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	Installation	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	RAID Manager Linking	This chapter explains how to link RAID Manager with ServerView S2 or the Management Console.
Chapter 5	Using RemoteControlService	This chapter explains how to use RemoteControlService.
Chapter 6	Using the Remote Service Board	This chapter explains how to use the Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104/PG-RSB105). This is available only for the server on which the Remote Service Board is installed.
Chapter 7	Using the Remote Management Controller	This chapter describes the Web interface functions and the configuration of the Remote Management Controller.
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:

IMPORTANT	These sections explain prohibited actions and points to note when using this software. Make sure to read these sections.
POINT	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].

Abbreviations

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		Windows
Microsoft® Windows Server® 2003 R2 Standard Edition Microsoft® Windows Server® 2003 R2 Enterprise Edition Microsoft® Windows Server® 2003 R2 Standard x64 Edition Microsoft® Windows Server® 2003 R2 Enterprise x64 Edition	Windows 2003 R2		
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		
Microsoft® Windows® 2000 Professional	Windows 2000 Professional		
Microsoft® Windows NT® Workstation Operating System 4.0	Windows NT Workstation 4.0		
Red Hat Enterprise Linux AS (v.4 for x86)	RHEL-AS4(x86)	Red Hat Linux	Linux
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.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)		
Novell SUSE LINUX Enterprise Server 9 for x86	SLES9(x86)	SUSE Linux	
Intel LANDesk® Server Manager	LDSM		
Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104/PG-RSB105)	Remote Service Board		

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

Contents

Chapter 1 Overview of ServerView

Chapter 2 Installation

Chapter 3 How to Use ServerView

Chapter 4 RAID Manager Linking

Chapter 5 Using RemoteControlService

Chapter 6 Using the Remote Service Board

Chapter 7 Using the Remote Management Controller

Appendix

Chapter 1

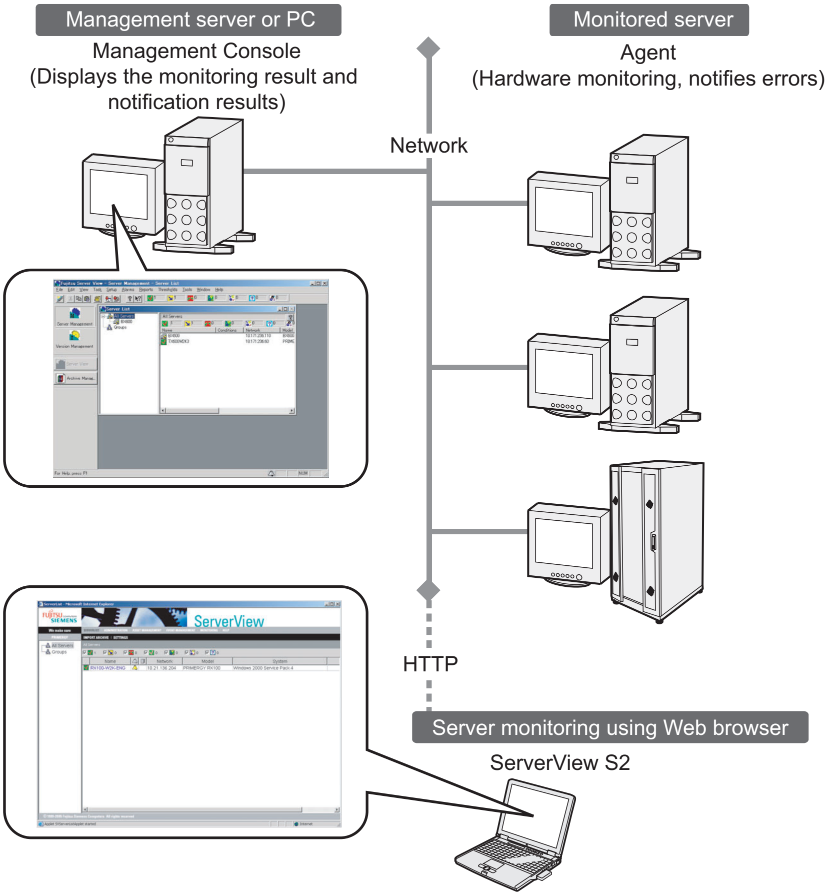
Overview of ServerView

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

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 Consol and Agent or to install them separately depending on the network configuration or the server OS.


Management server or PC
Management Console
(Displays the monitoring result and notification results)
Monitored server
Agent
(Hardware monitoring, notifies errors)
Network
HTTP
Server monitoring using Web browser
ServerView S2
ServerView

■ How to monitor the server

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

● 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, see "3.1 Starting and Exiting ServerView S2" (→pg.84).

● 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, see "3.9 ServerView Operation Using the Management Console" (→pg.215).

■ ServerView's functions

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

- Hardware Monitoring (→pg.14)
- Abnormality Occurrence Notification/Server Status Check (→pg.15)
- Automatic Reconfiguration & Restart (→pg.16)
- 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.
As for RAID monitoring (RAID Manager interaction), ServerView Alarm Service needs to be installed in the server to be monitored.

● Hardware components on the server unit

The monitorable hardware components vary depending on the server type. For more details, see "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, see "2.4.4 Registering the Interrupt (MIB) Information of Optional Devices" (→pg.67) 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

POINT

When SCSI RAID card is monitored:

- You need to install SCSI-RAIDmanager (ServerView RAID Manager, GAM (Global Array Manager), StorageManager) attached to the SCSI RAID card..

When IDE-RAID card is monitored:

- You need to install IDE-RAIDmanager (PROMISE Fasttrak, PAM (PROMISE ARRAY MANAGEMENT)) attached to the IDE-RAID card.

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, see "3.5 AlarmService" (→pg.138).

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, see "3.6 Performance Manager" (→pg.178). If you are using the Management Console, see "3.9.4 Threshold Manager" (→pg.224).

POINT

- The event log stored to ServerView Agent is the following:
  Log type: application
  Source name: ServerView Agents
- ServerView Linux Agent stores system logs with the following signature:
  Strings beginning with “Serverview:”

■ 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, see "3.2.9 Version Manager (Inventory)" (→pg.124).

● 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, see "3.7.1 Starting the Archive Manager" (→pg.198).

● 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, see "3.6 Performance Manager" (→pg.178). If you are using the Management Console, "3.9.5 Report Manager" (→pg.227) 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, see "3.9.6 Copying Settings to the Other Servers" (→pg.231).

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, see "3.4 Serious Error Handling (ASR)" (→pg.130).

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, see "Chapter 5 Using RemoteControlService" (→pg.265).

IMPORTANT

- 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 downs 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, see "Chapter 6 Using the Remote Service Board" (→pg.293).

1.1.6 Note

● Security

The ServerView console (ServerView S2, Management Console, or AlarmService) handles personal information, such as the administrator' s name, and other important information. We recommend that you do not install the ServerView console on a system that is set up in a domain accessible from outside. If you do install the ServerView console on such a system, take care of the security so that the specified information is inaccessible from outside and minimize the contents to be set.

