics.

- 1 Click [ASSET MANAGEMENT] from the ServerView S2 menu and select [ARCHIVE MANAGER].

When starting from Management Console

Click the [Archive Manager] icon or click the [Tools] menu → [Archive Manager].

The [Archive Manager] window appears.



POINT

- ▶ The [Settings] tab is automatically updated when each task starts/stops or when each archive settings are changed. Click [Refresh] to update an entire Web page including the server list and task information.

3.7.2 Creating Archive Data

1 Click the [Settings] tab.

Information of the server in which archive data is created appears.



table: Information of Server in which Archive Data Is Created

Items	Description
Name	The object name is displayed.
Schedule	The task schedule is displayed.
Last Archive	The last created archive is displayed.
Next Run	The time when the archive task is executed at the next run is displayed.
Journalize	Journalize information is displayed.

2 Select the server (group) for archive data from the displayed menu. Multiple servers can be selected.

3 Click [Start].

Creating the archive data of the selected server is started.

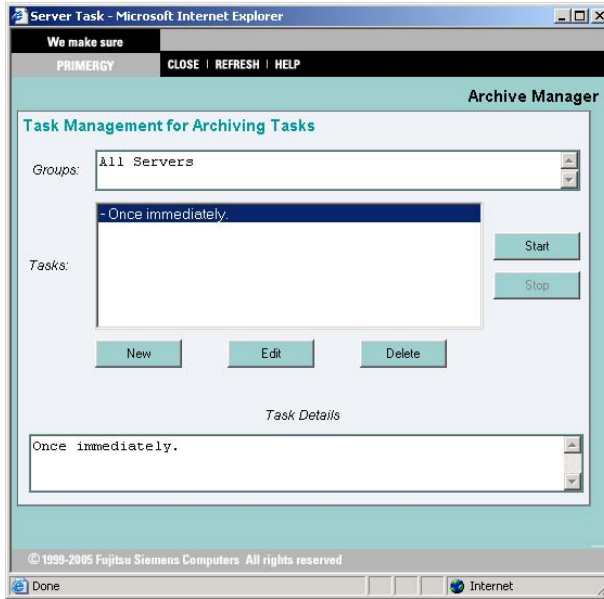
POINT

- ▶ The currently running archive acquisition stops by clicking [Stop].
- ▶ The directories where archive data is stored are as follows.
 - When ServerView Web-Server (Apache for Win32 base) is used
System Drive:\Program Files\Fujitsu\F5FBFE01\ServerView Services\wwwroot\ServerView\Archive[server name]\
 - When IIS is used
System Drive:\inetpub\wwwroot\ServerView\Archive[server name]\

3.7.3 Configuring Tasks for Retrieving Archive Data

- 1 Select a server/group for the task configuration and click [Task Management]. The following window appears.

The following window appears.

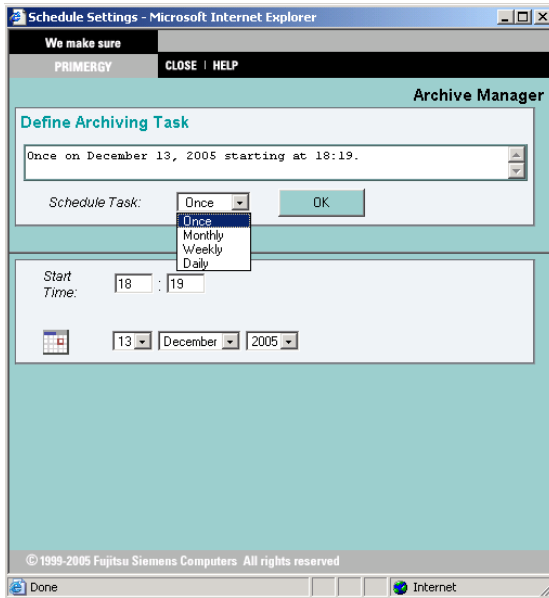


2 Click [New].

POINT

- ▶ The newly created configuration can be edited/deleted. (If the configuration is designated as [Once immediately], you can neither edit nor delete it.)

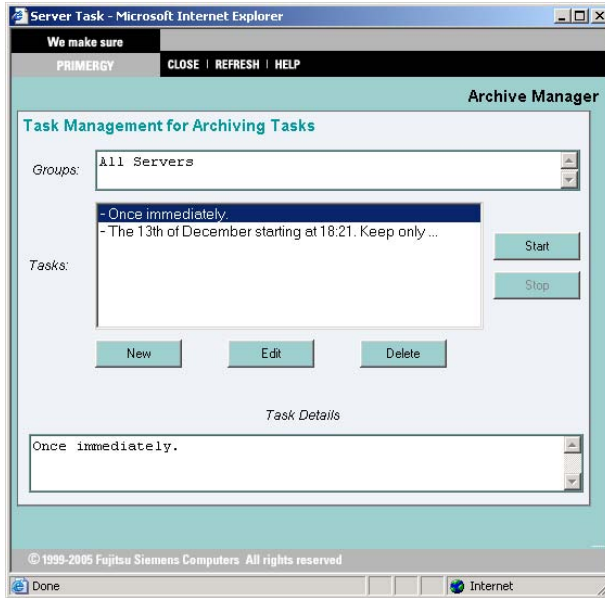
The following window appears.



3 Set the [Schedule Task].

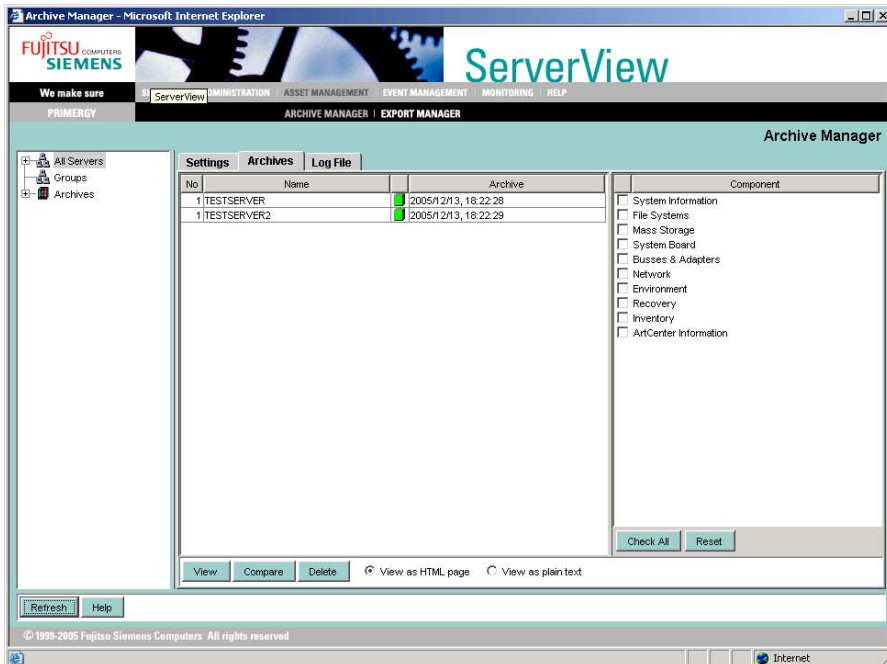
Select [Once], [Monthly], [Weekly] and [Daily], and configure the corresponding fields that need to be set.

- 4 Click [Start].
New task is set.



3.7.4 Displaying/Comparing/Deleting Archive Data

Display/compare/delete archive data in the [Archives] tab.



■ Displaying Archive Data

Follow the procedure below to display archive data.

- 1 Click the [Archives] tab and select the corresponding archive.
- 2 Select the archive data to be displayed.
- 3 Select the item you want to display in the component list.
- 4 Click [View]

The selected archive data is displayed in the archive manager window.

The screenshot shows the ServerView web interface in a Microsoft Internet Explorer browser window. The address bar shows the URL: http://10.21.136.204:3169/ServerView/SnmpArchive/MainFrame.html?Trace=0&CGIDirectory=scripts%2FServerView%2FSnmpArchive&CGIPath=&Ro. The page header includes the Fujitsu Siemens logo and the text "ServerView". Below the header, there is a navigation bar with "PRIMERGY" and "TESTSERVER" tabs, and a date/time stamp "2005/1/21 3, 18:22:28". The main content area is divided into several sections:

- System Information:** A table with the following data:

Name	iasys-ev-ldsm-remcs090.psd.cs.fujitsu.co.jp
Model	PRIMERGY TX200 S2
Processor Type	Intel(R) Xeon(TM) CPU 3200 Mhz, step 3
Number of Processors / Sockets	1 / 2
Total Memory (MB)	512
Cache (KB)	2048
Operating System	Red Hat Enterprise Linux AS 3 Revision V2.4 21-27 ELsmp
Location	Unknown (edit .letc/snmp/snmpd.conf)
Contact	Root <root@localhost> (configure .letc/snmp/snmp.local.conf)
Up-time	0 days, 08:10:43
Agent Product Version	4.11-10 (N4)
- Status Overview:** A table with the following data:

Status	Subsystem	Component
ok	System Status	
ok	MassStorage	
ok		Mass Storage Devices
ok	Systemboard	
ok		System Board Voltages
ok		Memory Modules
ok		System Processors
ok		BIOS Selftest
ok	PowerSupply	
ok		Power Supplies
ok	Environment	
ok		Environment System
- LAN Interfaces:** A table with the following data:

IP Address	Channel Type	Physical Address
10.21.136.90	primary	00300540821F
- Serial Ports:** A table with the following data:

Port	Word Length	Parity	Stop Bits	I/O Address
n.a.	n.a.	n.a.	n.a.	n.a.
- Parallel Ports:** A table with the following data:

Port	I/O Address
n.a.	n.a.

The footer of the page contains the copyright notice: © 1999-2005 Fujitsu Siemens Computers. All rights reserved.

■ Comparing Archive Data

Follow the procedure below to compare archive data in a server.

- 1 Click the [Archives] tab and select the corresponding archives.
- 2 Select the item you want to compare in the component list.
- 3 Click [Compare].

A comparative result is displayed.

The screenshot shows the ServerView web interface in a Microsoft Internet Explorer browser. The page displays a comparison of two archive data sets for a server named 'TESTSERVER'. The 'Up-time' field is highlighted in orange and green to show differences between the two data sets.

Field	Archive 1 Value	Archive 2 Value
Name	isys-sv-itm-remc1090.psd.cs.fujitsu.co.jp	isys-sv-itm-remc1090.psd.cs.fujitsu.co.jp
Model	PRIMERGY TX200 S2	PRIMERGY TX200 S2
Processor Type	Intel(R) Xeon(TM) CPU 3200 MHz, step 3	Intel(R) Xeon(TM) CPU 3200 MHz, step 3
Number of Processors / Sockets	1 / 2	1 / 2
Total Memory (MB)	512	512
Cache (KB)	2048	2048
Operating System	Red Hat Enterprise Linux AS 3 Revision Y2.4.21-27 ELtmp	Red Hat Enterprise Linux AS 3 Revision Y2.4.21-27 ELtmp
Location	Unknown (null:ntc:tmp:tmp.conf)	Unknown (null:ntc:tmp:tmp.conf)
Contact	Root -root@localhost- (configure:ntc:tmp:tmp.conf)	Root -root@localhost- (configure:ntc:tmp:tmp.conf)
Up-time	0 days, 00:24:10	0 days, 06:10:43
Agent Product Version	4.11.10 (RM)	4.11.10 (RM)

The 'Up-time' field is highlighted in orange for the first archive and green for the second archive, indicating a difference in the data.

Status Overview

Status	Subsystem	Component
ok	System Status	
ok	Mass Storage	
ok		Mass Storage Devices
ok	Systemboard	
ok		System Board Voltages
ok		Memory Modules
ok		System Processors
ok		BIOS Selftest
ok	PowerSupply	
ok		Power Supplies
ok	Environment	
ok		Environment System

LAN Interfaces

IP Address	Channel Type	Physical Address
10.21.1.36.90	primary	00:00:54:00:21f

Serial Ports

Port	Word Length	Parity	Stop Bits	IO Address
n.a.	n.a.	n.a.	n.a.	n.a.

Parallel Ports

Port	IO Address
n.a.	n.a.

Any difference is discriminated by the first field and displayed in two different colors. The information that exists only in either of the two archive data is discriminated from the information with different values that exists in both archive data.

■ Deleting Archive Data

Follow the procedure below to delete archive data in a server.

- 1 Click the [Archives] tab and select the corresponding archive.
- 2 Click [Delete]
The archive data is deleted.

3.7.5 Archive Data Log

Follow the procedure below to display a list of archive data logs.

- 1 Click the [Log File] tab.
Log files are listed.

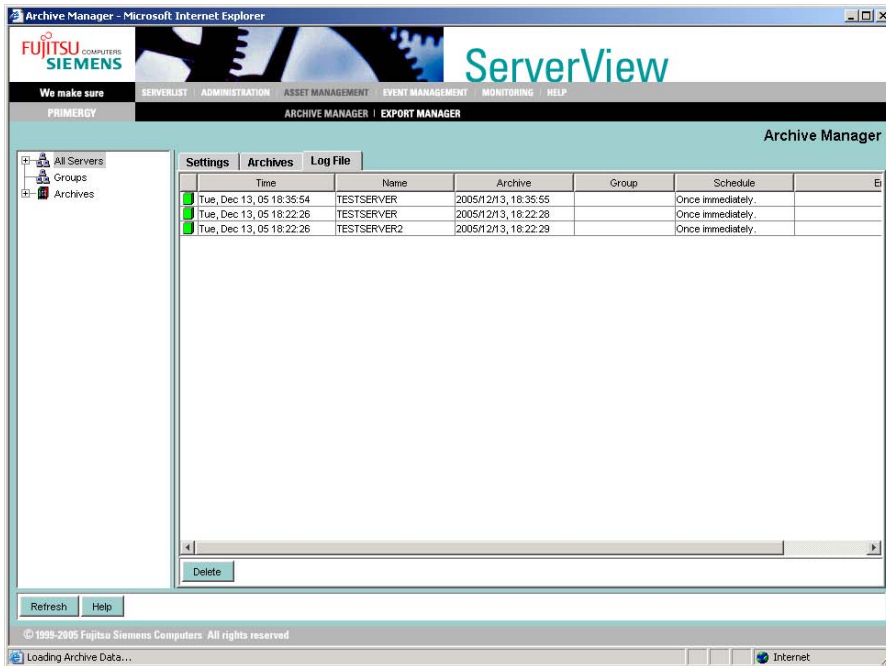


table: Log List in Archive Manager

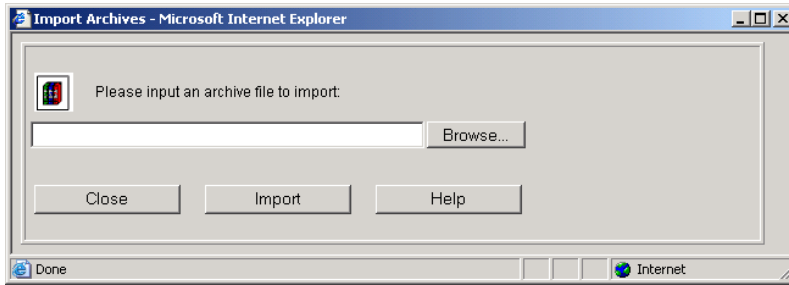
Items	Description
Time	The day and time when archive data is obtained are displayed.
Name	The object name is displayed.
Archive	The archive name is displayed.
Schedule	The format in which the archive is obtained is displayed.

3.7.6 Importing Archive Data

This section explains how to import the archive file.

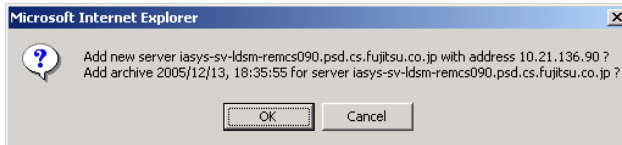
- 1 Click [SERVERLIST] from the ServerView S2 menu and select [IMPORT ARCHIVE].

The [Import Archives] window appears.



- 2 Click [Browse] and specify the archive file to import.
- 3 Click [Import].

The confirmation dialog box appears.



- 4 Click [OK].
- The archive data is imported.

3.8 Export Manager

This section explains how to create the export data from ServerView S2 and save it in a file.

3.8.1 Acquiring Export Data

- 1 Click [ASSET MANAGEMENT] from the ServerView S2 menu and select [EXPORT MANAGER].






POINT

- ▶ Export Manager can be also displayed using one of the following methods:
 - Select [Export Manager] from the [Tools] menu.
 - Right-click on the server and click [Export Manager].
 - When ServerView has not been started, click the [Start] button → [Programs] → [Fujitsu ServerView] → [Export Manager].
 - Click the [Version Management] icon on Management Console and click [Export Manager]

The [Export Manager] window appears.



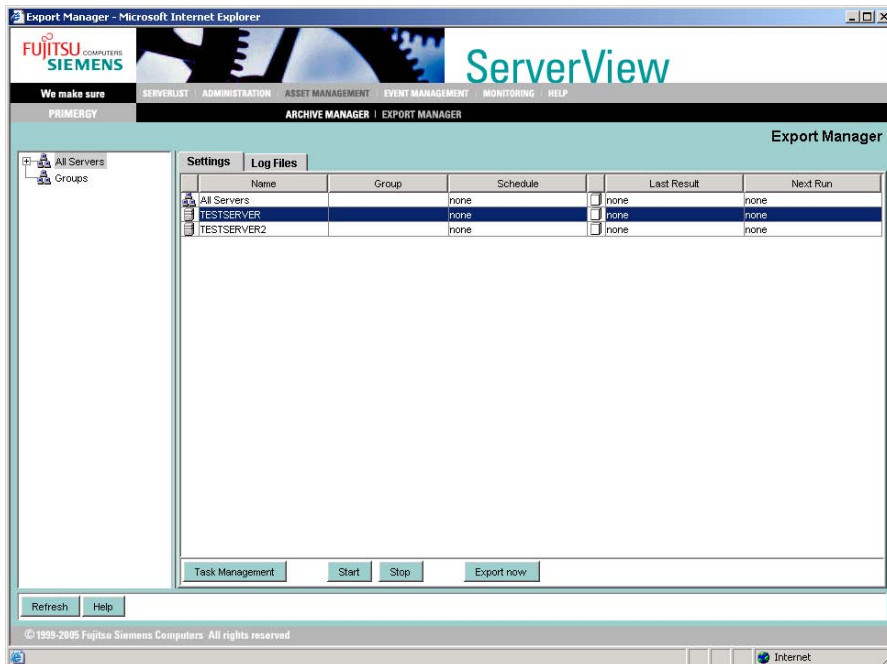
table: Information Displayed in the Export Manager Window

Name	Description
Name	The object name is displayed.
Group	The object group name is displayed.
Schedule	The task schedule is displayed.
Export Status Icon	Export status is displayed in the icon.
	Export data has been successfully obtained. The obtained file is stored in the server and can be read.
	Export data has been successfully obtained. The obtained file is stored in another server.
	Obtaining export data is in progress.
	Obtaining export data failed.
	Export data is unknown.
Last Result	The last time when export data is created is displayed.
Next Run	The time when an export task is executed at the next run is displayed.

 **IMPORTANT**

- ▶ To use Export Manager from ServerView S2 installed on the Linux OS, the path must be set.
 1. Execute following command to confirm the folder in which Java is installed.
rpm -ql j2re | grep bin/java
 2. Add following 2 lines to the /etc/profile and log off the OS.
The following is an example when the Java is install in /usr/lib/...
PATH=/usr/lib/j2rex.x.x_xx/bin:\$PATH
export PATH


- 2 Click the [Settings] tab and select the server in which export data is to be created.



- 3 Click [Start].

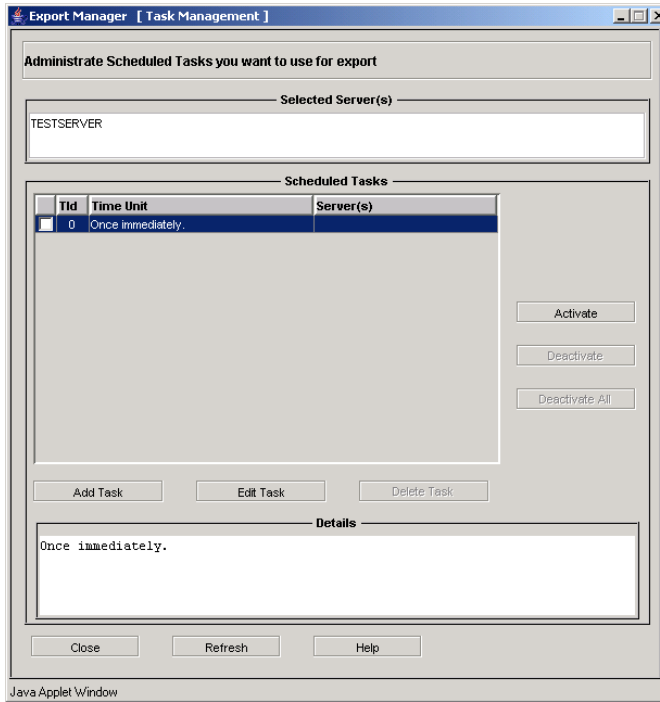
Creation of export data using the current information (quick export) starts and the export data is acquired. Click [Stop] to stop performance. Multiple servers can be selected.

POINT

- ▶ When you click [Export now] at the initial condition, you need to start from step 3 in "3.8.2 Configuring Export Data Retrieval" (→pg.195). After configuration for exporting, click [Activate] in Task Management window to obtain the export data.
- ▶ When export data is obtained without specifying any file names in the quick export ([Start]) or the schedule settings ([Task Management]), all the export files are stored in the server that obtained it last.
- ▶ When multiple servers are selected to obtain export data at once, the data for all the servers is stored in the file marked with  among the files created at the same Time.
- ▶ When exporting is executed with specified information to obtain, the data can be downloaded in the obtained results verification window if the [Show progress window] item is selected. For details, refer to help topics.

3.8.2 Configuring Export Data Retrieval

- 1 Select a server/group for the task configuration and click [Task Management]. The [Task Management] window appears.

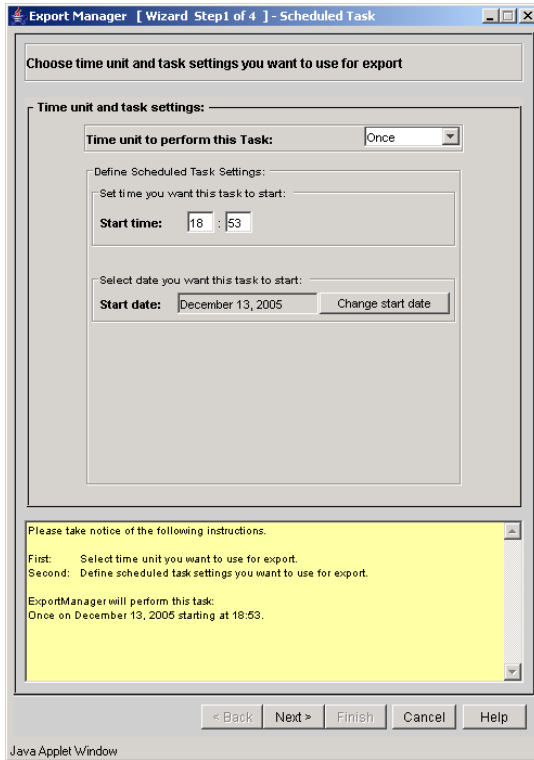


2 Click [Add Task].

POINT

- ▶ The newly created task can be edited/deleted. If the task is designated as [Once immediately], you can neither edit nor delete it.

The following window appears.

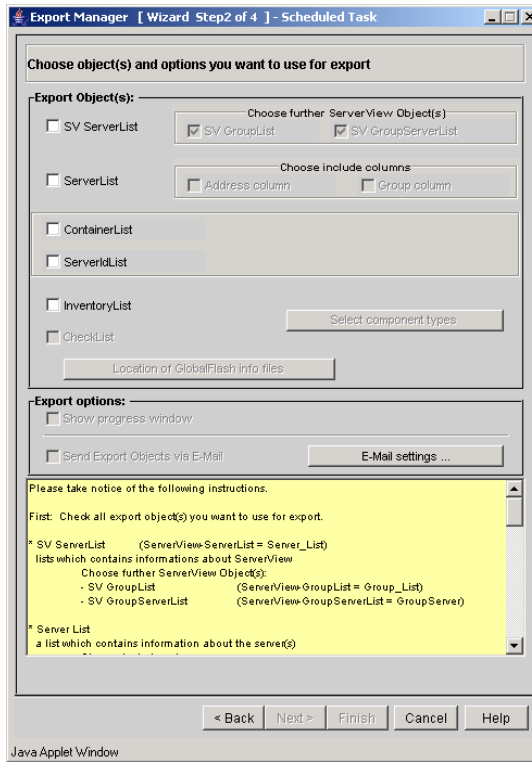


3 Set the task starting time and pattern.

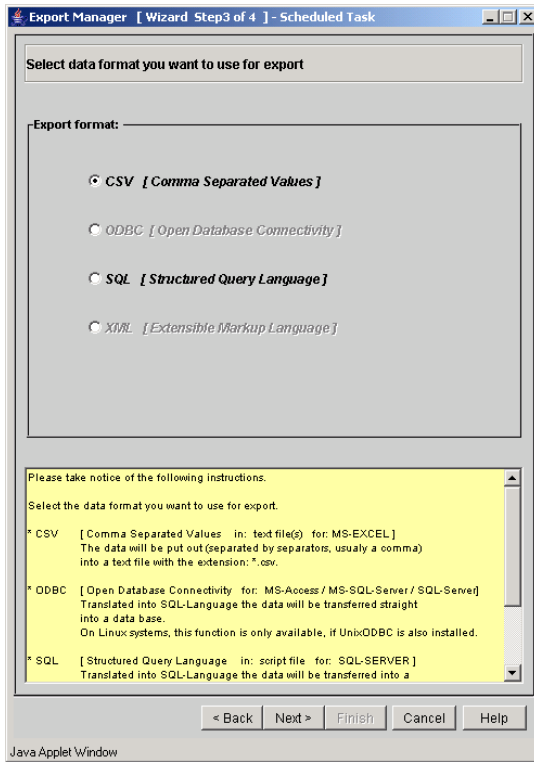
By switching the time unit between [Once], [Monthly], [Weekly] and [Daily], the corresponding values that need to be set are displayed at the [Define Scheduled Task Settings].

4 Click [Next].

The window for selecting objects appears.

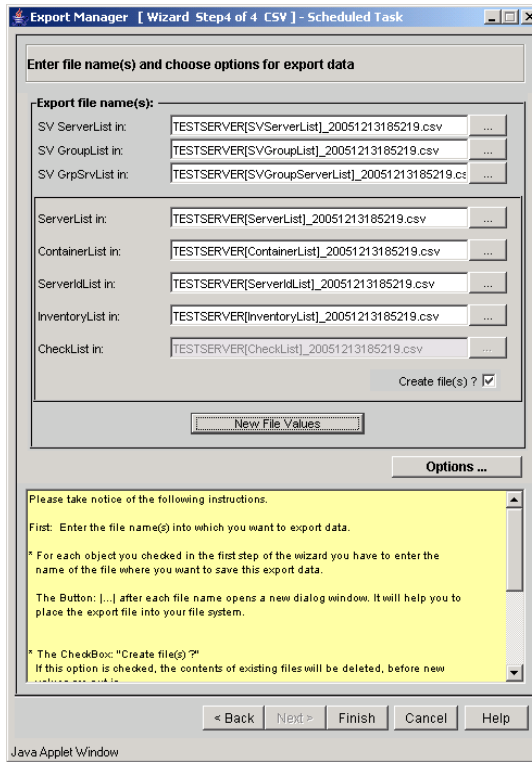


- 5 Select an object to export by checking its checkbox and click [Next].
The window for selecting a data type appears.



6 Select a data type and click [Next].

The window for specifying a file name appears.



7 Enter the file name and click [Finish].

The task is created. When you select the task and click [Activate], the task starts

3.8.3 Displaying Export Data

Click the [Log Files] tab to display the export data.

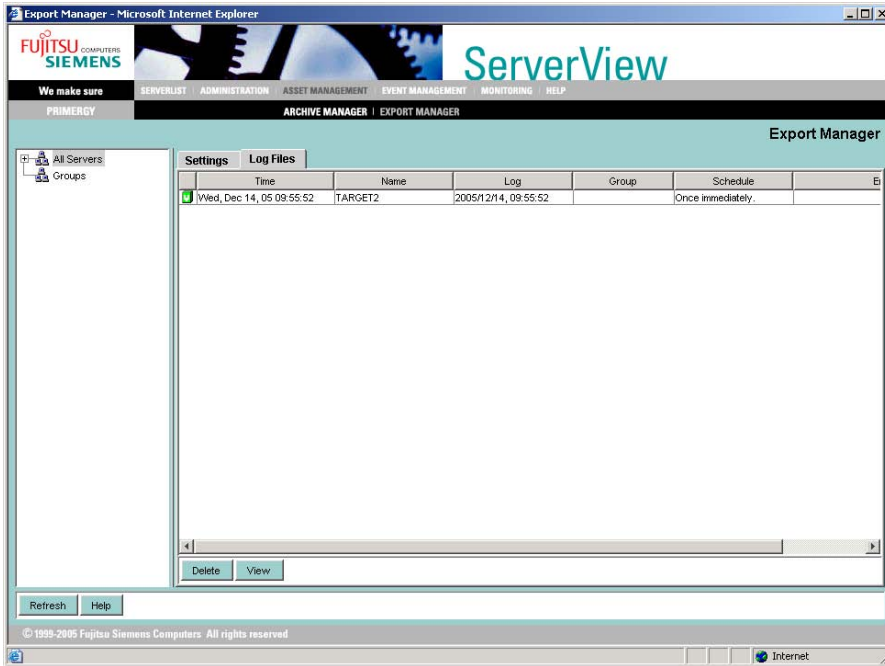
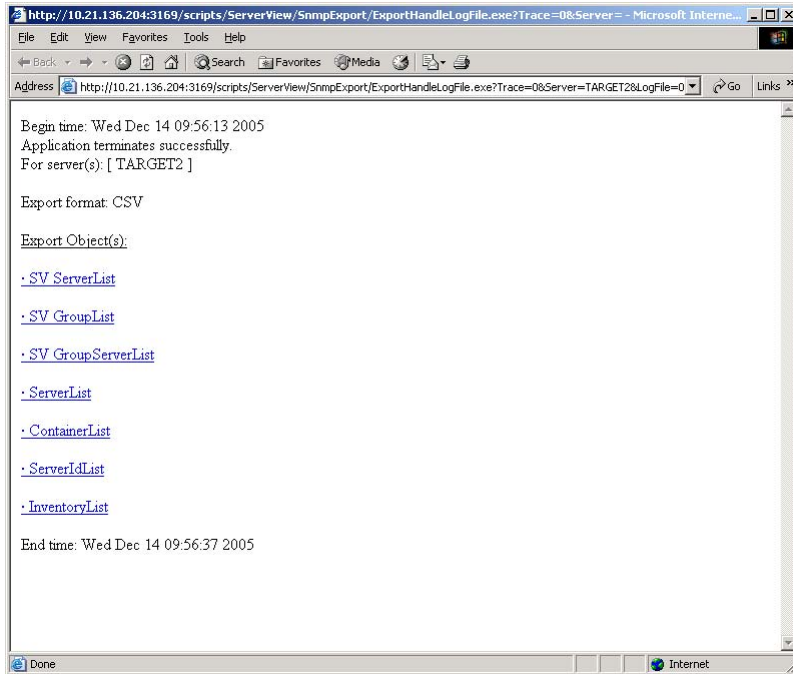


table: Description of Items of [Log Files] Tab in Export Manager

Name	Description
Time	The creation time of export file is displayed.
Name	The object name is displayed.
Log	The detailed time of file creation is displayed.
Group	The object group name is displayed.
Schedule	The schedule of obtaining task is displayed.
Error	The error information of export task is displayed.

- 1 Select the export data that you want to display and click [View].
The visible export data are listed.



- 2 Click the data that you want to browse. To save data, right-click on the data to save and click [Save Object to File].

3.9 ServerView Operation Using the Management Console

This section describes how to start Management Console in the administration terminal where ServerView Console was installed and how to operate ServerView using Management Console.

3.9.1 Starting the Management Console

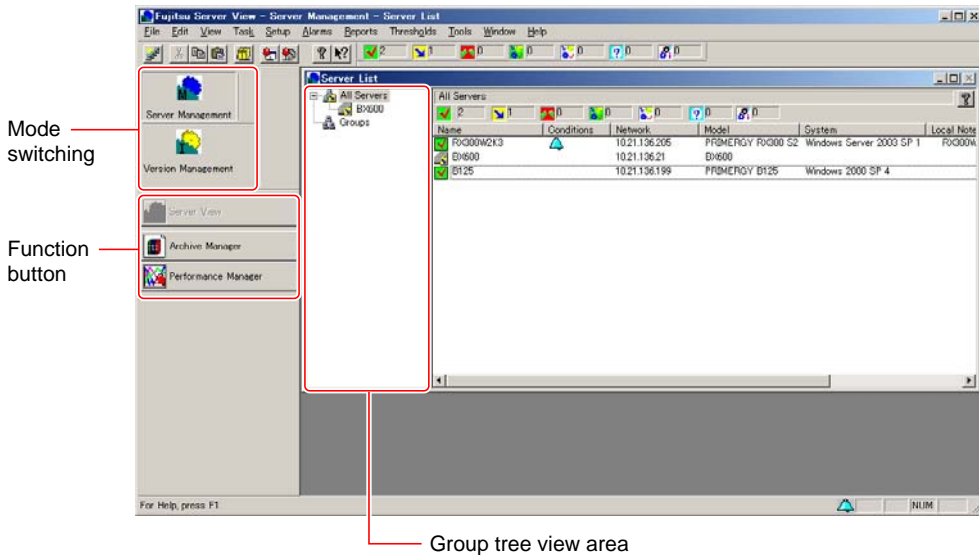
- 1 Click the [Start] button → [Programs] → [Fujitsu ServerView] → [ServerView(Win32)].

The management console starts and the [Server Management] window appears.

The [Server List] window appears within the [Server Management] window. The servers listed in this window will be monitored.

POINT

- ▶ When the management console is started at a local server in which ServerView Agent is installed, the local server is automatically added to the server list and displayed in the [Server List] window.



Mode Switching

The management console includes the [Server Management] mode and the [Version Management] mode. The available functions depend on the selected mode.

Function Button

The available functions are displayed according to the current mode of management console.

■ Menu List

table: Management Console Menu

Menu Item	Description
[File]menu	
New Server...	Adds a monitored server to the server list. →"3.9.2 Adding the Monitored Server (Object)" (pg.206)
New Group	Creates a new group in the server list. →"■ Creating Groups" (pg.209)
Import → Archive	Imports the archive data obtained at the other management servers. This is used in examination of environment.
Import → Server	Imports certain servers to the server list.
Open	Starts the [Server View] window for the server management mode or the [Inventory View] window for the version management mode. →pg.117
Applications...	All the registered applications are displayed in the application list box. To start the application for an object selected in the server list, select the application from the list box and then click [OK] or double-click the application that you want to start.
Print... Print Preview Printer Settings...	Starts the print dialog recognized from the other applications.
Remove	Deletes some objects from the server list.
Rename	Rename a group in the server list.
Server Properties	Opens the server properties page to define server parameters.
Blade Server Properties	Opens the blade server properties page to define blade server parameters.
Group Properties	Opens the group properties page to define group parameters.
Test Connection	Tests connection to the server and the cluster selected from the server list.
Redetect servers	Start the status check process for the selected object. This process dynamically checks if the server exists in the network. It also checks if the server can respond to the SNMP. The results obtained with this menu item selected are same as the results of automatic status checking regularly performed.
Exit	Exit ServerView.
[Edit] menu	
Cut	Moves a server object to the clipboard.
Copy Paste	Copies or pastes server objects to the server list.
Select All	Selects all the server objects.

table: Management Console Menu

Menu Item	Description
[View] menu	
Tool Bar	Displays or hides the tool bar at the top of the ServerView window.
Status Bar	Displays or hides the status bar at the bottom of the ServerView window.
Status Summary	Displays the status bar (a summary of server status) under the tool bar.
Task Bar	Displays the task bar.
Large Icon Small Icon List Details	Changes server representation in the server list. Each function is same as the Windows Explorer function.
Filter Servers...	Server Filter settings allow you to restrict servers displayed in the server list to a specific server. → "Filter the Server List" (pg.209)
Redetect All Servers	Detects all the defined servers. This checks that the server exists in the network and that it can respond to the SNMP protocol.
[Task] menu	
Server Management	Turns to the server management mode. The server management task function is available.
Version Management	Turns to the version management mode. The version management task function is available.
[Setup] menu (on the Server Management Mode Only)	
Disable Reporting	If this item is selected, all the reports that are collecting regular reports are suspended.
External Application	Defines an external application to be assigned to the server.
Default Settings	Defines server default settings. → "3.9.6 Copying Settings to the Other Servers" (pg.218)
Unit Settings	Specifies a measurement unit for temperature representation.
User Authentication	[Log on to Server] window appears. Defines the user name and password to log on to the selected server.
[Alarms] menu (on the Server Management Mode Only)	
Manager	Alarm Service starts and the alarm manager window appears. The alarm manager can see and edit alarm messages stored in the alarm log list. → "3.5.2 Alarm Manager" (pg.139)
Monitor	Alarm Service starts and the alarm monitor window appears. The alarm monitor window displays all the accepted alarms. → "3.5.1 Alarm Monitor" (pg.132)
Settings	Alarm Service starts and the alarm monitor window appears. The alarm monitor window displays all the accepted alarms. → "3.5.3 Alarm Settings" (pg.142)
Accept	Accepts alarms of the selected server.
Accept All	Accepts alarms of all the servers.
[Reports] menu (on the Server Management Mode Only)	
Manager	Starts the report manager. → "3.9.5 Report Manager" (pg.215)
List	Opens the report list and displays all the active reports.

table: Management Console Menu

Menu Item	Description
[Thresholds] Menu (on the Server Management Mode Only)	
Manager	Starts the threshold manager and enables or disables the server threshold. →"3.9.4 Threshold Manager" (pg.211)
List	Opens the threshold list and displays all the active thresholds.
[Tools] menu	
Archive Manager	Starts the archive manager. →"3.7.1 Starting the Archive Manager" (pg.183)
Export Manager	Starts the export manager. It is available on the version management mode only. →"3.8 Export Manager" (pg.192)
Performance Manager	Starts the Performance Manager. It is available on the server management mode only. →"3.6 Performance Manager" (pg.171)
Global Flash	This is unavailable.
[Window] menu	
Arrange Icons Cascade Tile Vertical	Switches the viewing manner for all the windows including the server list. This is same as the window menu of the other Windows applications.
Close All	Closes all the windows except for the server list.
[Help] menu	
Search Topics	Starts the ServerView help.
Alarm	Displays the alarm description assigned by Fujitsu.
Icon	Opens sections of the Server Manager Help system including descriptions of the ServerView display elements.
Glossary	Help starts and the system glossary appears.
About ServerView	Displays version information of ServerView.

■ Right-click Menu

Right-click the managed server and the following menus appear. Functions can also be selected from these menus.

table: Pop-up Menu

Menu Item	Description
New Server	Adds any undefined monitored server to the server list.
Open	Starts the "ServerView" for the server management mode or the "Inventory View" for the version management mode.
Status	Displays the status list of the selected server.
Applications	Displays the application list.
Export Manager	Starts the export manager. It is available on the version management mode only.
Copy	Copies a server to the clipboard.
Paste	Pastes a server copy on the clipboard.
Remove	Deletes a server.
Server Properties	Starts the server properties.
ASR Properties	Starts the ASR properties.

table: Pop-up Menu

Menu Item	Description
Test Connection	Test the connection.
Redetect servers	Check the server status.
Threshold manager	Starts the threshold manager.
Report manager	Starts the report manager.
Accept Alarms	Receives the alarm that has not been accepted.
Obtain Archives Now	Obtains archives for the current server status.

3.9.2 Adding the Monitored Server (Object)

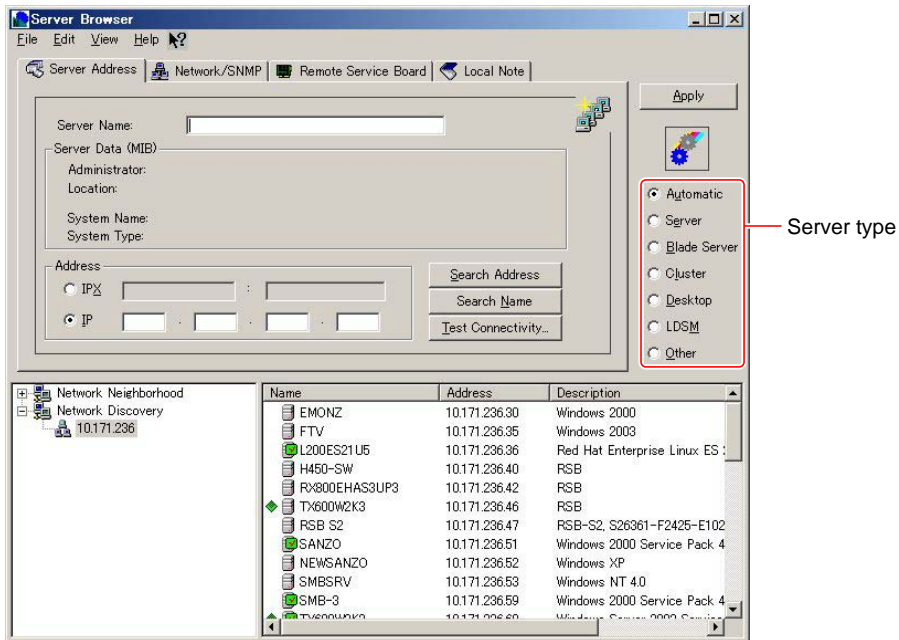
Add the monitored server on your network to the server list.

■ Add a New Server

Specify a newly monitored server (and object) in ServerView.

- 1 Click the [File] menu → [New Server].

The [Server Browser] window appears and information about the nodes existing on the network is displayed.



2 Specify a server type.

Make sure to specify an accurate type of the server to add. The incorrect entry may prevent the specified server from being properly monitored.

(Example: When a general server is assigned with the "Blade Server" type.)

table: Server Types

Type Name	Description
Automatic	The type of the added server is automatically detected.
Server	Add the server monitored by ServerView Agent.
Blade Server	Add a blade server.
Cluster	Select this item when a cluster system is added. This is not supported.
Desktop	Select this item when a desktop is added. This is not supported.
LDSM	Select this item when the server monitored with LDSM is added.
Other	Select this item when the TCP/IP objects other than servers are added.

3 Select the server to be added from the list.

- If you click the server to be added, the value is displayed in [Server Name] and [IP Address].
- Dragging a network group to the group tree view area in the [Server List] window also enables the entire group to be added.

POINT

- ▶ The server with the same name or network address as the server entered in the [Server List] window cannot be added.
- ▶ It is possible to add an entire network entity to the [Server List] window. In this case, all computers within a network are added as a new group (except for any computers that could not be found).
- ▶ Do not add individual server blades installed in a blade server to the [All Servers] group. For a blade server, individual server blades are not monitored. When you try to add a server blade to the [Server List] window, the window appears to confirm whether the entire blade server including the server blade is added.

4 Specify certain values in the following tab windows, if necessary.

[Network/SNMP] Tab

Specify certain network parameters.

[Community Name (a name of user community)]/[Polling Intervals]/[Timeout Value]/
[Connection Status Switching Trap (which sends a trap when server status changes)]/[Update Intervals] (the intervals at which an open window is updated) can be specified.

[Remote Service Board] Tab

When the remote service board is supported, specify an IP address for the secondary channel in the server. Click the [RSB Connection Test] to check that the RSB connection can be established.

[Local Note] Tab

Enter a local note for the server. This helps you to find some servers in the [Server List] window etc. MIB information obtained from the agent is added to a local note by clicking [Copy from MIB].

5 Click [Apply].

The [Server List] window is updated.

■ Adding Servers with Network Discovery

By specifying a subnet (the first three digits of IP address) or a domain name, Network Discovery searches and displays computer names and description information within the range.

Search by a subnet enables broader range of search than by the Windows NT domain. It is also possible to specify with DNS reference or PING.

This enables searching Linux servers and blade servers.

If you select a server and click [Apply] or drag, you can easily add your servers to the [Server List] window.

● Add a Subnet to the Network Discovery Group

- 1 Click the [File] menu → [Add Subnet].
- 2 Specify the first three digits of IP address.
The computers under the searched IP are listed.

● Add a Domain to the Network Discovery Group

To add a domain to the Network Discovery group, perform the following procedure:

To add the domain name for the Windows NT server only

- 1 Click the [File] menu → [Add Domain].
- 2 Enter a domain name.
When the domain name that Microsoft Windows Network could not detect is entered, an error message appears.

To add user-defined domains

- 1 Drag a domain in the My Networks group to the Network Discovery group.
All the user-defined domains can be added to the Network Discovery group.

○ POINT

- ▶ Delete a subnet or a domain from the Network Discovery group
Select a subnet or a domain that you want to delete from the Network Discovery group and then click the [File] menu → [Remove] or press the [Delete] key.
- ▶ Change browser options
Select the IP or domain to change and then right-click to select [Options].
The following two browser options are provided:
 - Acquire Host Name with DNS, WINS, or Broadcasting
Generally the SNMP is used to obtain the host name and description information for searching networks. When this option is selected, name resolution is enabled with DNS, WINS, or broadcasting even if the SNMP request fails.

- Check Controllability Using PING (ICMP)
Generally a browser uses the SNMP to check an object type and controllability. When this option is selected, it is checked if PING can access to the object even if the SNMP request fails.
- ▶ The valid range of browser options
Browser options settings are enabled for a particular subnet or the entire server browser. When you click [OK] in the browser options window, it is enabled only for the selected subnet. When you click [Update All], it is enabled throughout the server browser.
- ▶ When you specify the browser options for the My Networks or any domain, they are assigned throughout the server browser.
- ▶ If searching host names or checking with PING is disabled in the options settings window, browsing can stop.
When these options are selected, it may take very long time to complete the process.
- ▶ To display unknown servers
Click the [View] menu → [Display Unknown Servers] to display unknown servers in the browser window (they are not displayed by default).
Incidentally, unknown servers involve the following:
 - Do not have its hostname and description information.
 - Do not respond to the PING request (only when the PING option is selected).
- ▶ Updating a window
 - If you click the [View] menu → [Update], the information of a browser window is updated.
 - If you click the [View] menu → [Update ALL], the information of all the subnets and domains that are referenced is updated.

■ Creating Groups

Creating a group allows the monitored servers to be managed for each group.

- 1 Select the group that serves as a parent from the group tree.
- 2 Click the [File] menu → [New Group].
A new group is created. Specify any group name.

■ Deleting Servers

The servers that will not be monitored later are deleted from the monitored servers for ServerView.

- 1 Select the server to be deleted from the server list.
- 2 Click the [File] menu → [Remove].
It is now deleted from the [Server List] window.

■ Filter the Server List

The filter function allows you to restrict servers displayed in the [Server List] window to a specific server.