POINT

- For the configuration examples, see "F.8 Configuring Access Privileges" (→pg.440).

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		
ServerView Windows Console ServerView S2 Management Console AlarmService	Windows Server 2003 R2 Windows Server 2003 Windows 2000 Server Windows XP Professional Windows 2000 Professional	The status of all target servers can be monitored and controlled centrally. This is installed on the monitored servers and a management server or PC. • ServerView S2 This provides the client function to manage the server by Web browser. • Management Console This is client software of Windows application to manage the server. • AlarmService This receives the SNMP trap from the agent and executes the event action.
ServerView Linux Console ServerView S2 AlarmService	Linux	The status of all target servers can be monitored and controlled centrally. This is installed on the monitored servers. • ServerView S2 This provides the client function to manage the server by Web browser. • AlarmService This receives the SNMP trap from the agent and executes the event action.
ServerView Agent		
ServerView Windows Agent Agent	Windows Server 2003 R2 Windows Server 2003 Windows 2000 Server	This Agent is installed on the monitored server. This monitors the hardware status.
ServerView Linux Agent Agent	Linux	This Agent is installed on the monitored server. This monitors the hardware status.

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, see "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	• Windows 2003 R2 • 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

IMPORTANT

- 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	• Windows 2003 R2 • Windows 2003 • Windows 2000 Service Pack 4 or later • Windows XP Professional • Windows 2000 Professional Service Pack 4 or later
	Web server	• Microsoft Internet Information Server (Windows) or • ServerView Web-Server (Apache for Win32 based) (Installed automatically when it is selected during the ServerView installation) or • Apache2
	Protocol	TCP/IP is required to run
	Service	SNMP (service and trap) must be operated.
	Web browser	• Microsoft Internet Explorer 5.5 or later (recommended: 6.0 or later) • Java™ 2 Runtime Environment Standard EditionV1.4.2_08 or later. (It can be installed from PRIMERGY Document & Tool CD.)
	Account	Privileges equal to administrator must be assigned

IMPORTANT

- Microsoft Virtual Machine is not supported in ServerView V3.40 or later.
- When performing RAID monitoring (linked with RAID Manager) or REMCS linking, install AlarmService on the server to be monitored. If AlarmService is not installed properly, errors are not recorded in the system log and the monitoring cannot be linked.

■ 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	• 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)) • Novell SUSE LINUX Enterprise Server 9 for x86 (Abbreviation: SLES9(x86))
Protocol	TCP/IP is required to run
Service	SNMP (service and trap) must be operated.
Package (RPM)	For RHEL-AS4(x86)/ES4(x86)/AS4(EM64T)/ES4(EM64T) and RHEL-AS3(x86)/AS3(IPF)/ES3(x86) • net-snmp • net-snmp-utils • compat-libstdc++ • gcc • glibc • glibc-devel • binutils • libstdc++ • make • gawk • rpm • kernel-source(for RHEL-AS3(x86) / ES3(x86) / RHEL-AS3(IPF)) • kernel-devel(for RHEL-AS4(x86) / ES4(x86) / RHEL-AS4(EM64T) / ES4(EM64T)) • at For SLES9(x86) • net-snmp • gcc • glibc • glibc-devel • binutils • make • gawk • rpm • kernel-source • at
Account	Superuser

IMPORTANT

- 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	• 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)) • Novell SUSE LINUX Enterprise Server 9 for x86 (Abbreviation: SLES9(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	For RHEL-AS4(x86) / ES4(x86) / AS4(EM64T) / ES4(EM64T) and RHEL-AS3(x86) / AS3(IPF) / ES3(x86) • 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.) For SLES9(x86) • Mozilla V1.7.8 or later
Package (RPM)	For RHEL-AS4(x86) / ES4(x86) / AS4(EM64T) / ES4(EM64T) and RHEL-AS3(x86) / AS3(IPF) / ES3(x86) • net-snmp • net-snmp-utils • compat-libstdc++ • httpd • gnome-libs • rpm • gawk • openssl • mod_ssl • at For SLES9(x86) • net-snmp • apache2 • gnome-libs • rpm • gawk • openssl • at
Account	Superuser

IMPORTANT

- ServerView S2 and AlarmService cannot be used separately. Both must be installed.
- When performing RAID monitoring (linked with RAID Manager) or REMCS linking, install ServerView S2 and AlarmService on the server to be monitored. If ServerView S2 and AlarmService are not installed properly, errors are not recorded in the system log and the monitoring cannot be linked.

■ ServerView S2 Screen-displayed Requirements

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

● Web Browser

table: Web browser requirements

OS	Web browser
Windows	Microsoft Internet Explorer 5.5 or later (recommended: 6.0 or later)

RHEL-AS4(x86) / ES4(x86) / AS4(EM64T) / ES4(EM64T)
RHEL-AS3(x86) / AS3(IPF) / ES3(x86)
	• Mozilla V1.3 or later
	• Mozilla FireFox 1.0.4 or later

SLES9(x86)	Mozilla V1.7.8 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.)

IMPORTANT

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

Chapter 2

Installation

This chapter explains how to install ServerView.

2.1 Installation Flow

The installation flow of ServerView is as follows:

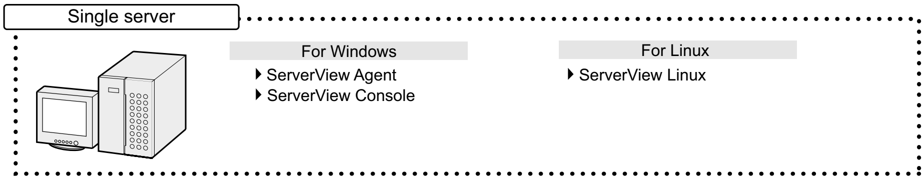
Checking before installation

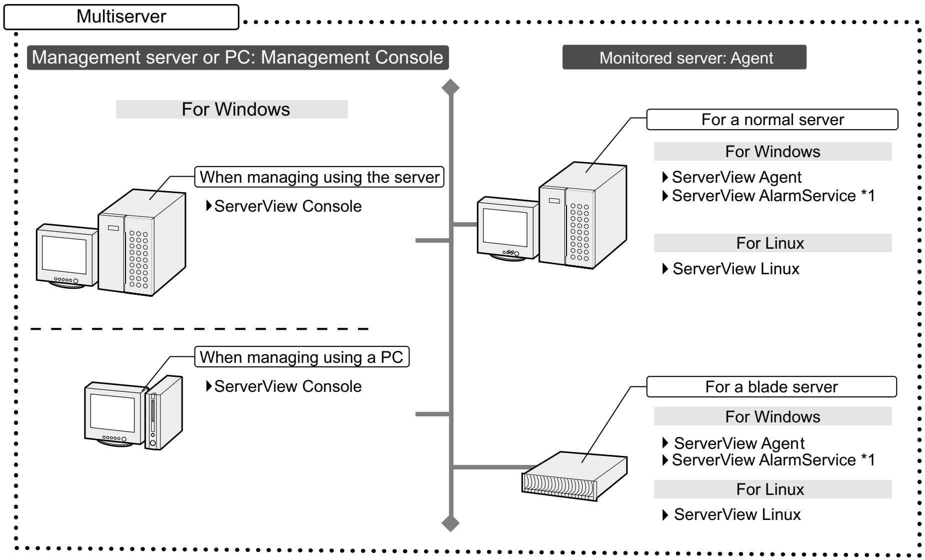
Before installing ServerView, check the following:

For Windows	For Linux
- Install TCP/IP and SNMP services.	- Install the Web server
- Apply Service Pack - Change the bind order	- Check the kernel and RPM
- Install the Web server	

Installing

Install the components necessary depending on the network configuration.
- For a single server,the required components for installation vary depending on the type of OS.
- For a multiserver environment, the required components for installation vary depending on the type of OS, normal server/blade server and method of monitoring.





*1 : ServerView AlarmService needs to be installed when performing RAID monitoring (linked with RAID Manager).

Settings after installation

After the installation of ServerView, perform the various settings and install OS components.

For Windows	For Linux
- Install Microsoft InternetExplorer	- Set various services (for a normal service)
- Install Java 2 Runtime Environment Standard Edition	- Set various services (for a blade server)
- Set an administrative user	- Install Java 2 Runtime Environment Standard Edition
- Register interrupt information of optional devices	- Register interrupt information of optional devices

2.2 Check before Installation

Before installing ServerView, check the following:

2.2.1 Installation of TCP/IP Protocol and SNMP Service

In order for ServerView to function correctly, the TCP/IP protocol and the SNMP service must be installed on the servers to be monitored.
In the description below, the example SNMP service community name is written as "public". The community name can be changed when necessary. For details about changing the community name, see the technical information.→"F Technical Information" (pg.431)

■ For Windows 2003:

1 Start up the [Control Panel].

2 Double-click [Network Connections].

3 Click the [Advanced] menu → [Optional Networking Components].

4 Perform one of the following actions:

<u>If the [Management and Monitoring Tools] in [Optional Networking Components Wizard] is already checked:</u>

1. Click [Management and Monitoring Tools], click [Details], and 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.

<u>If the [Management and Monitoring Tools] in [Optional Networking Components Wizard] is not checked:</u>

Follow the steps below to install the SNMP service.

1. Check [Management and Monitoring Tools] in the [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 in the window.

5 Open the Control Panel and double-click the [Administrative Tools] icon.

6 Click [Manage Computers].

7 In 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 to "Automatic" if it is not set already.

11 Click the [Traps] tab.

12 If "public" is already entered 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 the ServerView Console is installed and click [Add].

When installing the ServerView Console in a 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).

If "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 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 servers where the ServerView Agent is installed, make sure that the loopback address (127.0.0.1) is included.

19 Click [OK].

POINT

- In Windows 2003, PopUp (Messenger) is disabled with the initial settings. To use PopUp messages in the ServerView's monitoring function, follow the steps below to set the PopUp function.
  1. Click [Start] → [Administrative Tools].
  2. Click [Manage Computers].
  3. In 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 the [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 actions:

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

1. Click [Management and Monitoring Tools], click [Details], and 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.

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

Follow the steps below to install the SNMP service.

1. Check [Management and Monitoring Tools] in the [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 in the window.

5 Double-click the [Administrative Tools] icon in the [Control Panel].

6 Double-click the [Computer Management] icon.

7 In 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 to "Automatic" if it is not set already.

11 Click the [Traps] tab.

12 If "public" is already entered 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 the ServerView Console is installed and click [Add].

When installing the ServerView Console in a 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".

17 Click [Edit].

18 Select [READ_WRITE] or [READ_CREATE] from [Community rights] and click [OK] ([READ_WRITE] is recommended).

If "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 servers where the ServerView Agent is installed, make sure that the loopback address (127.0.0.1) is included.

20 Click [OK].

2.2.2 Changing the Binding Order

When multiple IP addresses exist in the server due to multiple LAN cards, etc., ServerView searches the IP addresses 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 order, follow the steps below.

1 Start up the [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 the order, and then change the order with the arrow buttons on the right side.

2.2.3 Service Pack Application

The Service Pack must be applied to all servers and PCs on which ServerView components are installed. However, this is not necessary for Windows 2003 R2.

- For Windows 2000, apply Service Pack 4 or later.
- For Windows 2003, apply Service Pack 1.

IMPORTANT

- 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 does not need to reapplied.
- Before applying the Service Pack, make sure that the SNMP service is installed.

2.2.4 Web Server Installation

Functions such as the alarm service (see "■ Abnormality occurrence notification" (→pg.15)), the archive function (see "● Archive function" (→pg.16)), and monitoring servers using the Web browser (see "● 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.
ServerView supports the following Web Server software.

- For Windows, use one of the following:
  - ServerView Web Server (Apache for Win32 based)
  - Microsoft Internet Information Server (IIS)
  - Apache2
- For Linux, use one of the following:
  - Red Hat Linux: httpd
  - SUSE Linux: apache2

POINT

- If the OS is Linux and ServerView S2/AlarmService is not used, the Web Server does not need to be installed.
- When installing ServerView automatically using ServerStart, you can choose either ServerView Web-Server or IIS.

■ ServerView Web Server

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

■ Microsoft Internet Information Server (IIS)

To use IIS, it should be installed before installing ServerView.

■ Apache2 (Windows)

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

■ httpd or Apache2

If the OS is Linux, the following RPM must be installed before installing ServerView Linux.

- Red Hat Linux: httpd
- SUSE Linux: apache2

2.2.5 Kernel and RPM Check

Insert the PRIMERGY Document & Tool CD and execute the following command.