For example, when there are a lot of monitored servers, this helps you to display servers focusing on the "abnormal" servers only.

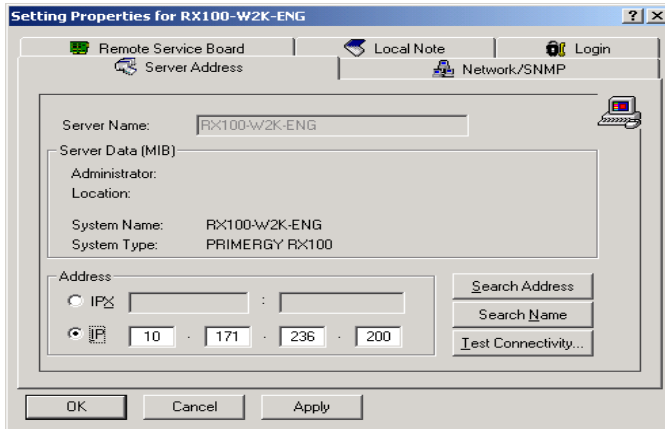
- 1 Click the [File] menu → [Filter Servers].
- 2 Select whether it is displayed or hidden and click [OK].

3.9.3 Verifying/Changing the Server Information

To verify/change any settings of your server, perform the following procedure:

- 1 Right-click on the server and click [Server Properties].

The [Server Properties] window appears.



POINT

- ▶ [Server Properties] can also appear in the following manner.
Select the server and click the [File] menu → [Server Properties].

- 2 Verify/change the settings in each tab window.

When you specify some items in each tab window, make sure to click [apply] before clicking another tab window.

[Server Address] Tab

This allows you to verify/change the IP address for the server. When the IP address is changed, click [Test Connection] to check if the connection is properly established.

[Network/SNMP] Tab

Certain network parameters are verified/changed. The items that can be specified are [Community Name (a name of user community)] / [Polling Intervals] / [Timeout Value] / [Connection Status Switching Trap(which sends a trap when server status changes)]/ [update Intervals] (the intervals at which an open window is updated).

When a load of your network or server is high, it can be improved by changing [Polling Intervals], [Timeout Value], and [Update Intervals].

[Remote Service Board] Tab

This allows you to verify/change the secondary channel of the server. By clicking [Test Connection], connection with the remote service board can be checked.

If you click [Settings], the Web interface to the remote service board starts and the window appears for entering [User Name] and [Password]. For the Web interface, refer to the following sections.

- For the remote service board (PG-RSB102/PG-RSB103/PG-RSB104): "5.3.1 Starting the Web Interface" (→pg.310)

[Local Note] Tab

This allows you to edit a local note for the server. The local note helps you to find certain servers in the [Server List] window. MIB information obtained from the agent is added to a local note by clicking [Copy from MIB]. When all excluding MIB information is identical in a local note, [MIBINFO<>] is displayed in the specific location.

[Login] Tab

Specifies [User Name] and [Password] used to write the assigned value to your server. To specify a password, select the [Password Settings] checkbox before assigning it. Passwords are not stored in any database for the security reason. When [Save Password] is selected, it is enabled until the program exits. If you restart the program, you must specify it again.

[TCP Applications] Tab

This tab appears only when a TCP/IP equipment is selected in the type of server. This allows you to specify applications for TCP/IP equipments.

Click [Browse] and then select the application path and the command line parameter or type them directly.

- 3 Click [OK] to close the properties window.

3.9.4 Threshold Manager

Any value may be specified for some parameters. This is called threshold and an upper/lower limit, a relative threshold value, and polling intervals can be assigned.

It can be associated with the actions specified in the alarm manager. Using four thresholds of the upper limit to relative values/the lower limit to relative values/the upper limit to fixed values/the lower limit to fixed values, it is linked to the alarm management. Thresholds measurement and alarm interruptions are separately handled with the server agent.

POINT

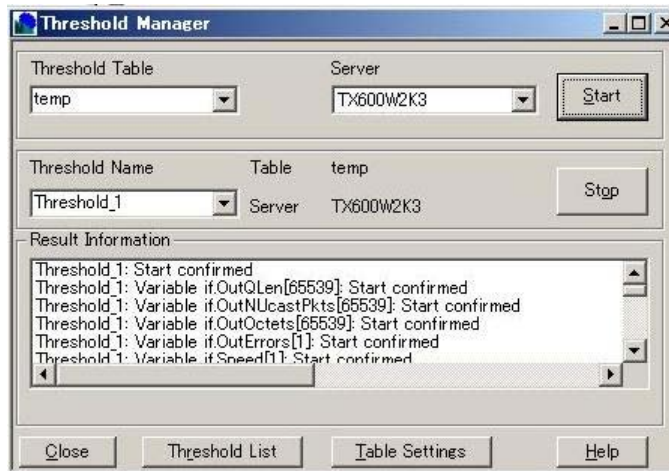
- ▶ The Linux server does not support the threshold monitoring with threshold settings.
- ▶ Selections and settings for the observed variables are grouped into a table (threshold table) and assigned to each server using the threshold manager. In order to avoid suspending one variable that is read by two tables by mistake, a single server can open only one table.
- ▶ When you specify the same item as the basic threshold for servers (hardware) using the threshold manager, it leads to monitoring from two sources in conjunction with the basic threshold. For more information about thresholds, refer to "Appendix E Threshold List" (→pg.390).
- ▶ Specifying relative values enables you to detect the variation beyond the relative values from the current value.

IMPORTANT

- ▶ Even if a threshold value is assigned with the threshold manager, ASR is not available. ASR is available only for the basic threshold assigned to servers (hardware). Additionally the threshold manager cannot change the basic threshold.

■ Specifying Thresholds

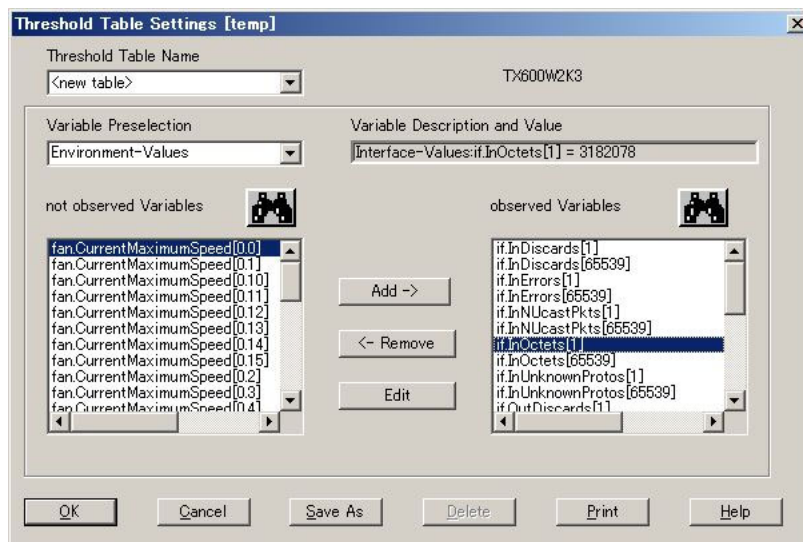
- 1 Select the server to specify a threshold.
- 2 Click the [Threshold] menu → [Threshold Manager].
The [Threshold Manager] window is displayed.



- 3 Select [Threshold Table] to specify for the server.
When you specify a new threshold table and change the value, click [Table Settings].

Table Settings

1. Click [Table Settings].
The [Threshold Table Settings] window appears.



2. Select a category from [Variable Preselection].
Items are listed in [not observed Variables].

3. Select an item from the [not observed Variables] list and then click [Add].
The [Add Threshold Settings] window appears.
For details on each item, refer to help topics.

4. Specify the threshold and then click [OK].
The assigned items are added to [observed Variables].
Specify the other items in a similar way.
5. Once you complete all the items, click [OK].
The [threshold table name settings] window appears.
6. Enter a threshold table name and click [OK].
The [Threshold Manager] window appears again.

- 4 Click [Start].
The [Save as] window appears.
- 5 Enter a threshold name and click [OK].
The [Confirm User Name and Password] window appears.
- 6 Enter the log-on name and password with administrator privileges and click [OK].
Monitoring with the specified threshold table is started.
When you terminate monitoring with a threshold table, click [Terminate].

POINT

- ▶ The specifications in the threshold manager do not directly relate to each monitoring items that ServerView originally monitors.
- ▶ When there occurs deviation from the range specified in the threshold manager, the following threshold deviation traps are sent. However errors are not reported because the original values, which are used in monitoring items such as the assigned range of temperature sensor displayed on [Environment], do not change.
 - Deviation from the Value Specified with Fixed Values: Threshold exceededATHreshold underflow

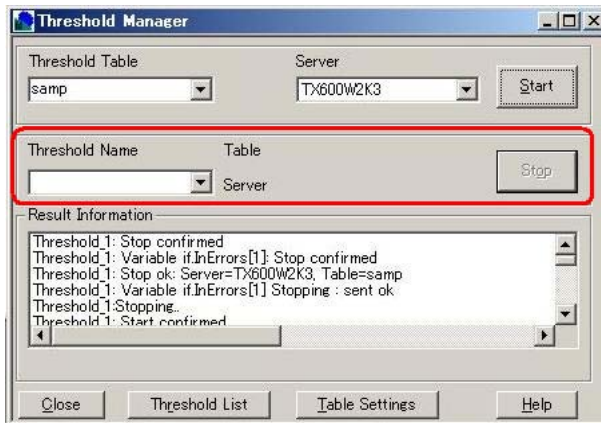
- Deviation from the Value Specified with Relative Values: DELTA-Threshold exceeded ADELTA-Threshold underflow

When you want to start any actions for these traps, specify the action for the corresponding Trap in the [Create/Edit Actions] window within [Alarm Settings].

■ Stopping Threshold Monitoring

Stop threshold monitoring:

- 1 Click the [Threshold] menu → [Manager].
The [Threshold Manager] window is displayed.
- 2 Select a [Threshold Name] to stop and click [Stop].



Threshold monitoring stops.

- 3 Click [Close] to exit.

■ Verifying Thresholds

To display the threshold list that is monitored with thresholds:

- 1 Click the [Threshold] menu → [List].
The [Threshold List] window is displayed.
- 2 Verify the information.
When you want to verify detailed thresholds, click [Threshold Manager]. When you change the settings in the running threshold table, stop it once to change the settings and then start it again.
- 3 Click [Close] to exit.

3.9.5 Report Manager

Creating reports helps monitor servers on a long-term basis.

The values selected in the report settings are regularly measured and recorded for a specific period.

Then the data is represented in a form of table or figure for evaluation.

This helps you to solve the problems at intervals caused by performance issues such as adding processors and disk capacity or installing a faster network adapter.

POINT

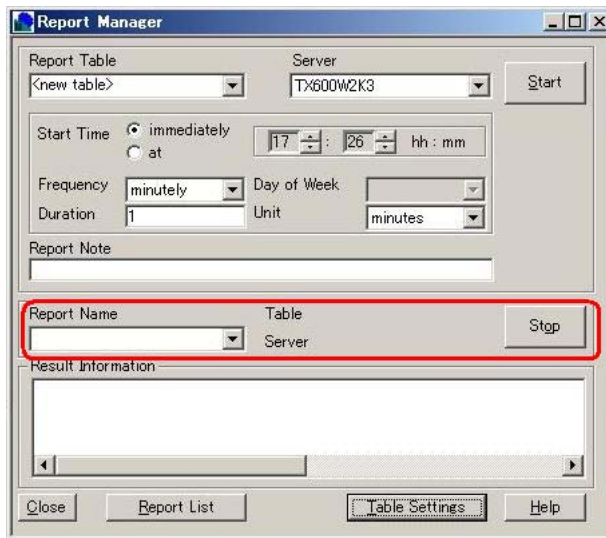
- ▶ The report manager settings do not directly relate to each monitoring items that ServerView monitors. Even if the report settings is not assigned, each of monitoring and notification is performed.
- ▶ To prevent one variable from being selected in two different tables, a single server can open only one table.
- ▶ The reports can be created up to 999. To create a new report when there are 999 reports already, delete an existing report.

■ Creating Reports

1 Select the server for which reports are created from the server list.

2 Click the [Reports] menu → [Report Manager].

The [Report Manager] window is displayed.



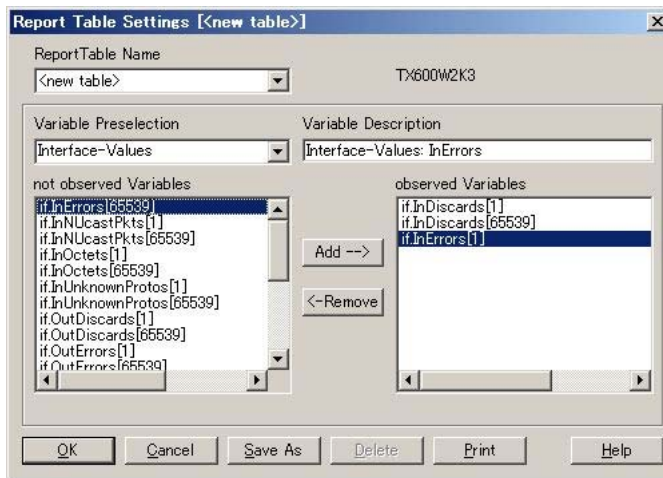
3 Select [Report Table] to specify for the server.

To specify a new report table and change the value, click [Table Settings].

Table Settings

1. Click [Table Settings].

The [Report Table Settings] window appears.



2. Select [Variable Preselection].
3. Select the item that you want from the [not observed Variables] list and then click [Add].

The item is added to [observed Variables].

Specify the other items in a similar way. Up to 13 items can be specified in one report table.

4. Once you complete the items to report, click [OK].

For a new table, the [Save as] window is displayed.

Enter a report table name and click [OK].

4 Specify starting time, frequency, and a reporting period.

Specify the reporting period in [Period]. If [Indefinite] is selected, the system value is monitored continuously.

5 Enter a report note.

For the report note, descriptions such as the report's contents are entered.

6 Click [Start].

The [Report Name Entry] window is displayed.

7 Enter a report name and click [OK].

The report will be created at the starting time specified.

When the period is specified, recording stops when it expires.

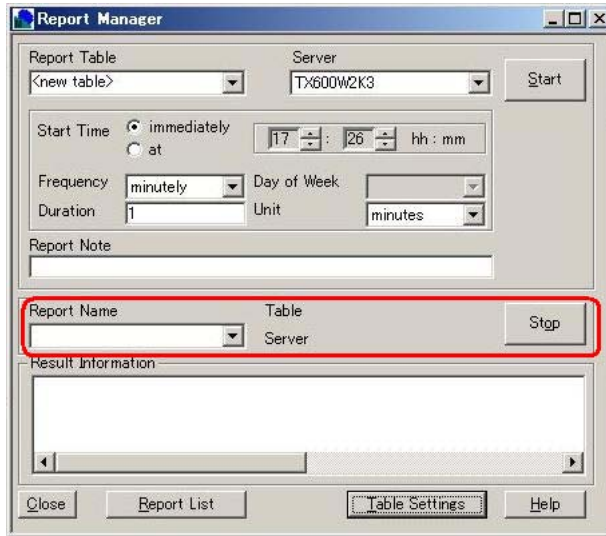
8 Click [Close].

The report manager exits.

■ Stopping Reporting

Stop reporting before a period limit expires.

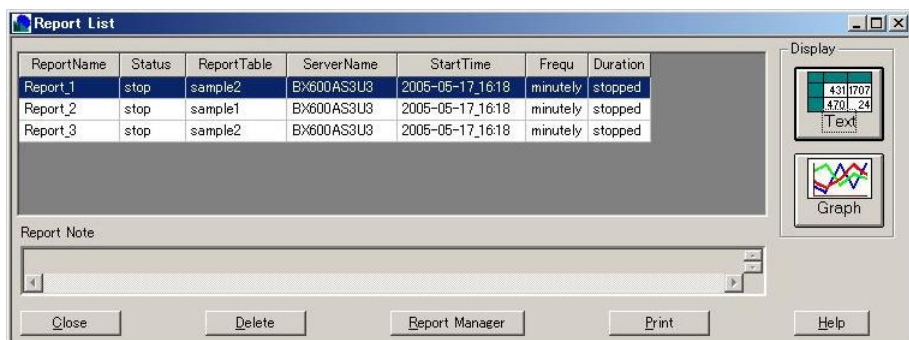
- 1 Select the server for which reports are created from the server list.
- 2 Click the [Reports] menu → [Report Manager].
The [Report Manager] window appears.
- 3 Select the report name to stop and click [Stop].



- 4 Click [Close].
The report manager exits.

■ Reviewing Reports

- 1 Click the [Reports] menu → [List].
The [Report List] window is displayed.



2 Verify the information.

Verifying details of reports

1. Select a report that you want to verify from the list and click [Text].
The [Text] window appears and the detailed information is displayed for each item of the report.

Verifying report Information in graphical representation

1. Click [Graph].
The [Graph] window appears and a history of report information is displayed in graphical representation.

3 Click [Close] to exit.

POINT

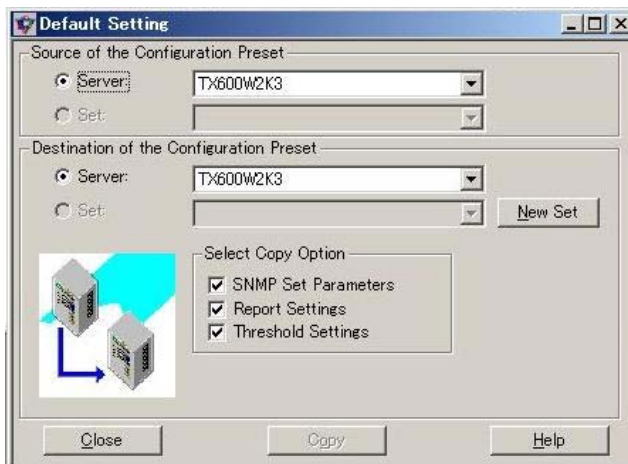
- ▶ Reports are created in the ASCII format. The created text file that is named "repnnn.txt" is saved in the "\ServerView_installDir\Reports\server_name" folder.
- ▶ This report can be exported to Excel in the following procedure:
 1. Import the report in Excel using the Excel text wizard.
Note that the fields in the report do not have fixed length and are delimited by a space at this time.
 2. Customize the Excel report layout or convert to a graphical format.

3.9.6 Copying Settings to the Other Servers

The settings assigned with ServerView (thresholds and reports) can be copied to the other servers to specify them. This helps to specify the same value in multiple servers.

- 1 After you complete the server settings, click the [Settings] menu → [Default Settings].

The [Default Setting] window appears.



- 2 Select the source server in [Source of the Configuration Preset].

3 Specify the server to which you copy the settings in [Destination of the Configuration Preset] and select the items to copy in [Select Copy Option].

4 Click [Copy].

The same settings as the source server are applied in the destination server.

■ Write Settings to a File or Read Settings from a File

You can also write the settings to a file or read them from a file.

In the [Default Setting] window, perform the following procedure:

- Select [Set] in [Source of the Configuration Preset] to specify the file from which the settings are read.
- Select [Set] in [Destination of the Configuration Preset] to specify the file to which the settings are written.

3.9.7 Monitoring Hardware

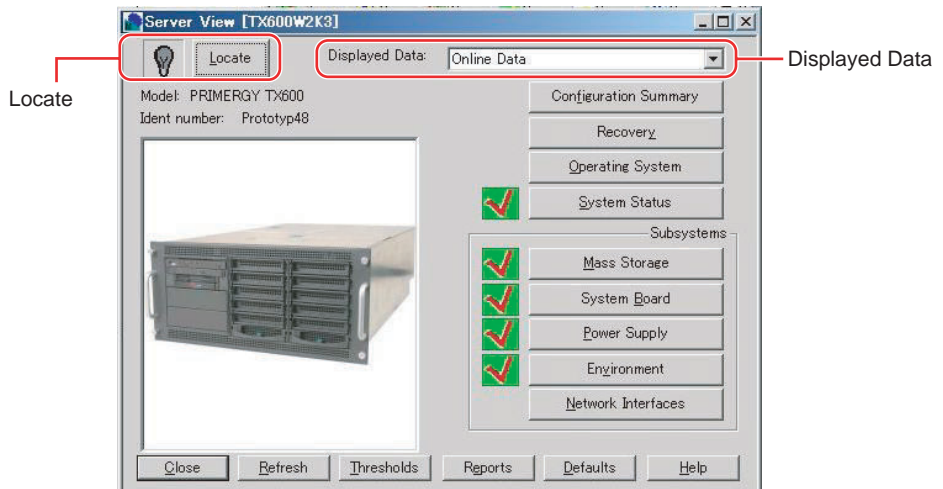
1 Select the server to monitor.

POINT

- ▶ For blade servers, refer to "3.9.8 Verifying the Status of the Blade Servers" (→pg.235).

2 Click [ServerView].

The [ServerView [Server Name]] window appears and the details of the selected server are displayed.



POINT

- ▶ The ServerView window can be displayed using one of the following methods.
 - Double-click the server.
 - Select the server and click the [File] menu → [Open].
 - Right-click on the server and click [Open].
- ▶ The following items are only available for the RSB mode. However they cannot be seen when the RSB mode is active and the remote service board (PG-RSB102/PG-RSB103/PG-RSB104) is installed.
 - Recovery
 - System Board
 - Power Supply
 - Environment
- ▶ When the RSB mode is active and the remote service board (PG-RSB102/PG-RSB103/PG-RSB104) is installed, the following dialog appears if you select the server to monitor and click [ServerView]. For a Web interface, refer to "5.3.1 Starting the Web Interface" (→pg.310).



Start the Web interface for the remote service board by clicking [Retry Access].

Locate

This enables the system identification LED display to switch. It is available only when a server supports the system identification LED display. The current status of system identification LED is displayed in icons.

There are three icons below.



Displayed Data

Either of the current data (Online Data) or the archive data (Archive Data - Creation date and time) can be specified. When a server is not accessible, [Archive Data] can be selected to display the created archive data. This allows you to verify the source of any trouble if necessary.

3 Verify the server status. Click the button of the item that you want to verify.

table: Status Verification of Servers

Items	Description
Configuration Summary	Displays general information for the selected server. The following information is displayed: <ul style="list-style-type: none"> • System Info (system information such as the installed OS) • MassStorage (information for hard disks, logical drives, file systems) • Network Interfaces (information for the connected network cards) • Expansion boards (information for expansion boards) • Recovery (contents of the error buffer) • Others (the power supply and up/down time of servers) • Overall Information (all information)
Recovery	Manages continuous monitoring and power supply for servers. This allows you to specify measures and restart/turn off servers when anomaly occurs. For more details, refer to "■ Recovery" (→pg.222).
Operating System	Displays data on the OS that is installed in the server. Data on the currently running process as well as its OS name, version, language, and system running hours are displayed.
System Status	Displays the system information in the status agent. Systems are divided into sub systems that consist of multiple components. The tree view displays an outline of status for all existing subsystems and components.
Mass Storage	Displays the details about hard disks and controllers. For more details, refer to "■ Verifying Mass Storage Status" (→pg.224).
System Board	Displays data for processors, memory modules, bus systems, and controllers (Ex. Board-ID of baseboards and a BIOS version of OS). For more details, refer to "■ Verifying the System Board Status" (→pg.231).
Power Supply	Displays the power supply settings and status for servers. For more details, refer to "■ Verifying the Power Supply Status" (→pg.232).
Environment	Displays temperature and status of fans for servers and memory expansion units connected to the server. Also displays whether or not some doors and the server's case are open. For more details, refer to "■ Verifying the Environment Status" (→pg.234).
Network Interfaces	Data on networks can be obtained. First, click the list entry required to obtain information continuously. <ul style="list-style-type: none"> • Information that can be obtained for existing network boards: e.g. Adaptor Model/Type/Physical Address/IPX Network/Speed/ IP Address/IP Subnet Mask/Bus Type & Number/Slot Number/ Function/IRQ/DMA Channel/I/O Address Range/Memory Address Range
Refresh	Refreshes information that is displayed in the window.
Thresholds	The threshold manager starts. For more details, refer to "3.9.4 Threshold Manager" (→pg.211).

table: Status Verification of Servers

Items	Description
Reports	The report manager starts. For more details, refer to "3.9.5 Report Manager" (→pg.215).
Defaults	The default settings start. For more details, refer to "3.9.6 Copying Settings to the Other Servers" (→pg.218).
Help	Help topics for each item appears.

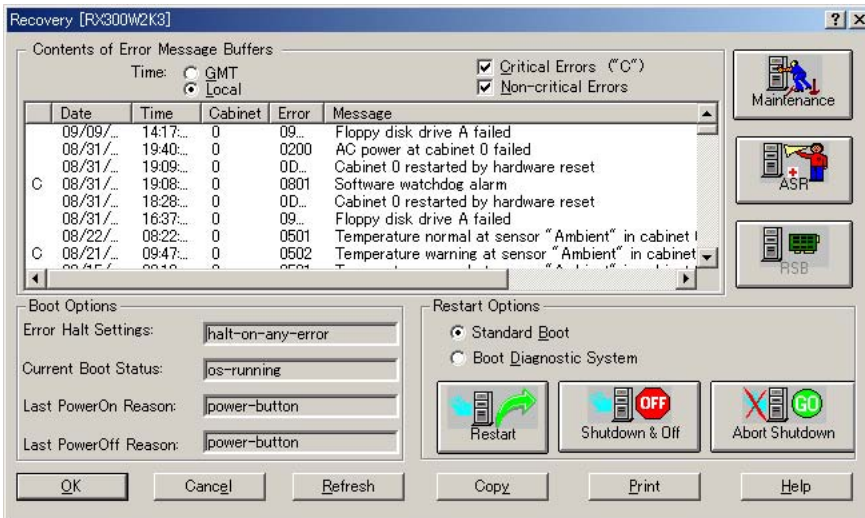
4 After completing verification for each item, click [Close].

The ServerView window closes and the server list window appears again.

■ Recovery

When you click [Recovery], the [Recovery] window appears.

Specify information about continuous monitoring and a response to alarms for servers.



POINT

- ▶ The [RSB] button is enabled only when RSB is available and the Sever Control agent supports it. The contents are not updated automatically while the window is being opened. Click [Refresh] to display latest information.

● Contents of the Error Message Buffer

Contents appeared in the error message buffer depend on whether the remote service board exists or not.

- When the remote service board exists
The SEL information that the remote service board acquired and errors that it detected itself appear in the contents of error message buffer.
- When the remote service board does not exist
The contents of SEL for a server itself appear in the error message buffer.

The list is sorted in the order of date/time and the latest entry is located at the top.

The message consists of five parts, which are "C" (when the message level is critical), date, time, an error number, and message texts.

Select time display either in Greenwich Mean Time or local time.

POINT

- ▶ The copy button and the print button can copy the contents of error message buffer displayed in the action window to a clipboard and print to a printer.

● Boot Options

Information about a booting process is displayed in the boot options. These are the information that ServerView displays for the information assigned to BIOS of the server.

- Error Halt Settings
The settings such as whether a system stops or not at the occurrence of errors are displayed.
- Current Boot Status
Displays the POST result.
- Last PowerOn Reason
The power-on reason is displayed.
- Last PowerOff Reason
The power-off reason is displayed.

● Maintenance

When you click [Maintenance], the [Maintenance] window appears. The amount of time already used for the internal CMOS battery and information about the fans are displayed.

● Automatic System Reconfiguration/Restart (ASR)

This allows you to specify server actions at the occurrence of faults. For more details, refer to "3.4 Serious Error Handling (ASR)" (→pg.123).

● Remote Service Board (RSB)

Click [RSB], and the [RSB Properties] window appears. RSB parameters can be specified.

- [Restart Settings] Tab
This provides the definition of startup/shutdown and restarting for servers and the boot status display. When ServerView is started in the RSB mode, the power-on and power-off operations are enabled. However the power-on and power-off operations for servers are protected with the password.
- [Backup Battery] Tab
This is not supported.
- [Interface] Tab
This displays the settings of the primary/secondary channel and the telephone number.

● Restart

Restarts the server. Specify the passed time required for the server to be restarted. When you click this button, the login window appears for security. The user name and password are required with ServerView administrator privileges.

● Shutdown & Off

This button shuts down the server and turns the power off. In addition, specify here the passed time required for the server to be shut down or its power is turned off. When you click this button, the login window appears for security. The user name and password are required with ServerView administrator privileges.

● Abort Shutdown

This button aborts any shutdown that is started by clicking [Restart] or [Shutdown & Off]. When you click this button, the login window appears for security. The user name and password are required with ServerView administrator privileges.

However when the shutdown has already started, aborting is disabled.

POINT

- ▶ When [Modify Default User] is executed in the login window, the default user is temporarily modified. However once ServerView exits, this information is lost. When you change the default login user, start [Server Properties] and specify it in the [login] tab window. For this procedure, refer to "3.9.3 Verifying/Changing the Server Information" (→pg.210).
- ▶ [Boot Diagnostic System] is not supported.

■ Verifying Mass Storage Status

If you click [Mass Storage], the detailed information appears about hard disks and controllers.

- Controller list
The critical data, number, status (OK or FAIL), type (EISA, PCI, ISA), slot, and driver name is displayed for controllers.
- Details for Selected Controller
Data on HD and EISA MIB is displayed.

POINT

- ▶ Make sure that you first select the list entry for which information is obtained. Otherwise information of another list entry may be displayed.

● Partition View

If you click [Partition View], the most critical server partition data (the number, status, type, name, offset, and size) is displayed in a table format.

No.	Status	Type	Name	Offset	Size
1	ok	7	NTFS Partition	0 MB	6997 MB
2	ok	15	Extended partition entry uses extended int13 servic...	6997 MB	28035 MB
3	ok	7	NTFS Partition	6997 MB	6997 MB
4	ok	5	Extended Partition	13994 ...	10001 MB
5	ok	7	NTFS Partition	13994 ...	10001 MB
6	ok	5	Extended Partition	23995 ...	11036 MB
7	ok	7	NTFS Partition	23995 ...	11036 MB

Details of the selected Partition

Associated Controller

Symbolic Name: AIC-7902(A4) Ultra320 PCI SCSI Controller
 Adapter Model: AIC-7902(A4) Ultra320 PCI SCSI Controller
 Bus Type & No. PCI 4 DeviceNumber: 2 Function: 2

Device Info

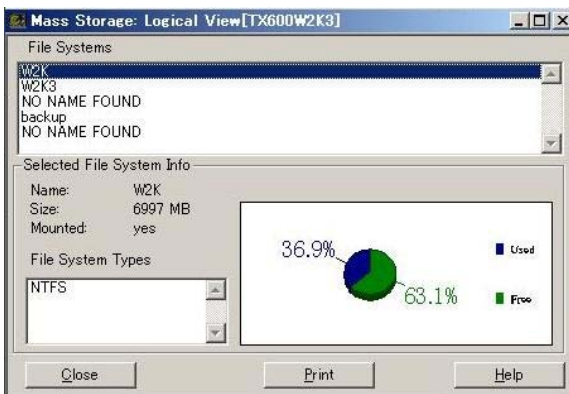
Type: directAccessDevice No: 2
 Name: FUJITSU MAP3367NC 0106

[Details of the selected Partition] displays some additional data on the partition selected from the list.

- Associated Controller
The controller that the partition belongs to is displayed.
- Device Info
The device in which the partition was created is displayed.

● Logical View

When you click [Logical View], the information about file systems that exist in logical drives is displayed.



- File Systems
The file systems of the selected server appears.

- Selected File System Info

The additional information (the name, size, mount, file system type, and Used/Free file system area in percentile unit) about the selected file system is displayed.

● Device View

When you click [Device View], detailed information about the storage devices connection to a specific controller appears.



- Details of the selected controller

The most critical data on the controller controlling devices is displayed again. The displayed data is the symbolic name, adapter model, and device number.
- List of the attached devices

The most critical data on devices attached to the controller is displayed. The displayed data is the number, status, S.M.A.R.T., type (refer to HD-MIB), and name. One or more devices can be selected from this list.
- Details of the selected device

The additional data on the device selected from the list is displayed. The displayed data is the capacity, SCSI channel, SCSI target ID, SCSI-LUN, sector, cylinder, block size, sector size, and symbol of Device Type with display status.

 - Self Monitoring and Reporting Technology (S.M.A.R.T.)

Information displayed in S.M.A.R.T. is returned from the S.M.A.R.T. procedure. S.M.A.R.T. is the technology used to detect an error of a hard device in its early stages (PDA = Prefailure Detection and Analysis). SCSI and ATA hard disk drives are supported.

● Configure

By clicking [Configure], you can open the RAID Manager window to configure the selected controller.

■ Mass Storage - the RAID controller

The status of the disk connected to the SCSI RAID card/the IDE-RAID card can be displayed. RAIDmanager/IDE-RAIDmanager is used to monitor and display the SCSI RAID card/the IDE-RAID card. Make sure to install RAIDmanager/IDE-RAIDmanager supplied with the SCSI RAID card/the IDE-RAID card.

The error information detected by RAIDmanager/IDE-RAIDmanager can be reported to the management console.



- ▶ The information of the SCSI RAID card/the IDE-RAID card may not be correctly displayed depending on a version number of ServerView and RAIDmanager/IDE-RAIDmanager. Therefore verify the status using RAID management tools such as RAIDmanager/IDE-RAIDmanager.
- ▶ For the settings of Global Array Manager (GAM), see below. When using the Linux installation representative service bundle type, refer to the release note supplied with the server. In addition, when using the Linux distribution in the SCSI type or the diskless type, obtain "Driver Kit" of the corresponding machine type from [Download Search] on the following home page to refer to "Installation Guide" contained in "Driver Kit".
 - The Fujitsu PRIMERGY website (<http://primergy.fujitsu.com>)

● Device View

System drives defined in the controller are listed in the left of the [Device View] window. Table entries are the serial number, status, SCSI ID (only PG-142B/PG-142C), size in MB, RAID level, and cache type.

When system drives are selected, the hard disk drive in which these system drives are defined is highlighted in the channel ID table. The selection button of the channel ID grid is used to display the status (colored symbols indicating Online/Dead/Standby-Rebuild) and size in MB. When an alternate device for a hard disk drive (CD-ROM Drives, streamers, printers) is connected, the corresponding image is displayed on the selection button.

● Adaptor View

When you click the [Controller] icon, the [Adaptor View] window appears.

Controller-specific data such as the device model, firmware version, BIOS version, cache size, bus type, slot, IRQ, base address, and EEPROM size (PG-143B only) appears in [Hardware Information].

The channel number, priority of recreating task, logical sector size, physical sector size, number of system drives, maximum number of system drives, number of physical devices, maximum number of physical devices, and BIOS version (PG-143B only) appear in [Disk Array Information].

● Display Physical Devices

When you click [Select Channel ID Grid], the [Display Physical Devices] window appears and the detailed information about the connected devices is displayed.

The information about the device model, device type (such as disks, CDROM Drives), adapter channel, channel adapter ID, and SCSI attribute (Fast SCSIWide SCSI and tagged queuing) is displayed in [SCSI Device Information].

The status, SMART status, capacity, recreating speed, parity errors, software errors, hardware errors, and other errors are displayed in [Disk Information].

● Details of the Bridge Controller

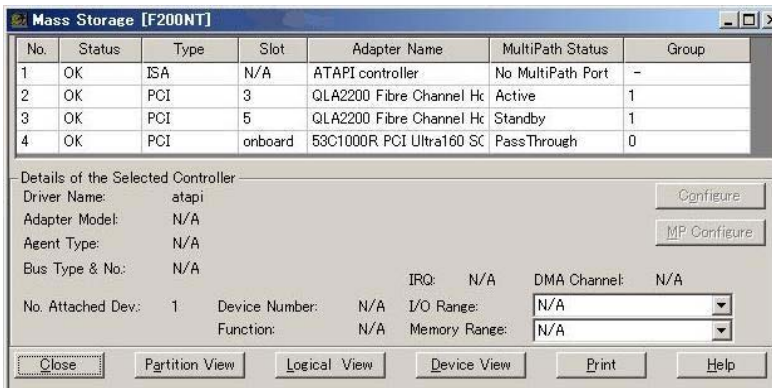
When a SCSI hard drive bridge controller is installed in a server, the information is displayed about the storage devices connected to a specific controller in the server when you click [Device View] in the [Mass Storage] window.

When you click [Configure], the application used to configure the selected controller is started.

When you click [View RAID], the information is displayed about the system drives defined in the selected controller. If the system drives are selected, the hard disk drive in which these system drives are defined is highlighted in the channel ID table.

■ Mass Storage - MultiPath

When MultiPath is installed, the detailed information about MultiPath is displayed by clicking [Mass Storage].



MultiPath allows you to connect multiple HBAs (some host bus adapters or fiber channel host bus adapters) to the same storage device through a redundant path. MultiPath provides high availability for devices even if some trouble occurs in connection or HBA. When a trouble occurs, input and output are transferred to devices through another I/O path. In addition, load balancing capability is provided to balance the load more uniformly.

Driver design does not depend on its original SCSI or fibre channel host adapter. The IDE disk controller is not supported. The driver design is compliant with MSCS.

When MultiPath is installed, the [MultiPath Status] information field, the [Group] information field, and the [MP Configure] button are added in the [Mass Storage] window.

● MultiPath Status

In the MultiPath status, one of the following values is displayed.

table: MultiPath Status

Value	Meaning
Path Through	The second port is not available.
Active	The channel is running. This is user-selected.
Standby (inactive)	Suspending. This is user-selected. When load balancing capability is enabled, this status is not displayed.
Disable	Suspending through maintenance activity.
Error	Any errors occurred at this port.
MultiPath Port does not exist.	This channel/port does not support the MultiPath function (Ex. atapi).

● Group

When there are no MultiPath group numbers or entries do not exist in the MultiPath function, "-" is displayed. One group, which consists of two (up to four) redundant connections between a system cabinet and an external storage cabinet, is wholly connected to the same device.

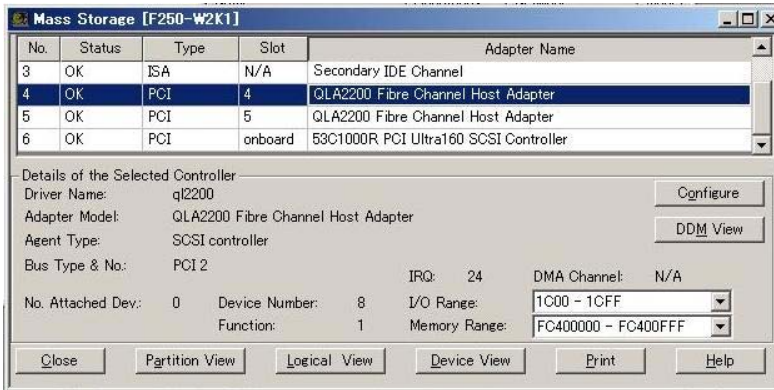
● MP Configure

When specifying the MultiPath group, select an entry in the external storage device list and click [MP Configure]. The [MultiPath Configuration Group 1] window appears. For details on each item, refer to help topics.



External Storage Devices - DuplexWrite

When DuplexWrite is installed, the information about DuplexWrite is displayed by clicking [Device View].



DuplexWrite is the software that improves the ability of disk storage sub system. DuplexWrite that is used with fibre channel connection technology can set up the disaster allowable settings. DuplexWrite duplicates writing operations so that the same information is contained in two disks of the different disk storage sub systems. This is called "Physical Mirroring" because it does not depend on logical data structure such as file system data.

If one of drives fails, DuplexWrite ensure that data processing can continue without interruption by accessing to the other disks that is still operating. When the drive that had a trouble is repaired, data can be recovered during the daily operation. It is not required to restart. This is applied to physical disks as well as complicated RAID volumes.

When DuplexWrite is installed, the following items are added:

- Write Status
- Duplex Disk
- [DW Configure] button

Write Status

In the Write status, one of the following values is displayed.

table: Write Status

Value	Meaning
Online	Indicates a DuplexWrite disk. This is read preferentially.
Error	The disk is offline because of an error state.
Recovery	The disk is under recovery.
Disable	The disk is set suspending through maintenance activity.
Simplex	The disk is not assigned for DuplexWrite.
N/A	DuplexWrite is not installed or can obtain no status.
MultiPath	This is the second, third, or forth path to the disk through MultiPath.
Missing	No disks exist (the entry created by COD of the partner disk).
<name>	The disk is used by the different MSCS cluster node <name>.

● Duplex Disk

Duplex Disk is required to specify the DuplexWrite group. The DuplexWrite group consists of one or two disks.

● DW Configure

When you specify the DuplexWrite group, select an entry in the [Device View] menu and click [DW Configure]. The [Disk Groups] window appears.

[DW Configure] can be selected when the DuplexWrite agent is installed in the selected server and the DuplexWrite status other than N/A, MultiPath, or <cluster node name> is displayed in the selected entry. For details on each item, refer to help topics.

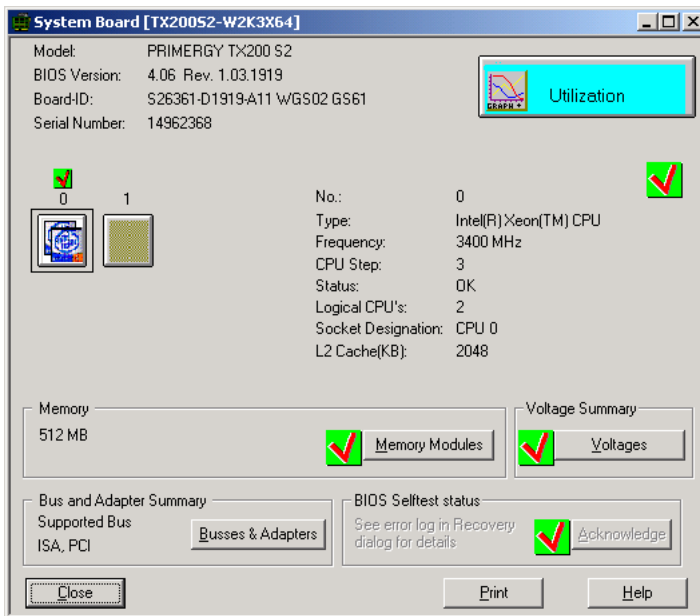
POINT

- ▶ ServerView provides the Archive Data mode for offline reading of data snapshots and the specified data. When this mode is enabled, DuplexWrite cannot be specified. It is not available except for closing, printing, or using help.

■ Verifying the System Board Status

The data for processors, memory modules, bus systems, and controllers (Ex. Board-ID of the system board and the BIOS version) is displayed by clicking [System Board].

Serial numbers may not be displayed depending on server machine types.



● Utilization

A usage percent of each processor or a usage percent of a single processor in multi-processor systems are displayed.

● **Memory Modules**

The number, bank, module state, starting address, size, approval, and name (optional) are displayed for every module by clicking [Memory Modules].

● **Voltages**

The information is displayed about voltage of the system board installed in the server is displayed by clicking [Voltages].

● **Busses & Adapters**

The information is displayed about the available bus systems (Ex. EISA, PCI), the connected controller, and its function is displayed by clicking [Busses & Adapters].

● **BIOS Selftest status**

The result of the self test executed by BIOS at PowerON is displayed for the server.

When it is the "abnormal" icon, it can be restored to the "normal" icon by clicking [Approve]. For details about "abnormal", verify [Contents of Error Message Buffer] within the [Recovery] window.

However this item is not displayed for BIOS that does not have its own self test notification function (including difference in versions).

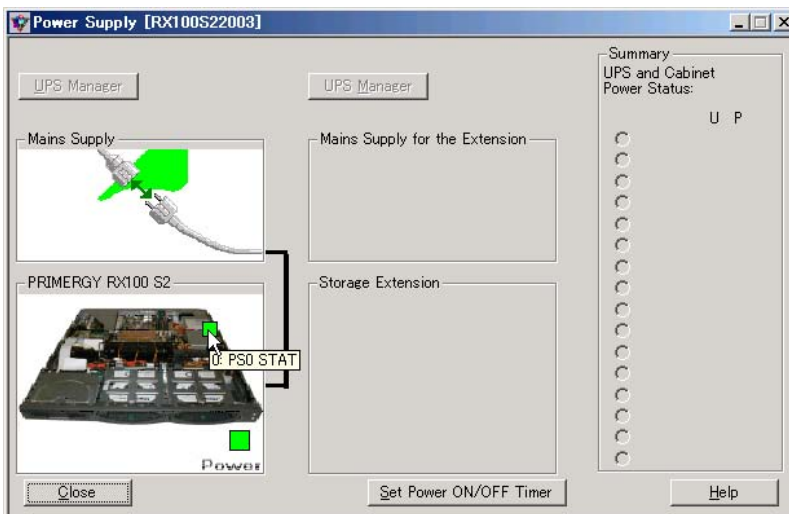
POINT

- ▶ If you reinstall ServerView Agent in the state where you have restored the "normal" icon by clicking [Acknowledge], the "abnormal" icon may appear again (a trap may occur at the same time). Click [Acknowledge] again to restore the "normal" icon.

■ **Verifying the Power Supply Status**

The power supply settings and status are displayed for servers are displayed by clicking [Power Supply]. When the mouse pointer is matched to status, the name is displayed. When the power supply operates properly, a green rectangle is displayed in the lower-right corner of the corresponding diagram.

For the redundant power supply, two cascaded rectangles are displayed.



● Main Supply

The connection status between the server and main supply. When connected to another expansion storage device, its main supply is also displayed.

Malfunction of a server or an expansion storage device is represented in a yellow or red rectangle. Usually a supply status is examined every 60 seconds.

● System Type

A server and BBU within a storage cabinet (if available) are displayed. The overall status of server power supply is represented in a green, yellow or red rectangle.

● Storage Extensions

Existing extension storage devices are displayed. This can also detect installation of BBU. The overall status of power supply in an expansion storage device is represented in a green or red rectangle.

● Summary

The selection radio button can be used to select an expansion storage device. At the same time, the green or red rectangle next to each selection button always reports the status of power supply within every expansion storage device.

● Set Power ON/OFF Timer

The ASR properties start and then the [Power ON/OFF] tab window is displayed by clicking [Set Power ON/OFF Timer]. The starting/exiting time of a server can be specified. For this procedure, refer to "[Power ON OFF] Tab (ServerView S2) / [Power ON/OFF] Tab (Management Console)" (→pg.129).

● UPS Manager

Unsupported.

When the UPS management software is installed and the settings for interaction with the UPS management software are assigned, the [UPS Manager] button is enabled.