- For Red Hat Linux

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
# /LinuxSVAgent/chksys (when installing only ServerView Linux
agent on the server to be monitored)
# /LinuxSVConsole/chksys (When installing only ServerView Linux
console on the server to be monitored)
```

When installing both ServerView Linux agent and ServerView Linux console, execute both commands above.

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

If an error message indicating insufficient RPM package is displayed, install the package from the Red Hat Linux or SLES9 (x86) CD-ROM.

IMPORTANT

- When the kernel is updated, make sure that the kernel version number matches the kernel source version number. If they do not match, 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 Installation

This section explains how to install each component of ServerView.

2.3.1 [Windows] Installing the ServerView Console

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

IMPORTANT

- If you want to change or update the Web Server (Apache2 or IIS) after the installation of the ServerView Console, uninstall the ServerView Console and install it again. If ServerView has been automatically installed with ServerStart, the ServerView Web-Server is selected as the Web Server or IIS.
  For information on how to uninstall the ServerView Console, see "B Uninstallation" (→pg.411).
- For a system on which a terminal server has been installed, the installation method is different from the usual methods. To install ServerView in a terminal server environment, perform Step 3 below after clicking [Start] → [Control Panel] → [Add/Remove Programs] → [Add Program].
- If Java has not been installed before the 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] to continue the installation. After installing the ServerView Console, install Java.
- The ServerView Console cannot be reinstalled if it has already been installed. In addition, the ServerView Console cannot be reinstalled or installed with additional functions if the ServerView AlarmService has been installed. Uninstall the currently installed the ServerView Console or the ServerView AlarmService, before reinstalling the ServerView AlarmService.
- If you have several different versions of ServerView, install the latest ServerView Console.

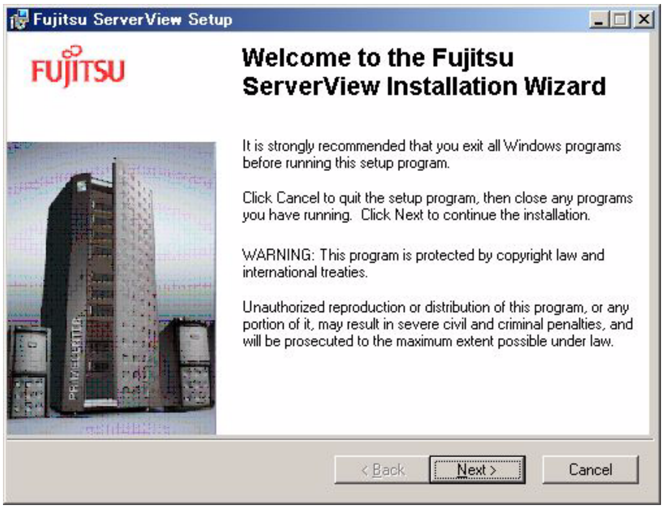
1 Log in as administrator or as a user with Administrator privileges.

2 Exit all running applications.

3 Insert the PRIMERGY Document & Tool CD and double-click the following installer:

[CD-ROM Drive]:\Svmanage\WinSVConsole\SV_Console.bat

The [Fujitsu ServerView Setup] window appears.



Welcome to the Fujitsu ServerView Installation Wizard

It is strongly recommended that you exit all Windows programs before running this setup program.

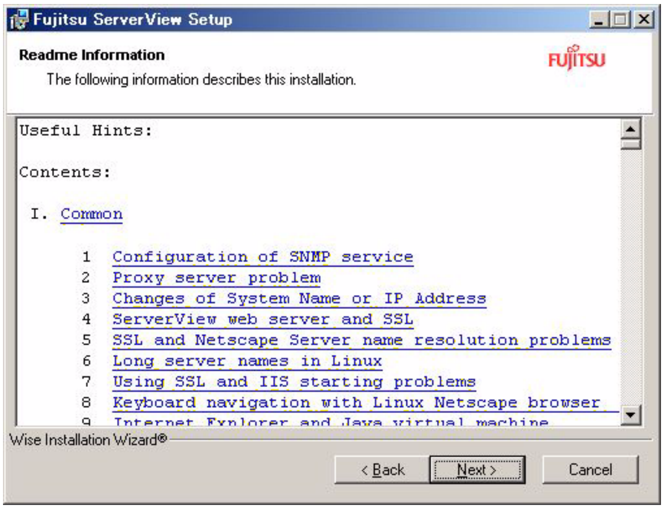
Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

4 Click [Next].

The [Readme Information] window appears.



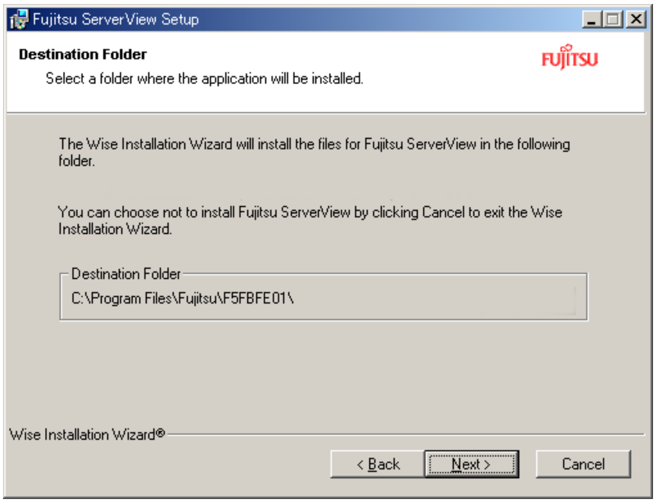
Readme Information

The following information describes this installation.

```
Useful Hints:

Contents:

 I. Common

      1  Configuration of SNMP service
      2  Proxy server problem
      3  Changes of System Name or IP Address
      4  ServerView web server and SSL
      5  SSL and Netscape Server name resolution problems
      6  Long server names in Linux
      7  Using SSL and IIS starting problems
      8  Keyboard navigation with Linux Netscape browser
      9  Internet Explorer and Java virtual machine
```

5 Click [Next].

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



Fujitsu ServerView Setup

Destination Folder

Select a folder where the application will be installed.

The Wise Installation Wizard will install the files for Fujitsu ServerView in the following folder.

You can choose not to install Fujitsu ServerView by clicking Cancel to exit the Wise Installation Wizard.

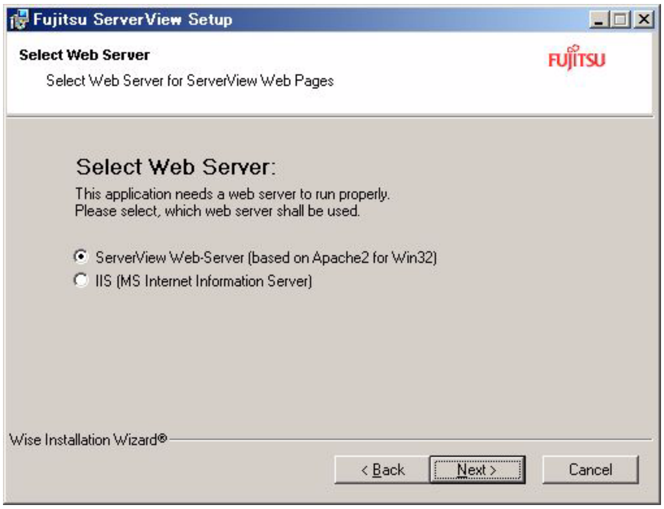
Destination Folder

C:\Program Files\Fujitsu\F5FBFE01\

6 Click [Next].

The [Select Web Server] window appears.

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



Fujitsu ServerView Setup

Select Web Server

Select Web Server for ServerView Web Pages

Select Web Server:

This application needs a web server to run properly.
Please select, which web server shall be used.

● ServerView Web-Server (based on Apache2 for Win32)

○ IIS (MS Internet Information Server)

IMPORTANT

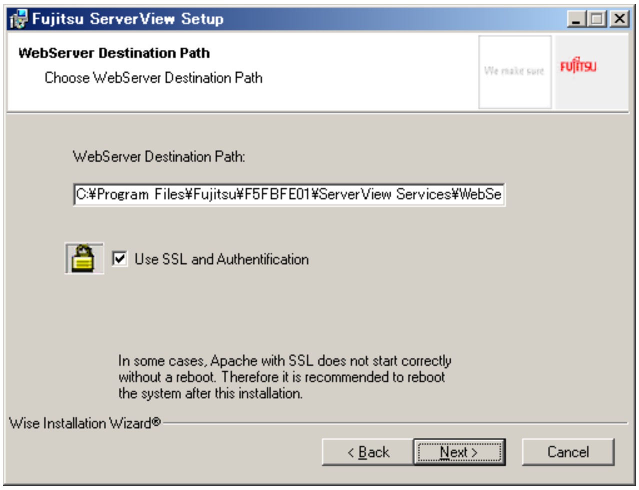
- When the ServerView Web Server is selected, the Apache2 for Win32-based Web Server is installed with ServerView. A task with the name "At**(**: task ID)" is added to the Windows Task Scheduler.
- When the IIS is selected, the installed IIS is used as the Web Server.
- When Apache2 has been already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

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

The [Web Server Destination Path] window appears.

The window varies depending on the selected Web Server.

When [ServerView Web Server] is selected as the Web Server:



Fujitsu ServerView Setup

WebServer Destination Path

Choose WebServer Destination Path

WebServer Destination Path:

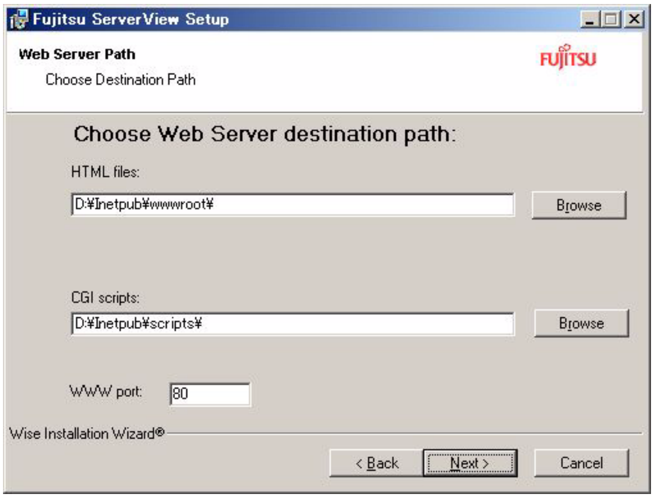
C:¥Program Files¥Fujitsu¥F5FBFE01¥ServerView Services¥WebSe

☑ Use SSL and Authentification

In some cases, Apache with SSL does not start correctly without a reboot. Therefore it is recommended to reboot the system after this installation.

Wise Installation Wizard®

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



Fujitsu ServerView Setup

Web Server Path

Choose Destination Path

Choose Web Server destination path:

HTML files: D:¥Inetpub¥wwwroot¥

CGI scripts: D:¥Inetpub¥scripts¥

WWW port: 80

Wise Installation Wizard®

POINT

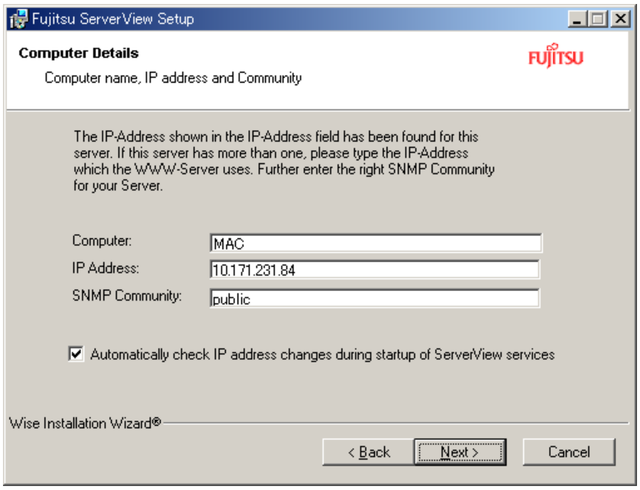
- When ServerView Web Server is selected from the [Select WebServer] window, the [Use SSL and authentication] checkbox appears.
  If the checkbox is selected, SSL connection is possible for connecting to the Web, and authentication will be requested when the connection is made.
  When this option is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

IMPORTANT

- Do not change the folder at the displayed location.
- 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 authentication, "svuser" is set as the user name and "fsc" as the password by default.
  For information on how to add or change the user name and password, see "● ServerView Web-Server and SSL" (→pg.408).

8 Click [Next].

The [Computer Details] window appears.



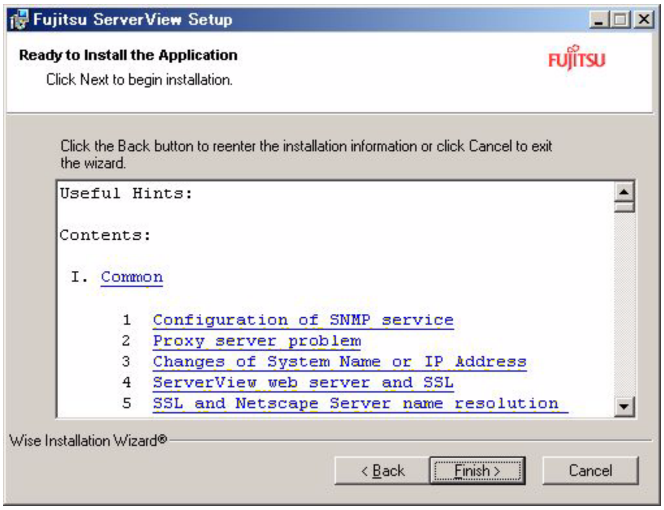
The IP-Address shown in the IP-Address field has been found for this server. If this server has more than one, please type the IP-Address which the WWW-Server uses. Further enter the right SNMP Community for your Server.

Computer: MAC
IP Address: 10.171.231.84
SNMP Community: public

☑ Automatically check IP address changes during startup of ServerView services

9 Click [Next].

The [Ready to Install the Application] window appears.


Fujitsu ServerView Setup
Ready to Install the Application
Click Next to begin installation.
FUJITSU
Wise Installation Wizard®
< Back
Finish >
Cancel

Click the Back button to reenter the installation information or click Cancel to exit the wizard.