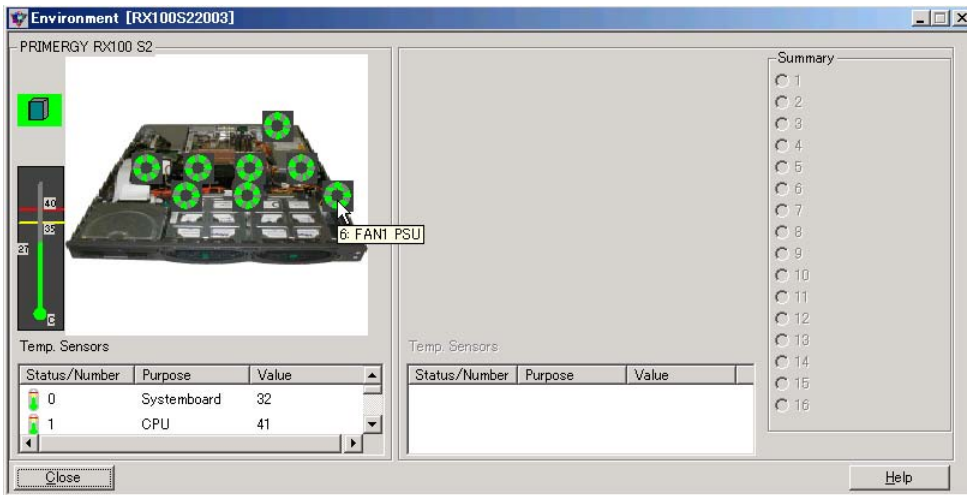
■ Verifying the Environment Status

Status of temperature and fans for servers and expansion units connected to the server is displayed by clicking [Environment]. When the mouse pointer is matched to status, the name is displayed. Also displays whether or not some doors and the server's case are open.

The threshold for such status display is determined by the basic threshold assigned to servers (hardware). This is not determined by the threshold assigned in the threshold manager.

POINT

- ▶ Some server types do not support the information whether doors or the server's case is open or shut.



A yellow server icon indicates that some doors or server's case is open. For an expansion storage device, a yellow rectangle is also displayed with in [Summary].

Fans and temperature are represented in icons. Each color indicates the status below.

table: Status of fans and temperature

	Shutdown	Danger	OK	Sensor Failure	No Verify
Temperature	red	yellow	green	blue	gray
Fan	red	yellow	green	---	gray

A temperature sensor always displays the value of the most critical sensor. When the values of all sensors are equal, the last sensor in the list is displayed. To call the status of a single sensor, click the line corresponding to the sensor from the list.

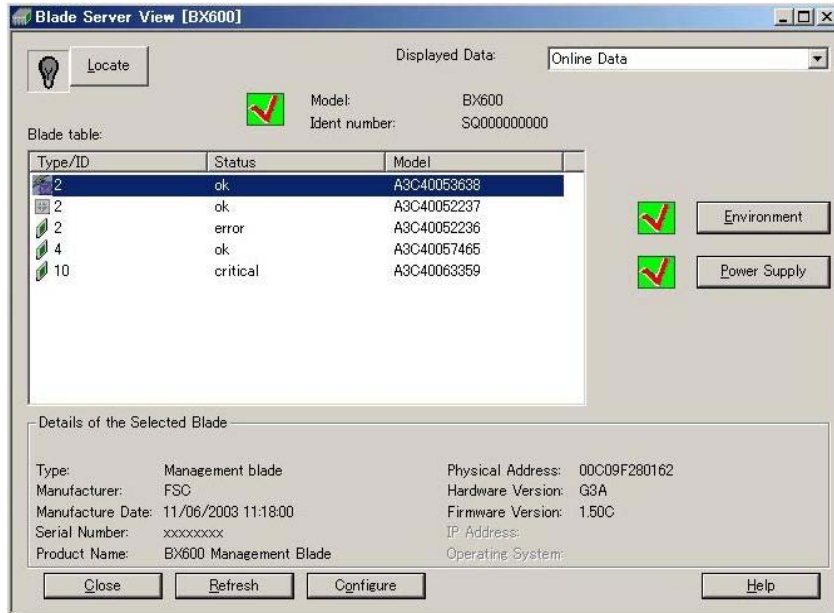
For redundant fans, two fan control symbols are cascaded. Both symbols must be green to indicate true redundancy.

3.9.8 Verifying the Status of the Blade Servers

Verify the blade server status.

- 1 Select a blade server.
- 2 Click the [File] menu → [Open].

The [Blade ServerView [Server Name]] window appears and the details for the selected server are displayed.



Locate

This enables the system identification LED display to switch. It is available only when a server supports the system identification LED display.

The current status of system identification LED is displayed in the icon. There are three icons below.

 :LED ON  : LED OFF

 :Flashing LED (Indicates a system error)

Displayed Data









Specify the data type to display for the selected blade server. When archive data is obtained, it can also be specified.

3 Verify the blade server status. Click the button of the item that you want to verify.



- ▶ When the security is enabled on the management blade, user login is needed for button operations. You can specify the user name and password by connecting to the management blade through Telnet or a Web interface.

table: Blade Server Status

Items	Description
Status of Entire System	The status of the entire blade server is displayed in the icon.
Model	The blade server system name specified in the management blade is displayed.
Ident Number	The ID number of the blade server system is displayed.
Blade Table	<p>The table for all the blades that exist in the blade server system is displayed. For Type/ID, the blade ID and blade type are displayed in the icon.</p> <p> : Management blade (master)</p> <p> : Management blade (slave)</p> <p> : Switch blade</p> <p> : fiber channel path through blade</p> <p> : LAN path through blade</p> <p> : KVM blade</p> <p> : fiber channel switch blade</p> <p> : Server blade</p>
Details of the Selected Blade	The detailed information of the selected blade is displayed.
Environment	Status for environment sub systems (fans, temperature) is displayed.
Power Supply	Status for power supply sub systems is displayed.
Refresh	Updates information that is displayed in the window.
Configure	<p>When the management blade or the switch blade is selected, the configuration window (Web browser) of each blade appears by clicking [Configure].</p> <p>For each blade settings windows, refer to the respective manual for the management blade or the switch blade.</p> <p>However when the server blade is selected, this button is disabled.</p>
Help	Help topics for each item appears.

4 After verification, click [Close] to exit.

3.10 Settings for ServerView Agent

Configuration Tools enables you to modify, save, and restore the settings of ServerView Agent.

3.10.1 Modify/Save/Restore Settings (Configuration Tools)

Configuration Tools enables you to modify, save, and restore the settings of ServerView Agent. It also helps you to modify, save, and restore the board settings when the remote service board is installed.

POINT

- ▶ Saving/Restoring is not allowed on the environment in which the versions of ServerView Agent are different.

■ Modifying Settings

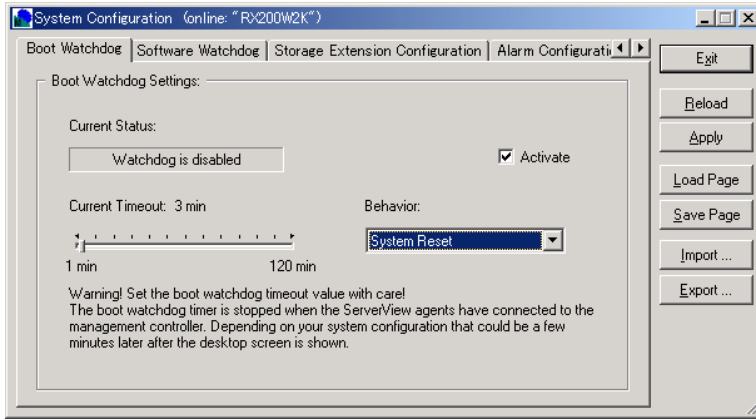
When ServerView Agents are installed in the Windows server, the remote service board can be configured. To change the configuration, perform the following procedure:

- 1 Click [Start] → [Programs] → [Fujitsu ServerView Agents] → [Configuration Tools] → [System Configuration].

The [System Configuration] window appears.



- 2 Select the [Change system selection manually] checkbox and click [OK].
A window appears for specifying items.



- 3 Click each Tab and set items if necessary.
This window includes the following configuration windows (tab windows).

table: System Configuration Settings Window

Tab Window	Contents
Boot Watchdog	The settings are associated with Boot Watchdog.
Software Watchdog	The settings are associated with Software Watchdog.
Storage Extension Configuration	The settings are associated with expansion external devices. They are not required to change.
Alarm Configuration (Management Controller/RSB)	The settings are associated with alarm notification. This is available only for the remote service board.
IP Configuration (Management Controller/RSB)	The settings are associated with IP. This is available only for the remote service board/controller.
Network Service Configuration (Management Controller/RSB)	The settings are associated with HTTP/Telnet. This is available only for the remote service board.
Remote User Configuration (Management Controller/RSB)	The settings are associated with user accounts. This is available only for the remote service board.
SNMP Configuration (Management Controller/RSB)	The settings are associated with SNMP. This is available only for the remote service board.
Serial Interface Configuration (Management Controller/RSB)	The settings are associated with serial interfaces. This is available only for the remote service board.
Disk Redirection	The settings are associated with disk redirection. This is available only for the remote service board. (This function is not supported.)
System Power On/Off Settings	The settings are associated with the power schedule. This is available only for the remote service board.

table: System Configuration Settings Window

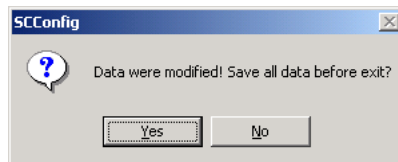
Tab Window	Contents
UPS Configuration	Unsupported. The settings are associated with UPS.
RSB S2 IP Configuration	The settings are associated with IP. This is available only for the remote service board (PG-RSB102/PG-RSB103/PG-RSB104).
RSB S2 Network Services	The settings are associated with HTTP. This is available only for the remote service board (PG-RSB102/PG-RSB103/PG-RSB104).

POINT

- ▶ Select the [Remote Service Board (RSB) installed] checkbox when the remote service board is installed.
- ▶ In addition, select the [Remote Service Board (RSB S2) installed] checkbox when the remote service board (PG-RSB102/PG-RSB103) is installed.
- ▶ Click [Reload] if you want to put back the settings. All the items are restored to the original settings.

4 Click [Apply] and [Exit].**POINT**

- ▶ When you change the settings without clicking [Apply] or read the settings with [Import], the message appears to confirm whether to save the settings. Click [Yes] for saving it or [No] otherwise.



Configuration Tools exits.

Save Settings

Save the settings as a file.

- 1** Start Configuration Tools.
- 2** Click [Export].
The [Save as] window is displayed.
- 3** Specify a file name and a location to which the file is saved, and click [Save].
The file is saved.
- 4** Click [Exit].
Configuration Tools exits.

■ Restoring Settings

Read the file in which the settings were saved and specify each item.

- 1 Start Configuration Tools.
- 2 Click [Import].
The [Open File] window is displayed.
- 3 Select the setting file to read and click [Open].
The information of the setting file to read is assigned to items.
- 4 Click [Exit].
The message appears to confirm whether to save the settings.
- 5 Click [Yes].
Click [No] when you suspend restoration of the setting.
Configuration Tools exits.

3.11 [Linux] How to Use ServerView Linux

This section describes how to use ServerView Linux (Agent/ServerView S2/AlarmService).

■ Displaying the ServerView Linux Agent Status

When you want to know status for the ServerView Linux agent, login as super user and execute the following command (an output result is shown).

```
# /etc/rc.d/init.d/srvmagt status
/usr/sbin/scagt: [ running ]
/usr/sbin/busagt: [ running ]
/usr/sbin/hdagt: [ running ]
/usr/sbin/unixagt: [ running ]
/usr/sbin/etheragt: [ running ]
/usr/sbin/biosagt: [ running ]
/usr/sbin/securagt: [ running ]
/usr/sbin/statusagt: [ running ]
/usr/sbin/invagt: [ running ]
/usr/sbin/vvagt: [ running ]
# /etc/rc.d/init.d/eecd status
eecd (pid 2085 2084 2059 1980 1979 1978 1977 1976 1975 1974 1973 1972
1971 1967 1965 1964 1963 1962) is running...
```

■ Starting and Exiting the ServerView Linux Agent

The ServerView Linux agent is automatically started at the server boot.

When you want to stop the ServerView Linux agent, login as super user and execute the following command (an output result is shown).

```
# /etc/rc.d/init.d/srvmagt stop
Stopping agent scagt [ OK ]
Stopping agent busagt [ OK ]
Stopping agent hdagt [ OK ]
Stopping agent unixagt [ OK ]
Stopping agent etheragt [ OK ]
Stopping agent biosagt [ OK ]
Stopping agent securagt [ OK ]
Stopping agent statusagt [ OK ]
Stopping agent invagt [ OK ]
Stopping agent vvagt [ OK ]
# /etc/rc.d/init.d/eecd stop
Shutting down eecd: TERM [ OK ]
```

IMPORTANT

- ▶ To start the ServerView Linux agent, login as super user and execute the following command.


```
# /etc/rc.d/init.d/eecd start
# /etc/rc.d/init.d/srvmagt start
```
- ▶ When you cannot start `/etc/rc.d/init.d/srvmagt`, execute the following command to verify status of the SNMP service. If the SNMP service stops, start it.


```
# /etc/rc.d/init.d/snmpd status
# /etc/rc.d/init.d/snmpd start
```

■ How to Operate ServerView S2/AlarmService

Connect to the < server > where ServerView S2 was installed using a browser as follows.

```
http://<server IP address >/sv_www.html
```

```
http://<server name >/sv_www.html
```

For the operation procedures of ServerView S2, refer to "3.1 Starting and Exiting ServerView S2" (→pg.76). For the operation procedures of AlarmService, refer to "3.5 AlarmService" (→pg.131).

● ServerView S2/AlarmService

When a Linux only environment is established, ServerView S2/AlarmService can monitor status of the other servers by installing it in any one server.

POINT

- ▶ Starting/exiting ServerView S2/AlarmService
ServerView S2/AlarmService, which operates as httpd service, cannot start/exit separately.
- ▶ Verifying operations of the installed ServerView S2/AlarmService
It is possible to verify the installed ServerView S2/AlarmService status by executing the following command:


```
# /etc/rc.d/init.d/sv_fwdserver status
snmptrapd (pid xxxx) is running...
```

■ Logs of the ServerView Linux Agent

The log created while the ServerView Linux agent runs is stored in `/var/log` with a name of `log.xxxx`.

However note that these logs are cleared when the ServerView Linux agent is restarted.

A log example is shown below.

```
-rw-r--r-- 1 root root 194 8 23 13:25 /var/log/log.biosagt
-rw-r--r-- 1 root root 193 8 23 13:25 /var/log/log.busagt
-rw-r--r-- 1 root root 30 8 23 13:25 /var/log/log.eecd
-rw-r--r-- 1 root root 746 7 7 13:25 log.eecd_mods_src
-rw-r--r-- 1 root root 195 8 23 13:25 /var/log/log.etheragt
-rw-r--r-- 1 root root 191 8 23 13:25 /var/log/log.hdagt
-rw-r--r-- 1 root root 193 8 23 13:25 /var/log/log.invagt
-rw-r--r-- 1 root root 257 8 23 13:25 /var/log/log.scagt
-rw-r--r-- 1 root root 194 8 23 13:25 /var/log/log.securagt
-rw-r--r-- 1 root root 195 8 23 13:25 /var/log/log.statusagt
-rw-r--r-- 1 root root 193 8 23 13:25 /var/log/log.unixagt
-rw-r--r-- 1 root root 280 8 23 13:26 /var/log/log.vvagt
```

POINT

- ▶ ServerView Linux Agent uses the operating system logrotate function, and restarts on a periodic basis. Logs (/var/log/log.xxxx) are cleared each time it restarts.

Chapter 4

Using RemoteControlService

4

This chapter explains how to use RemoteControlService.

4.1 Overview of RemoteControlService	246
4.2 Preparation	252
4.3 Starting and Exiting	268
4.4 How to Use	280

4.1 Overview of RemoteControlService

RemoteControlService is a software that remotely controls the PRIMERGY server. This section describes the functions of RemoteControlService and its system requirements.

■ RemoteControlService

RemoteControlService gives access to the server's system boot phase (POST) for remotely control from administration terminal. This helps to set up the server's BIOS from the administration terminal and start MS-DOS to run certain programs in the server from a MS-DOS floppy disk loaded in the terminal.

■ Components of RemoteControlService

RemoteControlService consists of the following two components on the server side and administration terminal side.

● RomPilot, RemoteConsoleManager (RCM), IPMI

RomPilot, RCM, and IPMI are components of the server side.

- RomPilot, RCM

These are the server's advanced BIOS functions that support a LAN driver at POST in servers.

RomPilot and RCM give access to server at POST through LAN. When the server has an onboard LAN, the server is regularly equipped with the onboard LAN driver.

- IPMI

This is the server's BMC function that provides reset, power OFF/ON, console redirection in text modes and so on.

Supported components depend on machine type.

- RomPilot

PRIMERGY B225/PRIMERGY C150/PRIMERGY C200/PRIMERGY F200/PRIMERGY F250/
PRIMERGY H200/PRIMERGY H250/PRIMERGY H450/PRIMERGY L200/PRIMERGY N400/
PRIMERGY N800/PRIMERGY P200/PRIMERGY P250/PRIMERGY R450/PRIMERGY L100

- RCM

PRIMERGY L100

- IPMI

- IPMI 1.5

PRIMERGY RX100 / PRIMERGY TX150 / PRIMERGY TX200 / PRIMERGY RX200 /
PRIMERGY RX300 / PRIMERGY TX150 S2 / PRIMERGY RX100 S2 / PRIMERGY RX200 S2 /
PRIMERGY RX300 S2 / PRIMERGY TX200 S2 / PRIMERGY RX100 S3 / PRIMERGY TX150 S4

- IPMI 2.0

PRIMERGY RX600 S2

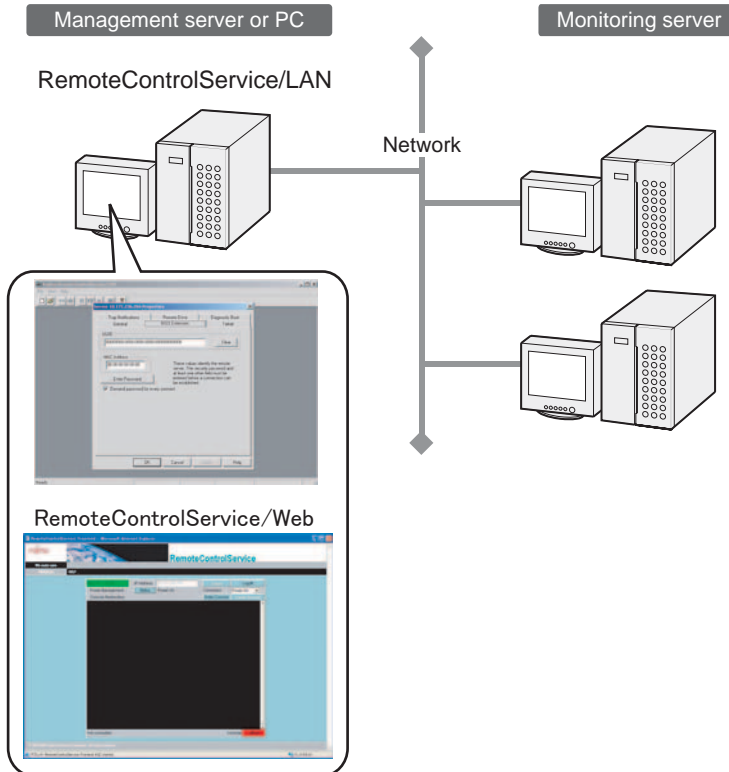
POINT

- ▶ For the support of blade servers, refer to "PRIMERGY BX600 Hardware Guide (Management Blades)".

● RemoteControlService/LAN, RemoteControlService/Web

This software that remotely controls the server is installed in an administration terminal.

RemoteControlService/Web installs as a plug-in of management console (ServerView S2), and is software of the Web base that remotely controls the server.



4.1.1 Functions

RemoteControlService includes the following functions:

- Remote Drive
- Console Redirection
- Wakeup On LAN (WOL)
- Support of Remote Service Board
- Power Management

● Remote Drive

This provides the function that starts MS-DOS in servers from a floppy disk or an image file loaded in the administration terminal. However this function is available only in the server that supports RomPilot/RCM.

● Console Redirection

This provides the function that remotely controls server's window display, keyboard operations, or restart from the administration terminal at POST phase in the server. When the server's MS-DOS is started using a remote drive, remote control is enabled while MS-DOS is operating.

● Wakeup On LAN (WOL)

When a network adapter supports WOL in a server, the server can be powered on from the administration terminal through LAN. For details of the server's WOL function, refer to "User's Guide".

● Support of Remote Service Board/Remote Service Controller

When a remote service board is installed in a server, the server's window display, keyboard operations (only in text modes) and power on/off are enabled through LAN or WAN. Further more the server that has an onboard remote service controller can run this operation basically.

When a remote service board is installed in disk array devices, power on/off and state display are enabled through LAN or WAN for them.

● Power Management

The power supply control of the server and the state of the power supply of present server can be displayed.

4.1.2 System Requirements

System requirements for servers and administration terminals are as follows.

■ Server

table: System Requirements for Servers

Hardware	Software
<ul style="list-style-type: none"> LAN card: required (when an onboard LAN is installed, it is only available) BMC: BMC of installing server since RX600 S2 (For RemoteControlService/Web) 	No particular conditions

■ Administration Terminal

● For RemoteControlService/LAN

This can be used for the management of servers that came with ServerView V3.60 or older. See "1.3 System requirements"-**■ ServerView Console (installation to server or PC)" (→pg.20)". Use RemoteControlService/Web for the management of servers that came with ServerView V4.10 or later.**

● For RemoteControlService/Web

This can be used for the management of servers that came with ServerView V4.10 L10 or later. See "1.3 System requirements"-**■ ServerView S2/AlarmService (when OS is Linux)"** (→pg.22). Use RemoteControlService/LAN for the management of servers that came with ServerView V3.60 or older.

4.1.3 Notes

■ PRIMERGY ECONEL 30

RemoteControlService/LAN does not support the remote control function in PRIMERGY ECONEL 30.

■ RomPilot

The RomPilot function depends on machine type. The RomPilot function is not available in the server that does not support RomPilot in the advanced BIOS function. For support of this function, refer to "User's Guide".

■ Wakeup On LAN (WOL)


RemoteControlService/LAN provides the WOL function for the servers in the same segment as the administration terminal. The WOL function cannot operate for the servers in the different segments through routers. For this reason, install RemoteControlService/LAN in an administration terminal within the same segment as the server which you want to run the WOL function.

■ RemoteConsoleManager (RCM)

The RCM depends on machine type. The RCM is not available in the server that does not support RCM in the advanced BIOS function. For support of this function, refer to "User's Guide".

● Notes for Use

Please take note of the following points when you use RCM.

- The RCM remote console window does not support the pause button () in the tool bar.
- When the cold reset (disable RCM) or the cold boot (disable RCM) is executed, the console redirection turns enabled in the following way:
 1. Start RemoteControlService.
 2. Start OS in the target server.
 3. Start ServerView.
 4. Click [ServerView] → [Action] and select [Start Diagnosis System] from [Restart Options] in the [Actions] window.
 5. Click [Restart].

The target server will shut down and reboot.

It may try to perform Console Redirection during server bootup.
 6. Start Console Redirection using RemoteControlService.
 7. Start the BIOS Setup Utility.

The Setup utility can be started with the [F2] key.

8. Set [Console Redirection] to "Enabled" in the [Console Redirection] menu within the Setup utility.
9. Set [Next Boot Use] to "Boot Selection" in the [IPMI Configuration] menu within the Setup utility.
10. Exit the Setup utility.

■ Intelligent Platform Management Interface (IPMI)

The IPMI function depends on machine type. For support of this function, refer to "User's Guide".

● Notes for TX200/RX300 (common information)

- To connect to TX200/RX300 IPMI in RemoteControlService/LAN on your administration terminal, use "the unique address in the network that is different from the one specified for this server's OS" as "IP address for a server".
- The BMC version can be verified in the BIOS Setup window by pressing the [F1] key. It is displayed as follows:
 - "BMC_FW 1.x" example: BMC Firmware : 001.0013b
 - "BMC_FW 2.x" example: BMC Firmware : 002.0008b

● Notes for PRIMERGY TX200/RX300 (BMC_FW 1.x)

- Execute "● Storing the Server Password" (→pg.281) to specify the password in connection. Use any user ID.
- When [Save Server Password] is disabled, check the [Advanced BIOS Function (Server)] to on and execute [Save Server Password]. Then uncheck [Advanced BIOS Function (Server)].
- The console direction with RX200/RX300 IPMI is not supported.
- The IPMI connection may be unstable immediately after power control or reset is performed in TX200/RX300. It recovers in dozens of seconds.
- For RX300, the IPMI connection and power operation are not supported while OS operates.

● Notes for PRIMERGY TX200/RX300 (BMC_FW 2.x)

- Use the user name and password specified in Server Management Tools as the password when connecting.
- If OS hangs up in TX200/RX300, do not use [PowerCycle]. When you want to run [PowerCycle], set [P-On] after executing [immediate power off].
- When you want to send the [Esc] key to the server side during the console redirection, it is necessary to press the [Esc] key twice on the administration terminal side.

● Notes for PRIMERGY RX200

- When the console redirection is executed with RX200 IPMI, it is necessary to install the "QLogic RMCP Filter" on the administration terminal side.
- For the information about how to install and use "Qlogic RMCP Filter", refer to "Fujitsu RemoteControlService Hints".
- When performing the console redirection with RX200 IPMI, make sure to use IPMI for the server's power control.

- To run BIOS Setup in the console redirection, press the [F4] key while the following message appears:

```
F2>BIOSsetup
```

● Notes for PRIMERGY RX200 S2

A console redirection may not start after logging in to the console redirection with IPMI in PRIMERGY RX200 S2.

In this case, press the [Esc] + [Shift] + [8] key, the [Esc] + [q] key, and the [Enter] key while logged in. As the link is disconnected, log in again.

● Notes for Selection of IPMI Machine Type Names

For [Server Properties] of the version prior to RemoteControlService/LAN V3.13.02, menu items correspond to machine type names as follows. No menu items are supported except for the items below.

table: Correspondence of Menu Items to Machine Type Names in [Server Properties]

Machine Type Name	BMC Version	Corresponding Menu Item
PRIMERGY L100E		RX100
PRIMERGY RX100		RX100
PRIMERGY TX100		TX150
PRIMERGY TX200	1.xxxx	TX200 (BMC_FW 1.x)
PRIMERGY TX200	2.xxxx	TX200 (BMC_FW 2.x)
PRIMERGY RX200		RX200 (BMC_FW 2.x)
PRIMERGY RX300	1.xxxx	RX300 (BMC_FW 1.x)
PRIMERGY RX300	2.xxxx	RX300 (BMC_FW 2.x)

For the RemoteControlService/LAN V3.13.02 or later, machine type names are selected automatically. It is not necessary to specify.

● Notes for IPMI Connection

The following message may appear without connection when the IPMI connection is executed:

```
Service processor not reachable
```

In this case, connect it again. If the same message still appears after a few attempts, execute the following command in a command prompt of your administration terminal:

```
C:\>arp -s <connecting destination IP address> <connecting destination MAC address>
```

Example: C:\>arp -s 192.168.1.10 01-23-45-67-89-ab

Range of the Redirection through IPMI

The redirection through IPMI covers a range between the time after the end of BIOS memory checking and the time prior to the OS startup as well as a period of the DOS mode.

The redirection in other states of the server is unsupported.

■ IPMI Connection between Different Segments

The IPMI connection can connect to any networks in different segments.

In this case, the port number 623 must be open to a target network.

4.2 Preparation

Set RomPilot, RCM or IPMI and install RemoteControleService/LAN, RemoteControleService/Web in preparation for the use of RemoteControleService.

4.2.1 Configuring RomPilot

To use the RomPilot function, it is necessary to configure RomPilot in the server.

Create the RomPilot setup disk to configure RomPilot and set up RomPilot according to the following procedure:

- 1** Prepare one formatted floppy disk.
- 2** Create the RomPilot setup disk.
Copy all the files in the following directory within the PRIMERGY Document & Tool CD to the floppy disk.
[CD-ROM drive]:\SVMANAGE\TOOLS\ROMPILOT\
- 3** Create a "floppy disk for starting the hardware configuration tool" or a "DOS floppy disk".
Use the ServerStart CD-ROM for creation. For the information about how to create the floppy disk, refer to "User's Guide" supplied with the server.
- 4** Insert the "floppy disk for starting the hardware configuration tool" or "DOS floppy disk" to a floppy disk drive and power on the server.
- 5** The DOS prompt appears.
When a menu window appears, select the [Basic (BIOS Environment Support Tools)] and press the [Enter] key.
- 6** Insert the RomPilot setup disk created in Step 2 to the server.
- 7** Enter the following command and press the [Enter] key.
A:\>rompilot.bat
The RomPilot setup starts.
- 8** Select [[Enabled] Settings (1)] in the first line to enable the RomPilot function.
Unless [Enabled] is selected, the other settings are not enabled.

9 Specify the other items.

The meaning of each item is shown in the table below.

table: RomPilot Setting Item

Items	Description
Network Driver/Slot	For LAN connection, a network adapter and its driver are required. The slot indicates a slot number of the network adapter used in LAN connection. The network adapter supported by RemoteControleService is displayed by pressing the [F2] key. Select the desired adapter to install its driver from the RomPilot setup disk. [Note]: Do not use the [F2] key. The driver for an onboard LAN has been installed on a regular basis.
Driver Load String	The strings entered in this item are transferred to the LAN driver. When the LAN driver is loaded with the [F2] key, the default strings appear in this entry. [Note]: Do not use the [F2] key. The driver for an onboard LAN has been installed on a regular basis.
Server Name	This is the name by which a server is identified. The server name allows up to 16 ASCII characters. Special characters are also available.
Local IP Address	This is an IP address of the LAN adapter installed in the server. Numerals only are available. Use the same IP address as the OS used.
Subnet Mask	This is a subnet mask of the LAN adapter installed in the server. Numerals only are available. Use the same subnet mask as the OS used.
Gateway Address	This is a gateway address of the LAN adapter installed in the server. Numerals only are available. Use the same gateway address as the OS used.
Front End 0/1/2 IP	This is an IP address (up to three) of the administration terminal running RemoteControleService/LAN. RomPilot attempts to connect first to the Front End 0, secondly to the Front End 1, and finally to the Front End 2. When there are no entries in these [Front End] items, the connection to RomPilot is not allowed.
Second SNMP Port	RomPilot sends a SNMP trap to the TCP port 9162. When this port has been used by another application, the alternative port can be specified in this item. [Note]: To use RemoteControleService, set the TCP port "9162".
Reset on lost conn.	When the settings are enabled, RemoteControleService/LAN is connected. If this connection is lost, RomPilot resets the server automatically.
Connect Timeout	If two or three administration terminals are configured in the Front End 0/1/2, the item indicates the intervals at which RomPilot attempts to connect sequentially to the Front End 0/1/2. If connection is not established within the time, it attempts to connect to the next Front End.
Password	This is a server password. A password is displayed in an encrypted format. When you connect to your server through RemoteControleService/LAN, you must enter the password specified in this item. [Note]: Make sure to specify the password.
Confirm Password	Enter the server password again for confirmation.
<F1>	The online help topics are displayed for the RomPilot setup by pressing the [F1] key.

table: RomPilot Setting Item

Items	Description
<F2>	A submenu is displayed by pressing the [F2] key. This allows you to select another network adapter and its driver. [Note]: RomPilot supports only the onboard LAN. Do not specify slot numbers other than the onboard LAN.
<F3>	The current settings are stored by pressing the [F3] key.
<ESC>	Exit the setup menu without changes stored by pressing the [ESC] key.

POINT

- ▶ When the RomPilot function is enabled, RomPilot sends a SNMP trap to an administration terminal at server bootup. When ServerView is installed on the administration terminal, the received SNMP trap can be referred to using the ServerView Alarm Service. When the administration terminal starts RemoteControlService/LAN and receives the SNMP trap from RomPilot, a remote window is opened automatically for the server.

10 Press the [F3] key to store the settings.

POINT

- ▶ The following message may be displayed when the settings of RomPilot is stored.

```
Network Driver/Slot inappropriate for detected
adapter(s): Select via <F2>
```

In this case, perform the following procedure:

1. Press the [F2] key to display the [Select Network Driver] menu.
2. Select [Onboard].
3. Press the [Enter] key to specify [Driver].
4. Press the [F3] key to store the settings.
5. Press the [ESC] key to exit the RomPilot setup.

11 Press the [ESC] key to exit the RomPilot setup.

4.2.2 Configuration for RCM

To use RCM, it is necessary to set [Console Redirection] in the BIOS Setup menu. For this procedure, refer to "User's Guide".

When setting RCM, please note the following points:

- Specify "Ethernet" for [Console Redirection] - [Connection over].
- Specify the same name as the server name of RemoteControlService/LAN in [Console Redirection] - [Server Name]. Inconsistency of server names causes failure in connection.
- Specify "Present" to [Console Redirection] - [Authorization password].

4.2.3 Configuration for IPMI

To use IPMI, it is necessary to set up in BIOS and Server Management Tools (IPMIview). Perform the following procedure. The setting procedure depends on machine type. For details, refer to "User's Guide" for your server.

■ For PRIMERGY L100E / RX100 / TX150

- 1 Start the BIOS Setup utility and set "Enabled" to the [ConsoleRedirection] item and "Ethernet" to the [Connection Over] item in the [Console Redirection] menu.
- 2 Select [User Management] from the [Server Management Tools] menu.
- 3 Specify the user name and password in [ID2] or under.
The user name and password specified in this item is necessary when connecting IPMI. However [ID1] is not available. Specify them in [ID2] or under.
- 4 Select "1" (enable user) for [Operation].
- 5 Press the [F1] key to store the settings.
- 6 Select the ID specified in Step 3 and press the [F2] key in the [User Management] window.
- 7 Set "4" to [Privilege Limit] and "0" to the other items.
- 8 Press the [F1] key to store the settings.
- 9 Select [LAN Configuration] from the [Server Management Tools] menu.
- 10 Select [LAN Channel] and specify the following items.

table: LAN Channel Setting Item

Items	Settings
BMC NIC IP Address	Enter the IP address of the server side.
MAC Address	Enter the MAC address of the server side.
SubnetMask IP Address	Enter the subnet mask for the network.
Default Gateway	Enter the default gateway for the IP Address network.
MAC Address	Enter the MAC address of the default gateway.

■ For PRIMERGY TX200 / RX300 (BMC_FW 1.x)

- 1 Start the BIOS Setup utility and configure [IPMI] in the [Advanced] menu as follows.

table: IPMI Setting Items

Items	Settings
ServerName	Enter a server name.
DHCP	Set "Disable".
LocalIP	Enter the unique IP address in the network that is different from the IP address specified in the server's OS.
SubnetMask	Enter the subnet mask for the network.
GatewayAddress	Enter the IP address of the default gateway.
User ID 1 Password	Do not enter anything.

■ For PRIMERGY TX200 / RX300 (BMC_FW 2.x)

- 1 Start the BIOS Setup utility and specify the following items.
Specify these items only for the console redirection. It is not necessary when using power control only.

table: Setting Items for BIOS Setup Utility

Items	Settings
[Server] - [Console Redirection]	
Console Redirect	Serial1
Baud Rate	115200
Media Type	LAN
Protocol	VT100+
Flow Control	None
Mode	Enhanced
[Advanced] - [Peripheral Configuration should]	
Serial 1	Enabled
Serial 1	3F8/COM1
Serial 1 Multiplexer	Shared

- 2 Select [User Management] from the [Server Management Tools] menu.
The following settings are also necessary when using power control only.
- 3 Specify the password for "Administrator" of [ID3].
The user name "Administrator" and its password specified in this item is necessary when connecting IPMI.
- 4 Select "1" (enable user) for [Operation].
- 5 Press the [F1] key to store the settings.
- 6 Select [Channel Configuration] from the [Server Management Tools] menu.

- 7 Select "#2 802.3_LAN" from [Select Channel] and enter the following items.

table: IP Address Setting Items

Items	Settings
BMC NIC IP Address/MAC Address	The IPMI is available only for the onboard LAN port 1. This does not allow the MAC address to be modified. Use the unique IP address in the network that is different from the IP address in the server's OS.
SubnetMask IP Address	Enter the subnet mask for the network.
Default Gateway IP Address	Enter the default gateway for the network.
MAC Address	Enter the MAC address of the default gateway.

- 8 Press the [F1] key to store the settings.

■ For PRIMERGY RX200

● Settings on the Server Side

- 1 Start the BIOS Setup utility and specify the following items.

Specify these items only for the console redirection. It is not necessary when using power control only.

table: Setting Items for BIOS Setup Utility

Items	Settings
[Server] - [Console Redirection]	
Console Redirect	Serial1
Baud Rate	115200
Media Type	LAN
Protocol	VT100+
Flow Control	None
Mode	Enhanced
[Advanced] - [Peripheral Configuration should]	
Serial 1	3F8/COM1
Serial 1 Multiplexer	Shared

- 2 Select [User Management] from the [Server Management Tools] menu.
The following settings are also necessary when using power control only.
- 3 Specify the password for "Administrator" of [ID3].
The user name "Administrator" and its password specified in this item is necessary when connecting IPMI.
- 4 Select "1" (enable user) for [Operation].
- 5 Press the [F1] key to store the settings.
- 6 Select [Channel Configuration] from the [Server Management Tools] menu.

- 7 Select "#2 802.3_LAN" from [Select Channel] and enter the following items.

table: IP Address Setting Items

Items	Settings
BMC NIC IP Address/MAC Address	The IPMI is available only for the onboard LAN port 1. This does not allow the MAC address to be modified. Enter the IP address assigned to the LAN port 1 in the server's OS.
SubnetMask IP Address	Enter the subnet mask for the network.
Default Gateway IP Address	Enter the default gateway for the network.
MAC Address	Enter the MAC address of the default gateway.

- 8 Press the [F1] key to store the settings.

● Settings on the Administration Terminal Side

The following steps are not necessary when using power control only. Perform them only when the console redirection through IPMI is used.

- 1 Install "QLogic RMCP Filter".
Refer to "Fujitsu RemoteControleService Hints".
- 2 Add the IP address of both BMC and the administration terminal to "QLogic RMCP Filter".
- 3 Reboot the administration terminal.

■ For PRIMERGY TX150 S2

● Settings on the Server Side

- 1 Start the BIOS Setup utility and specify the following items.
Specify these items only for the console redirection. This is not necessary when using power control only.

table: Setting Items for BIOS Setup Utility

Items	Settings
[Server] - [Remote Access Configuration]	
Remote Access	Enabled
Serial port number	COM1
Media Type	LAN
Baudrate	115200
Flow Control	None
Redirection After BIOS POST	Enhanced
Terminal Type	VT100
VT-UTF8 Combo Key Support	Disabled

table: Setting Items for BIOS Setup Utility

Items	Settings
[Advanced] - [Peripheral Configuration]	
Serial Port1 Address	3F8/IRQ4
Serial Multiplexer	Shared

- 2 Select [User Management] from the [Server Management Tools] menu.
The following settings are also necessary when using power control only.
- 3 Specify the password for "Administrator" of [ID3].
The user name "Administrator" and its password specified in this item is required when IPMI is connected.
- 4 Select "1" (enable user) for [Operation].
- 5 Press the [F1] key to store the settings.
- 6 Select [Channel Configuration] from [Server Management Tools] menu.
- 7 Select "#2 802.3_LAN" from [Select Channel] and enter the following items.

table: IP Address Setting Items

Items	Settings
BMC NIC IP Address/MAC Address	The IPMI is available only for the onboard LAN port. This does not allow to modify the MAC address. Enter the IP address assigned in the server's OS.
SubnetMask IP Address	Enter the subnet mask for the network.
Default Gateway IP Address	Enter the default gateway for the network.
MAC Address	Enter the MAC address of the default gateway.

- 8 Press the [F1] key to store the settings.

● Settings on the Administration Terminal Side

The following steps are not necessary when using power control only. Perform them only when the console redirection through IPMI is used.

- 1 Install "QLogic RMCP Filter".
Refer to "Fujitsu RemoteControlService Hints".
- 2 Add the IP address of both BMC and the administration terminal to "QLogic RMCP Filter".
- 3 Reboot the administration terminal.

■ For PRIMERGY RX100 S2

● Settings on the Server Side

1 Start the BIOS Setup utility and specify the following items.

Specify these items only for the console redirection. It is not necessary when using power control only.

table: Setting Items for BIOS Setup Utility

Items	Settings
[Server] - [Console Redirection]	
Console Redirect Port	Enabled
Baudrate	115200
Media Type	LAN
Protocol	VT100+
Flow Control	None
Mode	Enhanced
VT-UTF8 Combo Key Support	Disabled
[Advanced] - [Peripheral Configuration]	
Serial 1	Enabled
Base I/O Address	3F8/IRQ4
Serial Multiplexer	Shared

2 Select [User Management] from the [Server Management Tools] menu.

The following settings are also necessary when using power control only.

3 Specify the password for "Administrator" of [ID3].

The user name "Administrator" and its password specified in this item is necessary when connecting IPMI.

4 Select "1" (enable user) for [Operation].

5 Press the [F1] key to store the settings.

6 Select [Channel Configuration] from the [Server Management Tools] menu.

7 Select "#2 802.3_LAN" from [Select Channel] and enter the following items.

table: IP Address Setting Items

Items	Settings
BMC NIC IP Address/MAC Address	The IPMI is available only for the onboard LAN port. This does not allow the MAC address to be modified. Enter the IP address assigned in the server's OS.
SubnetMask IP Address	Enter the subnet mask for the network.
Default Gateway IP Address	Enter the default gateway for the network.
MAC Address	Enter the MAC address of the default gateway.

- 8 Press the [F1] key to store the settings.

● Settings on the Administration Terminal Side

The following steps are not necessary when using power control only. Perform them only when the console redirection through IPMI is used.

- 1 Install "QLogic RMCP Filter".
Refer to "Fujitsu RemoteControlService Hints".
- 2 Add the IP address of both BMC and the administration terminal to "QLogic RMCP Filter".
- 3 Reboot the administration terminal.

■ For PRIMERGY RX200 S2

● Settings on the Server Side

- 1 Start the BIOS Setup utility and specify the following items.
Specify these items only for the console redirection. It is not necessary when using power control only.

table: Setting Items for BIOS Setup Utility

Items	Settings
[Server] - [Console Redirection]	
Console Redirect Port	Enabled
Media Type	LAN
Baudrate	9800
Flow Control	None
Terminal Type	VT100+
Mode	Enhanced
[Advanced] - [Peripheral Configuration]	
Serial Port1 Address	3F8/IRQ4
Serial Multiplexer	Shared

- 2 Select [User Management] from the menu [Server Management Tools] menu.
The following settings are also necessary when using power control only.
- 3 Specify the password for "Administrator" of [ID3].
The user name "Administrator" and its password specified in this item is necessary when connecting IPMI.
- 4 Select "1" (enable user) for [Operation].
- 5 Press the [F1] key to store the settings.

- 6 Select [Channel Configuration] from the [Server Management Tools] menu.
- 7 Select "#2 802.3_LAN" from [Select Channel] and enter the following items.

table: IP Address Setting Items

Items	Settings
BMC NIC IP Address/MAC Address	The IPMI is available only for the onboard LAN port. This does not allow the MAC address to be modified. Enter the IP address assigned in the server's OS.
SubnetMask IP Address	Enter the subnet mask for the network.
Default Gateway IP Address	Enter the default gateway for the network.
MAC Address	Enter the MAC address of the default gateway.

- 8 Press the [F1] key to store the settings.

● Settings on the Administration Terminal Side

The following steps are not necessary when using power control only. Perform them only when the console redirection through IPMI is used.

- 1 Install "QLogic RMCP Filter".
Refer to "Fujitsu RemoteControlService Hints".
- 2 Add the IP address of both BMC and the administration terminal to "QLogic RMCP Filter".
- 3 Reboot the administration terminal.

■ For PRIMERGY RX300 S2 / TX200 S2

● Settings on the Server Side

- 1 Start the BIOS Setup utility and specify the following items.
Specify these items only for the console redirection. It is not necessary when using power control only.

table: Setting Items for BIOS Setup Utility

Items	Settings
[Server] - [Console Redirection]	
Console Redirect Port	Enabled
Media Type	LAN
Baudrate	9800
Flow Control	None
Terminal Type	VT100+
Mode	Enhanced

- 2 Select [User Management] from the [Server Management Tools] menu.
The following settings are also necessary when using power control only.

- 3 Specify the password for "Administrator" of [ID3].
The user name "Administrator" and its password specified in this item is necessary when connecting IPMI.
- 4 Select "1" (enable user) for [Operation].
- 5 Press the [F1] key to store the settings.
- 6 Select [Channel Configuration] from the [Server Management Tools] menu.
- 7 Select "#2 802.3_LAN" from [Select Channel] and enter the following items.

table: IP Address Setting Items

Items	Settings
BMC NIC IP Address/MAC Address	The IPMI is available only for the onboard LAN port. This does not allow the MAC address to be modified. Enter the unique IP address in the network that is different from the IP address assigned in the server's OS.
SubnetMask IP Address	Enter the subnet mask for the network.
Default Gateway IP Address	Enter the default gateway for the network.
MAC Address	Enter the MAC address of the default gateway.

- 8 Press the [F1] key to store the settings.

● Settings on the Administration Terminal Side

The following steps are not necessary when using power control only. Perform them only when the console redirection through IPMI is used.

- 1 Install "QLogic RMCP Filter".
Refer to "Fujitsu RemoteControlService Hints".
- 2 Add the IP address of both BMC and the administration terminal to "QLogic RMCP Filter".
- 3 Reboot the administration terminal.

■ For PRIMERGY RX600 S2

● Settings on the Server Side

- 1 Start the BIOS Setup utility and specify the following items.

Specify these items only for the console redirection. It is not necessary when using power control only.

table: Setting Items for BIOS Setup Utility

Items	Settings
[Server] - [Console Redirection]	
Console Redirect Port	Enabled
Flow Control	RTS/CTS + CD
Baud Rate	19.2k
Terminal Type	VT100+

- 2 Select [User Management] from the [Server Management Tools] menu.

The following settings are also necessary when using power control only.

- 3 Specify the password for "Administrator" of [ID3].

The user name "Administrator" and its password specified in this item is necessary when connecting IPMI.

- 4 Select "1" (enable user) for [Operation].

- 5 Press the [F1] key to store the settings.

- 6 Select [Channel Configuration] from the [Server Management Tools] menu.

- 7 Select "#2 802.3_LAN" from [Select Channel] and enter the following items.

table: IP Address Setting Items

Items	Settings
BMC NIC IP Address/MAC Address	The IPMI is available only for the onboard LAN port. This does not allow the MAC address to be modified. Enter the unique IP address in the network that is different from the IP address assigned in the server's OS.
SubnetMask IP Address	Enter the subnet mask for the network.
Default Gateway IP Address	Enter the default gateway for the network.
MAC Address	Enter the MAC address of the default gateway.

- 8 Press the [F1] key to store the settings.

■ For PRIMERGY TX150 S4 / RX100 S3

● Settings on the Server Side

- 1 Start the BIOS Setup utility and specify the following items.

Specify these items only for the console redirection. It is not necessary when using power control only.

table: Setting Items for BIOS Setup Utility

Items	Settings
[Advanced] - [Peripheral Configuration]	
Serial Multiplexer	BMC
[Server] - [Console Redirection]	
Console Redirect Port	Enabled
Media Type	LAN
Baud Rate	9600
Protocol	VT100+
Flow Control	None
Mode	Enhanced

- 2 Select [User Management] from the [Server Management Tools] menu.
The following settings are also necessary when using power control only.
- 3 Specify the password for "Administrator" of [ID3].
The user name "Administrator" and its password specified in this item is necessary when connecting IPMI.
- 4 Select "1" (enable user) for [Operation].
- 5 Press the [F1] key to store the settings.
- 6 Select [Channel Configuration] from the [Server Management Tools] menu.
- 7 Select "#2 802.3_LAN" from [Select Channel] and enter the following items.

table: IP Address Setting Items

Items	Settings
BMC NIC IP Address/MAC Address	The IPMI is available only for the onboard LAN port. This does not allow the MAC address to be modified. Enter the unique IP address in the network that is different from the IP address assigned in the server's OS.
SubnetMask IP Address	Enter the subnet mask for the network.
Default Gateway IP Address	Enter the default gateway for the network.
MAC Address	Enter the MAC address of the default gateway.