```
Useful Hints:

Contents:

 I. Common

     1   Configuration of SNMP service
     2   Proxy server problem
     3   Changes of System Name or IP Address
     4   ServerView web server and SSL
     5   SSL and Netscape Server name resolution
```

10 Click [Next].

Installation starts.
When the installation is finished, the [Exit] window appears.

11 Click [Exit].

This completes the installation. After finishing the installation, see "2.4 Checking after Installation" (→pg.61) and make the settings required to operate ServerView.

2.3.2 [Windows] Installing the ServerView Agent (Servers to Be Monitored)

Install the ServerView Agent on the Windows server to be monitored.

IMPORTANT

- If you want to update the ServerView Agent, uninstall the ServerView Agent and install it again. For information on how to uninstall the ServerView Agent, see "B Uninstallation" (→pg.411).
- For a system on which a terminal server has been installed, the installation method is different from the usual methods. To install the ServerView Agent in a terminal server environment, perform step 3 below after clicking [Start] → [Control Panel] → [Add/Remove Programs] → [Add Program].
- When using ServerView on Windows 2003 R2, do not install the [Hardware Management] component in [Add or Remove Programs] → [Add or Remove Windows Components] → [Management and Monitoring Tools]. Uninstall the [Hardware Management] component beforehand if it is installed.

POINT

- When performing RAID monitoring (linked with RAID Manager) on the server to be monitored, AlarmService needs to be installed. In that case, install the ServerView Console or the ServerView AlarmService. For installation procedures, see the following:
  - Installation of the ServerView Console
    →"2.3.1 [Windows] Installing the ServerView Console" (pg.35)
  - Installation of the ServerView AlarmService
    →"2.3.3 [Windows] Installing the ServerView AlarmService (Servers to Be Monitored)" (pg.41)

1 Log in as administrator or as a user with Administrator privileges.

2 Exit all running applications.

3 Insert the PRIMERGY Document & Tool CD and start the following installer:

```
[CD-ROM Drive]:\Svmanage\WinSVAgent\Agents_setup.EXE
```

The [ServerView System Requirements] window appears.

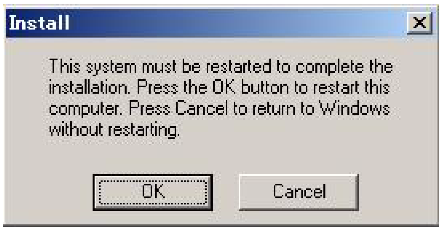
4 Click [OK].

The [ServerView Hints] window appears.

5 Click [OK].

When the installation is finished, the restart message appears.

6 Click [OK] or [Cancel].



Install

This system must be restarted to complete the installation. Press the OK button to restart this computer. Press Cancel to return to Windows without restarting.

After finishing the installation, see "2.4 Checking after Installation" (→pg.61) and make the settings required to operate ServerView.

2.3.3 [Windows] Installing the ServerView AlarmService (Servers to Be Monitored)

When performing RAID monitoring (linked with RAID Manager) on the Windows server to be monitored, the ServerView AlarmService needs to be installed.

IMPORTANT

- If you want to change or update the Web Server (Apache2 or IIS) after installing the ServerView AlarmService, uninstall the ServerView AlarmService and install it again. If ServerView has been automatically installed with ServerStart, the ServerView Console is installed and the ServerView Web Server is selected as the Web Server or IIS.
  For information on how to uninstall the ServerView Console, see "B Uninstallation" (→pg.411).
- For a system on which a terminal server has been installed, the installation method is different from the usual methods. To install ServerView in a terminal server environment, perform Step 3 below after clicking [Start] → [Control Panel] → [Add/Remove Programs] → [Add Program].
- If Java has not been installed before the ServerView AlarmService 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] to continue the installation. After installing the ServerView AlarmService, install Java.
- The ServerView AlarmService cannot be reinstalled if the ServerView Console has already been installed. Uninstall the currently installed the ServerView Console or the ServerView AlarmService, before reinstalling the ServerView AlarmService.
- If you have several different versions of ServerView, install the latest ServerView AlarmService.

POINT

- To use ServerView S2 or the ServerView Management Console on the server to be monitored, install the ServerView Console rather than the ServerView AlarmService. For how to install the ServerView Console, see "2.3.1 [Windows] Installing the ServerView Console" (→pg.35).

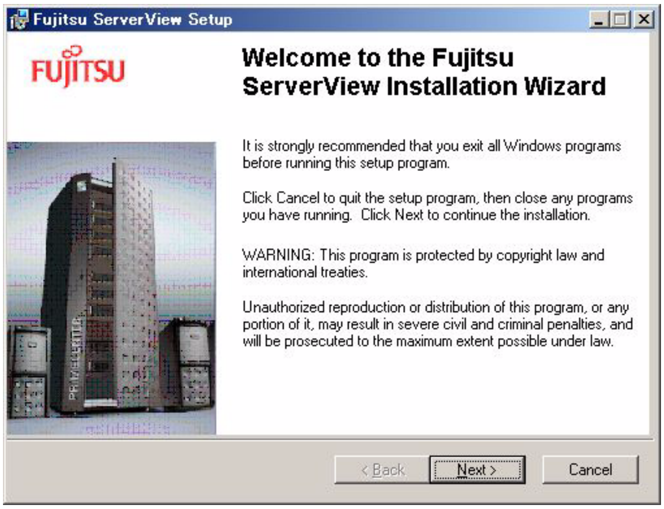
1 Log in as administrator or as a user with Administrator privileges.

2 Exit all running applications.

3 Insert the PRIMERGY Document & Tool CD and double-click the following installer:

[CD-ROM Drive]:\Svmanage\WinSVConsole\SV_AlarmSV.bat

The [Fujitsu ServerView Setup] window appears.



Welcome to the Fujitsu ServerView Installation Wizard

It is strongly recommended that you exit all Windows programs before running this setup program.

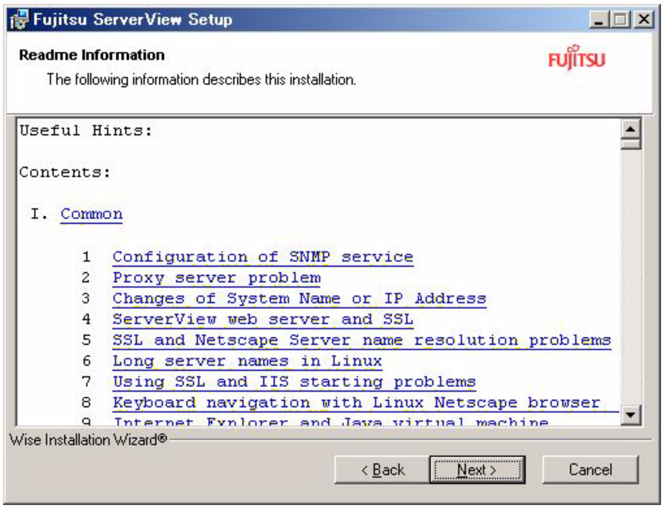
Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

4 Click [Next].

The [Readme Information] window appears.



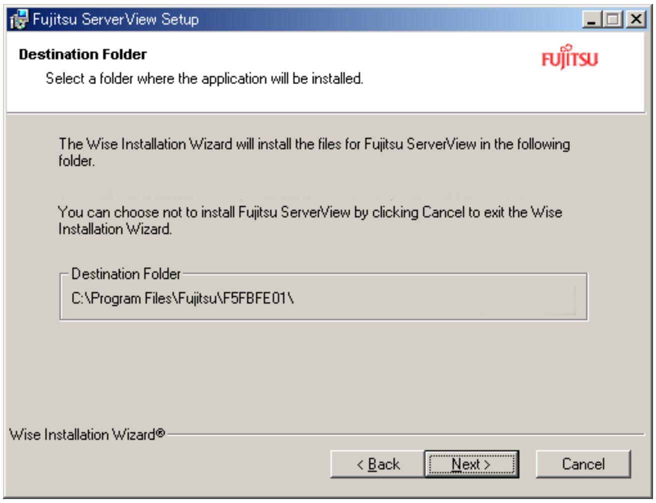
Readme Information

The following information describes this installation.

```
Useful Hints:

Contents:

 I. Common

      1  Configuration of SNMP service
      2  Proxy server problem
      3  Changes of System Name or IP Address
      4  ServerView web server and SSL
      5  SSL and Netscape Server name resolution problems
      6  Long server names in Linux
      7  Using SSL and IIS starting problems
      8  Keyboard navigation with Linux Netscape browser
      9  Internet Explorer and Java virtual machine
```

5 Click [Next].

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



Fujitsu ServerView Setup

Destination Folder

Select a folder where the application will be installed.

The Wise Installation Wizard will install the files for Fujitsu ServerView in the following folder.

You can choose not to install Fujitsu ServerView by clicking Cancel to exit the Wise Installation Wizard.

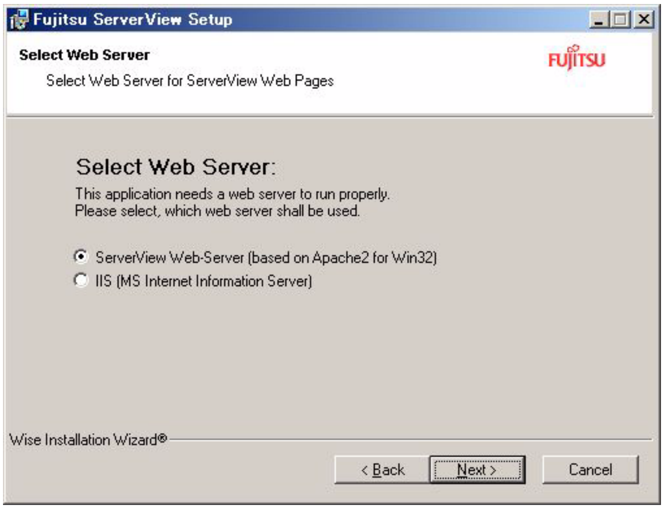
Destination Folder

C:\Program Files\Fujitsu\F5FBFE01\

6 Click [Next].

The [Select Web Server] window appears.

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



Fujitsu ServerView Setup

Select Web Server

Select Web Server for ServerView Web Pages

Select Web Server:

This application needs a web server to run properly.
Please select, which web server shall be used.

● ServerView Web-Server (based on Apache2 for Win32)

○ IIS (MS Internet Information Server)

IMPORTANT

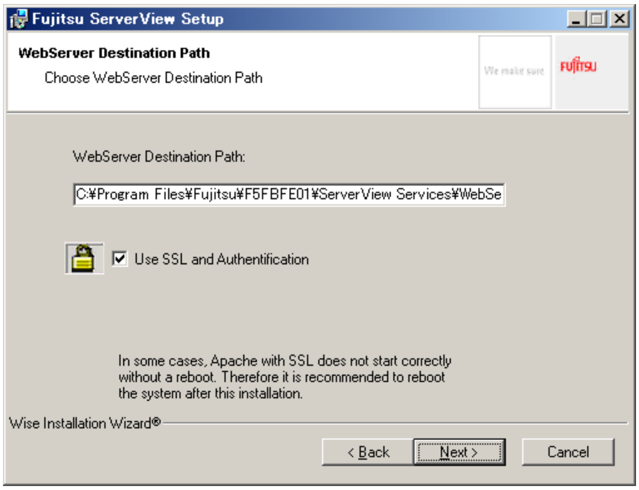
- When the ServerView Web Server is selected, the Apache2 for Win32-based Web Server is installed with ServerView. A task with the name "At**(**: task ID)" is added to the Windows Task Scheduler.
- When the IIS is selected, the installed IIS is used as the Web Server.
- When Apache2 has been already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

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

The [Web Server Destination Path] window appears.

The window varies depending on the selected Web Server.

When [ServerView Web Server] is selected as the Web Server:



Fujitsu ServerView Setup

WebServer Destination Path

Choose WebServer Destination Path

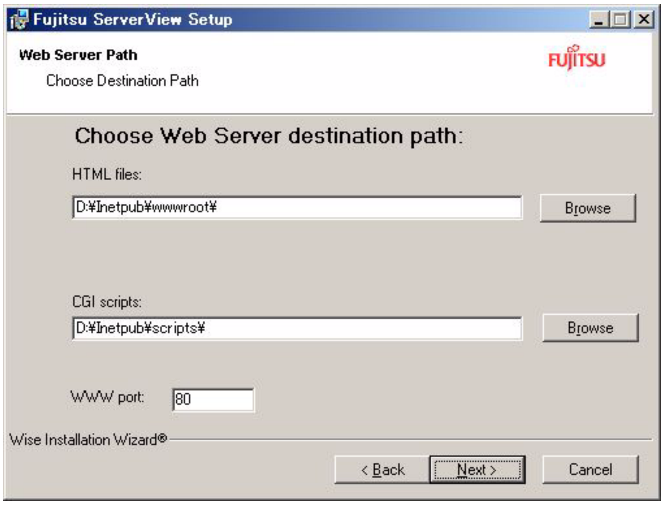
WebServer Destination Path:

C:¥Program Files¥Fujitsu¥F5FBFE01¥ServerView Services¥WebSe

☑ Use SSL and Authentification

In some cases, Apache with SSL does not start correctly without a reboot. Therefore it is recommended to reboot the system after this installation.

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



Fujitsu ServerView Setup

Web Server Path

Choose Destination Path

Choose Web Server destination path:

HTML files: D:¥Inetpub¥wwwroot¥

CGI scripts: D:¥Inetpub¥scripts¥

WWW port: 80

POINT

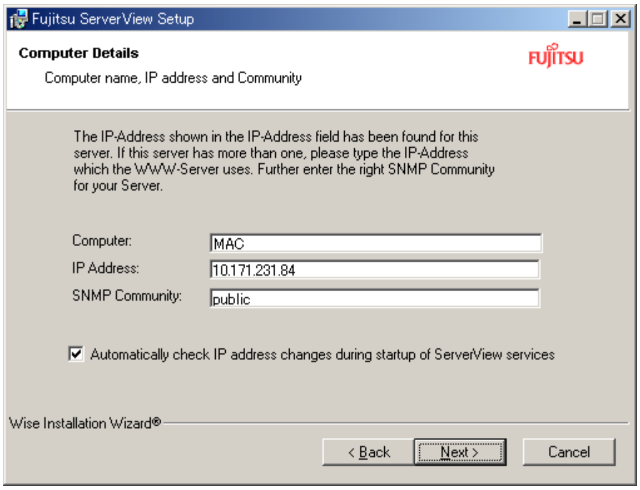
- When ServerView Web Server is selected from the [Select WebServer] window, the [Use SSL and authentication] checkbox appears.
  If the checkbox is selected, SSL connection is possible for connecting to the Web, and authentication will be requested when the connection is made.
  When this option is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

IMPORTANT

- Do not change the folder at the displayed location.
- 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 authentication, "svuser" is set as the user name and "fsc" as the password by default.
  For information on how to add or change the user name and password, see "● ServerView Web-Server and SSL" (→pg.408).

8 Click [Next].

The [Computer Details] window appears.



Computer Details

Computer name, IP address and Community

The IP-Address shown in the IP-Address field has been found for this server. If this server has more than one, please type the IP-Address which the WWW-Server uses. Further enter the right SNMP Community for your Server.

Computer: MAC

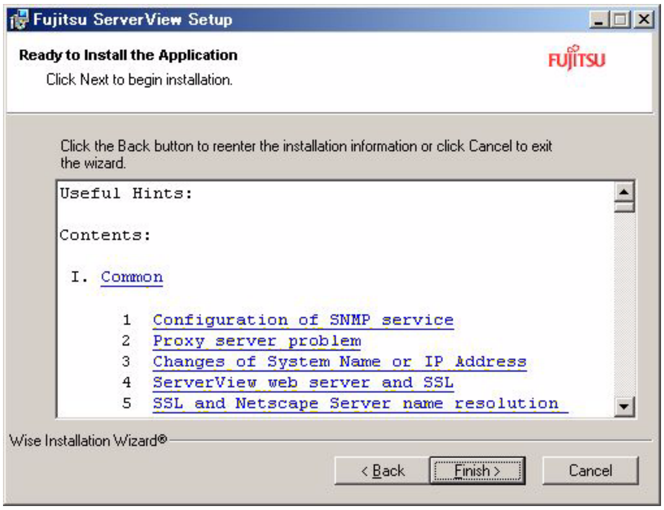
IP Address: 10.171.231.84

SNMP Community: public

☑ Automatically check IP address changes during startup of ServerView services

9 Click [Next].

The [Ready to Install the Application] window appears.



Ready to Install the Application

Click Next to begin installation.

Click the Back button to reenter the installation information or click Cancel to exit the wizard.