- 8 Press the [F1] key to store the settings.

● Settings on the Administration Terminal Side

The following steps are not necessary when using power control only. Perform them only when the console redirection through IPMI is used.

- 1 Install "QLogic RMCP Filter".
Refer to "H2 Hints".
- 2 Add the IP address of both BMC and the administration terminal to "QLogic RMCP Filter".
- 3 Reboot the administration terminal.

4.2.4 Installing/Uninstalling RemoteControleService/LAN

This section describes how to install/uninstall RemoteControleService/LAN into an administration terminal. The server attached PRIMERGY Document & Tool CD is used for the installation of RemoteControlService/LAN.

■ Installing

- 1 Log in as the user name with administrator privileges or equal privileges.
- 2 Exit all running applications.
- 3 Start the following installer from the PRIMERGY Document & Tool CD:
[CD-ROM drive]:\SVMANAGE\ENGLISH\RCS\RCSsetup.msi
RemoteControleService/LAN will be installed.

■ Uninstallation

Use [Add/Remove Programs] in [Control Panel] when uninstalling RemoteControlService/LAN. Make sure to uninstall "QLogic RMCP Filter" first when "QLogic RMCP Filter" has been installed.

4.2.5 Installing/Uninstalling RemoteControleService/Web

This section describes how to install/uninstall RemoteControleService/Web into an administration terminal.



- ▶ It is necessary to install ServerView S2 beforehand to install RemoteControlService/Web.

■ For Windows

● Installing

- 1 Log in as the user name with administrator privileges or equal privileges.
- 2 Exit all running applications.
- 3 Start the following installer from the PRIMERGY Document & Tool CD:
[CD-ROM drive]:\SVMANAGE\ENGLISH\RCS\RCSWsetup.msi
RemoteControleService/LAN will be installed.

● Uninstallation

Use [Add/Remove Programs] in [Control Panel] when uninstalling RemoteControlService/Web. Make sure to uninstall "QLogic RMCP Filter" first when "QLogic RMCP Filter" has been installed.

■ For Linux

● Installing

- 1 Log in as the user name with administrator privileges or equal privileges.
- 2 Exit all running applications.
- 3 Start the following installer from the PRIMERGY Document & Tool CD:

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svman-
age/Linux/JAPANESE/sv
# ./InstallRCSW.sh RemoteViewFE-X.X-X.i386.rpm
(X.X-X indicates version number.)
```

● Uninstalling

Execute the following command.

```
# rpm -e RemoteViewFE
```

4.3 Starting and Exiting

This section describes how to start and exit RemoteControlService/LAN, RemoteControlService/Web along with its menu.

4.3.1 Start and Exit for RemoteControlService/LAN

■ Starting

- 1 Click the [Start] button → [Programs] → [Fujitsu RemoteControlService] → [Fujitsu RemoteControlService LAN].
RemoteControlService/LAN is started.

POINT

- ▶ When RemoteControlService/LAN is started for the first time, the following window appears.



- 2 Enter the full pathname for the data directory and click [OK].
Data such as history files and message log files are stored in the data directory. The subdirectory<user name> is created in the data directory because data files are stored for each user who starts RemoteControlService/LAN.
A general path name for data directories is displayed as candidate. To change it, enter the full pathname.
If you click [Cancel], RemoteControlService/LAN will not be started.

- 3 Click [OK] when a message appears to confirm whether to create your password.
The [User Password] window appears.



4 After you enter the password and confirm it, click [OK].

The user password for RemoteControlService/LAN is created and RemoteControlService/LAN is started.

If you click [Cancel], RemoteControlService/LAN will not be started.

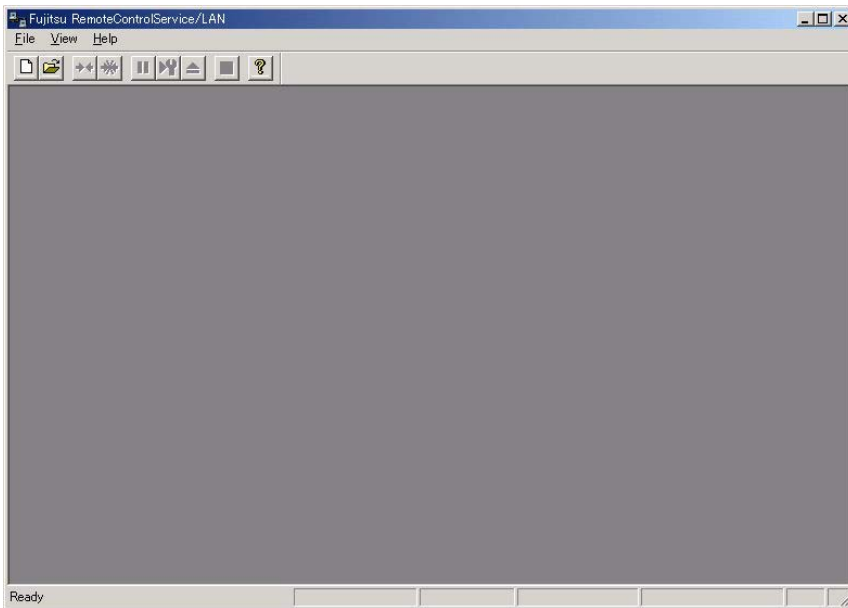
For the information about how to change a user password for RemoteControlService/LAN, refer to "■ User Password" (→pg.280).

POINT

- ▶ When RemoteControlService/LAN is started, the message "Warning: The file size of history log is too large. Please delete old logs". may appear.
In such a case, click [OK], enter the password, and then click the [View] menu → [History Log] to confirm the logs. When there are any unnecessary logs, it is recommended to delete those logs. However it is not necessary to delete logs when sufficient free space is left in the disk where the RemoteControlService data directory is located.

■ Menu List

The main window in RemoteControlService/LAN is displayed as follows.



This provides the connection to servers and the following control server tasks:

- Adding/removing servers
- Defining properties and default values for servers
- Connecting RemoteControlService/LAN to servers
- Options definition for server 's reboot and reset

● [File] Menu

table: File menu

Menu Item	Description
New	Specifies a new server name and IP address to be added.
Open	Selects the desired server from the server list for connecting.
Close	Disconnects the selected server. The remote console window is also closed.
Remove	Removes the server from the server list.
Properties	Specifies the server's properties (such as name, IP address, and device address).
Default	Defines the default value of the server's properties.
Settings	Specifies a data directory and user password.
Exit	Exits RemoteControlService/LAN and disconnects the server. When the server is being connected, a message appears to confirm whether to disconnect it.

● [View] Menu

table: View menu

Menu Item	Description
Tool Bar	Displays or hides the tool bar located at the top of the window.
Status Bar	Displays or hides the status bar located at the bottom of the window.
Object Summary	Displays the current status of all the servers in the server list.
History Log	Displays a history file in which all the actions are recorded.
Message Log	Displays a message file in which all the messages are recorded. When the Telnet window or the remote console window is open, this item does not appear.

● [Reset/Reboot] Menu

The [Reset/Reboot] menu is displayed only when the remote console window is active. Connect to any server and the menu item in the [Reset/Reboot] menu turn active.

table: Reset/Reboot Menu

Menu Item	Description
Cold Reset	Reboots the server.
Reset and Start Diagnosis System (Continue RomPilot)	Boots up the server from an IDE storage media using the RemoteControlService/Diagnosis system. [Note]: This function is not supported.
Next Reset Options	Defines the settings at the next system bootup. This item can also define the next reboot from a remote drive.
Wakeup	When a network adapter supports Wakeup On Lan (WOL) in a server, the server can be powered on from an administration terminal through LAN. For details of the server's WOL function, refer to "User's Guide".
Suspend at Next Connection	Suspends BIOS POST at the next connection. To resume BIOS POST, select [Run (Unload RomPilot)].

● [Window] Menu

Select a server from the server list and the [Window] menu turns active.

table: Window menu

Menu Item	Description
Cascade	Cascades the open windows.
Tile	Tiles the open windows.
Arrange Icons	Arrange icons.
Close All	Closes all the open windows.

● [Help] Menu

table: Help menu

Menu Item	Description
Overview	Displays the overview of RemoteControlService/LAN.
New Functions	Displays the overview of new functions.
Search Topics	Searches the RemoteControlService/LAN help topics.
How to Use Help	Displays how to use help.
RemoteControlService/LAN Online Manual	Displays the online manual.
To Contact Fujitsu	Displays the contact address of Fujitsu.
About RemoteControlService/LAN	Displays version information.

● Pop-up Menu

Depending on the current server status, certain menu items may not be available.

table: Pop-up Menu

Menu Item	Description
RomPilot Remote Console Window	
Close	Closes the RomPilot remote console window.
Connect	Connects to the server.
Connect/Setup	Connects to the server and starts the BIOS Setup.
Disconnect	Disconnects the server. The remote console window remains open.
Wakeup	When a network adapter supports Wakeup On Lan (WOL) in a server, the server can be powered on from an administration terminal through LAN. For details of the server's WOL function, refer to "User's Guide".
Change Disk Image	Changes a floppy/image file when a server is started from a remote drive.
Properties	Defines the desired server properties (such as name, IP address, and device address).
Run (Continue RomPilot)	When the server suspends at the POST stage through [Suspend POST] or [Suspend at Next Connection], it can be resumed by clicking [Run (Continue RomPilot)]. Use this function only when the server operates in the diagnosis mode. [Note]: The diagnosis mode is not supported.
Run (Unload RomPilot)	When the server suspends at the POST stage through [Suspend POST] or [Suspend at Next Connection], it can be resumed by clicking [Run (Continue RomPilot)].

table: Pop-up Menu

Menu Item	Description
Restore Last Window	The last remote console window reappears.
Erase	Erases the remote console window displayed with [Restore Last Window].
Change Colors	Changes a color palette in the remote console window.
Cold Reset	Reboots the server.
Reset and Start Diagnosis System (Continue RomPilot)	Boots up the server from an IDE storage media using the RemoteControlService/Diagnosis system. [Note]: This function is not supported.
Next Reset Options	Defines the settings at the next system restart. This item can also define the next restart from a remote drive.
Suspend at Next Connection	Suspends BIOS POST until the execute command is entered at the next connection setup.
RCM Window	
Close	Closes the RCM window.
Disconnect	Disconnects the server. The RCM window remains open.
Reconnect	Disconnects the server and reboots it.
Properties	Defines the desired server properties (such as name and IP address).
Restore Last Window	The last RCM window reappears.
Redraw	Redraws the RCM window.
Erase	Erases the RCM window.
Cold Reset	Reboots the server. The settings for Console Redirection are switched to "Disabled".
Power OFF	Power off the server.
Start BIOS Setup at Next Connection	Starts BIOS Setup at the next connection. This is not available along with [Reconnect].
Next Reset Options	Defines the settings at the next system reboot. This item can also define the reboot from a remote drive.
Help	Displays help topics.
Telnet Remote Manager Window	
Close	Closes the Telnet remote manager window.
Connect	Connects to the server.
Disconnect	Disconnects the server.
Sends Out Escape Sequence	Sends out an escape sequence to the server.
Properties	Defines the server properties.
Remote IPMI Manager Window	
Close	Closes the remote IPMI manager window.
Connect	Connects to the server.
Disconnect	Disconnects the server.
Erase	Erases the console redirection window.

■ Exiting

- 1 Click the [File] menu → [Close].
RemoteControleService/LAN exits.

4.3.2 Start and Exit for RemoteControlService/Web (For BMC connection)

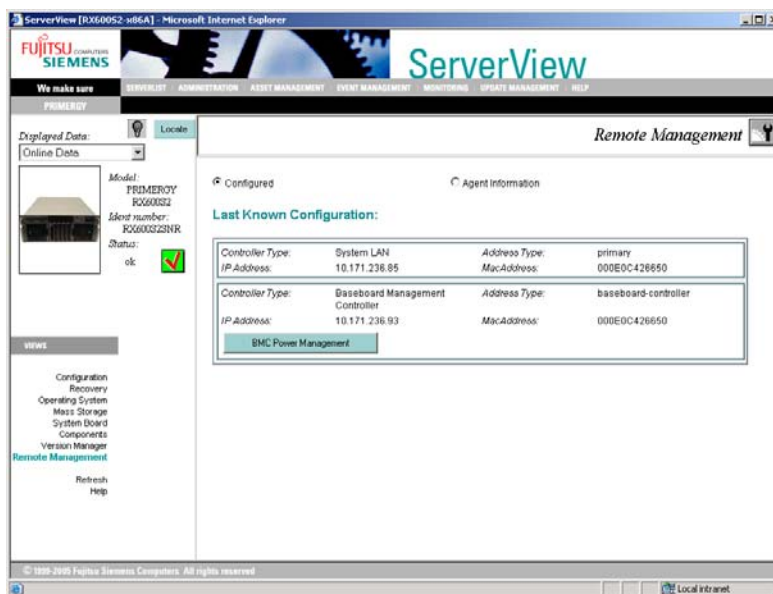
The start of RemoteControlService/Web is different when OS is started and when OS is not started.

■ Starting

● When OS is started

- 1 ServerView S2 window→[SERVERLIST] → Select of server →[VIEWS] →[Remote Manager].

The following window appears.

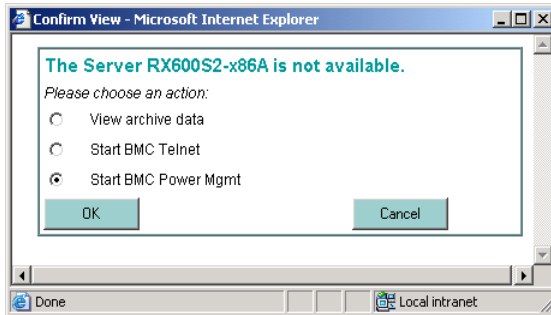


- 2 Click [BMC Power Management].
Starting RemoteConsoleService/Web.

● **When OS is not started**

1 The object server is selected from [ServerList] of ServerView S2 windows.

The following window appears.

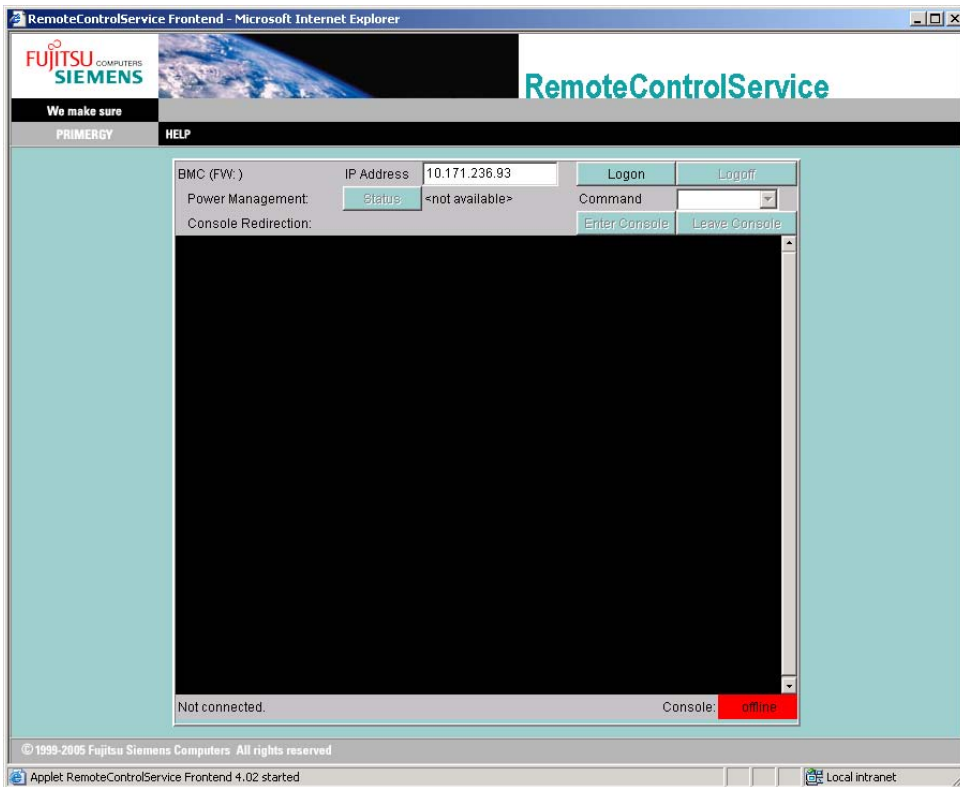


2 Select [Start BMC Power Mgmt], and click [OK].

Starting RemoteConsoleService/Web.

■ **RemoteConsoleService/Web Window**

When RemoteConsoleService/Web starts, the following window displayed.



After connected BMC, the following information references and the operations.

table: RemoteConsoleService/Web window

Item	Description
BMC(FW:)	After logon, the version of the BMC firmware is displayed.
IP Address	IP Address set to BMC is displayed.
[Loggon]	Logon to BMC displayed in "IP Address" .
[Loggoff]	Logoff BMC.
Power Management	Power supply control of the server. Select operation for the server from Command List. Click [Status], displaying the state of the power supply of present server.
Command	Select operation for power supply control of the server from following command.
Power On	Turning on the server.
Power Off	Turning off the server.
Reset	Restarting the server.
Power Cycle	Turning on and off the server.
Shutdown	Shut down the server.
Console Redirection	
[Enter Console]	Console Redirect is begun. When BMC is logged on, it is effective.
[Leave Console]	Console Redirect is ended.

■ Exiting

- 1 Click [Loggoff] when logging on to BMC.
- 2 Close RemoteControlService/Web browser.

4.3.3 Start and Exit for RemoteControleService/Web (For RSB connection)

The starting method of RemoteControlService/Web is different in whether or not OS is started.

IMPORTANT

- ▶ For connecting to the Remote Service Board, you can also use the Web interface, in addition to Telnet. For details, refer to "5.3 Displaying Each Monitoring Information" (→pg.310).
- ▶ When using Telnet to connect to the Remote Service Board (RSB), the Telnet port needs to be enabled using the RSB Web interface before the Telnet connection. For details, refer to "5.3.8 [Web/SSL Config] Page" (→pg.343).

● When OS is started

- 1 ServerView S2 window→[SERVERLIST] → Select of server →[VIEWS] →[Remote Manager].

The following window appears.

The screenshot shows the ServerView S2 web interface. The main content area is titled "Remote Management" and displays the "Last Known Configuration" for the selected server. The configuration table is as follows:

Controller Type	IP Address	Address Type	MacAddress
System LAN	10.171.236.225	primary	000E0C4267CA
RSB S2 LP	10.171.236.221	secondary	0030D309CB44
Baseboard Management Controller	10.171.236.233	baseboard-controller	000E0C4267CA

The "RSB S2 LP" controller is selected, and the "RSB Manager" button is highlighted. The "RSB Telnet" button is also visible.

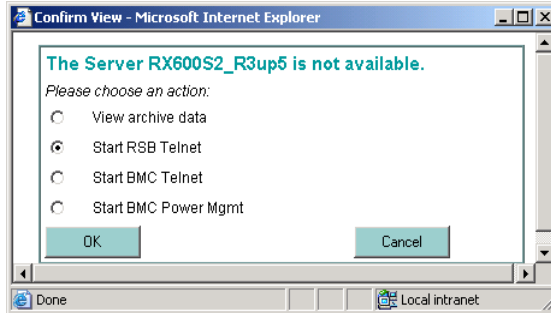
- 2 Click [RSB Telnet].
Starting RemoteConsoleService/Web.

POINT

- ▶ Web interface of remote service board can be started if [RSB Manager] is selected.

● When OS is not started

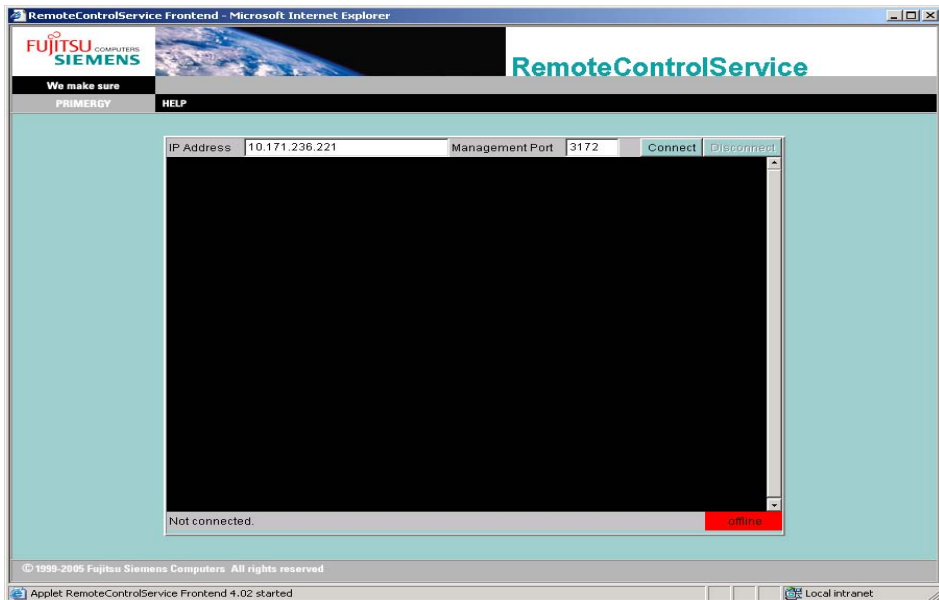
- 1 The object server is selected from [ServerList] of ServerView S2 windows.
The following window appears.



- 2 Select [Start RSB Telnet], and click [OK].
Starting RemoteConsoleService/Web.

■ RemoteConsoleService/Web Windows

When RemoteConsoleService/Web starts, the following window displayed.



After connected RSB, the following information references and the operations.

table: RemoteConsoleService/Web window

Item	Description
IP Address	IP Address set to RSB is displayed.
Management Port	Telnet Port number set to RSB is displayed.
[connect]	Logon to RSB displayed in "IP Address" .
[Disconnect]	Logoff RSB.

■ How to Use RSB Telnet

The RSB Telnet main menu for RemoteControlService/Web is the same as the RSB Telnet menu for RemoteControlService/LAN. Refer to "4.4.5 Support of the Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104)" - "■ Main Menu" (→pg.292).

■ Exiting

- 1 Click [Disconnect], when logon for RSB.
- 2 Close RemoteControlService/Web browser.

4.3.4 Start and Exit for RemoteControleService/Web (For ManagementBlade connection)

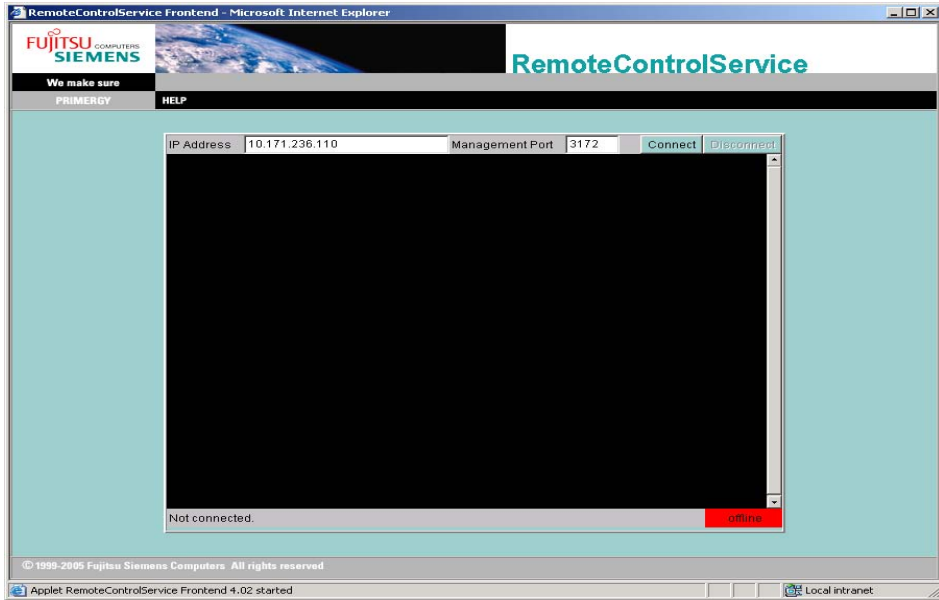
- 1 ServerView S2 window→[SERVERLIST] → Select of server →[Blade Server View] →[RemoteView].



Starting RemoteConsoleService/Web.

■ RemoteConsoleService/Web Window

When RemoteConsoleService/Web starts, the following window displayed.



After connected ManagementBlade, the following information references and the operations.

table: RemoteConsoleService/Web window

Item	Description
IP Address	IP Address set to ManagementBlade is displayed.
Management Port	Telnet Port number set to ManagementBlade is displayed.
[connect]	Logon for ManagementBlade, displayed in "IP Address" .
[Disconnect]	Logoff forManagementBlade.

■ Exiting

- 1 Click [Disconnect], when logon for ManagementBlade.
- 2 Close RemoteControlService/Web browser.

4.4 How to Use

This section describes how to use RemoteControleService/LAN.
For details, refer to the corresponding online help.

4.4.1 Password Management

RemoteControleService provides the password protection function to prevent unauthorized remote access to your server. Two passwords, one each for a user and a server are required.

■ User Password

A user password is used for authentication when logging in to RemoteControleService/LAN. To change the password specified at the first startup of RemoteControleService/LAN, follow the procedure below.

- 1 Click the [File] menu → [Settings] → [User Password].
- 2 Enter the old password and click [OK].
- 3 Enter a new password and click [OK].

POINT

- ▶ If you click [Cancel] without specifying any password at log in, you can enter a new password. However the server list is deleted.

■ Server Password

A server password is required to have access to the server's RomPilot/RCM using RemoteControleService/LAN.

The server password is specified for [Password] in the RomPilot setup or in the BIOS Setup menu of the server. For the RomPilot setup, refer to "4.2.1 Configuring RomPilot" (→pg.252).

The password is necessary each time connection is established and must be entered at the server's POST. The time of POST depends on the server hardware configuration.

● Disabling Password Prompt

If the server password prompt is disabled, it is not necessary to enter the server password when each connection is established.

IMPORTANT

- ▶ Disabling the password prompt causes a security risk. Understand fully the risk for specifying.

- 1 Click the [File] menu → [Properties].
The server list appears.

- 2 Select the server for which the password prompt is disabled.
When the server is connected, the properties for the server are displayed.
- 3 Click the [Advanced BIOS Function] tab.
- 4 Clear [Demand password for every connect].

● Storing the Server Password

The server password can be stored in RemoteControlService/LAN. When you store the server password and disable [Demand password for every connect], you can hide the password prompt at the connection to the server.

- 1 Click the [File] menu → [Properties].
The server list appears.
- 2 Select the server for which the password is stored.
When the server is connected, the properties for the server are displayed.
- 3 Click the [Advanced BIOS function] tab and click [Enter Password].
- 4 Enter a password and click [OK].

POINT


- ▶ The server password defined at the RomPilot setup is not changed.

4.4.2 Remote Server Management

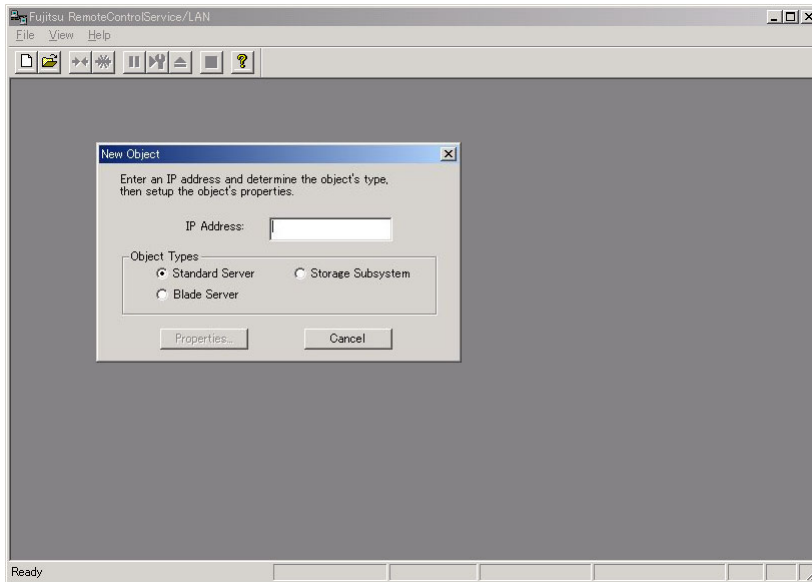
To manage the server remotely using RemoteControlService/LAN, connect to one of the server's RomPilot, RCM, IPMI, or remote service board (Telnet).

■ Adding a Server

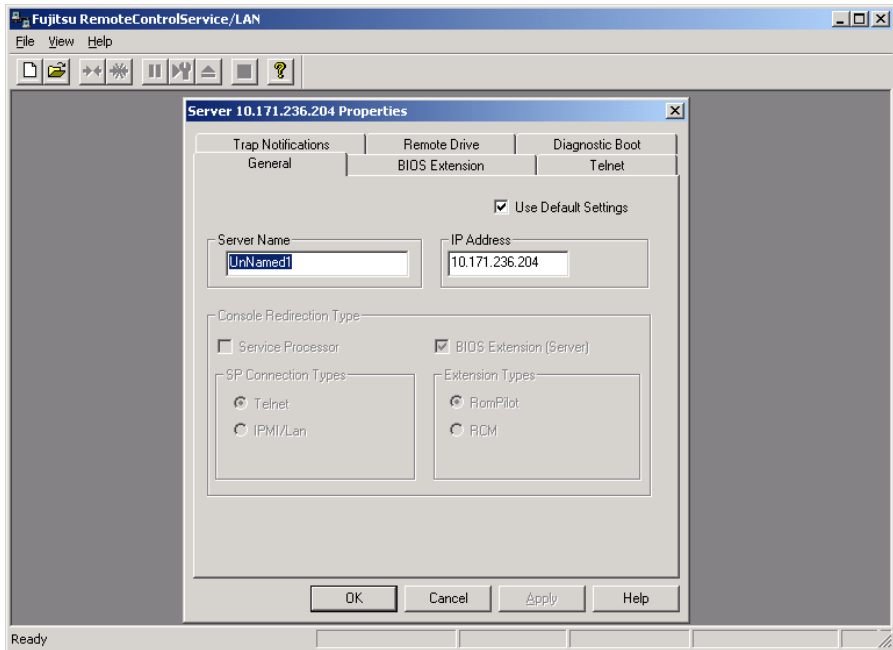
To register a server in the server list:

- 1 Click the [File] menu → [New] or click  icon in the tool bar.

The following window appears.



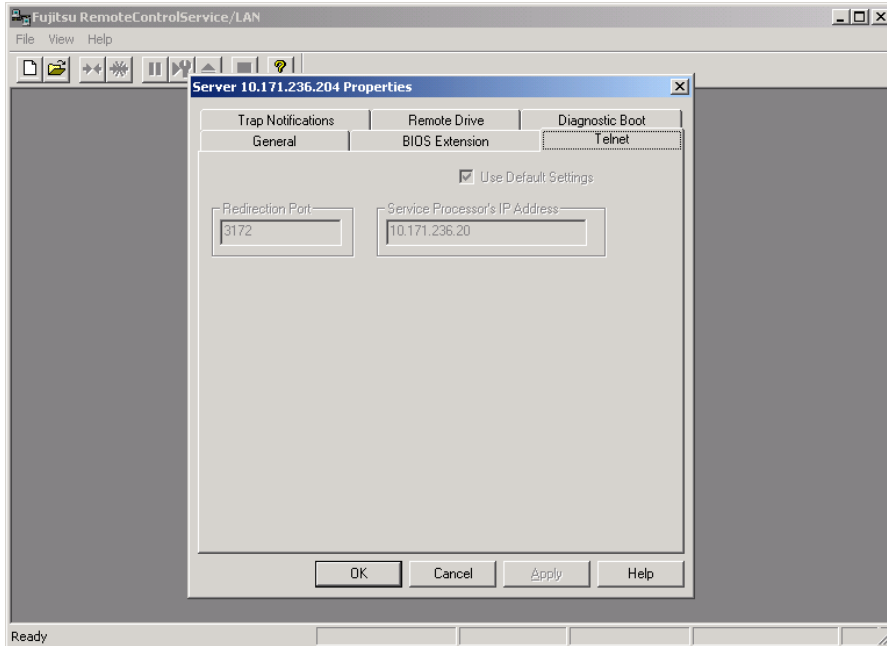
- 2 Enter the IP address for a new server, select the object's type (Standard Server/Blade Server/Storage Subsystem), and click [Properties].
The properties window for servers appears as follows.



- 3 Enter a server name in the [General] tab.
- 4 When a remote service board is installed in the server, clear [Use Default Settings] and select [Telnet].

- 5 Enter the IP address of the remote service board (for a blade server, the IP address of its management blade) for [Service Processor's IP address] in the [Telnet] tab and click [OK].

The following window illustrates a remote service board example.



For a remote service board

As a redirection port, specify the port number assigned in [LAN Interface] - [Telnet Port] for the remote service board.


For a blade server

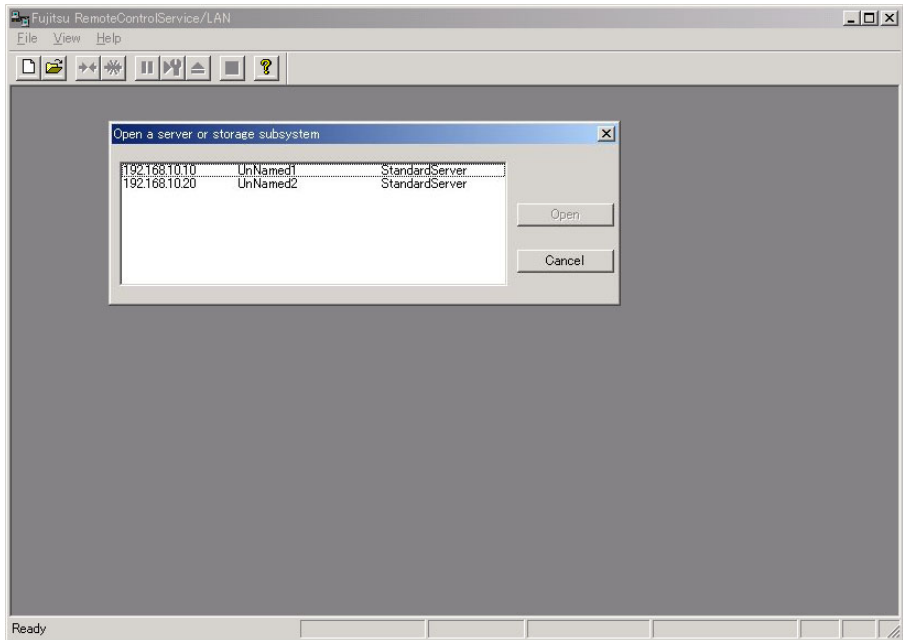
As a redirection port, specify the port number assigned for the management blade. The default value of a management blade is 3172.

POINT

- ▶ The default value of Telnet port number for the remote service board depends on its firmware version. The firmware version is displayed when the remote manager is connected:
 - 0.x.x.xx TelnetPort 2307
 - 1.x.x.xx TelnetPort 3172
 - 2.x.x.xx TelnetPort 3172

■ Open the Server's Remote Window

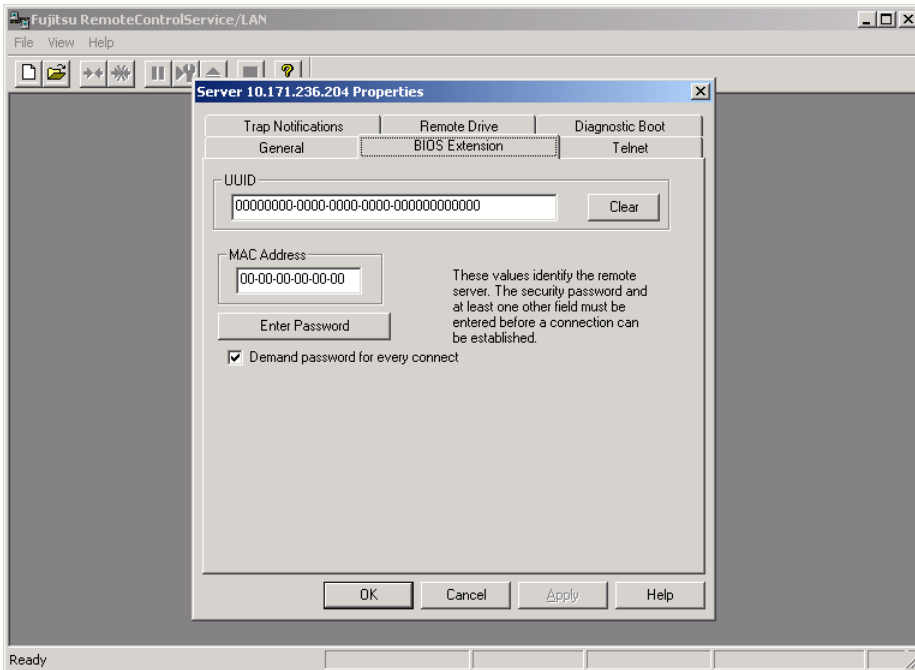
- 1 Click the [File] menu → [Open] or click  icon in the tool bar.



- 2 Select the desired server from the server list and click [Open].
The remote console window opens.
This server list displays all the server objects that the user has created.

POINT

- ▶ RemoteControlService provides connection to the server's RomPilot, RCM, remote service board (Telnet), and IPMI.
- ▶ For the connection to RomPilot
 - Click the [File] menu → [Properties], select [BIOS Extension (Server)] in the [General] tab, and then select [RomPilot]. When the connection to RomPilot is established, values are entered automatically into [UUID] and [MAC address] in the [BIOS Extension] tab.




- For the connection to RCM
 - Click the [File] menu → [Properties], select [Bios Extension (SERVER)] in the [General] tab, and then select [RCM].
- For the connection to a remote service board (Telnet)
 - Click the [File] menu → [Properties], clear [Use Default Settings] in the [General] tab, and then select [Telnet]. Enter the IP address of the remote service board for [Secondary IP address] in the [Telnet] tab.
- For the connection to IPMI
 - Click the [File] menu → [Properties], clear [Use Default Settings] in the [General] tab, and then select [IPMI].

■ Connecting to a Server

The RomPilot remote console window or the RCM window appears when the server starts POST and transmits a SNMP trap.

● For the connection to a remote service board


- 1 Right-click in the remote window and click [Connect] in the pop-up menu or click  icon in the tool bar.

When connecting to a remote service board, enter a user account for the remote service board. For more details, refer to "4.4.5 Support of the Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104)" (→pg.291).

● For the connection to RomPilot

- 1 You can also start the BIOS Setup by clicking [Connect/Setup].
Enter a server password when connecting to RomPilot/RCM.

■ Disconnect a Server


- 1 Right-click and click [Disconnect] in the pop-up menu or click  icon in the tool bar.
The server is disconnected. However the window remains open.

4.4.3 BIOS Setup

This section describes how to start the server's BIOS Setup through LAN using RemoteControlService/LAN.

POINT

- ▶ You must reboot the server before beginning operations. When the server operates, ServerView can reboot it from the administration terminal.
- ▶ When the server has not been registered in the server list, refer to "■ Adding a Server" (→pg.282) to add the server.

- 1 Click the [File] menu → [Open] or click  icon in the tool bar.
- 2 Select the desired server from the server list and click [Open].
- 3 Right-click in the RomPilot remote console window and then click [Connect/Setup] in the pop-up menu or right-click in the RCM window and then click [Start BIOS Setup at Next Connection].
- 4 Start or reboot the server.
- 5 Enter the server password.
When connection to the server is established, the [F2] key input is sent to the server automatically.
The BIOS Setup of the server appears after the server's POST.

4.4.4 Server's Boot Operations


This section describes how to control server's boot operations.

■ Power on for a Server

POINT

- ▶ To power on a server using RemoteControleService/LAN, one of the following conditions is required:
 - A network adapter supports Wakeup On Lan (WOL) in the server and power on through LAN is set "Enabled".
 - A remote service board is installed into the server.
 - The server is a blade server.
For the WOL function and the settings for a server, refer to "User's Guide".
- ▶ To power on a server from RemoteControleService/LAN, it is necessary to register the server in the server list of RemoteControleService/LAN and connect to it once.

● To use WOL

- 1 Click the [File] menu → [Open] or click  icon in the tool bar.
- 2 Select the desired server from the server list and click [Open].
- 3 Right-click and click [Wakeup] in the pop-up menu or click the [Reset/Reboot] menu → [Wakeup].


■ Starting Servers from a Remote Drive

A combination of RemoteControlService/LAN and RomPilot/RCM provides the function that boots a server from a remote drive.

The remote drive indicates a floppy disk or an image file on the administration terminal.

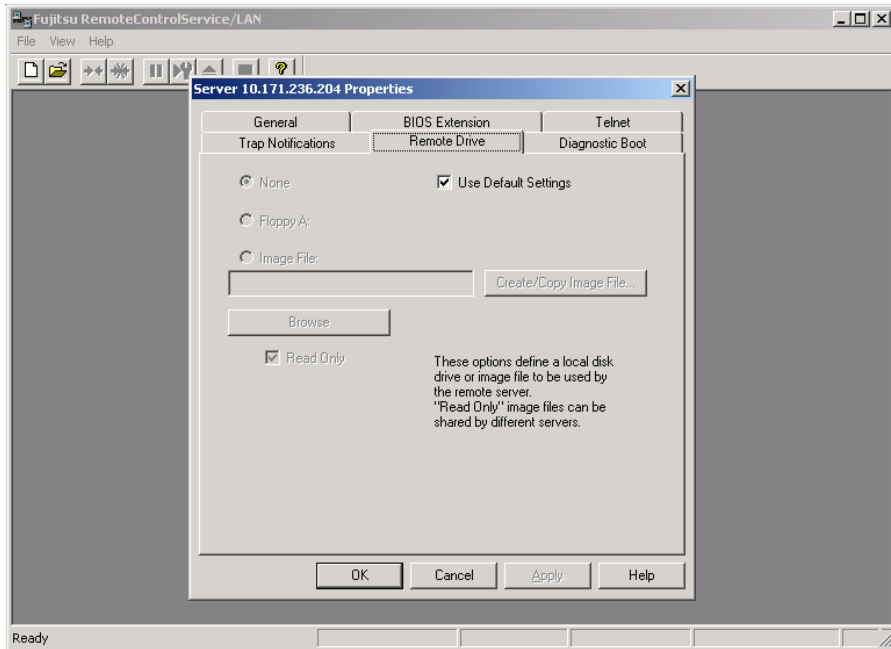
POINT

- ▶ When a server is started from a remote drive, remote control is also enabled while MS-DOS is operating.
- ▶ The image file indicates a hard-disk copy for the contents of a floppy disk.
This image file can be created in RemoteControlService/LAN.
Click the [File] menu → [Properties] → [Remote Drive] → [Create/Copy Image File] for creation.
- ▶ To use the remote drive function, RomPilot/RCM is necessary.
Even if you connect to a remote service board, the remote drive function would not be available.
- ▶ RCM does not support the remote drive function from a floppy disk.
To use the remote drive function in RCM, it is necessary to create an image file and configure the settings starting from the image file.

- 1 Click the [File] menu → [Open] or click  icon in the tool bar.
- 2 Select the desired server from the server list and click [Open].
- 3 Right-click and click [Suspend at Next Connection] (for RCM, [Start BIOS Setup at Next Connection]).
- 4 Start or reboot the server.
- 5 Enter the server password.
IF the server is connected, the server's POST suspends automatically.
- 6 Click the [Reset/Reboot] menu → [Next Reset Options] or right-click and click [Next Reset Options] in the pop-up menu.

7 Click [Remote Drive Options].

The [Remote Drive] tab in the properties for the server appears.



8 Clear [Use Default Settings], select [Floppy A:] or [Image File], and click [OK].

When you select [Image File], enter the image file name or click [Browse] and then specify the image file.

9 Select [Enable Remote Drive] and click [Cold Remote Boot].

The server will be rebooted from a remote drive.

10 Enter the server password.

The server is started from a remote drive after POST. The remote window displays [RD] indicating the remote drive.

4.4.5 Support of the Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104)

This section describes the remote service board (PG-RSB102/PG-RSB103/PG-RSB104) support. The "remote service board" described in this section indicates the "remote service board (PG-RSB102/PG-RSB103/PG-RSB104)".



- ▶ For the Remote Service Board (PG-RSB102), the Telnet interface is supported for firmware versions A.7.1.11.36 or later. If the firmware is older, Telnet is not supported.
- ▶ For the Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104), console redirection from the Telnet interface is not supported. Use the console redirection function in the Remote Service Board Web interface. For details, refer to "5.3.2 [Manage] Page" (→pg.313).

■ Connecting to the Remote Service Board

The remote service board includes the Telnet interface called remote manager, which can be connected from RemoteControlService/LAN. The remote manager allows you to verify the information about the target server. Certain information such as a system name appears only after the ServerView Agent is initially started, or only when the server is properly configured.

Connect to the remote service board through RemoteControlService/LAN according to the following procedure:

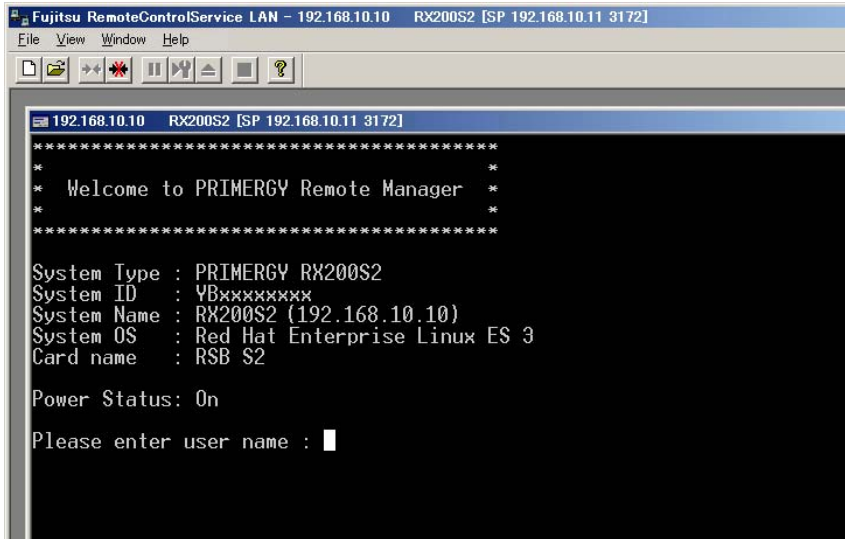


- ▶ Before starting Telnet connection, use a Web interface in the remote service board to enable a Telnet port. For more details, refer to "5.3.8 [Web/SSL Config] Page" (→pg.343).

- 1 Click the [File] menu → [Properties].
The [Properties] window appears for servers.
- 2 Clear [Use Default Settings] in the [General] tab and then select [Telnet].
Enter an IP address of the remote service board for [Secondary IP address] in the [Telnet] tab.
When the Telnet port number for the remote service board has been changed, clear [Use Default Settings] and enter the Telnet port number in [Redirection Port].
- 3 Click [OK].
- 4 Click the [File] menu → [Open].
- 5 Select a server and click [Open].
The report manager window appears.

6 Right-click and Click [Connection].

The following window appears.



7 Log in as a user account for the remote service board.

After log in, the main menu appears for the remote manager.

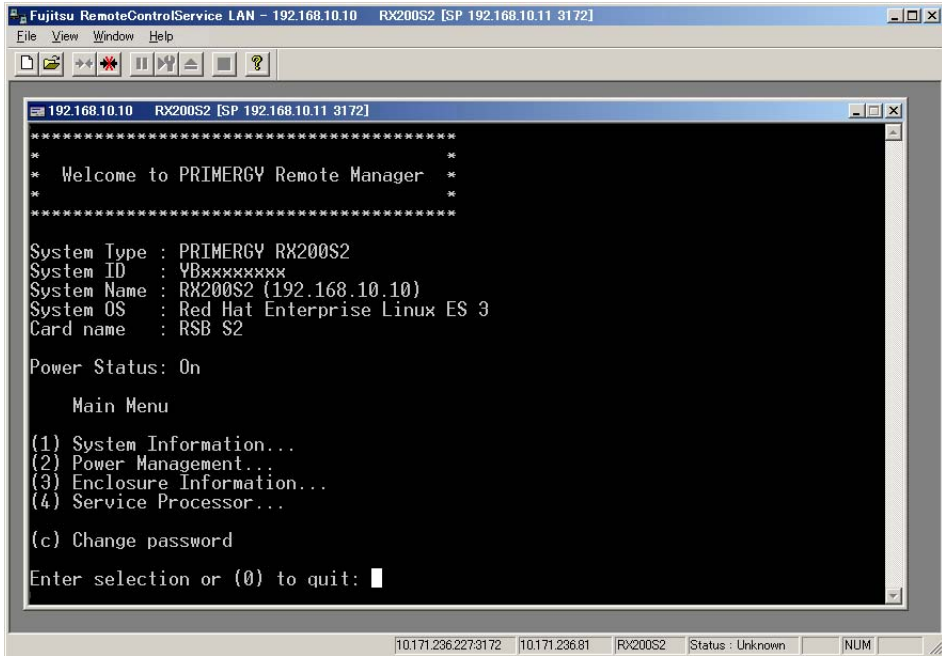
■ Main Menu

The main menu in the remote manager is shown as follows.

The menu depends on machine type and an applicable menu will appear.

table: Main Menu

Menu Item	Description
System Information	Displays system information. If this is selected, the system information menu appears.
Power Management	Controls the server power supply. If this is selected, the power management menu appears.
Enclosure Information	Displays server information. If this is selected, the server information menu appears.
Service Processor	Displays the configuration and information of the remote service board. If this is selected, the RSB menu appears.
Change password	Changes a password.



The above window is a main menu example.

If the number or character on the left of each item is entered, the corresponding item is executed or its submenu items appear. The unavailable functions are marked (*).

If the [0] key is pressed, the higher menu would appear. If the [0] key is pressed, the remote service board would be disconnected while the main menu (the above figure) is displayed.

● System Information

Select [System Information] in the main menu and the following menu appears.

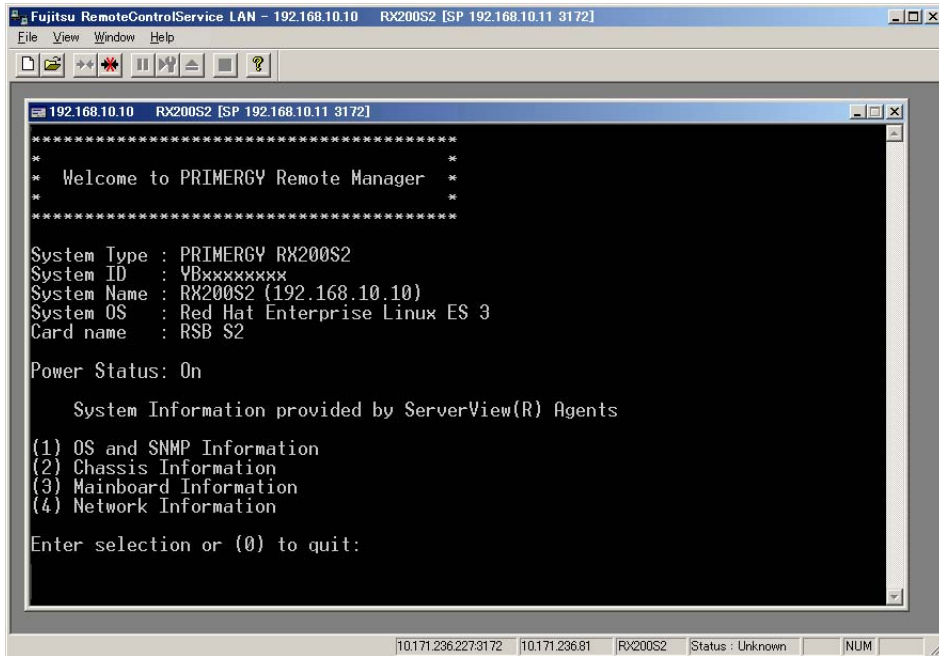


table: System Information Menu

Menu Item	Description
OS and SNMP Information	OS names and ServerViewAgent versions are displayed.
Chassis Information	The server's type name and serial number are displayed.
Mainboard Information	BIOS versions and board information are displayed.
Network Information	Information on network nodes is displayed.

● Power Management

Select [Power Management] in the main menu and the following menu window appears.

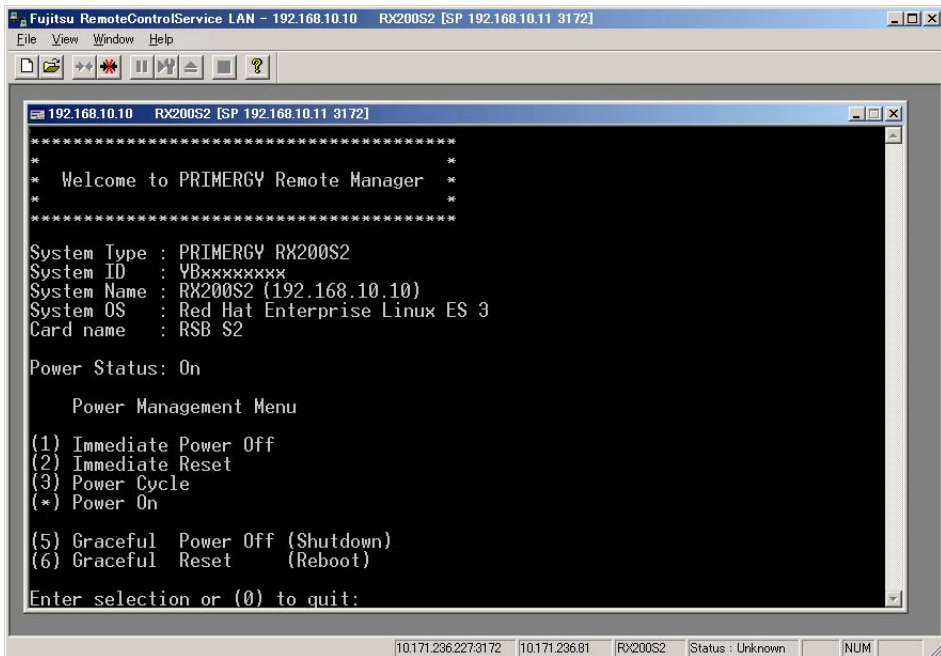


table: Power Management Menu

Menu Item	Description
Immediate Power Off	Turns the server off regardless of the state of the OS.
Immediate Reset	Reboots the server regardless of the state of the OS.
Power Cycle	Powers off the server and powers on it again, regardless of OS status.
Power On	Turns the server on.
Graceful Power Off (Shutdown)	Shuts down the Server. The remote service board sends a shutdown request to the ServerView Agent in the server. When the remote service board cannot send the shutdown request because the agent is not installed and so on, it goes to another dialog and displays a message to confirm whether to shut down the server regardless of OS status (Immediate Power Off).
Graceful Reset (Reboot)	Reboots the server. The remote service board sends a reset request to the ServerView Agent in the server. When the remote service board cannot send the reset request because the agent is not installed and so on, it goes to another dialog and displays a message to confirm whether to reset the server regardless of OS status (Immediate Reset).

● Enclosure Information

Select [Enclosure Information] in the main menu and the following menu appears.

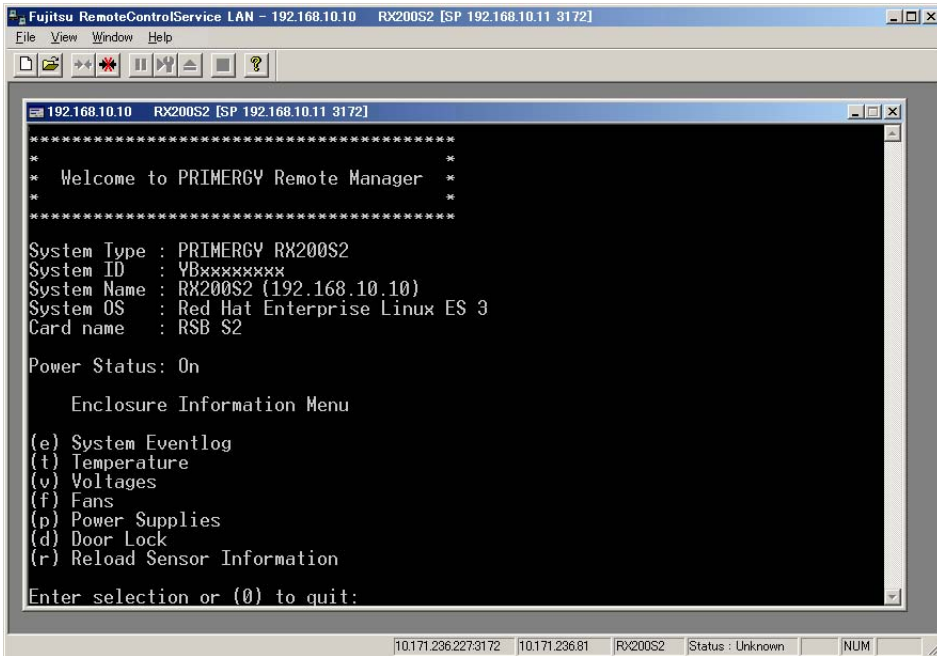


table: Enclosure Information Menu

Menu Item	Description
System Eventlog	Displays the [System Eventlog] menu window.
Temperature	Information on temperature is displayed.
Voltages	Information related to voltages is displayed.
Fans	Information on fans is displayed.
Power Supplies	Information on power supplies is displayed.
Door Lock	The open or closed state of a front door is displayed.
Reload Sensor Information	Reloads sensor information.

● System Eventlog

Select [System Eventlog] in the main menu and the following menu appears.

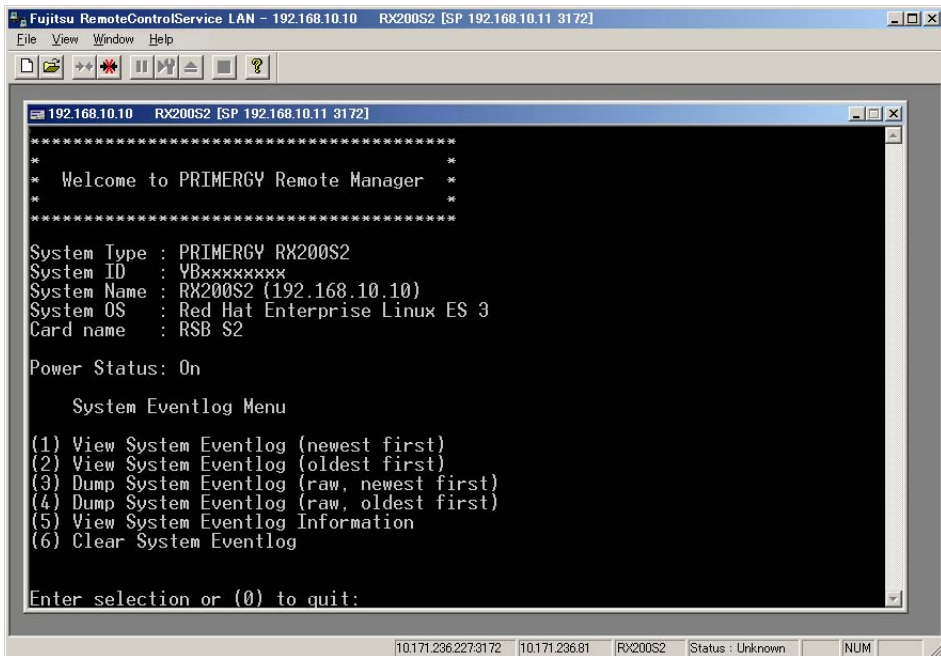


table: System Eventlog Menu

Menu Item	Description
View System Eventlog (newest first)	The contents of an event log are listed in order of time (the newest entry is located at the top) for the remote service board.
View System Eventlog (oldest first)	The contents of an event log are listed in order of time (the oldest entry is located at the top) for the remote service board.
Dump System Eventlog (raw, newest first)	Binary data of an event log are listed in order of time (the newest entry is located at the top) for the remote service board.
Dump System Eventlog (raw, oldest first)	Binary data of an event log are listed in order of time (the oldest entry is located at the top) for the remote service board.
View System Eventlog information	Information of an event log is displayed for the remote service board.
Clear System Eventlog	Clears event logs in the remote service board.

● Service Processor

Select [Service Processor] in the main menu and the following menu appears.

```

Fujitsu RemoteControlService LAN - 192.168.10.10  RX200S2 [SP 192.168.10.11 3172]
File View Window Help
[Icons]

192.168.10.10  RX200S2 [SP 192.168.10.11 3172]
*****
* Welcome to PRIMERGY Remote Manager *
*****

System Type : PRIMERGY RX200S2
System ID   : YBxxxxxxxx
System Name : RX200S2 (192.168.10.10)
System OS   : Red Hat Enterprise Linux ES 3
Card name   : RSB S2

Power Status: On

Service Processor Menu

(1) Firmware Update Status
(2) Firmware Update Configuration
(3) Firmware Update (Start)
(4) Firmware Update (Resume)
(5) Reset RSB S2 board

(6) Configure IP Parameters
(7) List IP Parameters
(8) Configure Card Name

Enter selection or (0) to quit:

```

table: Service Processor Menu

Menu Item	Description
Firmware Update Status	Displays the state of firmware update in the remote service board. This function is not supported.
Firmware Update Configuration	Displays configuration of firmware update in the remote service board. This function is not supported.
Firmware Update (Start)	Starts firmware update in the remote service board. This function is not supported.
Firmware Update (Resume)	Resumes firmware update in the remote service board. This function is not supported.
Reset RSB S2 board	Reboots the remote service board.
Configure IP Parameters	Changes an IP address in the remote service board.
List IP Parameters	Displays an IP address in the remote service board.
Configure Card Name	Rename the remote service board.

4.4.6 IPMI Support

This section describes IPMI support through RemoteControleService/LAN.

This provides connection to an IPMI interface called remote IPMI manager from RemoteControleService/LAN.

■ Connecting to IPMI

- 1 Click the [File] menu → [Properties].
The [Properties] window appears for servers.
- 2 Clear [Use Default Settings] in the [General] tab and then select [IPMI].
- 3 Selects a machine type name for the server to be connected from the pull-down menu and click [OK].
For selection of a machine type name, refer to "● Notes for Selection of IPMI Machine Type Names" (→pg.251).
- 4 Click the [File] menu → [Open] to select a server.
- 5 Click [Open].
The remote IPMI manager window appears.
- 6 Right-click and then click [Connection].
- 7 Enter the user name and password.
The main menu in the remote IPMI manager window appears.

■ Main Menu for the Remote IPMI Manager

The main menu in the remote IPMI manager is shown as follows.

The menu depends on server and an applicable menu appears.

table: Main Menu for the Remote IPMI Manager

Menu Item	Description
Console Redirection	Redirects a console.
Power Management	Controls the power state of the server.

● Console Redirection

The console redirection enables you to redirect the server's windows and keyboard operations to a remote console. If the console redirection is selected, the server's window would be transmitted to the remote manager window. Input information from a keyboard is sent to the server's keyboard controller. The following operations are enabled by the console redirection:

- Window display during POST
- BIOS Setup
- Displays the latest contents and available window (in a text mode) and recovers the system when OS crashes.

The console redirection exits if a tilde (~) and period (.) are sequentially entered within two seconds.

● Power Management

Select [Power Management] in the main menu and the following menu window appears.

table: Power Management Menu

Menu Item	Description
Immediate Power Off	Turns the server off regardless of the state of the OS.
Immediate Reset	Restarts the server regardless of the state of the OS.
Power Cycle	Powers off the server and then powers on it again, regardless of OS status.
Power On	Turns the server on.

Chapter 5

Using the Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104)

This chapter explains how to use the Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104).

5.1 Overview	302
5.2 Preparation	303
5.3 Displaying Each Monitoring Information	310

5.1 Overview

This chapter explains the Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104).

In this chapter, "Remote Service Board" represents "Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104)". The Remote Service Board is an optional extension card having its own CPU, OS, communication interface, power supply, and USB port. With the Remote Service Board, it is possible to monitor and operate a server irrespective of the server state.

5.1.1 Functions

● Remote Service Board functions

- Server state monitoring (OS hang, power failure, abnormal temperature, voltage trouble)
- Notification to the administrator in case of server trouble
- Remote server operation (restart, power on/off)
- Server keyboard and mouse operation from the management console (Advanced Video Redirection functions)
- Booting the server with devices and bootable files on the management console

● Communication interfaces supported by the Remote Service Board

- LAN interface
- USB interface

5.1.2 Notes

- Each sensor item registered on the [Sensors] page is initialized after logging out from the Web interface.
- Although [Red PSU FAN] can be selected as a fan sensor on the [Sensors] page, the fan does not actually exist.
- Depending on the type of the server on which the RSB is installed, history information may not be displayed properly (Web interface → [Sensor] tag → [History Configuration]).
Example: The following error occurs while viewing history information:
Error gettings values Status Bar!
- Java™ 2 Runtime Environment Standard Edition V1.5 or later is not supported.

5.2 Preparation

This section explains preparation for using the Remote Service Board.

5.2.1 Setting the LAN Interface

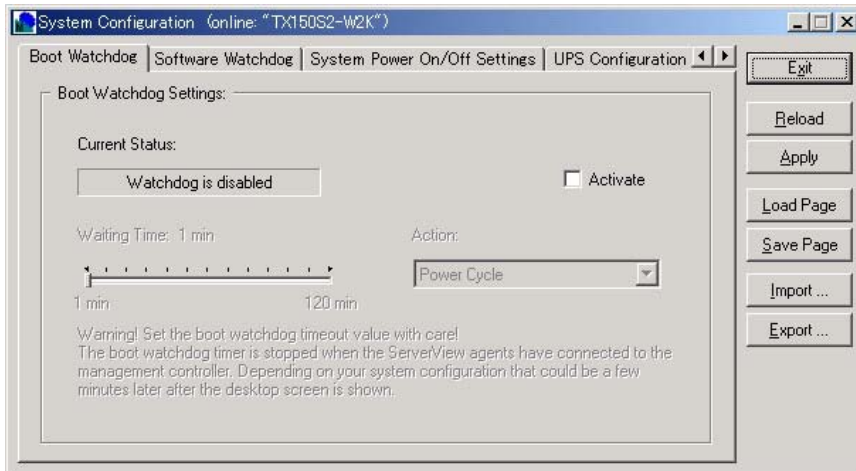
■ For Windows

- 1 Log in to the server using the local user account belonging to the local Administrators group.
Setting is not available when using the Domain Admins group.
- 2 Exit all running applications.
- 3 Click [Start] → [Programs] → [Fujitsu ServerView Agents] → [Configuration Tools] → [System Configuration].
The [System Configuration] window appears. Make sure that the server type name is correct.

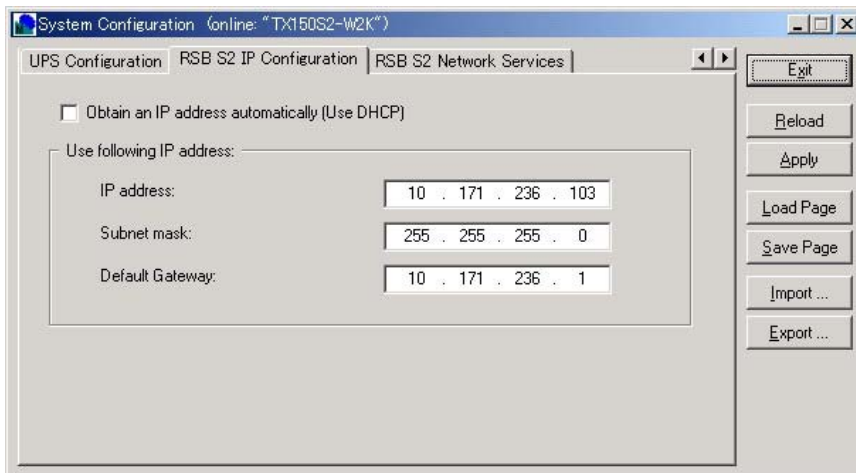


- 4 Check the [Change system selection manually] and [Remote Service Board (RSB S2) installed] checkboxes and click [OK].

The following window appears.



- 5 Click [▶] and select the [RSB S2 IP Configuration] tab.



- 6 Uncheck the [Obtain an IP address automatically (Use DHCP)] checkbox and enter the IP address, subnet mask, and default gateway for the Remote Service Board.
- 7 Click [Apply].
- 8 Click [Exit].

■ For Linux

- 1 Log in as a super user.
- 2 Set the PRIMERGY Document & Tool CD and run the following command:
If a specific application has been installed, the CD-ROM is mounted automatically when it is set (the command need not be run).

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
```

- 3 Run the following command to start the utility from the CD-ROM.

```
# /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/SVMANAGE/Linux/  
TOOLS/RSB_UTILITY/rsbs2_ut
```

- 4 Select [LAN Interface].

The following information currently set appears.

- IP address
- Subnet mask
- Default gateway
- DHCP (Enabled/Disabled)

- 5 Select "e" to proceed to item editing.

- 6 Set each item following the message displayed.

After entering an item, press the [Enter] key to edit the next item. When only the [Enter] key is pressed, the setting of the item will not be changed. After the settings of all items are completed, the [LAN Interface] window appears again.

- 7 Select "s" to save the settings.

- 8 Select "x" to exit [LAN Interface].

- 9 Select "x" to exit the utility.

- 10 Unmount and remove the CD-ROM.

Be sure to unmount the CD-ROM before removing it.

```
# umount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
```

5.2.2 Installation and Configuration of the Management Server Application (MSA)

MSA provides the Remote Storage function, which is used for iSCSI connection to the Remote Service Board, and also handles login user management using the directory service function.

● Remote Storage Function

The Remote Storage function is used for connecting drives or other devices installed in other terminals on the network to the server in which the Remote Service Board is installed. MSA provides the Remote Storage function for iSCSI connection to the Remote Service Board. Once the connection is established, the server OS recognizes a disk image file stored in `\management_server\iscsi_root` as a disk drive. For how to establish iSCSI connection, see "● iSCSI connection" (→pg.323).

● Directory Service Function

The directory service function manages the users who access the Remote Service Board. When a user logs in to the Remote Service Board, the Remote Service Board checks the user against the users registered in the internal database.

POINT

Environment Required to Use MSA

- ▶ To use MSA, the following environment is required:
 - JDK 1.3.1_01 or later version must be installed.
 - At least 30MB disk space available for installation, in addition to the disk image size.
 - A ZIP file expansion environment that can retain the directory structure.

■ Installing MSA

Install MSA by the following procedure.

- 1 Log in as Administrator or a user with Administrator privileges.
- 2 Exit all running applications.
- 3 Insert the PRIMERGY Document & Tool CD and copy the following file to the installation destination folder on the server:
[CD-ROM Drive]:\SVMANAGE\TOOLS\management_server.zip
- 4 Expand the copied ZIP file.
The folder "management_server" is created.

■ Configuring MSA

To use MSA, open and edit the file "msa.conf" with a text editor or similar software. The file "msa.conf" is stored at the following path in the folder "management_server":

management_server\conf\msa.conf

For the values for each item, see the comments in the file "msa.conf".



- ▶ Do not use the [Tab] key when editing the file.
- ▶ Usually, only the parts enclosed with "%%" (e.g. "%%test%%") need to be modified.
- ▶ If you don't use the directory service function, comment out all the lines below # AccessControlService.
- ▶ The directory service function supports only "Active Directory Service". It does not support "iPLANET".

■ Starting the MSA Service

MSA can be started in the two following ways:

● Starting MSA by Executing the File "msa.jar"

Execute [installed folder]\management_server\msa.jar.

In this case, MSA starts as a background service and nothing appears on the display.

● Starting MSA by Executing the File "start_msa.bat"

Execute [installed folder]\management_server\start_msa.bat.

If the OS is Windows, the Command Prompt window opens and the startup status or error is displayed.

If you close the Command Prompt window, the service also stops.

5.2.3 Configuring the Directory Service Function

This section explains the settings necessary for using the directory service function.

■ Password Encryption

You need to encrypt the "Active Directory Service" login password that is specified after "GU_SECURITY_CREDENTIALS = " in the file "msa.conf".

- 1 Execute the file "pwd.bat" in the folder "management_server".

The following message is displayed:

```

*****
Please enter Access Control Server configuration file name:

```

- 2 Enter the path to the file "msa.conf" and press the [Enter] key.

3 Enter a user name and press the [Enter] key.

4 Enter a password and press the [Enter] key.

The following message is displayed:

```
*****  
Please enter Access Control Server configuration file name: ./conf/msa.conf  
Please enter general user security principal: testserver/testname  
Please enter general user security credentials: testpass  
  
*****  
Input information summary:  
  
Access Control Server configuration file name: ./conf/msa.conf  
General User security principal: testserver/testname  
General User security credentials: testpass  
  
*****  
Confirm? [y/n/exit]:
```

5 Press the [y] key and then the [Enter] key.

■ Settings on the [DS Config] Page

Start the Web interface of the Remote Service Board, and click the [DS Config] tab for configuration.

Directory Service (DS) Authentication Properties

Enable Directory Service connectivity

Access Control Server 1: 0.0.0.0

Access Control Server 2: 0.0.0.0

DS Group Name: RMCALL

History of User Login's since last card reset

User ID	Login Time	Login Name
0x3	2005/09/16 17:28:05	admin
0x3	2005/09/16 17:30:34	admin
0x3	2005/09/16 17:32:53	admin
0x3	2005/09/20 11:40:58	admin
FAILED	2005/09/27 14:22:12	admin
FAILED	2005/09/27 14:22:17	admin
FAILED	2005/09/27 14:24:35	admin
0x3	2005/09/27 14:24:47	admin
0x3	2005/09/27 14:26:57	admin
0x3	2005/09/27 14:28:33	admin
0x3	2005/09/27 14:29:25	admin
0x3	2005/09/29 19:55:30	admin
0x3	2005/09/29 19:56:55	admin

Apply Cancel Help Logout

RSB S2 Server: off Connected users: 1 | User ID: admin 2005/10/24 18:04

table: Configuration Items on the [DS Config] Page

Item	Description
Access Control Servers 1 Access Control Servers 2	Specifies the server on which MSA is running. Designate the primary MSA server as "1" and the secondary MSA server as "2".
DS Group Name	Specifies a part of the "Description" for the Remote Service Board login account registered in the Active Directory. For example, when registered as "testdis:administrator", enter "testdis". Because this value is the key for the Remote Service Board authorization, make sure that it is identical to the part of "Description".

■ Registration of Accounts

Register at least two user accounts in the domain controller. For each account, a "Description" needs to be set, as well as a "User name" and a "Password".

Depending on the account type, the "Description" value should be set as follows:

- Account for MSA to log in to the domain controller
"RMCALL:administrator" is automatically set as the "Description". The value cannot be changed.
- Account for the domain controller to authorize users using RSB.

In the "DS Group Name" field on the "DS Config" page of the Web interface, specify a part of the "Description" for the Remote Service Board login account registered in the Active Directory.

5.3 Displaying Each Monitoring Information

This section explains how to display server monitoring information using the Web interface.

5.3.1 Starting the Web Interface

The Remote Service Board supports the Web interface and can be accessed from the following Web browsers:

To use the Web interface, Java™ 2 Runtime Environment is required on the browser.

The following environment is recommended:

- For Windows
 - Microsoft Internet Explorer 5.5 or later (6.0 or later is recommended)
 - Java™ 2 Runtime Environment Standard Edition V1.4.2_08 or later
- or
- Netscape Navigator/Communicator V4.78 or later (6.2 or later is recommended)
- Java™ 2 Runtime Environment Standard Edition V1.4.2_08 or later
- For RHEL-AS3 (x86)/ES3 (x86)
 - Mozilla V1.3 or later
 - Java™ 2 Runtime Environment Standard Edition V1.4.2_08 or later
- For RHEL-AS4 (x86)/ES4 (x86)
 - Firefox 1.0 or later
 - Java™ 2 Runtime Environment Standard Edition V1.4.2_08 or later

POINT

- ▶ To use a Web browser, it must be installed and set in advance. Refer to "2.4.1 Installing a Web Browser" (→pg.58) and "2.4.2 Installing Java™ 2 Runtime Environment Standard Edition" (→pg.59).
- ▶ Please download Java™ 2 Runtime Environment Standard Edition V1.4.2_08 (or later) from HP of Sun Microsystems.
- ▶ Java™ 2 Runtime Environment Standard Edition V1.5.x is not supported.

1 Start the Web browser and enter one of the following addresses in the address bar:

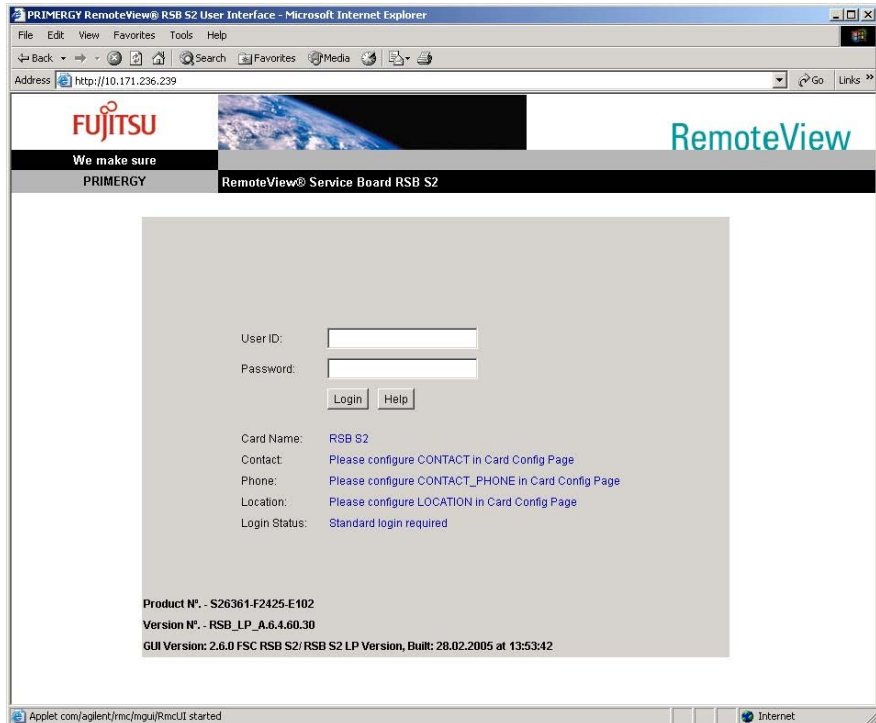
- `http://<IP address>:<Port number (default: 80)>` (when http is enabled)
- `https://<IP address>:<Port number (default: 443)>` (when https is enabled)

The following warning window appears:



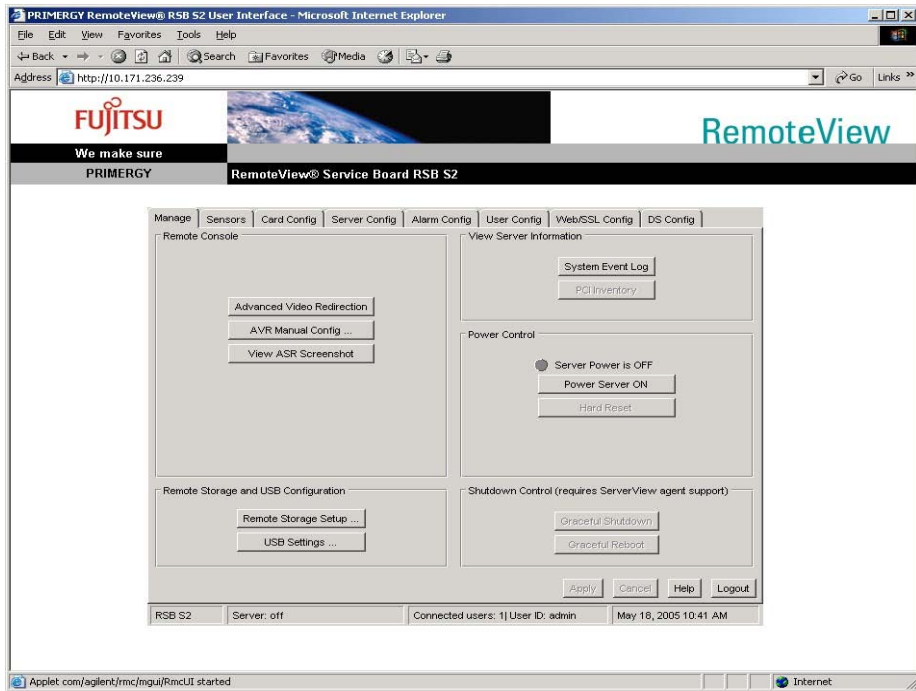
2 Click [Yes].

The login window appears.



3 Enter the [User ID] and [Password].

After authentication succeeds, the following window appears:



On the Web interface, each function is displayed respectively under a tab. Click a respective tab to open each page. The following sections describe functions on each page.

5.3.2 [Manage] Page

The [Manage] page is available for setting how to display images and controlling power supply.

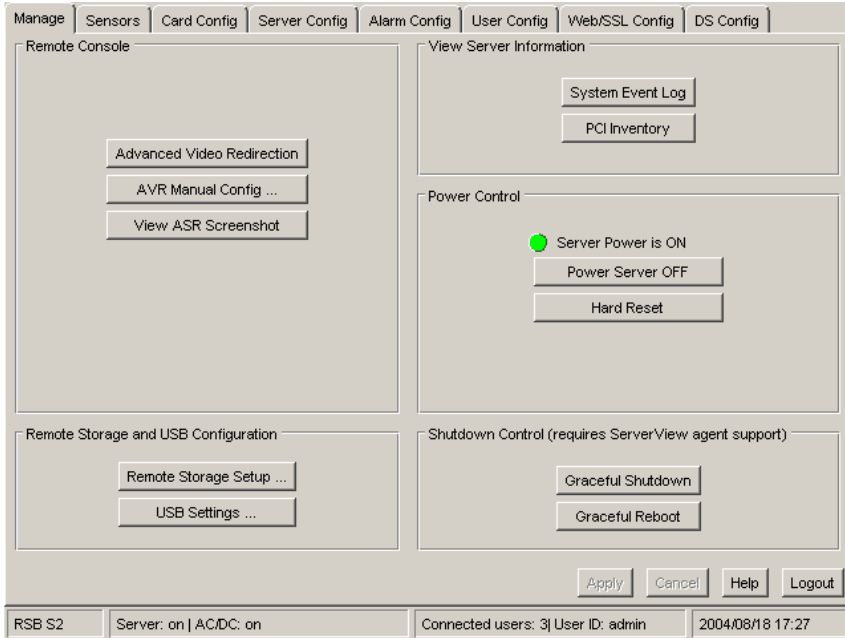


table: Functions on the [Manage] Page

Item	Description
Remote Console	This function allows the server screen to be displayed in the AVR window of the console, and allow server operation from the console.
[Advanced Video Redirection]	Opens the AVR window and starts redirection of the server window. → "■ Advanced Video Redirection (AVR) Functions" (pg.314)
[AVR Manual Config ...]	Available for setting AVR functions. → "■ AVR Manual Configuration" (pg.317)
[View ASR Screenshot]	Displays the screenshot of the server window captured at watchdog detection. → "■ View ASR Screenshot" (pg.318)
Remote Storage and USB Configuration	Available for loading other drives on the network from the Remote Service Board.
Remote Storage Setup	Available for setting Remote Storage functions. → "■ Remote Storage Functions" (pg.319)
USB Setting	Available for setting USB functions. → "■ USB Settings" (pg.331)
View Server Information	Displays server information.
System Event Log	Displays server SELs.
PCI Inventory	Displays PCI device information. This function is available only for the Remote Service Board (PG-RSB102).

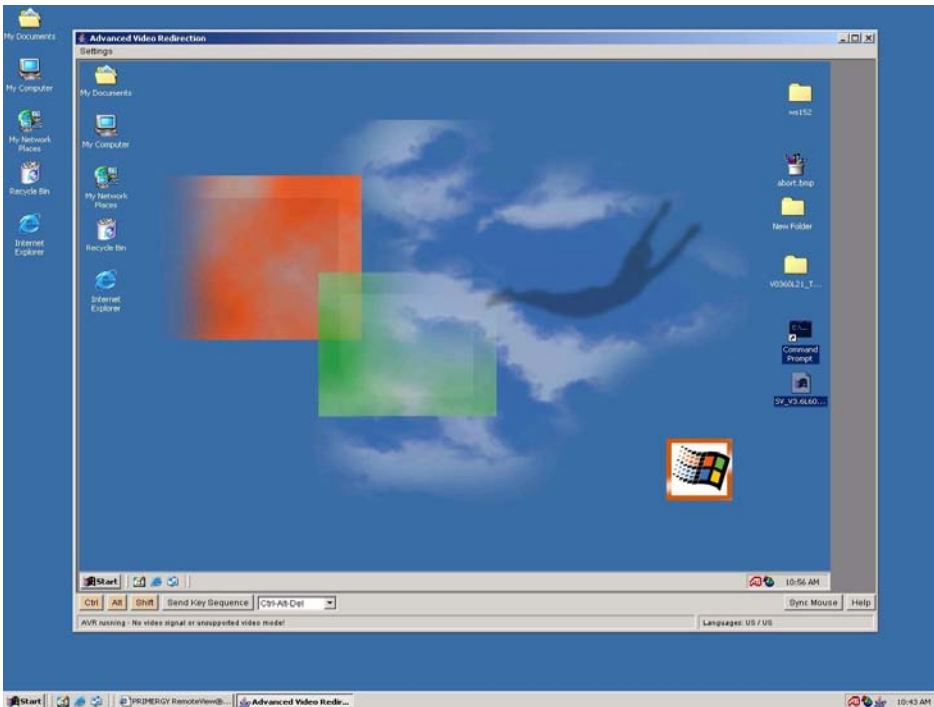
table: Functions on the [Manage] Page

Item	Description
Power Control	Available for controlling the server power supply.
Power Server On/Off	<p>If the server is turned on, it performs power-off regardless of the state of the server. Performs power-on if the server is turned off.</p> <p>POINT</p> <ul style="list-style-type: none"> If the OS freezes, this may be the same as [Graceful Shutdown] for PG-RSB104. In this case, use [Hard Reset].
Hard Reset	Performs reset regardless of the state of the server.
Shutdown Control	Shuts down and reboots the server. For this operation, a ServerView Agent must have been installed on the OS of the server.
Graceful Shutdown	Shuts down the OS of the server.
Graceful Reboot	Reboots the OS of the server.

■ Advanced Video Redirection (AVR) Functions

Advanced Video Redirection (AVR) is a function to display images shown on the server window on the AVR window of the console and allow server operation from the console.

Click the [Advanced Video Redirection] button to open the following AVR window. The window displayed on the server window appears as it is on the AVR window. Key and mouse operations on the AVR window are sent to the server, though there are exceptions.





- ▶ Performance of the AVR window varies depending on multiple factors such as drawing capacities, OS screen resolutions, and window colors of the server and console. Select appropriate settings for your use and purpose. Basically, the higher the graphics performance of the console is, the more effectively AVR functions.
- ▶ [Send Ctrl-Alt-Del] button
Press the [Send Ctrl-Alt-Del] button to set the server in the state where [Ctrl], [Alt], and [Del] are pressed.
- ▶ [Ctrl] / [Alt] / [Shift] buttons
The color of the buttons changes depending on how many times they are pressed. The meanings of each color are as follows:

table: Meanings of Displayed Colors

Color	Meaning
Gray	Standard state when [Sticky Key Mode] is disabled.
Orange	Standard state when [Sticky Key Mode] is enabled.
Yellow-green	The state where the key is pressed. The state is reset by one action using a combination with another key.
Green	State where the key is always pressed. Any number of actions can be taken using a combination with another key. This appears only when [Sticky Key Mode] is enabled.

- ▶ [Send Key Sequence] button
Select a key action in the combo box next to the button and press the [Send Key Sequence] button to set the server in the state where the same key is pressed. Key actions can be selected from the following options:
 - Ctrl-Alt-Del
 - Alt-SysRq
 - Alt-Tab
 - Alt-F4
 - Ctrl-Alt-F4
 - Ctrl-Tab
 - Ctrl-Esc
 - Ctrl-Alt-Backspace
 - Print Screen
- ▶ [Sync Mouse] button
Initializes the mouse position. Use this button when the mouse cursor position becomes different between the console and server.



- ▶ Since the configuration utility [WebBIOS] window of the MegaRAID SCSI RAID card uses its original mouse driver, proper mouse operation is not available for Advanced Video Redirection functions when using the RSBS2/S2LP Web interface.
- ▶ To use AVR, set [Enable] in [USB Legacy Support] in the server BIOS settings. If [Disable] is set in [USB Legacy Support], mouse and keyboard may not be enabled for AVR in a certain server state. For server BIOS settings, refer to the manual attached to the server.

● [Settings] menu

Click the [Settings] menu on the top of the window to display the following submenus on which you can set AVR window images, mouse, and keyboard.

table: Functions on the [Settings] Menu

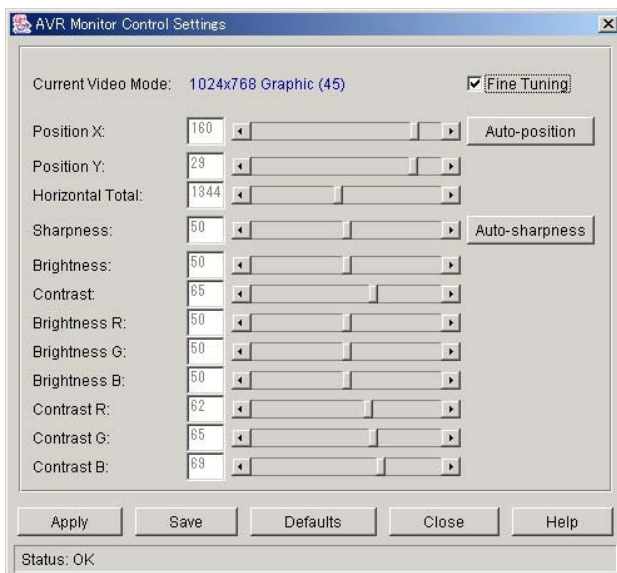
Item	Description
Display	Setting items related to window display.
Monitor Controls	Opens the " [AVR Monitor Controls Settings] window" (→pg.316). Available for setting AVR window display.
Video Capture Parameters	Opens the " [AVR Video Capture Settings] window" (→pg.317). Available for setting the AVR capture function.
Keyboard	Setting items related to the keyboard.
Typing Mode	Enables/disables the typing mode of the console keyboard on the server.
Sticky Key Mode	Sets the entry mode of special key operations (such as [Ctrl], [Alt], and [Shift]).
Secure Keyboard	Disables [Typing Mode] and [Sticky Key Mode].
Mouse	Setting items related to the mouse.
Read Mouse Acceleration	Enables/disables mouse cursor acceleration.
Show Client Cursor	Enables/disables the display of the console mouse cursor on the AVR window.
View-Only mode	Blocks mouse and keyboard operations when it is enabled.



- ▶ If [View-Only mode] is enabled on the [Settings] menu for the Remote Service Board (PG-RSB102), [View-Only mode] cannot be disabled until the AVR window is exited. To disable it, exit the AVR window once and then open it again.

[AVR Monitor Controls Settings] window

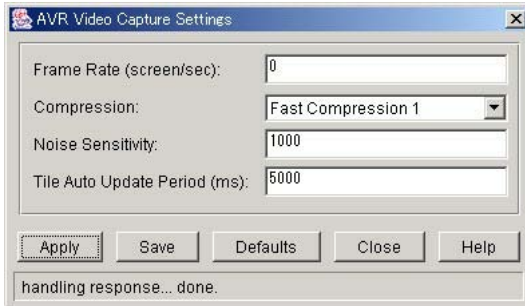
Available for setting AVR window display. Use the scroll bar to set each value.



Click [Apply] to enable the settings. The window display may become improper after settings are changed. In such a case, click [Defaults] to initialize them.

[AVR Video Capture Settings] window

Available for setting the AVR capture function. It is possible to set the frame rate, noise sensitivity, and resolution switching speed of the AVR function.



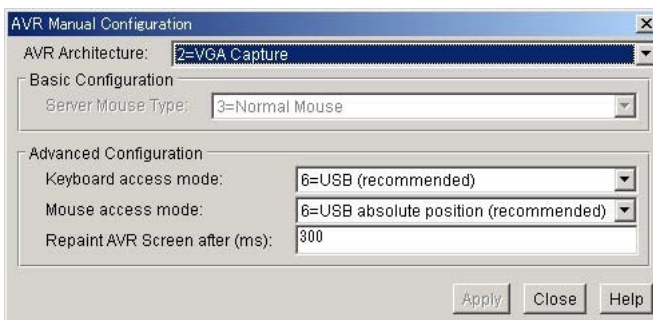
See the following table for settings in [Compression].

table: Settings in [Compression]

Item	Performance	Required Bandwidth	Image Quality
No Compression	Slow	Highest	Highest
Fast Compression 1/2	Highest speed	Medium	Lowest
Good Quality Compression	High speed	Lowest	Low
Best Quality Compression 1/2	Medium	Low	Medium

Click [Apply] to enable the settings. The window display may become improper or nothing may appear after settings are changed. In such a case, click [Defaults] to initialize them.

■ AVR Manual Configuration



Available for setting basic AVR functions.

table: Basic AVR Settings

Item	Description
AVR Architecture	Select [2=VGA Capture].
Keyboard access mode	Select [6=USB (recommended)].
Mouse access mode	The settings differ depending on the OS on the server. Set [6=USB absolute position (recommended)] for Windows and [7=USB relative position] for Linux.

table: Basic AVR Settings

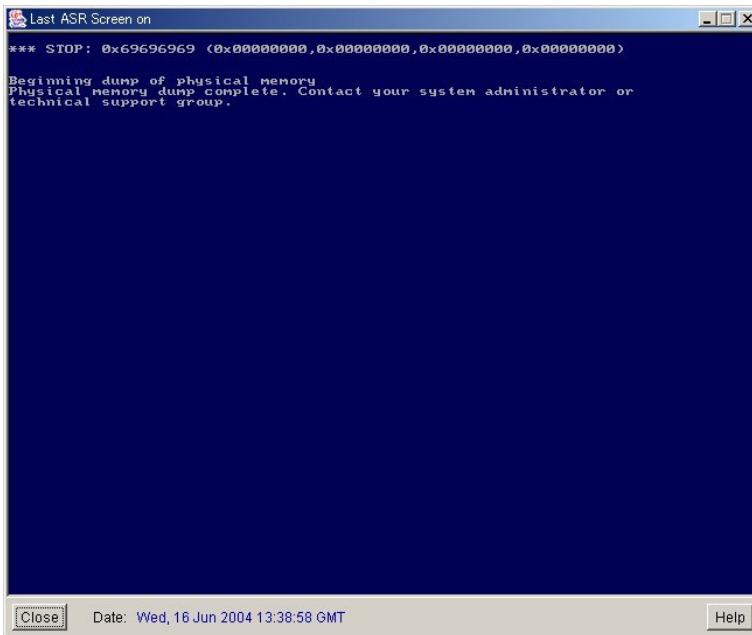
Item	Description
Repaint AVR Screen after (ms)	Set the update interval of the AVR window. Normally, it is not necessary to be changed from the default value (300).

POINT

- ▶ If [7=USB relative position] is set in [Mouse access mode], a menu is added to set mouse acceleration independently. In such a case, select "2" for normal use. This value differs depending on the server environment. If this setting does not correspond to the mouse acceleration setting on the server, the mouse cursor position may be different on the AVR window.

■ View ASR Screenshot

If the watchdog of the server is detected, the Remote Service Board automatically captures the screenshot of the server at this time. Click [View ASR Screenshot] to view the latest screenshot.



POINT

- ▶ For AVR, multiple consoles cannot be used for the same server. If AVR is executed from the console B to the Remote Service Board which is executing AVR on the console A, AVR on the console A is forcibly exited.
- ▶ Be sure to execute AVR on an administration terminal different from the target server. If AVR of a server is executed on the browser of the said server, window displays will not stop.
- ▶ [View ASR Screenshot] does not show the server window in real-time. Keyboard and mouse operations are not available.
- ▶ To use the mouse except when OS is operating such as using WebBIOS, switch the setting of "Mouse access mode" to [7=USB relative position] or [6=USB absolute position (recommended)]. Take on the setting in which the mouse can be used.
Restart Advanced Video Redirection (AVR) when you switch the setting of "Mouse access mode".

■ Remote Storage Functions

Remote Storage is a function to connect drives or other devices of different terminals on the network to a server on which the Remote Service Board is installed. The following two connection types are available for remote storages:

- Connection to a drive or other devices on a console which is executing the Web interface
→ "● Local connections" (pg.319)
- Connection to a drive or other devices on an "iSCSI server"
→ "● iSCSI connection" (pg.323)

The following functions can be performed using Remote Storage functions:

- Remote drive on the server OS
- Remote server boot

In addition, remote installation on the server OS can be performed from the console in combination with AVR described above.

● Local connections

Perform the following procedures for Local connections:

POINT

- ▶ [Local connection] is provided via USB. However, if you are using PG-RSB102, you can select connection via PCI on the screen. In Steps 2 and 5, the choice between USB and PCI appears on the screen. Choose [PCI] if you prefer connection via PCI.
If the connection is via PCI, note the following:
 - Virtual CD-ROM drives via PCI are not supported.
 - The server needs to be restarted to recognize remote storage devices via PCI.
- ▶ The server can only boot from the remote storage device via USB if the BIOS supports "USB Legacy". In the BIOS Setup Utility, set [Multiboot] and [USB Legacy Support] to [Enabled]. However, for some models, these settings are not available in the BIOS Setup Utility or cannot be changed manually.

Steps 1 and 2 are only required for PG-RSB102. When using PG-RSB103 or PG-RSB104, begin from Step 3.

1 Click [Remote Storage Setup].

The following window appears.



2 Set the interface between the server and Remote Service Board.

Set [Remote Storage via USB] to [Remote Storage Connection:].

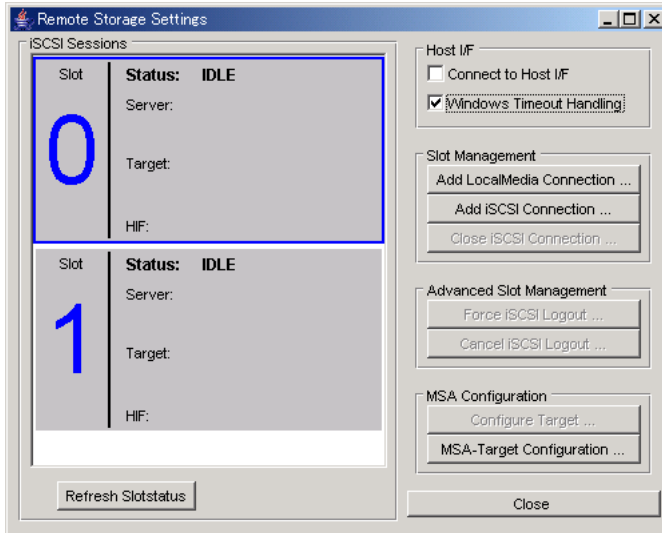
IMPORTANT

- ▶ If any setting is changed in [Remote Storage Connection:], the Remote Service Board requests resetting. To enable the change, reset the Remote Service Board.

Whether options are enabled or disabled depends on the settings of the Remote Service Board and server.

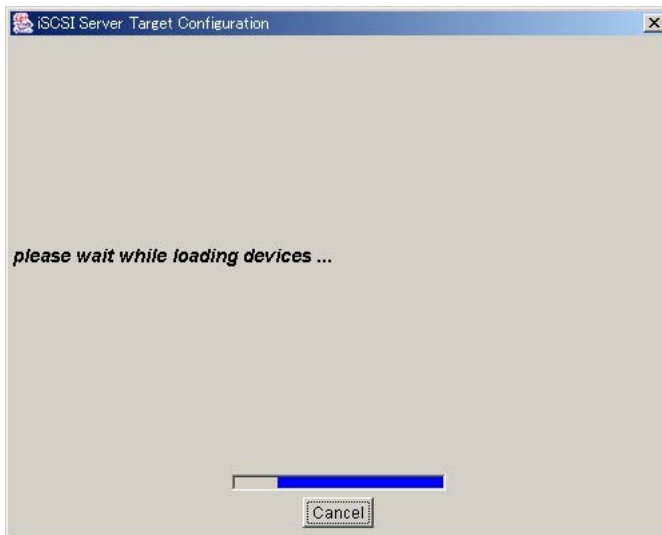
3 Click [Remote Storage Setup].

The following window appears.



4 Select a slot and click [Add Local Media Connection].

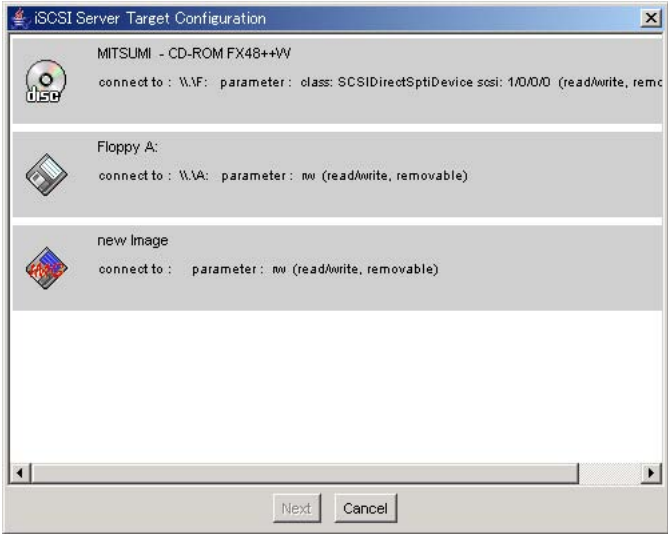
Search for drives on the console starts.



POINT

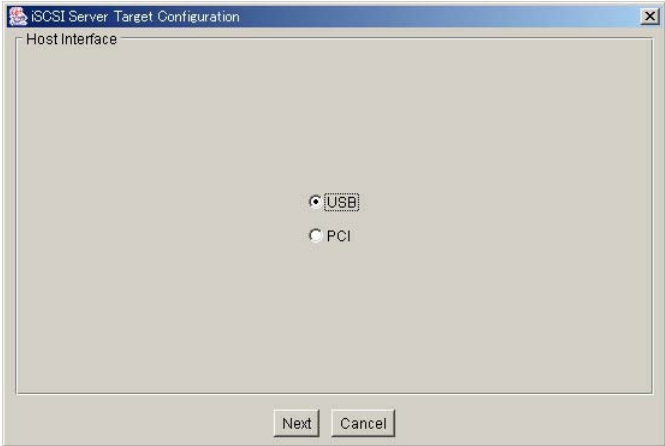
- ▶ You may be asked whether to search for CD-ROM drives during search. If CD-ROM drives are used on RemoteStorage, click [Yes].

5 The following window appears after search is completed. Select an item and click [Next].



Devices displayed here depend on the console which is running the Web interface. In other words, only devices that can be recognized by the Web interface are displayed among those connected to the console. The following setting procedures differ depending on the selected drive. The procedures may also differ depending on the console hardware environment. Refer to the following example for setting.

Example: CD-ROM



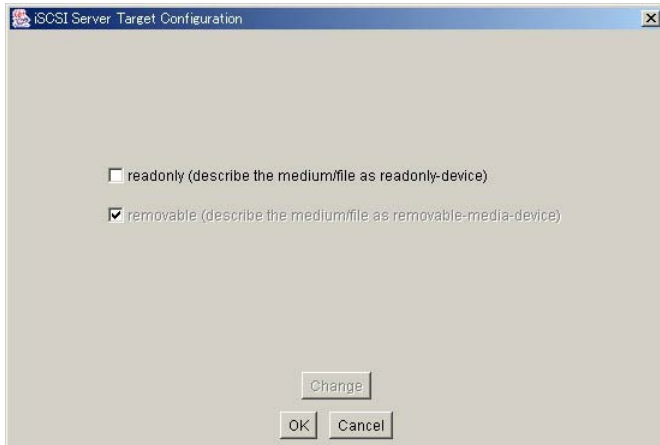
1. A window appears for selecting a connection interface. Select [USB] and click [Next].

After connection succeeds, the following window appears:



2. Click [OK].

Example: Floppy disk



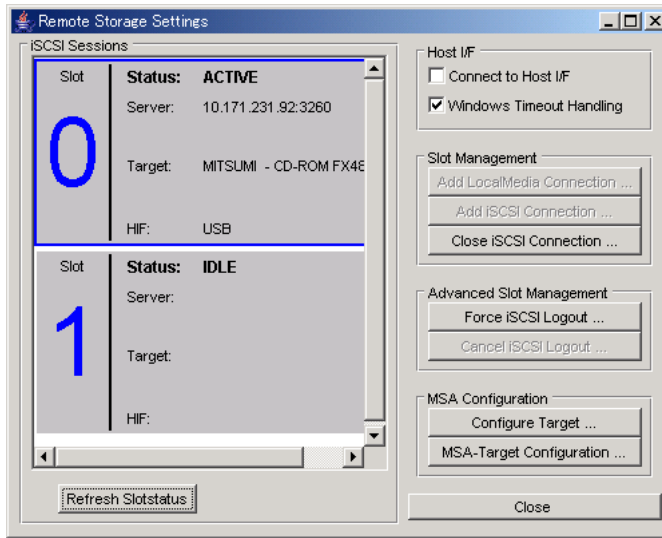
1. To read a floppy disk as "ReadOnly", check [readonly (describe the medium/file as readonly-device)] and click [OK].

If there is no floppy disk in the drive, the following warning message is displayed:



2. Set a floppy disk in the drive and click [OK].
3. Select [USB] on the interface selection window and click [Next].

6 Make sure that device information is stored in the slot selected in Step 4.



[ACTIVE] is displayed as the status of a slot in which a device is set and [IDLE] for a slot in which no device is set.

Select the slot marked [ACTIVE], check the [Connect to Host I/F] checkbox, and click [Configure Target].

This completes Local connection.

7 Click [Close] to close the [Remote Storage Setup] window.

● iSCSI connection

For iSCSI connection, the Remote Service Board works as an iSCSI client. To execute iSCSI connection, at least one "iSCSI server" is required on the network and the server must be physically different from the server on which the Remote Service Board is installed. The Remote Service Board connects to the iSCSI server to perform iSCSI connection.

An iSCSI server can be established by installing the Management Server Application (MSA) on the server OS. For more details on the MSA such as installation and setup, refer to "5.2.2 Installation and Configuration of the Management Server Application (MSA)" (→pg.306).

POINT

- ▶ The Web interface of the Remote Service Board cannot be opened from an iSCSI server.
- ▶ It is possible to connect to one iSCSI server from multiple Remote Service Boards.

Perform the following procedures for iSCSI connections:

Steps 1 and 2 are only required for PG-RSB102. When using PG-RSB103 or PG-RSB104, begin from Step 3.

1 Click [Remote Storage Setup].

The following window appears.



2 Set the communication interface between the server and Remote Service Board.

Set [Remote Storage via USB] to [Remote Storage Connection:].

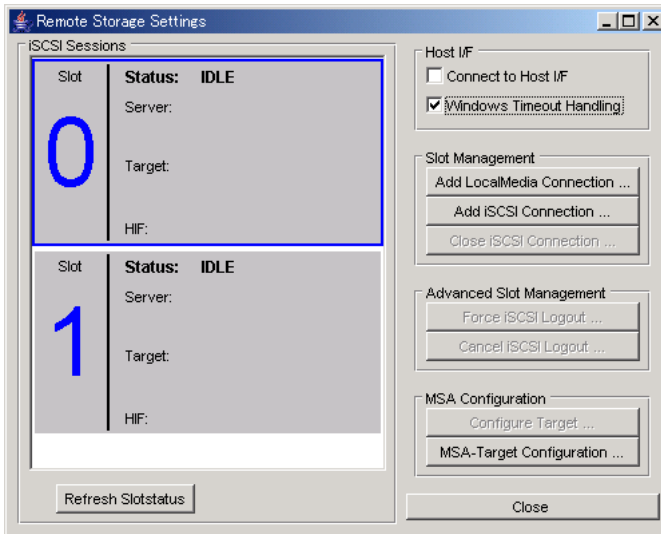


- ▶ If any setting is changed in [Remote Storage Connection:], the Remote Service Board requests resetting. To enable the change, reset the Remote Service Board.

Whether options are enabled or disabled depends on the settings between the Remote Service Board and server.

3 Click [Remote Storage Setup].

The [Remote Storage Settings] window appears.



4 Click [MSA- Target Configuration].

The following window appears.

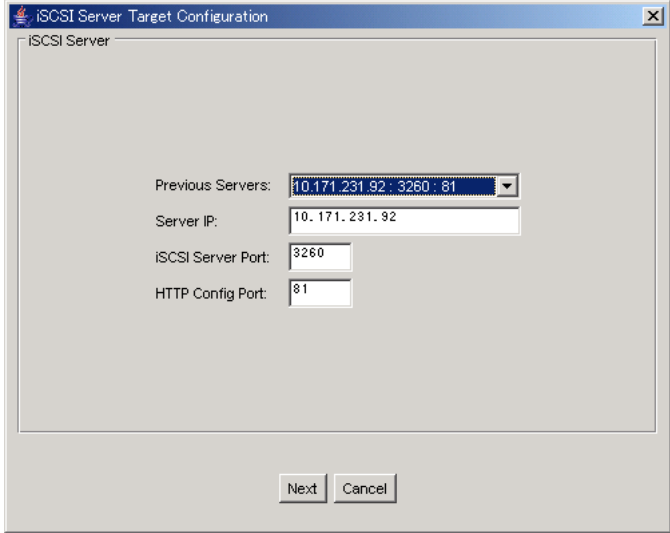
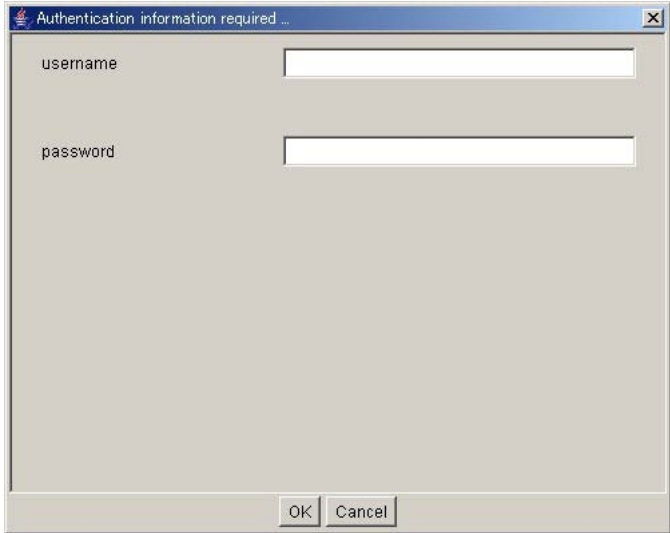


table: iSCSI Server Setting Items

Item	Description
Previous Servers	Select a destination from the history of the servers previously connected. Nothing appears if there is no previous connection.
Server IP	Enter the IP address of the server on which the MAS is installed.
iSCSI Server Port	Enter the port number of the iSCSI server. The default value is "3260".
HTTP Config Port	Enter the port number of the HTTP management port of the MAS. The default value is "81".

5 Set each item and click [Next].

The following window appears.

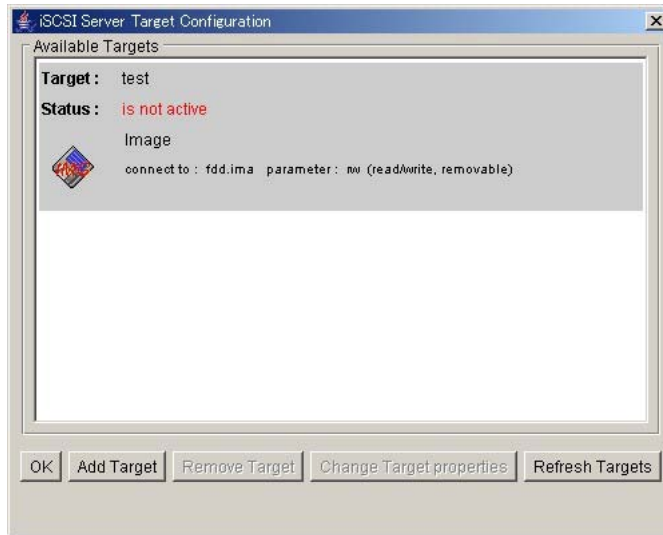


- 6 Enter the user name and password and click [OK].

POINT

- ▶ The user name and password can be changed on MAS settings.

The following window appears.



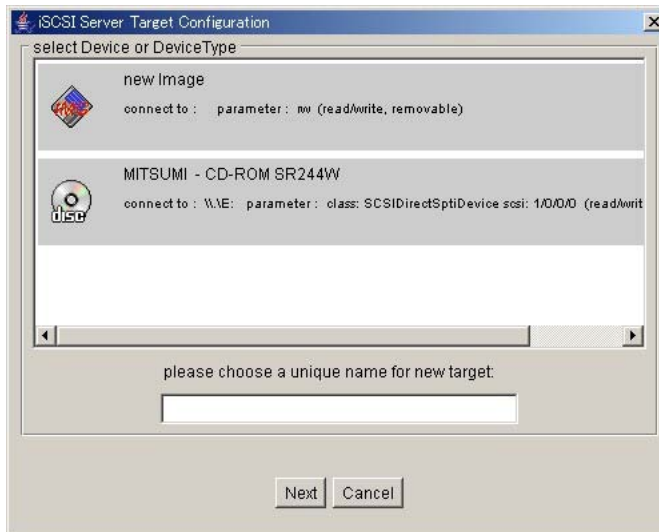
- 7 Create an iSCSI target object.

It is possible to remove iSCSI target objects or change their settings if necessary.

Creating an iSCSI target object

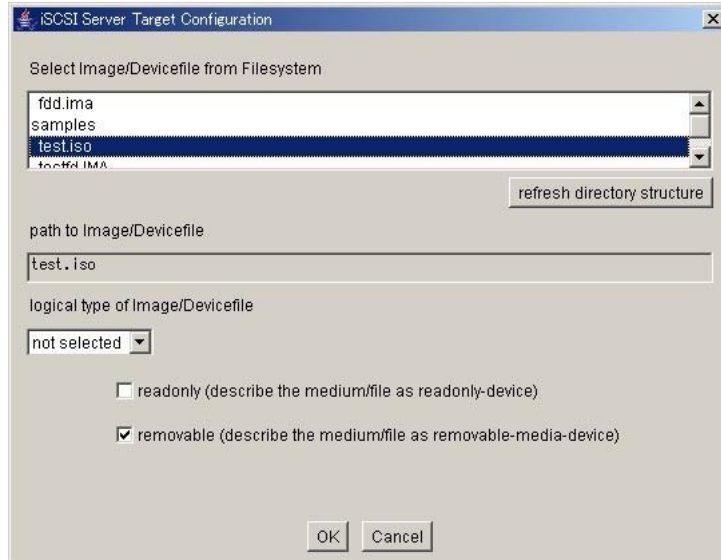
1. Click [Add Target].

The following window appears.



2. Select a media type, enter a target object name in the text box, and click [Next]. Available media types depend on the hardware configuration of the iSCSI server. They also differ depending on MAS settings.

Click [Next] to display a window for selecting an image file from the stored image files.



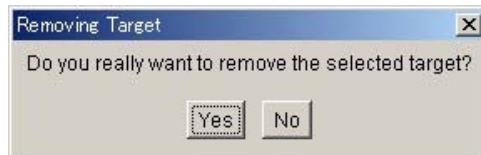
3. Select an image file, select a file type from the [Logical type of image/devicefile] list, and click [OK].

The [Remote Storage Settings] window appears again.

Removing an iSCSI target object

1. Select a target object to be removed and click [Removing Target].

A confirmation message appears.



2. Click [Yes].

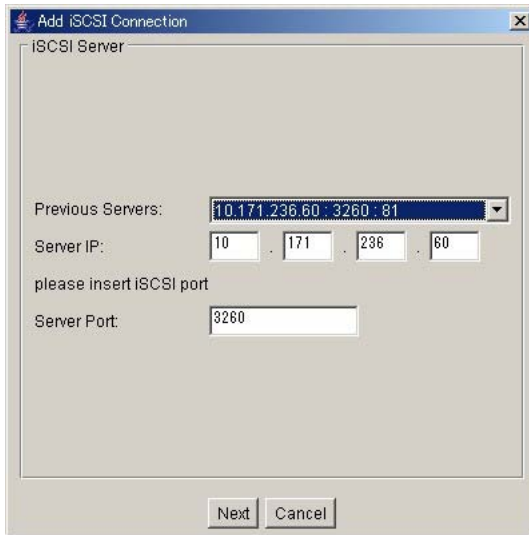
The selected target object is removed.

Changing iSCSI target object settings

1. Select a target object to be changed and click [Change Target properties]. A window appears for selecting an image file.
2. Change settings as necessary and click [OK].

8 Click [Add iSCSI Connection].

A window appears for selecting an iSCSI server.



9 Select the iSCSI server set in Step 4 to [Previous Servers] and click [Next].

A window appears for selecting a target object.



10 Select the target object created in Step 7 and click [Next].

When using PG-RSB102, the following window appears for selecting a connection interface. When using PG-RSB103/PG-RSB104, this window does not appear. The window in step 11 appears.

**POINT**

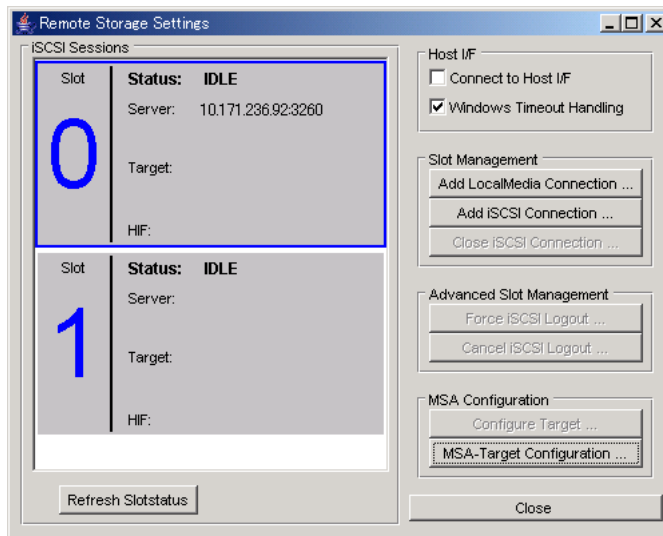
- ▶ The following procedure describes iSCSI connection via USB. For connection via PCI, select [PCI] in the following procedure. Differences between USB and PCI connections are as follows:
 - Virtual CD-ROM via PCI is not supported.
 - To enable remote storages to be recognized via PCI, the server need be restarted.
- ▶ The server can only boot from the remote storage device via USB if the BIOS supports "USB Legacy". In the BIOS Setup Utility, set [Multiboot] and [USB Legacy Support] to [Enabled]. However, for some models, these settings are not available in the BIOS Setup Utility or cannot be changed manually.

11 Select [USB] and click [Next].

After connection succeeds, the following window appears:



- 12 Click [OK] to return to the [Remote Storage Settings] window. Make sure that the device information has been added.



[ACTIVE] is displayed as the status of a slot in which a device is set and [IDLE] for a slot in which no device is set.

- 13 Select the slot marked [ACTIVE], check [Connect to Host I/F], and click [Configure Target]. This completes iSCSI connection.
- 14 Click [Close] to close the [Remote Storage Settings] window.

■ USB Settings

Set up USB functions on the Remote Service Board.



table: USB Function Settings

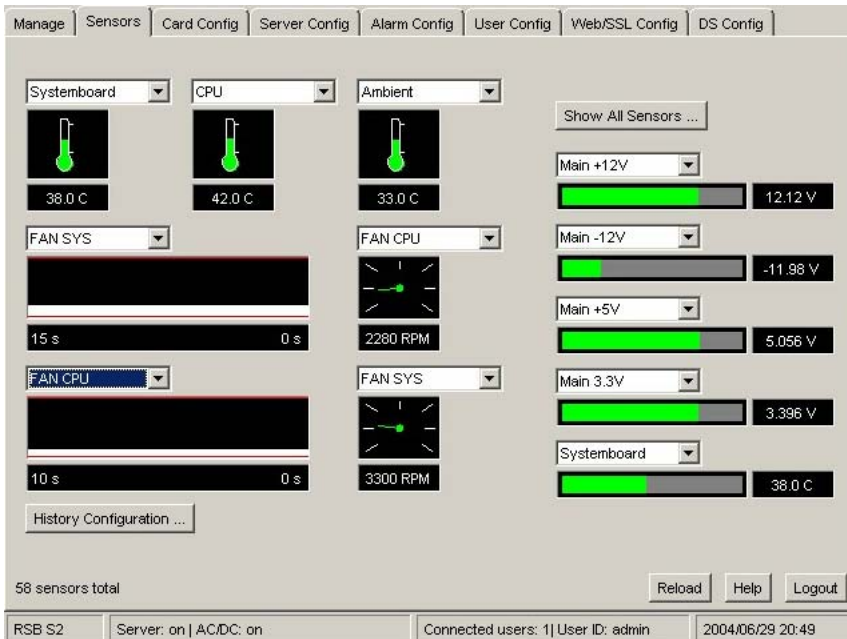
Item	Description
Enable USB HID Devices	Enables keyboard and mouse via USB. Make sure to check this checkbox to use AVR.
HID Devices always active	Check this checkbox if USB hot plug is not supported by the server BIOS.
Enable USB Storage Devices	Enables RemoteStorage via USB. Check this checkbox to use RemoteStorage.
Enable USB High Speed Capability	Enables high speed storage for RemoteStorage via USB.

POINT

- ▶ When “Enable USB High Speed Capability” is checked, the keyboard and mouse of USB might not be able to use it. In this case, this item check is removed.

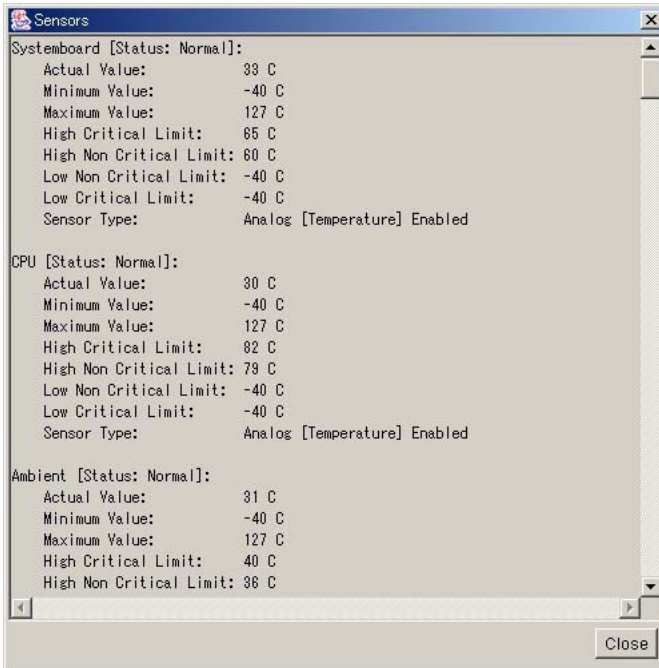
5.3.3 [Sensors] Page

The [Sensors] page is available for viewing values of each sensor of the server.



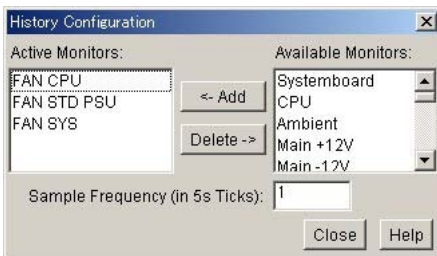
■ [Show All Sensors ...]

Shows values of all sensors.



■ [History Configuration ...]

Shows values of a sensor at a certain frequency. The following window appears after [History Configuration ...] is clicked:



Select a target sensor from [Available Monitors] and click [<-Add] to add it to [Active Monitors]. The added sensor can be selected from the pull-down menu on the upper part of the window.

■ [Reload]

Reloads values of all sensors. The sensor currently displayed may be unselected. Select it again to display it. The progress is displayed on the lower left of the window.

5.3.4 [Card Config] Page

The [Card Config] page is available for setting the Remote Service Board or checking its state.

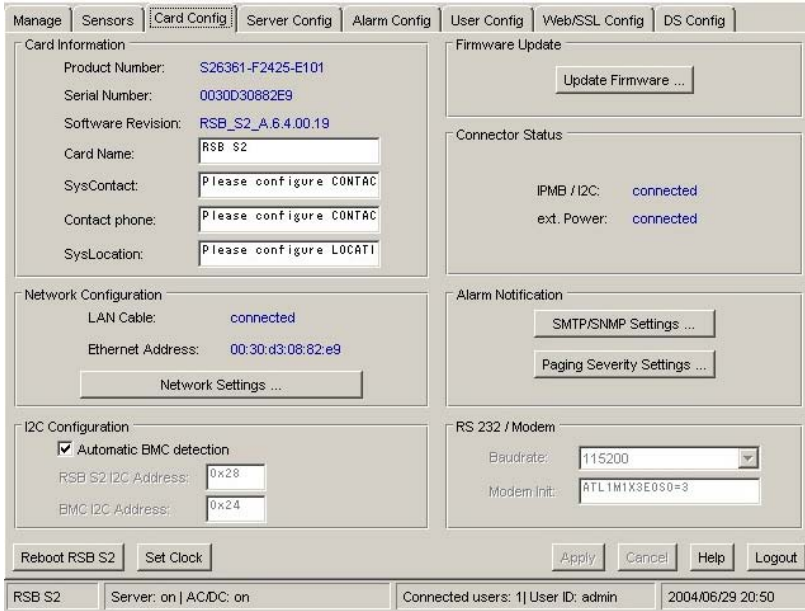


table: Functions on the [Card Config] Page

Item	Description
Card Information	Information related to the Remote Service Board.
Product Number	Displays the product number of the Remote Service Board.
Serial Number	Displays the serial number of the Remote Service Board.
Software Revision	Version of the firmware applied to the Remote Service Board.
Card Name	Sets the name of the Remote Service Board.
SysContact	Sets an emergency contact.
Contact Phone	Sets the phone number of the emergency contact.
SysLocation	Sets location information of the server on which the Remote Service Board is installed.
Network Configuration	Sets the network interface of the Remote Service Board. → "■ Network Settings" (pg.334)
LAN Cable	Displays the connection status of a LAN cable.
Ethernet Address	Displays the MAC address of the network interface of the Remote Service Board.
I2C Configuration	Available for setting I2C functions.
Automatic BMC detection	Connects automatically to the BMC on the server. Check this checkbox.
Firmware Update	Updates the firmware of the Remote Service Board. This item is not supported.
Connection Status	Displays the connection status of the Remote Service Board.
IPMB/I2C	Displays the IPMB/I2C connection status.
Ext.Power	Displays the connection status of an external power supply of the Remote Service Board. When RSB has not outside power connect, this item is not displayed.

table: Functions on the [Card Config] Page

Item	Description
Alarm Notification	Click [SMTP/SNMP Settings ...] to set mail server and SNMP. → "■ SMTP/SNMP Settings" (pg.335) Click [Paging Severity Settings ...] to set severities for each group. → "■ Paging Severity Setting" (pg.335)
RS 232/Modem	Sets connections with serial port and modem. This item is not supported.

■ Network Settings

Set the DNS and IP address of the Remote Service Board.

Network Settings

Ethernet

Card Name: RSBS2-LP

IP Address: 10 . 171 . 236 . 221

Netmask: 255 . 255 . 255 . 0

Gateway IP: 10 . 171 . 236 . 1

DHCP Server: 10 . 171 . 134 . 25

LAN Mode: Auto Negotiation

Use DHCP

DHCP Hostname Configuration

Register DHCP Address in DNS

Use Cardname instead of Hostname

Add Card Serialnumber

Add Extension

Extension: -RSB

DNS Name: RSBS2-LP-0030D309CB44

DNS Settings

DNS enabled

Obtain DNS configuration from DHCP

DNS Domain: fujitsu.co.jp

DNS Server 1: 10 . 171 . 133 . 2

DNS Server 2: 10 . 0 . 8 . 3

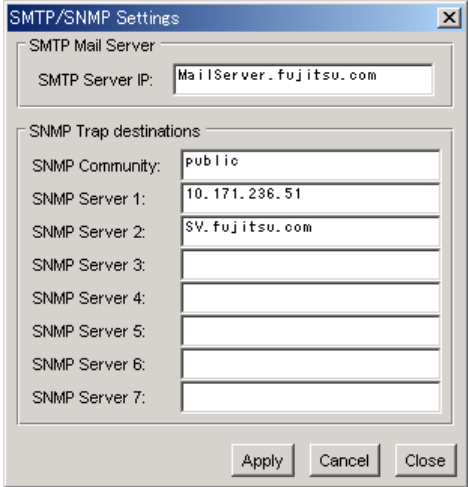
DNS Server 3: 10 . 23 . 4 . 3

Apply Cancel Close Help

■ SMTP/SNMP Settings

When DNS is set with Network Settings, the server name can be specified for mail server and SNMP trap destination.

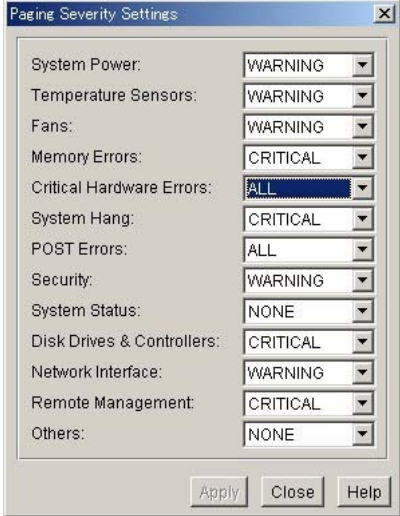
However, when the setting of DNS is wrong, the IP specification is also invalid.



- SMTP Server IP
The Remote Service Board sends mail to the SMTP server set here. Use the [Alarm Config] page for detailed settings such as mail destinations.
- SNMP Trap destinations
Set destination IP addresses of SNMP traps sent by the Remote Service Board.

■ Paging Severity Setting

Set values (severities) to trigger "SNMP trap transmission and SEL writing" for each group.



"SNMP trap transmission and SEL writing" are triggered when each group reaches the set severity. Each severity means as follows:

table: Severity Settings

Item	Description
None	SNMP trap transmission and SEL writing are not triggered.
Critical	SNMP trap transmission and SEL writing are triggered by events at the critical and higher levels.
Warning	SNMP trap transmission and SEL writing are triggered by events at the warning and higher levels.
All	SNMP trap transmission and SEL writing are triggered by all events.

■ [Reboot RSB S2] Button

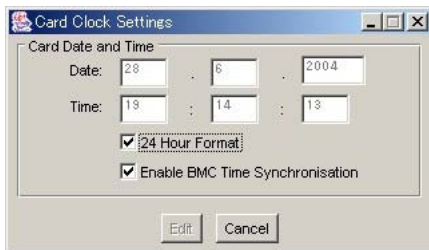
Reboots the Remote Service Board.

Rebooting disconnects all login users and connection to the Remote Service Board becomes temporarily disabled. After rebooting, do not operate the Web interface until the normal login window appears.

■ [Set Clock] Button

Set the internal clock of the Remote Service Board.

Normally, this setting need not be changed. The following window appears after the [Set Clock] button is clicked:



POINT

- ▶ The internal clock of the Remote Service Board is always synchronized with the module called "BMC" on the baseboard.
If the [Enable BMC Time Synchronisation] checkbox is unchecked, the Remote Service Board is no longer synchronized with the BMC and starts to work only with its own internal clock. In such a case, the [Edit] button is enabled so that you can set the time of the internal clock of the Remote Service Board.

5.3.5 [Server Config] Page

Obtains and displays various server information.

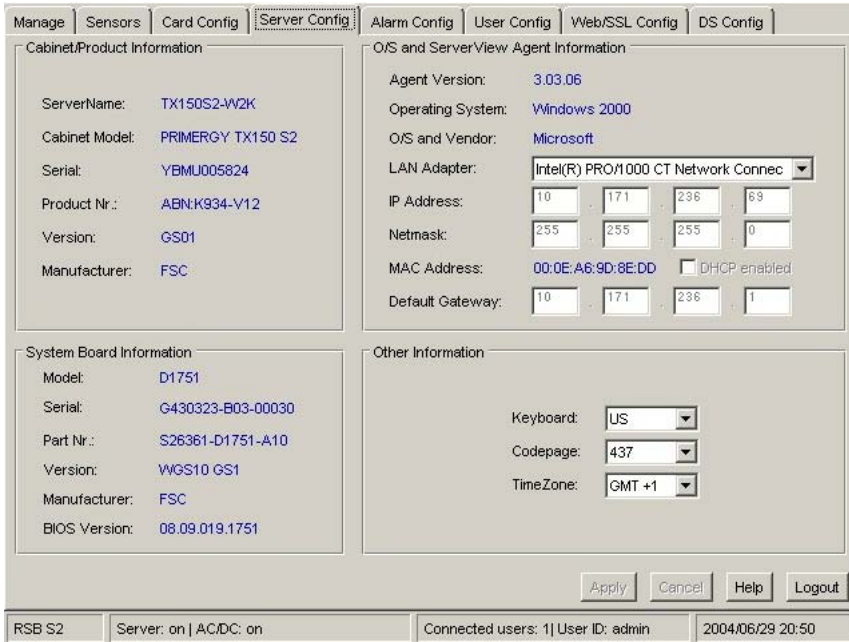


table: Functions on the [Server Config] Page

Item	Description
Cabinet/Product Information	Displays cabinet/product information.
Server Name	Displays the server name.
Model	Displays the model name.
Serial	Displays the serial number.
Product Nr	Displays the product number.
Version	Displays version information.
Manufacturer	Displays the manufacturer name.
System Board Information	Displays baseboard information.
Model	Displays the model name.
Serial	Displays the serial number.
Part Nr	Displays the part number.
Version	Displays version information.
Manufacturer	Displays the manufacturer name.
BIOS Version	Displays the BIOS version.

table: Functions on the [Server Config] Page

Item	Description
O/S and ServerView Agent Information	Displays OS and ServerView Agent information.
Agent Version	Displays the Agent version.
Operating System	Displays the OS name.
O/S and Vendor	Displays the OS vendor name.
LAN Adapter	Displays the name of the LAN adapter installed on the server. If there are more than one LAN adapters, you can view information on each adapter by switching them using the pull-down menu.
IP Address	Displays the IP address.
Netmask	Displays the IP of the subnet mask.
Gateway	Displays the IP of the gateway.
MAC Address	Displays the MAC address.
DHCP enabled	Displays whether DHCP is enabled or disabled.
Other Information	Available for setting keyboard, time zone, etc.
Keyboard	Set the language of the keyboard.
Codepage	Set the code page used on the server.
TimeZone	Set the time zone.

5.3.6 [Alarm Config] Page

Set alarm functions.

table: Setting Items on the [Alarm Config] Page

Item	Description
Global Email Paging Configuration	Set various mail items.
Mail Format	Set the mail format used for sending mail. The following formats are available: <ul style="list-style-type: none"> • Standard (default) • ITS-Format • Fujitsu REMCS Format
SMTP Server	Set the IP address of the SMTP server. The default value is "0.0.0.0".
SMTP Retries	Set the retry count for SMTP transmission. The default value is "3".
SMTP Retry Delay[sec]	Set the interval to retry SMTP transmission in seconds. The default value is "30".
To	Set a destination mail address.
Enable Email Paging	Enables/disables e-mail paging. Check this checkbox to enable paging.
Mail Format dependend Configuration	Set various items on the mail format. Available items depend on the mail format.
From	Set a sender's mail address. Not available when [Standard] is set to [Mail Format].
Subject	Set a mail subject. Not available when [Standard] or [Fujitsu REMCS Mail] is set to [Mail Format].
Message	Set any mail message. Not available when [Standard] or [Fujitsu REMCS Mail] is set to [Mail Format].
Admin.Name	Set an administrator name. Not available when [Standard] or [Fujitsu REMCS Mail] is set to [Mail Format].
Admin.Phone	Set the phone number of the administrator. Not available when [Standard] or [Fujitsu REMCS Mail] is set to [Mail Format].
REMCS Id	Set a device ID. Not available when [Standard] or [ITS-Format] is set to [Mail Format].
Server URL	Set the server URL. Not available when [ITS-Format] or [Fujitsu REMCS Mail] is set to [Mail Format].

5.3.7 [User Config] Page

Set the user account-related items.

The screenshot displays the 'User Administration' interface. At the top, there are navigation tabs: Manage, Sensors, Card Config, Server Config, Alarm Config, **User Config**, Web/SSL Config, and DS Config. The 'User Administration' section includes a 'User ID' dropdown menu set to 'admin', with 'New User ...' and 'Delete' buttons. Below this is a 'Group' dropdown menu set to 'ADMINISTRATOR', a 'Description' text field containing 'Default Administrator', and a 'Dialback Number' text field containing '1-800-DIAL-ADMIN'. There is an unchecked 'Enable Paging' checkbox and buttons for 'Paging Settings...', 'Change Password', and 'Autologon Settings'. The 'Currently Connected Users' section shows a table with two columns: 'User ID' and 'Description'. The table contains one entry: 'admin' with 'Default Administrator'. At the bottom right, there are 'Apply', 'Cancel', 'Help', and 'Logout' buttons. The status bar at the very bottom shows 'RSB S2', 'Server: on | AC/DC: on', 'Connected users: 1 | User ID: admin', and '2004/06/29 20:51'.

table: Functions on the [User Config] Page

Item	Description
User ID	Displays the Agent version. After a user account is selected in the combo box, information on the user account is displayed on the following items.
[New User ...]	Creates a new user. → "■ New User" (pg.341)
[Delete]	Deletes the user account displayed in [User ID]. When a confirmation message appears, click [OK].
Group	Displays the name of the group to which the user account selected in [User ID] belongs. It is possible to change the group name to that of another group. The following groups are available: "ADMINISTRATOR", "CALLBACK", "NO_ACCESS", "OEM", "OPARATOR", "USER"
Description	Displays detailed information on the user account selected in [User ID]. It is also possible to modify the current information.
Dialback Number	Displays the phone number of the user account selected in [User ID]. It is also possible to modify the information currently set.
Enable Paging	Check this checkbox to enable mail paging with the user account selected in [User ID].
[Paging Settings ...]	Set the mail paging-related information. This is available only when [Enable Paging] is checked. → "■ Paging Settings" (pg.341)
[Change Password]	Changes the password of the user account selected in [User ID]. When clicking [Change Password], the window for changing the password appears. Enter the password and click [OK].
[Autologon Settings]	Enables autologon of the user account selected in [User ID]. → "■ Autologon Settings" (pg.342)

table: Functions on the [User Config] Page

Item	Description
Currently Connected Users	Displays information on the users who are currently logging in to the Remote Service Board. <ul style="list-style-type: none"> • User ID: User account • Description: Detailed information

■ New User

When [New User ...] is clicked, the following window appears. Set each item to create a new user account.

table: Setting Items for a New User Account

Item	Description
UserID	Set a user account name.
Group	Set the name of the group to which the user account will belong. Select "ADMINISTRATOR", "CALLBACK", "NO_ACCESS", "OEM", "OPARATOR", or "USER".
Description	Set detailed information on the user account.
Dialback Number	Set the phone number of the user account.
Password	Set the password of the user account.
Confirm Password	Enter the above password again.

■ Paging Settings

When [Paging Settings ...] is clicked, the following window appears. If any specified event occurs, you may receive email paging.

The following settings are required to enable email paging:

table: Setting Items for Mail Paging

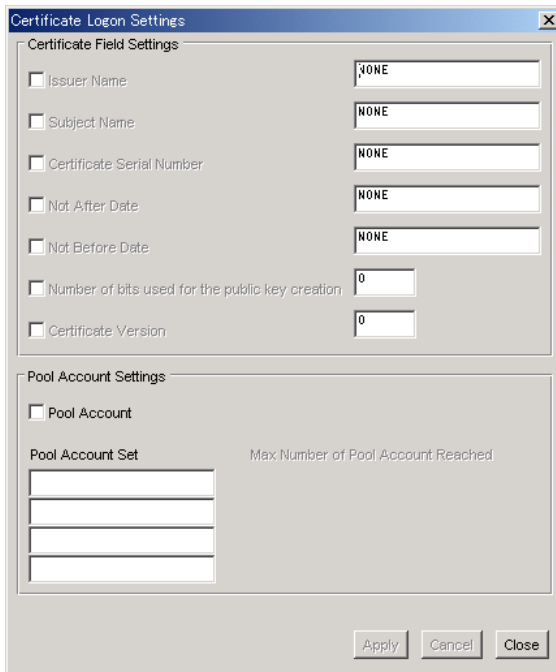
Item	Description
[Enable Email Paging]	Check this checkbox to enable it.
Email Address	Set the user's e-mail address.

POINT

- ▶ In [SMTP Server], the IP address of the SMTP server is displayed. This is the value set in [SMTP/SNMP Settings] on the [Card Config] page.
- ▶ Click [Test Paging] to test email transmission.

■ Autologon Settings

When [Autologon Settings] is clicked, the following dialog appears for enabling autologon for the user account selected in [User ID].



The following settings are necessary to enable autologon. Define which fields of the user certificate will be used by the Remote Service Board during autologon.

Each of the following items is selected when the value is input in the text box to the right of the item. If the word "NONE" in uppercase (or "0" for numeric items) is input, the item is unselected.

- Issuer Name
- Subject Name
- Certificate Serial Number
- Not After Date
- Not Before Date
- Number of bits used for the public key creation
- Certificate Version

IMPORTANT

- ▶ Make sure to select two or more from the following items:
 - Issuer Name
 - Certificate Serial Number
 - Subject Name

POINT**[Pool Account] checkbox**

- ▶ Check the [Pool Account] checkbox to allow multiple users to use the displayed account.

5.3.8 [Web/SSL Config] Page

The screenshot shows the [Web/SSL Config] page with the following details:

- Navigation Tabs:** Manage, Sensors, Card Config, Server Config, Alarm Config, User Config, **Web/SSL Config**, DS Config
- Setup Section:**
 - Standard Web Access (HTTP Port: 80)
 - Secured Web Access (SSL) (HTTPS Port: 443)
 - Telnet Access (Telnet Port: 3172)
 - Auto log-on
 - Symmetric Encryption Strength (bit): 128
- Notification Section:**
 - Notification on Certificate Expiration
 - 30 days to notify before expiration
- Server Certificate Section:**
 - View ...
 - Request Generation ...
 - Request Status ...
 - Upload ...
- Certificate Authority Certificate Section:**
 - View ...
 - Upload ...
 - Enforce Client Certificate
- Buttons:** Apply, Cancel, Help, Logout
- Status Bar:** RSB S2 | Server: on | AC/DC: on | Connected users: 1 | User ID: admin | 2004/06/29 20:51

The [Web/SSL Config] page has the following functions:

table: Functions on the [Web/SSL Config] Page

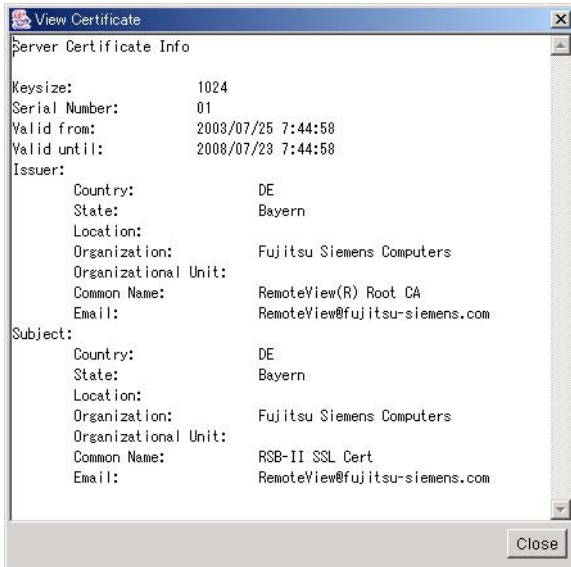
Item	Description
Setup	Set the port numbers of HTTP and Telnet to access the Remote Service Board.
Standard Web Access	Enables/disables HTTP access. If checked it is possible to perform HTTP access to the Remote Service Board.
HTTP Port	Set the port number for HTTP. The default value is "80".
Secured Web Access (SSL)	Enables/disables HTTPS (SSL) access. If checked, it is possible to do HTTPS (SSL) access to the Remote Service Board.
HTTPS Port	Set the port number for HTTPS. The default value is "443".
Telnet Access	Enables/disables Telnet access. This function is not supported for the Remote Service Board (PG-RSB102).
Telnet Port	Set the port number for Telnet. The default value is "3172".
Auto log-on	Enables/disables autologon. If checked, it is possible to autologon to the Remote Service Board. This is available only when [Enforce Client Certificate] is checked in [Certificate Authority Certificate].
Symmetric Encryption Strength (bit)	Set the encryption strength. Select "40" or "128". The default is "128".
Notification	Set whether to notify the user of certificate expiration.
Notification on Certificate Expiration	Enables/disables notification on certificate expiration. If checked, certificate expiration is notified to the login user.
days to notify before expiration	Set the certificate expiration period. The default value is "30".
Server Certificate	Controls the server certificate. For more details, refer to "■ Server Certificate" (→pg.345).
[View ...]	Displays information on the server certificate to be used next time the Remote Service Board is rebooted.
[Request Generation ...]	Generates a new server certificate.
[Request Status ...]	Displays the status for server certification requests.
[Upload ...]	Updates the server certificate.
Certificate Authority Certificate	Controls the CA certificate. For more details, refer to "■ Certificate Authority Certificate" (→pg.346).
[View ...]	Displays information on the CA certificate to be used next time the Remote Service Board is rebooted.
[Upload ...]	Updates the CA certificate.
Enforce Client Certificate	If checked, it is allowed the user having the client certificate installed on the Web browser to connect to the Remote Service Board using SSL.

■ Server Certificate

Available for controlling the server certificate.

● View ...

Displays information on the server certificate to be used next time the Remote Service Board is rebooted.



● Request Generation

Generates a new server certificate.

Set each item in the [Request Generation] window and then click [Start CSR Generation ...].



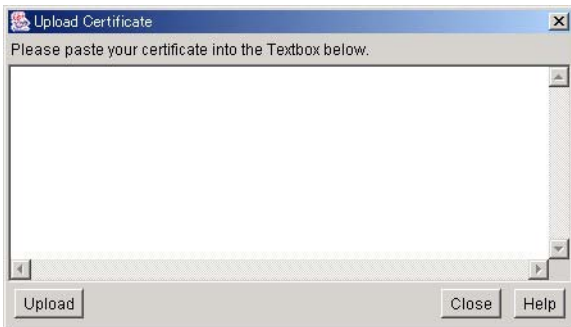
● **Request Status ...**

Displays the current status for server certification requests.



● **Upload ...**

Updates the server certificate.

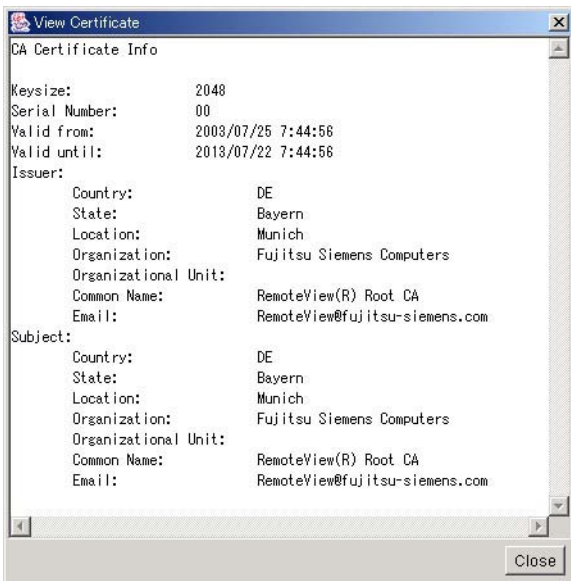


■ **Certificate Authority Certificate**

Available for controlling the CA certificate.

● **View...**

Displays information on the CA certificate to be used next time the Remote Service Board is rebooted.

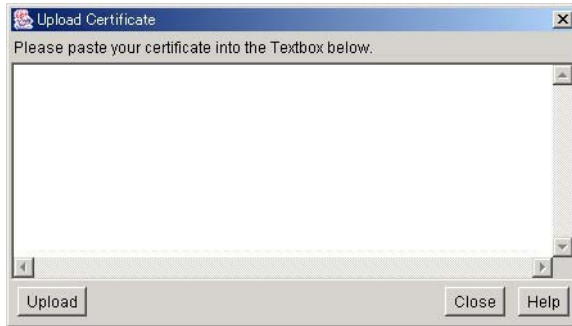


● Upload...

Updates the CA certificate. Perform the following procedures to update it:

- 1 Copy and paste the certificate sent from the CA in the text box on the [Upload Certificate] dialog.
- 2 Click [Upload] on the bottom of the window.

The updated certificate is enabled after the Remote Service Board is rebooted.



● Enforce Client Certificate

If checked, it is allowed the user having the client certificate installed on the Web browser to connect to the Remote Service Board using SSL.



- ▶ When the [Enforce Client Certificate] checkbox is checked, it is not possible to log in to the Remote Service Board without the client certificate. In such a case, access to the Remote Service Board menu during server boot (press the [F3] key) and change the setting.

5.3.9 [DS Config] Page

The directory service (DS function) component is a database for existing directory services, which is available for managing users accessing to the Remote Service Board.

When a user tries to log in to the Remote Service Board, the Remote Service Board checks whether the user is included in its internal database.

If the user is not included in the database and the DS function is enabled, the Remote Service Board requests the existing user from the Access Control Servers.

Following users can log in to the Remote Service Board:

- Users being managed in the internal database of the Remote Service Board
- Users belonging to a group registered with the directory service database

The [DS Config] page has the following functions:

Directory Service (DS) Authentication Properties

Enable Directory Service connectivity

Access Control Servers: 0.0.0.0:0

DS Group Name: RMCALL

History of User Login's since last card reset

DS User Log

User ID	Login Time	Login Name
0x3	2004/06/24 21:39:00	admin
0x3	2004/06/25 10:08:12	admin
0x3	2004/06/25 10:55:12	admin
0x3	2004/06/25 11:06:17	admin
FAILED	2004/06/25 11:32:11	admin
FAILED	2004/06/25 11:32:19	admin
0x3	2004/06/25 11:59:41	admin
0x3	2004/06/25 12:12:07	admin
0x3	2004/06/25 13:27:55	admin

Apply Cancel Help Logout

RSB S2 Server: on | AC.DC: on Connected users: 1 | User ID: admin 2004/06/29 20:52

table: Functions on the [DS Config] Page

Item	Description
Directory Service (DS) Authentication Properties	Set directory service authentication properties.
Enable Service Directory connectivity	If checked, it is possible to set the server and group for which connection is allowed.
Access Control Servers	Set the IP address of the Access Control Server or the server name, and the port number to which the ACS software of the Remote Service Board responds. <ul style="list-style-type: none"> • for example 192.168.1.1:7777 server.yourcompany.com:8888 Multiple values can also be specified as follows: 192.168.1.1:7777, server.yourcompany.com:8888
DS Group Name	Set the name of the directory service group to which the directory service group belongs.
History of User Login's since last card reset	Displays the history of the login user. This history is cleared when the Remote Service Board is rebooted. The following information is displayed: <ul style="list-style-type: none"> • User ID • Login time • Login name

Appendix

This chapter explains supplementary information such as troubleshooting and how to uninstall ServerView.

A	Troubleshooting	352
B	Uninstallation	376
C	Icon List	379
D	Trap List	389
E	Threshold List	390
F	Technical Information	396

A Troubleshooting

This section explains notes for using ServerView and error messages.

A.1 Troubleshooting of Installation Script

Installation script displays an error message when it detects an installation error.

If the error is not resolved by the corrective actions below, refer to "■ Installing ServerView Linux manually" (→pg.45) and perform the installation without using the installation script.

table: Error messages of installation script

Error No.	Error messages
	Cause and corrective action
1001	login user is not root! Please try again as root.
	The log in user is not a superuser. Log in again as a superuser and execute ServerView's installation script.
1004	Not supported Distribution.
	This distribution is not supported.
1005	Available disk space is not enough.
	Not enough free disk space.
1006– 1999	kernel version is under X.X.XX
	The installation failed because the kernel version is less than X.X.XX. For the kernel version supported by PRIMERGY, refer to our information Website (http://primergy.fujitsu.com).
2001– 2999	"***" package is not installed.
	The RPM package that is required for installing ServerView has not been installed. After installing the "***" RPM package from Red Hat Linux CD-ROM, execute ServerView's installation script. For details on how to install RPM package, refer to "■ Installing ServerView Linux manually" (→pg.45).
2020	SELinux is effective.
	Because SELinux is Enabled, ServerView Agent cannot be installed. SELinux is Disabled, and try to installation script again. Change the following value in "/etc/selinux/config" file, and restart the server. After installation, set back this item, and restart the server. <ul style="list-style-type: none"> • (Before edit) SELINUX=enforcing • (After edit) SELINUX=disabled
3001– 3005	fail to uninstall XXX. (XXX is a RPM name)
	Error occurred during the uninstallation of XXX. After the uninstallation with "rpm -e XXX" command is done, execute ServerView's installation script.
4101	failure in "mv" command.
	Error occurred in the Linux system command. Refer to "■ Installing ServerView Linux manually" (→pg.45) and then perform the installation.

table: Error messages of installation script

Error No.	Error messages
	Cause and corrective action
4102	/etc/snmp/snmpd.conf is not exist.
	The setting file of the SNMP service was not found. After the command below is executed, execute ServerView's installation script. # cp /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/Linux/snmpd.conf /etc/snmp/snmpd.conf
4103–4401	failure in "****" command.
	Error occurred in the Linux system command. Refer to "■ Installing ServerView Linux manually" (→pg.45) and then perform the installation.
4402	failure in "/etc/rc.d/init.d/snmpd start" command.
	Failed to start up the snmp service. Check whether the /etc/rc.d/init.d/snmpd file exists. If it does not exist, re-install the RPM package of net-snmp (or ucd-snmp for RHEL-AS2.1(x86) / ES2.1(x86)) from Red Hat Linux CD-ROM and then execute ServerView's installation script. For details on how to install RPM package, refer to "■ Installing ServerView Linux manually" (→pg.45).
6000	"srvmagt-mods_src" installation failed.
	Failed to install ServerView Agent (srvmagt-mods_src). After the command below is executed, try to install srvmagt-eecd again. rpm -e srvmagt-agents rpm -e srvmagt-eecd rpm -e srvmagt-mods_src # cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/Linux/Agent/ # rpm -i srvmagt-mods_src-X.XXXX.redhat.rpm # rpm -i srvmagt-eecd-X.XXXX.redhat.rpm # rpm -i srvmagt-agents-X.XXXX.redhat.rpm (X.XX-XX means version number.) # cd / # /etc/rc.d/init.d/srvmagt stop # /etc/rc.d/init.d/eecd stop # /etc/rc.d/init.d/eecd start # /etc/rc.d/init.d/srvmagt start
6001	"srvmagt-eecd" installation failed.
	Failed to install ServerView Agent (srvmagt-eecd). After the command below is executed, try to install srvmagt-eecd again. # rpm -i /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/Linux/Agent/srvmagt-eecd-X.XX-XX.redhat.rpm (X.XX-XX means version number.) # cd / # /etc/rc.d/init.d/srvmagt stop # /etc/rc.d/init.d/eecd stop # /etc/rc.d/init.d/eecd start # /etc/rc.d/init.d/srvmagt start

table: Error messages of installation script

Error No.	Error messages
	Cause and corrective action
6002	"srvmagt-agents" installation failed.
	Failed to install ServerView Agent (srvmagt-agents). After the command below is executed, try to install srvmagt-agents again. # rpm -i /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/Linux/Agent/srvmagt-agents-X.XX-XX.redhat.rpm (X.XX-XX means version number.) # groupadd svuser # cp /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/Linux/config /etc/srvmagt/config # chmod 644 /etc/srvmagt/config # cd / # /etc/rc.d/init.d/srvmagt stop # /etc/rc.d/init.d/eecd stop # /etc/rc.d/init.d/eecd start # /etc/rc.d/init.d/srvmagt start
6003	"AlarmService" installation failed.
	Failed to install AlarmService. After the command below is executed, try to install AlarmService again. #cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/Linux/ENGLISH/Sv/ # ./InstallAlarmService.sh AlarmServiceStarter-X.X-X.i386.rpm (X.X-X means version number.)
6004	"ServerView S2" installation failed.
	Failed to install ServerView S2. After the command below is executed, try to install ServerView S2 again. # cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/Linux/ENGLISH/ ServerView_S2/ # ./InstallServerView_S2.sh ServerView_S2Starter-X.X-X.i386.rpm (X.X-X means version number.)
7001	failure in "groupadd" command.
	Failed to create a group. Execute the command below. # groupadd svuser
7002	failure in copy default config file.
	Failed to copy the default setting file of the ServerView Agent. Execute the command below. # cp /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/Linux/config /etc/srvmagt/ config # chmod 644 /etc/srvmagt/config # cd / # /etc/rc.d/init.d/srvmagt stop # /etc/rc.d/init.d/eecd stop # /etc/rc.d/init.d/eecd start # /etc/rc.d/init.d/srvmagt start
7003	failure in \"chmod\" command.
	Failed to change the privilege of the /etc/srvmagt/config file. Execute the command below. #chmod 644 /etc/srvmagt/config

table: Error messages of installation script

Error No.	Error messages
	Cause and corrective action
7004 7006	<p>failure in "cd /" command.</p> <p>Failed to change the current directory. Execute the command below. # cd / # /etc/rc.d/init.d/srvmagt stop # /etc/rc.d/init.d/eecd stop # /etc/rc.d/init.d/eecd start # /etc/rc.d/init.d/srvmagt start</p>
7008	<p>failure in "/etc/rc.d/init.d/srvmagt start" command.</p> <p>Failed to start up ServerView Agent (srvmagt-agents). Execute the command below. # cd / # /etc/rc.d/init.d/srvmagt stop # /etc/rc.d/init.d/eecd stop # /etc/rc.d/init.d/eecd start # /etc/rc.d/init.d/srvmagt start</p>
7009	<p>failure in "/etc/rc.d/init.d/eecd start" command.</p> <p>Failed to start up ServerView Agent (srvmagt-eecd). Execute the command below. # cd / # /etc/rc.d/init.d/srvmagt stop # /etc/rc.d/init.d/eecd stop # /etc/rc.d/init.d/eecd start # /etc/rc.d/init.d/srvmagt start</p>

A.2 Troubleshooting of Management Console

■ Question and answer about Management Console

● How to specify the server to be monitored

It is required to set the server that communicates through TCP/IP.

When the application is started up, first the [Server List] window appears.

Click [New Server] on the [Server List] window and the server settings become available.

Then, the window for entering the IP address and name of the server appears (refer to "3.9.2 Adding the Monitored Server (Object)" (→pg.206)).

● How to schedule the power on/off

Monitored server operations can be scheduled.

For details about the settings, refer to "■ [Power ON OFF] Tab (ServerView S2) / [Power ON/OFF] Tab (Management Console)" (→pg.129).

 **IMPORTANT**

- ▶ This function is not always supported in all servers.
- ▶ These settings are also stored in BIOS of the scheduled server.
When ServerView is uninstalled from the scheduled server, disable the scheduling in advance.
Uninstalling the ServerView with the scheduling enabled can result in the power off without server OS being shut down during the power off process by the scheduling.

■ Troubleshooting of Management Console

● The figure of the server is not properly displayed on the [Display Properties] window.

When the display colors have been set less than 256 colors in the [Display Properties], the figure of the server displayed on ServerView or InventoryView window may not be correctly displayed.

To display the figure correctly, use the application in the environment with 65536 colors or more. The operation has still no problem when using with 256 colors. Just the display of the server photograph loses colors.

● Archive file or report file is not created.

If the data has not been stored in the archive file or the file has been incomplete, it might be judged that no free space exists in the disk or ServerView might judge that no free space exists in the disk.

Check the error log file "ArchErr.log" in the Program Files\Fujitsu\F5FBFE01 to verify whether an error occurred in the application. An error dialog will be displayed when ServerView cannot write data into the ArchErr.log file because there is no free space in the disk.

If there are no more free space in the disk, the problem can be solved by moving some files. If free space remains in the disk, restart the ServerView. It is also effective to restart the computer after checking the files.

When the data cannot be stored in the report file, the same reason as above is applicable.

● ServerView does not recognize Remote Service Board although it is installed

The Remote Service Board may not be recognized by ServerView when the OS is started immediately after ServerView or the Remote Service Board is installed.

Restart the OS.

● The model name of monitored server is displayed as [Unknown].

The model name of monitored server may be displayed as [Unknown] in ServerView window.

Wait awhile, and click [Update] in the [ServerView] window.

If [Unknown] is still displayed even above step is taken, restart ServerView Agent by following the steps below or restart the OS.

When monitored server is Windows

- 1 Click [Start] → [Programs] → [Fujitsu ServerView Agents] → [Diagnostic Tools] → [Restart ServerView Base Services].
- 2 Enable the [Search for management hardware] and click [Restart].

 **IMPORTANT**

- ▶ Generally, do not start [Restart ServerView Base Services].

When monitored server is Linux

- 1 Login as a root user.
- 2 Execute # /etc/rc.d/init.d/eecd stop.
- 3 Execute # /etc/rc.d/init.d/eecd rescan.
- 4 Execute # /etc/rc.d/init.d/srvmagt restart.

● The information is not correctly displayed on [Power/Environment] window.

On [Power/Environment] window, it takes some time to display the information correctly. Wait a while, and try the operation again.

● The contents of the error message buffer is not displayed.

The contents of the error message buffer may not be displayed on [Action] window. Wait a while, and try the operation again.

● ServerView start-up error has occurred

When a ServerView error has occurred, remove the "CTTxxxx.tmp" (xxxx = 0000 - FFFF) file under the ServerView directory.

● Device is not displayed

When you select [Adaptec/DPT SCSI Raid 3200 Controller] for the adapter name of the external storage device and display it in the [Display Devices] window, make sure the display for each slot. The display of the system driver on the adapter is not supported in the [Display Devices] window.

● The rebuilt status in ServerView is not displayed.

In RAID0+1 configuration, the rebuilt status in ServerView is not displayed (0% view). Use RAIDmanager to check rebuilt status (StorageManager).

● [System Identification LED Display] is not displayed.

When the monitor target server type is PRIMERGY C150:

There is no system identification LED in C150.

When the monitor target server type is other than PRIMERGY C150:

Follow the steps below to restart the agent and then the [System Identification LED Display] will be displayed.

- 1 Click [Start] → [Programs] → [Fujitsu ServerView Agents] → [Diagnostic Tools] → [Restart ServerView Base Services].
The [Restart Services] window appears.
- 2 Click [Restart].
- 3 When the restart has finished, the message "Restart Services completed successfully!" is displayed. Click [Exit].

IMPORTANT

- ▶ Generally, do not start [Restart ServerView Base Services].

● A message "The server is uncontrollable" is displayed

If the load of the network or the computer is high, the process would not finish within the time and [Uncontrollable] icon would be displayed.

In this case, you can follow the steps below to change polling intervals, timeout value, and update intervals to reduce the load or extend the timeout value.

- 1 Right-click the server having trouble on the [Server List] and select [Server Properties] → [Network/SNMP] from the menu displayed.
- 2 Change the setting values to the environment.

table: Setting values of Network/SNMP

Item	Description
Polling intervals	The time interval for polling the server. The server is requested to send the system information for each interval time specified here (default is 60 sec).
Timeout	Time to wait the server's response to the request (default is 5 sec).
Update interval	Interval to update the display contents (default is 60 sec).

IMPORTANT

- ▶ The appropriate values differ depending on the load status. Try to set values a few times to determine the most suitable values.
- ▶ When the timeout value is set to too large, the response will be delayed in real uncontrollable situations. Do not set too large value (more than 12 sec).

● Double start up of GAM client

When you try to open the GAM client from the ServerView (click [Setting] on the external storage device window) during the GAM client of the SCSI RAID Ctrl 2-Channel 128MB w/ BBU (PG-142E) is opened, the following message is displayed. Close this message window since there is no problem for the operation.

Can't write Profile for error #123

- Meaning: The syntax of file name, directory name, or volume label is incorrect.

- **In spite of the status icon of the power/environment group being normal, individual voltage sensor or temperature sensor status sometimes shows abnormality (voltage: below the lower limit / exceed the upper limit. Temperature: yellow/red)**

Even if the voltage/temperature sensor value returned from abnormal value to normal value (within threshold), the sensor status continues to show the abnormal status as-is until the value returns within the fixed value. This is provided to prevent the voltage/temperature abnormal event or normal event frequently occurring when the voltage/temperature value transition occurs in the vicinity of threshold (generally this fixed value is called as hysteresis).

On the other hand, this phenomenon occurs since the icon in the voltage/temperature group displays the normal icon regardless of the hysteresis if the voltage/temperature sensor value is within the threshold. Even if this phenomenon occurs, the voltage/temperature value is normal and there is no specific problem.

■ Notes for Management Console

- **Keyboard operation**

The shortcut key or the Tab key may not work properly. Use the mouse for operation.

- **Exit operation of ServerView Management Console**

When you exit the Management Console, exit all opened ServerView windows.

- **Multi-bit error in memory module**

When the multi-bit error (uncorrectable) occurs in the memory module, the error may not be reported since the OS will not be able to operate depending on the location or the timing of the error.

- **Action setting for hard disk cabinet**

Action setting at fan and temperature failure against the hard disk cabinet is disabled.

- **Restriction for table name of report or threshold**

Text which contains a space character can not be used in the table name of the report or the threshold. The table can be created but cannot be deleted or started since it cannot be selected.

- **[Memory Module] window**

The bank number may not be displayed properly.

- **[Action] window**

When you select [Restart] or [Shutdown & off] in restart option and specify "0" minute (immediately shut down), the execution of Abort Shutdown immediately after you specify the time will be disabled.

- **WOL (Wakeup On LAN) function**

When you turn on the server unit through the LAN from the client by the WOL (Wakeup On LAN) function, [N/A] may be displayed for the [Power-on Factor] on the [Action] window.

● [Operating System] window

When OS is Windows, the [Current Session] and the [Peak Session] on the [Operating System] window is unsupported.

● Trap settings

Do not enable the following traps on the [Server Properties] window. When it is enabled, the alarm may continue to occur (refer to "● Storing event log" (→pg.366)).

- Error entry in eventlog
- Warning entry in eventlog
- Information entry in eventlog
- Failure entry in eventlog
- Success entry in eventlog

● Report Manager operation

- Do not enter the data of more than 256 characters into the report note. When more than 256 characters are entered, the data of the 256th character and all following characters are ignored.
- In the [Text Display of Report], the screen looks odd when you perform printing, however, it does not affect the system operation.

● Display operations of the report graph

- Set the display operations of the report graph separately. The contents to be displayed are not guaranteed when multiple report graphs are set up at the same time.
- When you display a report graph of the report whose status is running in the report list, the report graph may not be displayed properly. Reselect the report graph in the report list and display it again.

● Threshold monitoring

When the threshold monitoring is performed on the server, the processes shown below is performed.

- ServerView Management Console saves the threshold table of the server.
- The server (agent) obtains the setting request and monitors the variables of the table.

This information is retained in the Management Console and the server, the inconsistency may occur in the following situations.

When the Management Console server has been deleted without stopping the threshold and then a new server is created:

In this case, the Management Console does not show that the server is having the threshold currently and the server continues to monitor the threshold. Therefore, stop the threshold on the Management Console side by using the threshold manager or reinstall the agent.

When the agent does not monitor the values since shut down or reinstallation might have occurred:

In this case, the Management Console shows that the server is having the threshold currently and the server does not have the threshold. Therefore, stop the threshold for the server on the Management Console side by using the threshold manager and reinstall as necessary.

For details about threshold, refer to the following information.

[System drive]: \Program Files\Fujitsu\F5fbfe01\Thresh.hlp

● Operation in [ASR Properties] window

- When you select any [FAN] and specify [Shut down], perform the setting for all enabled fans.
- Do not perform the operation when the archive data is being displayed.

● Status icon display in ServerView

When the following conditions are met, the status icons become failure status.

- In the monitored servers
- When starting OS
- The period until all ServerView monitoring programs start

When the monitoring server is operating properly and all ServerView monitoring programs start, the icons are displayed properly.

● [External Storage Devices] window

- [Connection Slot Adapter] may not be displayed properly. Wait awhile, and try to display the window again.
- [Number of Connected Devices] may not be displayed properly. On the [Display Devices] window, verify the [Number of Connected Devices].
- When you click the [Settings], the folder into which associated application is installed may be displayed.

A.3 Troubleshooting of AlarmService

■ Question and answer about AlarmService

● Is the Virtual Machine other than Microsoft VM able to co-exist with Microsoft VM?

ServerView operates properly when Microsoft Virtual Machine (version 5.0.3309 or higher) co-exists with other Virtual Machine (for example, Sun Java VM) on the same machine.

● When I want to use proxy and if I register [localhost] to the exception, does the AlarmService properly operate?

Even if [localhost] is specified, the machine can work properly depending on the system. However, enter machine's own IP address.

● What does the error code of the mail transmission test mean?

When the mail transmission test was performed in the AlarmService and error recover occurred, refer to the following:

When the recover error code is a code other than one shown below, contact us.

table: Errors in the transmission test

Error code	Contents
1:	SMTP server error.
2:	Mail server error, wrong from or to address ?
4001:	Malloc failed (possibly out of memory).
4002:	Error sending data.
4003	Error initializing gensock.dll.
4004:	Version not supported.
4005:	The winsock version specified by gensock is not supported by this winsock.dll.
4006:	Network not ready.
4007:	Can't resolve (mailserver) hostname.
4008:	Can't create a socket (too many simultaneous links?).
4009:	Error reading socket.
4010:	Not a socket.

table: Errors in the transmission test

Error code	Contents
4011:	Busy.
4012:	Error reading socket.
4013:	Wait a bit (possible timeout).
4014:	Can't resolve service.
4015:	Can't connect to mailserver (timed out if winsock.dll error 10060).
4016:	Connection to mailserver was dropped.
4017:	Mail server refused connection.

● **Can I save the alarm setting before the Management Console is uninstalled?**

Backup and restoration of the alarm setting are not supported. Write down your alarm setting before the uninstallation. Configure the alarm setting after the re-installation.

■ Troubleshooting of AlarmService

● AlarmService does not start

In the cases shown below, the AlarmService cannot start.

When the computer name or the IP address has been changed:

If the computer name or IP address of the system is changed after AlarmService has been installed, AlarmService will not run correctly.

From the [Start] button, execute [Change Computer Details] (refer to "2.4.8 Changing Computer Information after Installation" (→pg.73)).

When the proxy server has been set:

If a proxy server is set to be used in the Web browser, the AlarmService window may not appear. In the management server or the management terminal, register your IP address in [Exceptions] in the Web browser settings so that a proxy server is not used for connecting to your server.

When AlarmService has been installed without connecting the LAN (for only Windows 2003):

Perform the following steps:

- 1 Connect the server's LAN.
- 2 Set server's IP address.
- 3 Click [Start] → [Programs] → [Fujitsu ServerView] → [ChangeComputerDetails] to set the new computer information.
- 4 Restart the server.

● The test trap becomes time out

You can execute the test trap to the server on which ServerView SNMP Agent has been installed properly. The test trap will be time out in the cases shown below.

When the time-out time is short:

The default time-out time may be short depending on the network status. Extend the time-out time after checking the network environment.

When the SNMP service has not been set properly:

Check the following:

- Is the management terminal IP address registered to the trap destination of the SNMP service in the monitored server?
- In the SNMP service security of the monitored server/management terminal, is the right for the community set to [READ_WRITE] or [READ_CREATE] ?

When the Agent (SNMP Agent) has not been set properly:

Uninstall the ServerView and install it again.

● The alarm cannot be deleted

When deleting multiple alarms in the alarm manager or the alarm monitor, some alarms may remain. In this case, perform the deletion again.

You can set in the [Shared Settings] window so that the alarm that elapsed the specified days is deleted, however, this deletion is executed when new alarm is received after the specified days have elapsed.

● Script error occurred

When using the alarm manager or the alarm monitor, script error may occur. In this case, exit the AlarmService and restart the Alarm Manager or Alarm Monitor.

When you click [Close] to close the Alarm Manager and did not exit, the script error may occur at the next start up. To close the Alarm Manager, you must click [Close]. In this case, restart also the Alarm Manager.

● The Alarm Manager/Alarm Monitor is not updated automatically

Confirm that the automatic update is checked. Even if it is checked, the window of the Alarm Manager/Alarm Monitor may not be updated. In this case, restart the Alarm Manager/Alarm Monitor or read again using update function of the browser.

■ Notes for AlarmService**● Window operation**

In each window, do not operate to maximize or restore the standard display. The screen may look odd. When the window looks odd, close the window and restart it again.

● Mail transmission

The mail transfer with MAPI is not supported.

When the test transmission is done, the mail is transmitted to the address specified in the [To:].

It is not transmitted to the address specified in the [Copy].

● Starting multiple [Alarm Settings] windows

Sometimes multiple [Alarm Settings] windows can be started, however, please start only one window.

● Exit operation of [Alarm Filter Settings] window

When the [Alarm Filter Settings] window is being opened, exit this window before you exit the Alarm Manager.

● Notes when exiting the window you are processing

Do not exit the window you are currently processing until the process is done completely (for example, when deleting many alarms on the Alarm Monitor). When the window is exited before the process is done completely, the process is canceled and does not work properly.

● RomPilot trap

In the alarm regarding the RomPilot trap, the MAC address may not be displayed properly.

● Storing event log

When the all conditions shown below are met, the alarm may continue to occur.

- When ServerView Console has been installed on the system:
- When the server itself is included into the monitor target:
- When the following traps are enabled on the [Server Properties] window:
 - Error entry in eventlog
 - Warning entry in eventlog
 - Information entry in eventlog
 - Failure entry in eventlog
 - Success entry in eventlog
- When one of the following setting is enabled in the alarm setting:
 - [Store Event Log] is enabled on the default action of the [Shared Settings] window.
 - In the alarm group setting, the [Log] is enabled as an action against the alarm from the server itself.

As a prevention measure, you can disable the above trap in the [Server Properties] window or disable the above setting in the alarm setting.

● Alarm when disconnecting/turning on the AC power

When the system is started up by disconnecting/turning on AC power, a message may be displayed or an error is stored into the event log. This does not affect the system operation.

The message displayed is as follows:

```
Alarm received from server ServerName
An error was recorded on server ServerName.
See server management event / error log (Recovery)
for detailed information
```

The event log stored is as follows (source: Server Control):

```
An error was recorded on server N400. See server
management event / error log (Recovery) for
detailed
information.
```

● Error during reboot/shut down

An error may occur in `SVxxx.exe` (such as `SVFilterServer.exe`, `SVConvertServerList.exe`) during reboot or shut down.

However, this does not affect the system operation after reboot.

● Broadcast transmission

The broadcast transmission may not be executed because of your Windows Messenger's problem. To test to verify whether this service operates properly, open the command prompt and execute the following command.

- When testing the broadcast transmission to all users in the domain:

```
net send * <message>
or
net send /domain:<yourdomain> <message>
```

- When testing the broadcast transmission to all users in the session:

```
net send /users <message>
```

- When testing the broadcast transmission to all specific users:

```
net send <user> <message>
```

When one of the above tests fails, check the network.

IMPORTANT

- ▶ Even if the test result shows successful completion message, the "net send" to the domain administrator always seems to be unoperatable.

● Station's transmission mode

You can specify two types of station's transmission mode: [Normal], [Direct].

When [Direct] is specified, the transmitted alarm type is displayed on the destination alarm monitor.

And, [ServerView alarm passed through] is displayed for the alarm type in Alarm Manager.

A.4 ServerView S2 Troubleshooting

● ServerView S2 does not start

For Windows 2003, when ServerView S2 has been installed without connecting the LAN, perform the following procedures.

- 1 Connect a LAN to the server.
- 2 Set an IP address for the server.
- 3 Click [Start] → [Programs] → [Fujitsu ServerView] → [ChangeComputerDetails] to set the new computer information.
- 4 Reboot the server.

● When using ServerView S2 in Windows 2000, error message is displayed or a server cannot be added to the server list

When ServerView S2 is executed in Windows 2000, the following problems may occur.

- Message such as "Could not find <Installationpath_Html>\uid\1\GettingStatus" or "Error on SnmpMgrTrapListen 1062" may be displayed.
- A new server cannot be added to the server list.
- The server list is not displayed (seems to be hang up).

These problems occur for the following reasons.

When installing ServerView S2 (executing Setup.exe), user normally logs in as a user having administrator privilege.

When executing ServerView S2, the user normally logs in as "IUSR_<computername>". Therefore, this user will not have permission to change the ServerView S2's database (for example, the server list) or ServerView S2 specific setting files.

To resolve this problem, perform the following procedure:

- 1 Right-click the [My Computer] on the desktop and click [Manage] from the popup menu.
The [Computer Management] window appears.
- 2 Perform the following procedure to create a new user.
 1. Click [Local Users and Groups] from [System Tool] and right-click [Users] and then click [New User] from the popup menu.
The [New User] window appears.
 2. Enter the required information and click [Create]. The new user must be placed into the same group as the user (i.e. administrator) who installed ServerView S2.

- 3 Set the new user in the ServerView script directory.
From [Services and Applications] in the [Computer Management] window, click [Microsoft Internet Information Services] → [Default Web Site] → [scripts] and right-click [ServerView] and click [Properties] from the popup menu.
The [ServerView Properties] window appears.
- 4 Click the [Directory Security] tab.
- 5 Click [Edit] under [Anonymous access and authentication control].
The [Authentication Method] window is displayed.
- 6 Click [Edit] under [Anonymous Access].
The [Anonymous Users] window appears.
- 7 Click [Browse] and select the user created in the step 2 or [Administrator].
- 8 Check [Allow IIS to control password].
- 9 On all the windows displayed, click [OK] or [Yes].

● **If the problem persists:**

If the problem persists, perform the following steps or change.

When the default is specified for the installation location and ServerView S2 is installed, the path is as follows:

<Installationpath_Html> = <Drive name>:\InetPub\wwwroot\ServerView

- 1 Click [Start] → [Programs] → [Accessories] → [Explore].
- 2 Open [<Installationpath_Html>].
- 3 Right-click [<Installationpath_Html>] and click [Properties] from the popup menu.
- 4 Click the [Security] tab.
- 5 Set [Everyone] to the [Name] and check [Change] and [Write] in the [Grant Access].
- 6 Click [Apply] or [OK].

● Setting not to start "ServerStatus" process

ServerView S2's "ServerStatus" process may start a few times since ServerView S2 does not have any permission to modify specific files. To prevent starting, perform the following procedures:

- 1 Reboot the server.
- 2 Perform the following procedures from the Task Manager.
 1. Press [Ctrl] + [Alt] + [Delete] key.
The [Windows Security] window appears.
 2. Click [Task Manager].
The [Task Manager] message appears.
 3. Select the [Process] tab.
- 3 Perform the following procedure to exit all "ServerStatus.ex" processes.
 1. Right-click [ServerStatus.ex] and click [End Process] from the popup menu.
The [Warning] window appears.
 2. Click [Yes].
The process ends.
- 4 Repeat above steps to exit all "ServerStatus.ex" processes.
- 5 If you have no permission to exit all "ServerStatus.ex" processes, reboot the server.

A.5 Other

■ General question & answer

● What is "Fujitsu Server Control"?

It is a software that is to be installed at the same time when ServerView Agent is installed. "Fujitsu Server Control" is required to operate ServerView properly.

● What is "Server Control Service"?

It is a service that is to be installed when "Fujitsu Server Control" is installed.

● The "svtmpdir" folder is created within C:\Winnt\Temp when ServerView is installed. Can I delete this folder after the installation?

This folder is used to store the debug information.

Deleting this folder causes no problem, however, when the system (Fujitsu ServerView Service) is restarted, this folder will be recreated.

● How many servers can be monitored from ServerView's Management Console?

There is no limitation to the number of monitorable servers from ServerView's Management Console. However, the information is collected using SNMP service when monitoring the servers from ServerView's Management Console. Therefore, as the number of the monitored servers increases, the network load will be higher.

● What is the protocols and port number used in ServerView?

In ServerView related programs, the following protocols and ports are used:

ServerView

- SNMP (TCP/UDP: 161,162)
- PINGFICMP (there is no port number concept in this protocol)

AlarmService, ServerView S2 (Web service provider side)

- SNMP (TCP/UDP: 161,162)
- HTTP (TCP for IIS: 80, TCP for ServerView Web-Server: 3169)

The followings are used only for SSL connection:

- HTTPS (TCP for IIS: 443, TCP for ServerView Web-Server: 3170))

AlarmService, ServerView S2 (Management Console side)

- SNMP (TCP/UDP: 161,162)
- HTTP (TCP for IIS: 80, TCP for ServerView Web-Server: 3169)

The followings are used only for SSL connection:

- HTTPS (TCP for IIS: 443, TCP for ServerView Web-Server: 3170)

● Is Server Monitor Module (SMM) is supported?

It is not supported.

The SMM cannot be installed on the server to which ServerView is installed.

In ServerView, the Remote Service Board (RSB) can link and enable functions and realize the functions equal to those of SMM.

● When ServerView Management Console is installed, what function does the task that is registered with the name At* (ID number) provide?

When ServerView Web-Server is selected for WebServer and ServerView Management Console is installed, a task is registered into the Task Scheduler with the name At* (ID number).

This task prevents the WebServer's log file increasing in size.

To disable the task's scheduler, check the following file size regularly.

```
[System drive]:\Program Files\Fujitsu\F5FBFE01\ServerView Services
\WebServer\logs\access.log
```

■ Browser troubleshooting

Not all browsers operate properly at all times. There are many possible causes and the effects vary.

● **ServerView only detects computers whose power is currently turned on**

Some network information may not be detected while scanning Microsoft Windows network.

This phenomenon occurs due to the method (the usage of broadcast method) Windows uses to obtain the network information.

● **Cannot access to the domain because of the security policy setting Cannot access to the domain because of inaccessibility to the domain server Cannot access to other network system (such as NetWare)**

After the time out limit has been exceeded, the browse operation would be canceled. However this might take a few minutes.

● **The browser has failed completely and the browser window is blocked for a few minutes**

The browser window may be blocked or the entire ServerView application may be blocked during the browser process. This phenomenon may occur when Windows NT domain has a problem or the network performance is significantly deteriorated.

In this case, do not use the browser function.

● **Takes time to resolve the computer name to its IP address**

Windows Internet Name Services (WINS) or Domain Name System (DNS) may not be set up properly in the log in computer. The address of primary or secondary WINS server or the address of DNS server may not be valid. When the WINS protocol is not started properly, name query broadcast at very low speed is used for IP address resolution. WINS or DNS can be set in the [TCP/IP Properties] of the [Network Settings].

● **No IP address was found**

There may be some causes such as follows:

- TCP/IP has not been installed on the remote computer.
- WINS is disabled in the log in computer.
- There is no WINS server, DNS information or the LMHOSTS file in the LAN.
- WINS database has not been updated.

● **Using WINS, DNS, or either of LMHOSTS file could not resolve the address**

The name query broadcast is currently used. This broadcast may fail because of the problem of network topology or performance, for example when the domain router does not transmit the name query broadcast.

■ General notes

● Notes for uninstallation

Application error may occur during uninstallation, however, the system operates with no problem.

● Log file

When ServerView is installed, the log information storage folders ("C:\svtmpdir", "C:\winnt\Temp\svtmpdir") will be created.

The log information is created and updated even while the system operates properly. The log information may be deleted when the amount of free disk space has been reduced.

Delete the log information after ServerView is closed and Fujitsu ServerView Service is stopped from the service window. Application error may occur when Fujitsu ServerView Service is stopped, however, the system operates with no problem.

● ServerView Web-Server and SSL

When ServerView WebServer is selected as a Web server and [Enable SSL and authentication] is enabled during the installation, ModSSL and OpenSSL are installed in conjunction with ServerView Web Server.

In this case, using "https:" as URL instead of "http:", and "3170" as a port number instead of "3169" enables the SSL connection. To use SSL, it is required to obtain the security certificate. The security certificate installed by default must be used only for test purpose.

For details, refer to OpenSSL site (<http://www.openssl.org>).

In the URL that uses SSL, the authentication is requested during the connection.

To add a user, perform the following procedure:

- 1 Execute the following two commands continuously from the command prompt.

```
cd "[system drive]:\Program Files\Fujitsu\F5fbfe01\ServerView
Services\WebServer\bin"
htpasswd passwd <user name>
```

- 2 Enter a new password.

```
Automatically using MD5 format on Windows.
New password:
```

3 Enter the new password again to verify.

```
Re-type new password:
```

When the passwords match, the following message will be displayed and a user will be added.

```
Adding password for user <user name>
```

If the following message is displayed, the password is invalid. Execute the command again.

```
htpasswd: password verification error
```

To delete a user, open the following file on the text editor and delete the line that contains the user name to be deleted.

```
[system drive]:\Program Files\Fujitsu\F5fbfe01\ServerView
Services\WebServer\bin\passwd
```

By default, "svuser" has been set to the user and the password "fsc" has been set to the password. Delete this user and add an appropriate user for your security.

● BootRetryCounter

When the shut down process occurred because of failure, the value specified in [Maximum number of reboot tries] remains at reduced value and it does not recover automatically even if it starts up normally. To recover this value, perform the following procedure:

- 1 In ServerView, select the corresponding server.
- 2 Right-click, and click [ASR Properties].
The [ASR Properties] window appears.
- 3 Click the [Restart Settings] tab.
- 4 Click [Default] on the right side of [Maximum number of reboot tries].
If the log in to the corresponding server has not been performed, the log in is requested.

● During the Windows startup, the error "SWITCH: TIMEOUT" is logged in the Event Viewer.

During the Windows startup, the following error is logged in the application log of the Event Viewer.

```
Type: Error
Source: Server Control
Category: None
Event ID: 0
Description: SWITCH: TIMEOUT - extension module
EM_xxx did not start within yyy seconds.
```

If this occurs, perform the following procedure to restart ServerView Agent or restart Windows.

- 1 Click [Start] → [Programs] → [Fujitsu ServerView Agents] → [Diagnostic Tools] → [Restart ServerView Base Services].
- 2 Enable the [Search for management hardware] and click [Restart].



- ▶ Generally, do not start [Restart ServerView Base Services].

B Uninstallation

This appendix describes how to uninstall the ServerView.

B.1 Uninstalling ServerView



- ▶ Uninstall ServerView after all ServerView programs are closed. After ServerView is uninstalled, the directories, subdirectories and files may not be deleted. In addition, ServerView may not be deleted from the program group after the uninstallation.
- ▶ When the process is suspended on the way or the steps other than those shown below are performed during uninstallation, ServerView may not be uninstalled properly. The uninstallation should be performed completely.
- ▶ The items saved on the server's BIOS are not restored even when ServerView is uninstalled. Restore the setting to the original state and then uninstall ServerView.
- ▶ The characters get garbled on the uninstallation window, however, it does not affect the operation.
- ▶ After uninstallation, ServerView's short cut may remain. Delete the shortcut manually (right-click the shortcut icon and select [Delete]).
- ▶ After the ServerView Console has been uninstalled, the task with the name "At**(**: task ID)" may remain. In this case, open the [Task Properties] and delete the task if the [Run:] is the same as the file shown below.
 - The file executed in ServerView's Task Scheduler:
system drive:\Program Files\Fujitsu\F5FBFE01\ServerView\Services\WebServer\ClearMyLogs.exe

■ Uninstalling ServerView Console

When you raise the level of the server and re-build the server's monitoring system, perform the following steps and uninstall the following items of ServerView Agents.

When switching the management terminal to other PC and use the PC or raising the level of ServerView, follow the steps below to uninstall the current Management Console from the management terminal.

The Management Console and ServerView S2 will be deleted at the same time. It is not possible to select the target to delete.

- 1 Log in as an administrator or a user name with the equivalent privilege.
- 2 Exit all running applications.
- 3 Start up [Control Panel] and double-click [Add/Remove Programs].
- 4 Select [Fujitsu ServerView] and click [Delete].
ServerView Console will be uninstalled.

■ Uninstalling ServerView Agent



- ▶ Make sure to do the followings before uninstalling ServerView Agent.
 - Disable Software Watchdog, BOOT Watchdog and Power ON/OFF settings.
Refer to "■ [Power ON OFF] Tab (ServerView S2) / [Power ON/OFF] Tab (Management Console)" (→pg.129) and "■ [Watchdog] Tab (ServerView S2) / [Watchdog Settings] Tab (Management Console)" (→pg.129).
 - Stop monitoring by Treshold Manager of Management Console.
Refer to "■ Stopping Threshold Monitoring" (→pg.214).
 - When applying threshold monitoring and report creation by Performance Manager, cancel applying these performance to the server.
Refer to "3.6.6 Applying the Settings to Servers" (→pg.180).

To uninstall ServerView Agent, perform the following procedure:

- 1 Log in as an administrator or a user name with the equivalent privilege.
- 2 Exit all running applications.
- 3 Start up [Control Panel] and double-click [Add/Remove Programs].
- 4 Select [ServerView Agents] and click [Delete].
ServerView Agent will be uninstalled.

■ [Linux]Uninstalling ServerView Linux Agent



- ▶ Make sure to do the followings before uninstalling ServerView Linux Agent.
 - Disable Software Watchdog, BOOT Watchdog and Power ON/OFF settings.
Refer to "■ [Power ON OFF] Tab (ServerView S2) / [Power ON/OFF] Tab (Management Console)" (→pg.129) and "■ [Watchdog] Tab (ServerView S2) / [Watchdog Settings] Tab (Management Console)" (→pg.129).
 - Stop monitoring by Treshold Manager of Management Console.
Refer to "■ Stopping Threshold Monitoring" (→pg.214).

To uninstall ServerView Linux, perform the following procedure:

- 1 Log in as a super user.
- 2 Execute the following command.

```
# rpm -e srvmagt-agents
# rpm -e srvmagt-eeed
# rpm -e srvmagt-mods_src
```

ServerView Linux will be uninstalled.

If necessary, change the value to "/etc/snmpd/snmpd.conf" to an initial value.

■ [Linux]Uninstalling ServerView S2/AlarmService

To unistall ServerView S2/AlarmService, perform the following procedure:

- 1 Log in as a super user.
- 2 Execute the following command.

```
# rpm -e ServerView S2  
# rpm -e AlarmService
```

ServerView S2/AlarmService will be uninstalled.

C Icon List

This section lists the icons displayed on each window and describes their meanings. Those icons are displayed so that the status of one or more objects or the status change can be seen at a glance.

C.1 Server List

The list of icons shown on the [Server List] window and their meanings are as follows:

table: Icons shown on the [Server List] window





















Icon	Meaning
	OK. All components are OK.
	Error. Any errors occurring in one or more components.
	The status deteriorates. The status for one or more components deteriorates.
	Uncontrollable. Status of components is not determined.
	Investigation status. Undetermined status during investigation status.
	Unknown. Server is inaccessible.
	DeskInfo. The DiskInfo tool can start.
	The advanced server manager can be activated.
	Intel LANDesk® Server Manager (LDSM) can be activated.
	ServerView receives an alarm from the server.
	The threshold measurement starts on this server.
	The archive data is available on this server.
	The status of clusters is normal.
	Investigation status. Undetermined status during investigation status.
	Error. Any errors occurring in one or more clusters.
	OK. All components in the cluster are OK.
	Uncontrollable. Status of cluster is not determined.













table: Icons shown on the [Server List] window

Icon	Meaning
	Status of cluster is not determined.
	The status deteriorates. The status for one or more components in the cluster deteriorates.
	RSB responds through the secondary channel because the server does not respond.

C.2 ServerView menu

The list of icons shown on the [Server List] menu and their meanings are as follows:

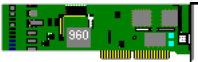

table: List of icons shown on the [Server List] menu

Icon	Meaning
	Maintenance Buttery support
	ASR: Automatic System Reconfiguration/Restart Automatic server search
	Restart Restarting the server
	Terminating server shutdown/power-off
	Shut down and OFF Server shut down and power off
	Memory module
	Temperature (red: danger, green: operating, yellow: stand-by condition, blue: sensor failure, grey: unknown)
	Fan (red: failure, green: operating, yellow: stand-by condition, grey: unknown)
	Server's door is closed
	Server's door is opened
	Server's case is closed
	Server's case is opened

C.3 Mylex's [Device View] window

The list of icons shown on the [Device View] window and their meanings are as follows:





table: Icons shown on the [Device View] window

Icon	Meaning
	Mylex controller
Capacity in MB or GB	Mylex Red characters: suspending Yellow characters: standby mode Green characters: OK Operating Purplish red characters: S.M.A.R.T. failure Blue characters: Unknown status or re-building status
	Host

C.4 [DPT Disk Array Agent] window

The list of icons shown on the [DPT Disk Array Devices] window and their meanings are as follows:

table: Icons shown on the [DPT Disk Array Devices] window

Icon	Meaning
	Status: best suited (green)
	Status: investigation, warning, status deteriorated, re-building, investigation completed (yellow)
	Status: error, during device formatting, during device set up (red)
	Status: disabled, missing, not set up, cleared (blue)

C.5 Network Interfaces window

The list of icons shown on the [Network Interfaces] window and their meanings are as follows:

table: Icons shown on the [Network Interfaces] window

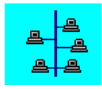
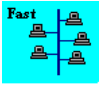


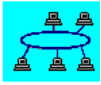



Icon	Meaning
	Ethernet network card
	Fast Ethernet network card
	Ethernet network card (multiple network connections multipoint)
	Fast Ethernet network card (multiple network connections multipoint)


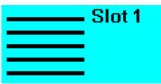



table: Icons shown on the [Network Interfaces] window

Icon	Meaning
	Token Ring network card
	FDDI network card
	Input statistical information
	Output statistical information

C.6 Bus and Adaptor window

The icon list shown on the [Bus and Adaptor] window and the meanings are as follows:

table: Icons shown on the [Bus and Adaptor] window

Icon	Meaning
	Slot location on the systemboard: Slot 1 is bottom
	Slot location on the systemboard: Slot 1 is top
	Branch of selection level opens
	Branch of selection level closes
	Bottom selection level, no more selectable

C.7 Alarm Manager window and Alarm Monitor window

The list of icons shown on the [Alarm Manager] window and [Alarm Monitor] window and their meanings are as follows:

table: Icons shown on the [Alarm Manager] window and [Alarm Monitor] window




















Icon	Meaning
	Red alarm: danger
	Pink alarm: severe
	Yellow alarm: slight
	Blue alarm: information
	White alarm: unknown






table: Icons shown on the [Alarm Manager] window and [Alarm Monitor] window

Icon	Meaning
	Alarm has been accepted by user's entry.
	Other program that can be executed has been started by this alarm.
	Broadcast message was transmitted for this alarm.
	Mail was sent for this alarm.
	Pager call was started by this alarm (unsupported).
	This alarm will be transmitted to manager or management station.
	This alarm will be transmitted to local NT event log.
	This alarm will be stored to the database.
	Green: Pager is confirmed (unsupported).
	Yellow: Pager is completed (unsupported).
	Red: Pager exists (still operating) (unsupported).
	Green: Transmission is confirmed.
	Yellow: Transmission is completed.
	Red: Transmission exists (still operating).

C.8 Cluster status (unsupported)

The icon list showing cluster objects and their meanings are as follows:







table: Icons showing cluster objects

Icon	Meaning
	Cluster status icons
	Cluster server node status icons
	Cluster group status icons
	Cluster resource status icons
	Cluster network status icons

■ Server node status

The cluster server node status icons and their meanings are as follows:







[table: Cluster server node status icons](#)

Icon	Meaning
	Unknown: Cannot determine node status or cannot match any status shown on this table.
	Up: Server node is operating.
	Down: Server node is in failure state.
	Suspending: Server node does not provide group service currently.
	Combination: The server node starts to provide the cluster service currently, however, the service is not available yet.
	Unavailable: Server node is unavailable.

■ Group status

The cluster group status icons and their meanings are as follows:

[table: Cluster group status icons](#)

Icon	Meaning
	Unknown: Cannot determine group status or cannot match any status shown on this table.
	Online: Group is in online status.
	Offline: Group is in offline status.
	Partially online: Group is in online partially.
	Failure: Group is in failure state.
	Unavailable: Group is unavailable.

■ Resource status

The cluster resource status icons and their meanings are as follows:

[table: Cluster resource status icons](#)











Icon	Meaning
	Unknown: Cannot determine resource status or cannot match any status shown on this table.
	Online: Resource is available.






table: Cluster resource status icons

Icon	Meaning
	Offline: Resource is unavailable currently.
	Failure: Resource is in failure state.
	Online waiting: Resource is in launching process.
	Online waiting: Resource is in shutdown process.
	Uncertain online status: Resource status cannot be determined and resource is unavailable currently.
	Unavailable: Resource is unavailable.
	Inherited: Resource is inherited.
	Initialization stage: Resource is being initialized currently.

■ Network status

The cluster network status icons and their meanings are as follows:

table: Cluster network status icons

Icon	Meaning
	Unknown: Cannot determine network status or cannot match any status shown on this table.
	Up: Network interface is operating fully.
	Shutdown Network has been shut down.
	Connection interrupted: Communication between one or more nodes in the cluster is interrupted.
	Unavailable: Network is unavailable.

■ Network interface status

The cluster network interface status icons and their meanings are as follows:

table: Cluster network interface status icons






Icon	Meaning
	Unknown: Cannot determine network interface status or cannot match any status shown on this table.
	Up: Network interface is operating.







table: Cluster network interface status icons

Icon	Meaning
	Failure: Network interface is not operating.
	Inaccessible: Other nodes cannot access to the network interface.
	Unavailable: Network interface is unavailable.

C.9 Blade server status

The blade server status icons and their meanings are as follows:




table: Blade server status icons

Icon	Meaning
	The status of blade servers is normal (the status of all blades is OK).
	Status of blade servers is under investigation.
	The status of blade servers deteriorates (the status of at least one blade deteriorates).
	The status of blade servers is error (the status of at least one blade is error).
	Uncontrollable. (The blade server does not respond).
	Unknown. Blade server is inaccessible.

■ Blade server status LED

The blade server status LED icons and their meanings are as follows:





table: Blade server's status LED icons

Icon	Meaning
	Lights up
	Lights off
	Flashing (shows system failure)

■ Blade type

The types of blade in blade server are as follows:

table: Blade in blade server

Icon	Meaning
	Management blade (master)
	Management blade (slave)
	Switch blade
	Server blade

C.10 Other icons

The list of icons not associated with specific windows and their meanings are as follows:

table: Icons not associated with specific windows



























Icon	Meaning
	CD-ROM (red: error, green: online, yellow: stand-by, blue: unknown)
	Communication device (red: error, green: online, yellow: stand-by, blue: unknown)
	CPU (red: error, green: online, yellow: stand-by, blue: unknown)
	Jukebox, automatic CD-ROM changer (red: error, green: online, yellow: stand-by, blue: unknown)
	MOD (red: error, green: online, yellow: stand-by, blue: unknown)
	Printer (red: error, green: online, yellow: stand-by, blue: unknown)
	Scanner (red: error, green: online, yellow: stand-by, blue: unknown)
	Tape drive device (red: error, green: online, yellow: stand-by, blue: unknown)
	WORM (Write Once Read Many) device (red: error, green: online, yellow: stand-by, blue: unknown)
	Hard disk Hard disk (red: failure, green: OK)
	Unknown device (red: error, green: online, yellow: stand-by, blue: unknown)
	Graphical view
	Graph view
	Representation with text or table

table: Icons not associated with specific windows

Icon	Meaning
	Pager monitoring (red: error, green: online, yellow: stand-by, blue: unknown)
	OK
	Unmanageable
	Investigation mode
	Error
	Initial setting, Environment [<Server>], or Power [<Server>]
	All windows related to network: Network interface [<Server>], Token Ring statistics [<Server>], Ethernet MAC statistics [<Server>], FDDI MAC statistics [<Server>]
	All windows related to external storage device: External storage devices [<Server>], Display Devices [<Server>], External storage devices: Partition view [<Server>], External storage devices: Logical View [<Server>] Mylex Disk Array window: Device view [<Server>], Adapter view [<Server>], Physical device view [<Server>]
	System information (particularly OS)
	Baseboard [<Server>]
	Server Manager on Windows Desktop, Server List, ServerView [<Server>], Alarm Manager, Threshold Manager, Report Manager, Threshold List, Report List
	Server Manager Help System on Windows Desktop

D Trap List

Trap is a SNMP Protocol Data Unit alarm transmitted from SNMP agent. This is used to notify an unexpected event, such as an error message or the status change that occurs because the selected threshold level has been exceeded, to the management station.

You can launch the [Shared Settings] window in [Alarm Settings] and select different actions against each server and severity (danger, severe, slight, and information).

- Log
An event is written into the alarm log list in the database table.
- Pop-up
Start the alarm monitor.

The danger alarm event is always written into the alarm log list in the log file.

All traps received are displayed on the Alarm Monitor, however, only the events written into the log file would be displayed on the Alarm Manager.

For the list of the messages displayed when ServerView receives OS's SNMP trap and the events stored to the OS event log, refer to "ServerView Trap List".

The traps are classified for each category and are classified in the order of "Specific Code" within the category.

The event log of the traps AlarmService received and stored is recorded with the following source name.

- Source name: Fujitsu ServerView Service

The following message is written at the beginning of the stored event log:

- ServerView received the following alarm from server <server name>:

■ Trap list

For more details on the trap list, refer to "ServerView Trap List".

E Threshold List

This section describes ServerView variables used for threshold monitoring.

E.1 Monitored values

The following thresholds are monitored:

table: Monitored thresholds

Value	Meaning
DAC960-AdapterInfo-Values	DAC960 adapter setting threshold
DAC960-PhysicalDevice-Values	Device error threshold for the device connected to DAC960 adapter.
Environment-Values	Fan speed threshold
Ethernet-MAC-Statistics	Ethernet MAC error threshold
FDDI-MAC-Statistics	FDDI-MAC error threshold
FDDI-Port-Statistics	FDDI port error threshold
Interface-Values	Interface statistics and interface error thresholds
IP-Info	IP statistics threshold
Memory-Values	Memory error threshold
NetWare-Info	NetWare connection threshold
OnOffTimes	Power on/off time threshold
PC-Inventory-CPUValues	CPU usage threshold
PC-Inventory-FileSystem	Usable block's threshold
PC-Inventory-Info	Mounted file system threshold
SystemBoard-Info	Bus loading threshold
SystemControl-Info	Cabinet number threshold
TokenRing-MAC-Statistics	Token Ring error threshold
UPS-Values	Battery running hours threshold

E.2 Meaning of each value

■ DAC960-AdapterInfo-Values

table: DAC960-AdapterInfo-Values

Value	Meaning
mylex.NumChannels	Current channel number
mylex.NumLogicalDrives	Current logical drive number
mylex.NumPhysicalDevices	Current physical device number

■ DAC960-PhysicalDevice-Values

table: DAC960-PhysicalDevice-Values

Value	Meaning
physDev960.HardErrorCount	Hardware error count (configured DAC disk only)
physDev960.MiscErrorCount	Various error counts (configured DAC disk only)
physDev960.ParityErrorCount	Parity error count (configured DAC disk only)
physDev960.SoftErrorCount	Software(normal) error count (configured DAC disk only)

■ Environment-Values

table: Environment-Values

Value	Meaning
fan.CurrentMaxSpeed	Current fan speed at Max. power (rpm/min) (-1 = unknown)
fan.CurrentSpeed	Current fan speed (rpm/min, -1 = unknown)

■ Ethernet-MAC-Statistics

table: Ethernet-MAC-Statistics

Value	Meaning
ethS.AlignmentErrors	A count of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.
ethS.CarrierSenseErrors	The number of times that the carrier detection test failed and was not executed when transmitting a frame on a particular interface had been attempted.
ethS.DeferredTransmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.
ethS.ExcessiveCollision	A count of frames for which transmission on a particular interface fails due to excessive collisions.
ethS.FCSErrors	A count of frames received on a particular interface that are not an integral number of bytes in length and do not pass the FCS check.
ethS.FrameTooLongs	A count of frames received on a particular interface that exceeds the maximum permitted framer size.
ethS.InternalMacReceiveErrors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
ethS.InternalMacTransmitErrors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
ethS.LateCollisions	The number of times that a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.
ethS.MultipleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
ethS.SingleCollisionFrames	A count of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.
ethS.SQETestErrors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.

■ FDDI-MAC-Statistics

table: FDDI-MAC-Statistics

Value	Meaning
fddiM.ErrorsCts	Error_Count (refer to ANSI MAC 2.2.1)
fddiM.ErrorsCts	Frame_Count (refer to ANSI MAC 2.2.1)
fddiM.LostCts	Lost_Count (refer to ANSI MAC 2.2.1)

■ FDDI-Port-Statistics

table: FDDI-Port-Statistics

Value	Meaning
fddiP.LCTFailCts	The number of times in which the link reliability test failed continuously during managing connection.
fddiP.LemCts	The number of errors detected by the link error monitor that is reset to zero when power is turned on.
fddiP.LemRejectCts	The number of link error monitor events for the hours in which link was rejected.

■ Interface-Values

table: Interface-Values

Value	Meaning
if.InDiscards	The number of incoming packets selected to discard in spite of there being no error in which packet cannot be used on upper layer protocol.
if.InErrors	The number of incoming packets that contains an error in which a packet cannot be used on upper layer protocol.
if.InNUcastPkts	The number of non-multicast (non-broadcast) packets transmitted to the upper layer protocol.
if.InOctets	The total number of bytes received on the interface, including framing characters.
if.InUcastPkts	The number of subnetwork-unicast packets sent to an upper layer protocol.
if.InUnknownProtos	The number of packets received via the interface that were discarded because of an unknown or unsupported protocol.
if.OutDiscards	The number of outbound packets that were chosen to be discarded--even though no errors had been detected--so that they would not be transmitted.
if.OutErrors	The number of outbound packets that could not be transmitted because of errors.
if.OutNUcastPkts	The total number of packets that upper level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
if.OutOctets	The total number of bytes transmitted out of the interface, including framing characters.
if.OutQLen	The length of the output packet queue (in packets).
if.OutUcastPkts	The total number of packets that upper level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
if.Speed	An estimate of the interface's current bandwidth in bits per second.

■ IP-Info

table: IP-Info

Value	Meaning
ip.ForwDatagrams	The number of input datagrams for which this entity had not been their final IP destination. As a result, an attempt had been made to find a route to forward them to that final destination.
ip.InReceives	The total number of input datagrams received from interfaces, including those received in error.
ip.OutRequests	The total number of IP datagrams supplied to IP by local IP user protocols (including ICMP), during requests for transmission.

■ Memory-Values

table: Memory-Values

Value	Meaning
memModule.Errors	The number of (parity) errors that occurred in this module after the last error count has been reset (-1 = unknown).

■ NetWare-Info

table: NetWare-Info

Value	Meaning
sniNW.ConnectionsInUse	The number of connections that is used currently.
sniNW.PeakConnectionsUsed	The peak numbers of connections that were used.

■ OnOffTimes

table: OnOffTimes

Value	Meaning
#power.OffDuration	The hours for which the power has been turned off during the system lifetime (represented in hours, -1 = unknown).
power.OnCounts	The number of times that the power has been turned on during the server lifetime (in hours, -1 = unknown).
power.OnDuration	The hours for which the power has been turned on during the system lifetime (represented in hours, -1 = unknown).

■ PC-Inventory-CPUValues

table: PC-Inventory-CPUValues

Value	Meaning
sni.CPUUtilization	The percentage of hours in which CPU processes data.

■ PC-Inventory-FileSystem

table: PC-Inventory-FileSystem

Value	Meaning
sni.AvailableBlocks	The number of unused blocks in the file system (unused blocks * block size = number of usable bytes in the file system).

■ PC-Inventory-Info

table: PC-Inventory-Info

Value	Meaning
sni.MountedFileSystems	The number of file systems mounted currently.

■ SystemBoard-Info

table: SystemBoard-Info

Value	Meaning
utilization.EisaLoad	Load on EISA bus (represented by percentage, -1 = unknown).
utilization.PciLoad	Load on PCI bus (represented by percentage, -1 = unknown). This object should not be used when implementing newly. This object has been changed to pciUtilizationTable.

■ SystemControl-Info

table: SystemControl-Info

Value	Meaning
NumberCabinets.Detected	The number of detected cabinets (minimum value is 1 since server itself is included).

■ TokenRing-MAC-Statistics

table: TokenRing-MAC-Statistics

Value	Meaning
tokS.AbortTransErrors	This counter is incremented when a station transmits an abort delimiter.
tokS.ACErrors	This counter is incremented when a station receives an AMP or SMP frame in which A = C = 0, and then receives another SMP frame with A = C = 0 without first receiving an AMP frame. It denotes a station that cannot set the A and C bits properly.
tokS.BurstErrors	This counter is incremented when a station detects the absence of transitions for five half-bit timers (burst-five error).
tokS.FrameCopiedErrors	This counter is incremented when a station recognizes a frame addressed to its specific address and detects that the FS field A bit is set to 1 indicating a possible intermittent disconnection or duplicated address.
tokS.InternalErrors	This counter is incremented when a station recognizes an internal error.
tokS.LineErrors	This counter is incremented when a station copies or repeats a frame or token, the E bit is zero in the frame or token, and one of the following conditions exists: <ul style="list-style-type: none"> • There is a non-data bit (J or K bit) between the start delimiter (SD) and the end delimiter (ED) of the frame or token. • There is an FCS error in the frame.
tokS.LostFrameErrors	This counter is incremented when a station is transmitting and its TRR timer expires.
tokS.ReceiveCongestions	This counter is incremented when a station recognizes a frame addressed to it, but there is no available buffer space, and it indicates station congestion.
tokS.SoftErrors	The number of soft errors the interface has detected. It directly corresponds to the number of report error MAC frames that this interface has transmitted.
tokS.TokenErrors	This counter is incremented when a station acting as the active monitor recognizes an error condition that needs a token transmitted.

■ UPS-Values

table: UPS-Values

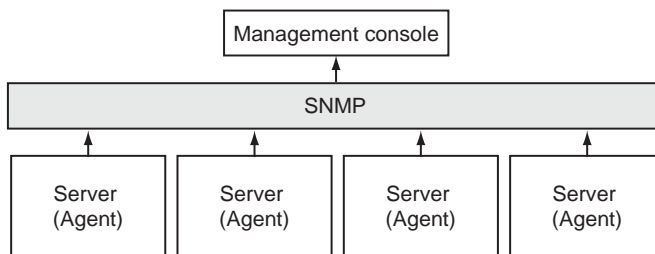
Value	Meaning
ups.TimeOnBattery	The elapsed time since the UPS switched to battery power.

F Technical Information

This section describes various technologies that constitute ServerView.

F.1 Agent and Management Console

A software package called as "Management Console" is used to manage networks, systems and applications. The Management Console can access to the management information provided by the network components. In short, all information related to networks, systems, and applications are provided by the Management Console.



The information exchanged between the Management Console and network components can be classified into two categories as shown below.

- The jobs the Management Console transmits to the network components. For example, an instruction that executes a query for the start of action or system usage.
- The autonomous message sent from the network component to the Management Console. For example, the message that notifies a component status to the Management Console.

It is required to define officially the exchange rules between the layout of this management information and the management information. This definition is called as management protocol. SNMP (Simple Network Management Protocol) is the standard management protocol.

The Management Console needs the monitored network component that can communicate based on this protocol to have the same function as those the Management Console has. There is the same function as the Management Console; it is called as an Agent. The Agent can access not only to the local resources and components but also to the information if it uses the protocol. This interrelation between the Management Console and the Agent is called a criterion between them.

The Agent is an OS-dependent software and should be install on all servers on the network. The Agent has the following characteristics:

- As a program, it must be very small and efficient. Using a large amount of system resource is not permitted to prevent the existence of the Agent affecting on the components themselves.
- It has a basic function to communicate with the Management Console as a standard function.
- Against the Management Console, it acts as a substitution of affected network components and the characteristics related to the components.
- It can be integrated to the network management concepts.

F.2 Management Information Base

A common management protocol must be implemented in the communication between the Management Console and the Agent. In addition, the Management Console and its corresponding Agent must agree what information should be provided and requested. Therefore, the management model for resource monitoring must match between them.

When the management model matches, it is assured that a job transmitted from the Management Console to the Agent can be executed by the Agent that receives it. Conversely, the Management Console must be able to interpret the message transmitted from the Agent that relates to a specific network event.

Therefore, both communication partners must have a common information base they can use freely. This common information base is called Management Information Base (MIB).

Any agent on the network provides MIB. As a result, the abstract data model of the corresponding component is made up by the MIB.

The special aspect of the MIB is that the Agent can act as a special resource provided by the MIB and configure itself by using the MIB. This is done, for example, when the Fujitsu Agent is used to monitor the MIB object threshold.

To describe the value to be included into the MIB, the official description language ASN.1 (Abstract Syntax Notation One) is used. ASN.1 is defined in ISO 8824 and ISO 8825.

Contrary to the Agent that should recognize only its own territory, the Management Console requires a complete information base of the entire network to execute its task. Therefore, all MIB files provided by the Agent on the network must exist on the Management Console system.

The following two categories of the MIB description is important for the Agent.

- The standard MIB file accepted by IEC.
For example, one of those standard MIB file is "MIB II" file and is mandatory to be used in all network components on Internet. In MIB II, the appropriate data model for managing systems and routers has been defined already.
- The private MIB file that contains manufacturer's own extensions.
Normally, the manufacturer who sells new network component products would define the private MIB file that exceeds the application range of the standard MIB to describe the management aspect of the component.

F.3 Principles of SNMP

In ServerView program, Simple Network Management Protocol (SNMP) is used.

SNMP is a standard protocol that has been accepted by Internet Engineering Task Force (IETF) and is used to manage TCP/IP network worldwide.

■ Data elements of SNMP

The individual section of information contained in the MIB is described by MIB's own object. Each object receives a unique object identifier globally. The access type is specified also.

■ Protocol elements of SNMP

The information is transmitted on the network using protocol elements. SNMP requires four different protocol elements to request, set, and display the value that is contained in the management information. The fifth protocol element (trap) allows the Agent to report an important event asynchronously.

table: Protocol elements of SNMP

Protocol element	Type	Functions
GetRequest PDU	0	Read MIB object request transmitted from the Management Console.
GetNextRequest PDU	1	Read the following MIB object requests transmitted from the Management Console (by entity ID).
GetResponse PDU	2	From the Agent, respond the contents that contain the requested value or the specified value.
SetRequest PDU	3	Write MIB object request transmitted from the Management Console.
Trap PDU	4	Asynchronous message when special event occurs

SNMP message consists of a SNMP header and PDU (Protocol Data Unit). The header contains a version ID code and a community string for the authentication check. PDU itself is a list of PDU type (refer to table) and "variable binding". The variable binding is to assign values to MIB object. This list consists of MIB object names and values to be assigned.

■ Community

A community is a group to which multiple systems (Management Console and Agent) that communicates with each other using SNMP are organized. The group is identified using a community string for group. The systems that belong to the same community can communicate each other. One system may belong to multiple communities. When the Management Console and the Agent communicate with each other, this community string is used like a password. The Agent can provide information in the agent system after it has obtained the community string from the Management Console. This restriction applies to each SNMP packet.

The access types such as read only or read-write access is defined for each MIB object. The Management Console's access right to the Agent information is bound to the community string also. The MIB access types can be limited further by the access right bound to the community string. Those access rights cannot be extended. When the MIB definition defines so that read only access right is defined to an object, that object cannot be used even if the community string is bound to the read-write access right. The following example shows how to use the community string and access right.

● Example

A SNMP agent belongs to the community named "public" and has read only access right. The public community contains a Management Console. This Management Console can request the information transmitted from this SNMP agent by using the public community string to transmit corresponding message. Concurrently, this SNMP agent also belongs to the second community named "net_5". The read-write access right has been associated to this community. The net_5 community contains one more Management Console. In this example, the right for writing operation via the SNMP agent is given to the second Management Console (the Management Console for the net_5 community).

■ Trap

When a special event occurs on the network component, the SNMP agent can notify the event occurrence by transmitting a message to one or more Management Consoles. This message is called a trap in SNMP. The Management Console can handle an event that occurred on the network based on the trap received. The fact that the Management Console received a SNMP trap is also shown on the community string. When the SNMP agent transmits the trap message to the Management Console, the community string of the trap that is required to receive the message must be used.

For the ServerView trap, refer to "D Trap List" (→pg.389).

■ Fujitsu server management

Behind the server management, there is a basic idea that there must be the Management Console accesses to the server management information on the network.

To accomplish this function, the server hardware and firmware are designed to follow this concept.

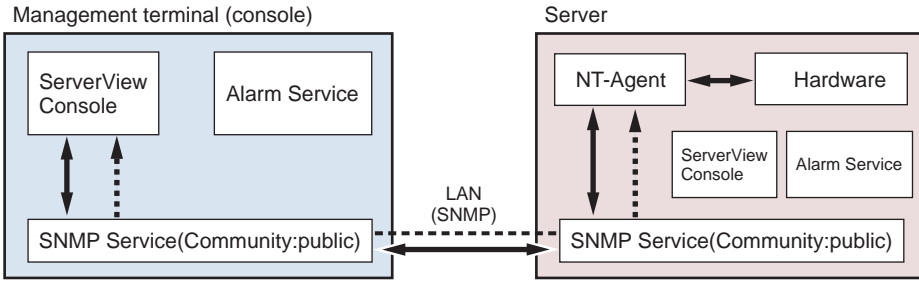
The Agent accesses the existing information and allows the Management Console to access the information through SNMP.

■ ServerView configuration

The component that is installed on the server varies depending on the OS used. ServerView Console is installed on the management terminal. The dotted lines on each figure show the communication by SNMP protocol.

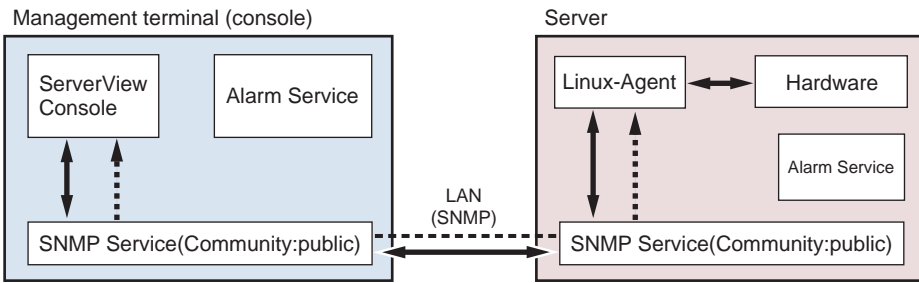
● **For Windows:**

Install ServerView Agent on the server.



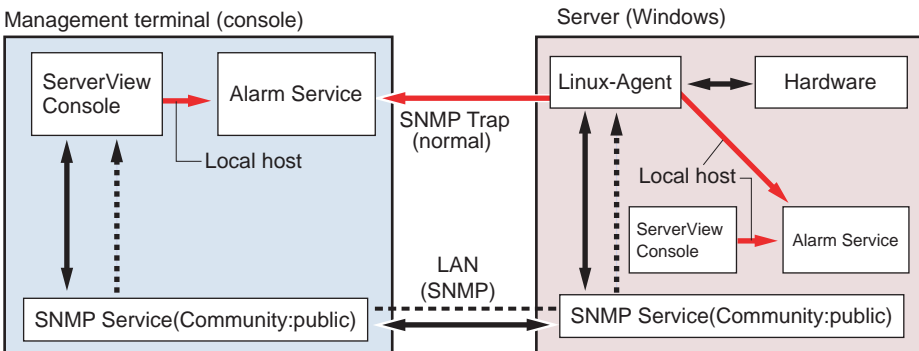
● **For Linux:**

Install Linux Agent and Linux AlarmService on the server.



● **Trap transmission**

The trap is transmitted to the IP address specified by the property setting of SNMP service. In normal trap transmission, NT-Agent trap on the server is received by Consoles's AlarmService. The localhost must be set for Console to receive its own trap. The localhost must be also set to receive the server's own trap by using its AlarmService.



■ Monitoring function

● Watchdog

The ServerView Agent functions are monitored by software watchdog. When the ServerView Agent is connected to BIOS, the software watchdog starts.

The ServerView Agent must report to the server management firmware at the intervals defined by the watchdog time setting. When the ServerView agent stops reporting to the server management firmware, it is assumed that the system is not operating properly, and the specified actions (to reboot, continues to operate or turn off/on) is launched.

The time intervals can be set in minutes to [Watchdog Timeout Delay]. The validity of the time is confirmed by the Management Console and Agent. The minimum time is one minute.

The available value is 1 to 120 minutes. If the values other than 1 to 120 minutes are specified, "N/A" is displayed on ServerView. When the Agent stops (for example, by SNMP command net stop), the watchdog stops automatically to prevent unscheduled restart.

● Boot monitoring

The watchdog monitors the time period until ServerView Agent becomes available after the system has been started. When the ServerView does not establish the connection with the server management firmware within the specified time periods, it is assumed that the boot process failed, and then the specified actions (to reboot, continues to operate or to turn off/on) is launched. The time intervals can be set in minutes to [Watchdog Timeout Delay]. The available value is 1 to 120 minutes. If the values other than 1 to 120 minutes are specified, "N/A" is displayed on ServerView.

F.4 Version Management (Inventory View)

Inventory View is one of the functions that ServerView Version Management Task provides. The version management task is part of ServerView and uses common framework in server management task and version management task.

The main task of Inventory View is to check the configuration of hardware and software on the specific machine. Also, it provides an integrated management tool that enables Inventory View function to be executed on all servers on the network that supports acquisition of Inventory View's own inventory information. This tool allows a system administrator to define one or more central management stations that executes Inventory View's task. Since this function is similar to the server management function, Inventory View has been built into the ServerView's Management Console. The tasks in ServerView and Inventory View use the same lists as those of managed server.

Inventory View consists of two modules.

- Management Console function

This operates in the management terminal. This consists of the components that receive the data on the installed components from the Agent.

Inventory View receives the information on the installed components from Inventory View SNMP Agent. Each result is shown on the window in conjunction with updated view of Inventory View.

- Agent function

This works on the client machine. This function allows the inventory of each server to be used on the network. The Management Console obtains and evaluates this inventory information of the specific server and then displays each result.

POINT

- ▶ The SNMP agent provides all Inventory View information about specific machine. In order to allow the Management Console to show the information on the client who is being down currently, the inventory information is saved to a file.

F.5 List of Contents to be Exported

The contents to be exported are as follows:

● Server list contents

- Server_ID
- IP_Address
- Server_Group
- Server_Name
- Location
- Contact
- Model
- Serial_Number
- BIOS_Version
- Number_of_Processors
- Number_of_Processor_Sockets
- Processor_Type
- Memory_Size_MB
- Cache_KB
- Number_of_File_Systems
- Size_of_File_Systems_MB
- Largest_Available_Space_MB
- Operating_System

● Container list contents

- Server_ID
- Time
- Functional_Container_No
- Functional_Container_Name
- Container_Parent_No
- Server ID list contents
- Server_ID

- Time
- Server_Name
- IP_Address

● Inventory list contents

- Server_ID
- Time
- Component_Name
- Product_Number
- Vendor
- Version
- Component_Type
- Manufacturing_Date
- Serial_Number
- Language
- Functional_Container_No
- Functional_Container_Name
- Physical_Container_No
- Physical_Container_Name

● Checklist contents

- Server_ID
- Time
- Component_Name
- Product_Number
- Vendor
- Version
- Component_Type
- Manufacturing_Date
- Serial_Number
- Language
- Update_Status
- Update_Information
- Systemboard_Compatibility
- Missing_Required_Components
- Exclusion_Information
- ComponentsAddedByRequirement
- Functional_Container_No
- Functional_Container_Name
- Physical_Container_No
- Physical_Container_Name

F.6 How to Change SNMP Settings

The SNMP community name must be the same for both the Management Console and the server.

- Setting properties of SNMP service (trap)
On the server side, it is necessary to specify the host name or IP address of the Management Console to the trap destination.
- Setting properties of SNMP service (security)
The community name that would be accepted on the server side must have the same setting as those in the Management Console.

■ How to change community name (public) on Windows

● How to set in the Management Console

- When changing the server that has been registered:
Click [File] (or select and right-click the target server) → [Server Properties] → [Network/SNMP] Tab and change the community name.
- When adding a new server:
 1. Click [File] (or right-click on the Server List) → [New Server] → [Network/SNMP] Tab and enter the community name.
 2. Open the server address.
 3. Close the server browser once.
 4. Open the new browser again.

● How to set on the server

When [Accept SNMP packets from these hosts] is selected, it is necessary to enter the followings:

- The host name or IP address of Management Console.
- The host name or IP address of the monitored server.
- The loop back address (172.0.0.1 or localhost) of the monitored server.

If an error exists in above settings, the monitoring function does not operate properly.

■ How to change community name (public) on Linux

POINT

- ▶ Management Console is not supported on Linux.

● How to set on the server

- 1 Change "public" in the following three lines in the /etc/snmp/snmpd.conf to any community name.

```
com2sec svSec localhost public
com2sec svSec default public
(snip)
trapsink 127.0.0.1 public
```

- 2 Add the following lines to the [Configuration] sections of /etc/srvmagt/VersionView.ini and /etc/srvmagt/Status_MIB.ini.

```
SnmpCommunity = new community name
```

- 3 After editing, execute the following commands.

```
# /etc/rc.d/init.d/srvmagt stop
# /etc/rc.d/init.d/snmpd stop
# /etc/rc.d/init.d/eecd stop
# /etc/rc.d/init.d/eecd start
# /etc/rc.d/init.d/snmpd start
# /etc/rc.d/init.d/srvmagt start
```

F.7 Firmware Version of Remote Service Board (RSB)

This section describes how to check the firmware version of remote service board (REB).

■ Using the Web Interface

- On the Web interface startup screen, look for [Version N" RSB_LP_A.X.X.XX.XX].
- Log in to the Web interface and look for [Software Revision: "RSB_LP_A.X.X.XX.XX"] on the [Card Config] tab.

Index

A

- Abort Shutdown 101
- Aborting shutdown 224
- Advanced Video Redirection (AVR). 314
- Agent 12, 396
- Alarm Group
 - Creating 148
 - Destination 150
- Alarm Service 15
- AlarmService 18, 131
 - Alarm Group 147
 - Alarm Manager 139
 - Alarm Monitor 132
 - Alarm Settings. 142
 - Overview 163
 - Question and answer 362
 - Setting Example 163
 - Starting 131
 - System requirements 22
 - Troubleshooting 364
- Apache 32
- Archive 16
 - Archive Data Log. 190
 - Archive Manager. 183
 - Comparing archive data 189
 - Configuring Tasks 185
 - Creating archive data 184
 - Deleting archive data. 190
 - Displaying archive data 188
 - Importing Archive Data 191
 - Starting the archive manager. 183
- ASR 17
- ASR settings. 123
 - Fan 126
 - Power ON/OFF 129
 - Restart settings 128
 - Temperature sensor 127
 - Watchdog Settings 129
- Automatic Reconfiguration & Restart 17
- Auto-start setting of httpd service 66
- Auto-start setting of SNMP service
 - Blade server 70
 - Normal server 66

B

- Binding order 31
- BMC connection 273
- BOOT Watchdog 130
- Bridge Controller. 228

C

- Configuring RomPilot 252
- Controller View 103
- Copying settings to other server 16

D

- Default Settings 218
- Directory Service Function 306, 307

E

- Export Manager
 - Acquiring Export Data 192
 - Displaying Export Data 200

I

- Icon List 379
- Installation script. 41, 49
- Installing
 - Microsoft Virtual Machine 59
 - RemoteControlService/LAN 266
 - RemoteControlService/Web 267
 - ServerView Agents 39
 - ServerView Console 34
 - ServerView Linux (blade server) 48
 - ServerView Linux (to normal server) 40
 - SNMP service 27
 - TCP/IP protocol. 27
 - Web server 32
- Inventory View 401
- IPMI 246

M

- Management Console. 12, 202, 396
 - Adding the Server 206
 - Archive data display 220
 - Configuration information 221
 - Copying Settings to the Other Servers . 218
 - Environment 221, 234
 - External Storage Devices - DuplexWrite 230
 - Locate. 220
 - Mass Storage 221, 224
 - Mass Storage - MultiPath 228
 - Mass Storage - RAID controller. 227
 - Monitoring hardware 219
 - Network Discovery 208
 - Operating System 221
 - Power Supply 221, 232

Question and answer	355
Recovery	221
Report manager	215
RSB mode	220
Server Properties	210
ServerView Operation	202
Starting	202
Status (Blade Server)	235
System Board	221
System Board Status	231
System status	221
Threshold Manager	211
Troubleshooting	356
Management Information Base	397
ManagementBlade connection	278
Measures at abnormal temperature	123
Measures at fan failure	123
Microsoft Internet Information Server	32
Monitored servers	
Adding to the monitored object	206
Creating groups	209
Deleting from the monitored objects	209
Notes in adding	207
Verifying/changing the server settings	210
Monitoring hardware	
Blade Server	235
Normal server	219
MSA	306
MultiPath Status	229
P	
Performance Manager	171
Applying the settings to servers	180
Checking/Resolving the differences	182
Defining/Modifying reports	178
Defining/Modifying thresholds	173
Report View	181
Reports	171
Set of Reports	179
Set of Thresholds	177
Starting	172
Threshold settings	171
Q	
Question and answer	
AlarmService	362
General questions & answers	370
Management Console	355
R	
RCM	246
Recovery	222
Boot Options	223
Error Message Buffer	223
Redect Server	
All Servers	91
the Selected Server	91
Registering the interrupt information of the optional devices	62
Remote management	17, 282
Remote Service Board	17
Remote Service Board (PG-RSB102)	302
Autologon Settings	342
Directory service	348
Displaying server information	337
Functions	302
Notes	302
Power control	313
Remote Service Board Settings	333
Setting alarm functions	338
Setting the LAN Interface	303
Setting user accounts	340
Starting the Web Interface	310
USB Settings	331
Viewing each sensor value	331
Window display setting	313
Remote Service Board (PG-RSB103)	302
Remote Storage Function	306
Remote Storage Functions	319
iSCSI connection	323
Local connections	319
RemoteControlService	17, 246
System requirements	248
RemoteControlService/LAN	247
BIOS Setup	287
Connecting to IPMI	299
Exit	272
Installing	266, 267
Menu list	269
Password management	280
Power on for a server	288
Remote server management	282
Starting	268
Starting servers from a remote drive	289
Uninstallation	266
RemoteControlService/Web	
Uninstallation	267
RemoteControlService/Web(BMC connection)	
Exiting	275
Starting	273
RemoteControlService/Web(ManagementBlade connection)	
Exiting	279
Starting	278
RemoteControlService/Web(RSB connection)	
Exiting	278
Starting	276
Report	16

Contents to be exported	402	Window menu	205
Creating reports	215	Server Management mode	202
Graphical representation	218	Server Properties	210
Report list	217	Server shutdown/power-off	224
Stopping Reporting	217	Server Status	
Verifying details of reports	218	Configuration Information	95
Report manager	215	Connection Verification	89
Restarting the Server	101	Current Status	91
Restarting the server	224	Server Status Icon	88
RomPilot	246	Verifying Details	92
RomPilot/RCM		ServerView	12
Starting servers from a remote drive	289	ServerView Agent	
RPM		Modifying Settings	237
Checking the version (of blade server)	54	Restoring Settings	240
Checking the version (of normal server)	48	Save Settings	239
Version up (blade server)	54	Uninstallation	377
Version up (of normal server)	48	ServerView Agents	
RSB	17, 302	Installing	39
RSB connection	276	System requirements	19
RSB properties	224	ServerView Console	18
		Installing	34
		System requirements	20
		Uninstallation	376
		ServerView Linux	
		How to Use	241
		Installing (blade server)	48
		Installing (to normal server)	40
		Status display	241
		Uninstallation	377
		Using ServerView S2/AlarmService	242
		ServerView Linux agent	18
		Log	242
		Starting and exiting	241
		System requirements	21
		ServerView S2	
		Baseboard Status	108
		Environment	112
		Environment (Blade Server)	121
		Export Manager	192
		How to Use	76
		Mass Storage	103
		Menus	79
		Power Supply	113
		Power Supply (Blade Server)	122
		Registering MIB	87
		Registering the Monitored Servers	81
		Starting	76
		Verifying/Changing the Server Settings	84
		ServerView WebExtension	12
		System requirements (Linux)	22
		Troubleshooting	368
		ServerView Web-Server	32
		Service Pack Application	31
		Setting an Administrative User	60
		Setting each service	
S			
SCSI RAID card			
Adaptor View	227		
Bridge Controller	228		
Device View	227, 228		
Searching servers			
Network Discovery	208		
Serious Error Handling	123		
Server Browser window			
Adding the monitored server	206		
Server Configuration Information	95		
Agent Status	95		
Expansion Boards	98		
Fans and Temperature Sensors	99		
Mass Storage	97		
MIB- II	99		
Network Interfaces	97		
Recovery	98		
System Information	96		
Server List window			
Alarm menu	204		
Edit menu	203		
File menu	203		
Filtering	209		
Help menu	205		
Pop-up Menu	205		
Reports menu	204		
Settings menu	204		
Task menu	204		
Threshold menu	205		
Tools menu	205		
View menu	204		
Window description	202		

Blade server	70
Normal server	65
Settings for restarting	123
Shutdown/Power-off of the Server	101
SNMP	397
Software Watchdog	130

T

Threshold	15
Specifying thresholds	211
Stopping Threshold Monitoring	214
Threshold list	214
Threshold manager	212
Threshold List	390
Trap list	389
Troubleshooting	
AlarmService	364
Browser	372
Installation script	352
Management Console	356
ServerView WebExtension	368

U

Uninstallation	
RemoteControlService/LAN	266, 267
ServerView Blade-Agent	377
ServerView Linux	377
WebExtension/AlarmService	378
UPS Manager	233

V

Version Management	16
Export Manager	192
Version Management mode	202

ServerView V4.11

User's Guide

B7FH-4191-01ENZ0-00

Issued on January, 2006

Issued by FUJITSU LIMITED

- The contents of this manuals may be revised without prior notice.
- Fujitsu assumes no liability for damages to third party copyrights or other rights arising from the use of any information in this manual.
- No part of this manual may be reproduced in any form without the prior written permission of Fujitsu.