```
Useful Hints:

Contents:

 I. Common

        1  Configuration of SNMP service
        2  Proxy server problem
        3  Changes of System Name or IP Address
        4  ServerView web server and SSL
        5  SSL and Netscape Server name resolution
```

10 Click [Next].

Installation starts.
When the installation is finished, the [Exit] window appears.

11 Click [Exit].

This completes the installation. After finishing the installation, see "2.4 Checking after Installation" (→pg.61) and make the settings required to operate ServerView.

2.3.4 [Linux] Installing ServerView Linux Agent

Install ServerView Linux (only ServerView Linux Agent) on the Linux server to be monitored.
There are two ways to install ServerView Linux:

- Installation using the installation script (→pg.55)
- Manual installation (→pg.57)
  If you have problems with the installation when using the installation script, or if you need to reinstall without modifying the snmpd.conf configuration, install ServerView Linux manually.

POINT

- 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.
- Even if ServerView S2/AlarmService is not installed, the server to be monitored (the ServerView Linux Agent) can be monitored from the Windows Management Console.
- When performing RAID monitoring (linked with RAID Manager) on the server to be monitored, AlarmService needs to be installed. In that case, install ServerView Linux referring to the procedures in "2.3.5 [Linux] Installing ServerView Linux Console" (→pg.54).

IMPORTANT

- When installing ServerView Linux using the installation script, the SNMP service needs to be started in advance. Execute the following command to confirm that the SNMP service has been started.

```
# /etc/init.d/snmpd status
```

If the service has been started successfully, the following message is displayed:

- For Red Hat Linux

```
snmpd (pid xxxx) is running...
```

- For SUSE Linux

```
Checking for service snmpd : running
```

If it is not started, execute the following command:

```
# /etc/init.d/snmpd start
```

■ Installing ServerView Linux Agent Using the Installation Script

The installation script on the PRIMERGY Document & Tool CD allows you to install ServerView Linux Agent and edit the SNMP service configuration file (snmpd.conf).

During reinstallation, using the installation script will not change the snmpd.conf settings. If any changes are neccessary, make sure to edit snmpd.conf before running the installation script.
If the installation script terminates with an error message displayed, see "A.1 Troubleshooting of Installation Script" (→pg.388).

POINT

- The path to the SNMP service configuration file (snmpd.conf) may vary depending on the OS.
  - Red Hat Linux: /etc/snmp/snmpd.conf
  - SUSE Linux: /etc/snmpd.conf
- The snmpd.conf file can also be edited manually after the installation of ServerView.
  If the file is edited manually, execute the following command:
  /etc/init.d/snmpd restart

IMPORTANT

For Red Hat Linux

- The snmpd.conf file may also exist in the /usr/share/snmp directory.
  The snmpd service also loads the configuration in /usr/share/snmp/snmpd.conf.
  Edit /usr/share/snmp/snmpd.conf if necessary.
- When "SELINUX" is "Enabled" for RHEL-AS4/ES4(x86) or RHEL-AS4/ES4(EM64T), follow the procedures below to set it to "Disabled" before installation.
  Change the following value in the "/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 a superuser and insert the PRIMERGY Document & Tool CD, and then execute the following commands.

- For Red Hat Linux

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
LinuxSVAgent/
# ./insagt
```

- For SUSE Linux

```
# mount /media/cdrom/ or /media/dvd/
# cd /media/cdrom/ or /media/dvd/Svmanage/LinuxSVAgent/
# ./insagt
```

● Entering the SNMP Trap Destination IP Address

When installing ServerView Linux for the first time using the installation script, after the title of installation script is displayed, you will be prompted to enter the SNMP trap destination IP address. If ServerView Linux Agent has been already installed, you will be prompted to enter the SNMP trap destination IP address after the uninstallation is done.

Enter the IP address to which you want to send SNMP traps and press the [Enter] key.
It is not necessary to re-enter the server's own IP address (127.0.0.1) since it is set automatically. If you want to send the traps to multiple devices, enter the IP address for each device. The IP address entered is written into snmpd.conf.
Enter the IP address and press the [e] key. Go to the steps below.
The following is an example of the output result.

```
ServerView Console install script version V1.0
Copyright(C) FUJITSU LIMITED 2006

Install in Red Hat Linux system.

checking necessary RPMs ...
RPMs check [OK]

available disk space check [OK]
(Uninstallation is performed if ServerView Linux was already installed)

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

When installing ServerView Linux for the first time using the installation script, you will be prompted to enter the server location.
The entered location is written to the syslocation item in snmpd.conf and will be shown as a "Location" among the server properties in ServerView.
Up to 64 bytes can be entered.
Enter the location and press the [Enter] key. Go to the steps below.
If 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)
```

POINT

- If the server is equipped with an LCD panel, the location information that is input here is displayed on the LCD panel. When the location is not input, it is displayed as “Unknown”.

● Entering the Administrator

When installing ServerView Linux for the first time using the installation script, you will be prompted to enter the server administrator.
The entered administrator name is written to the syscontact item in snmpd.conf and will be shown as an "Administrator" among the server properties in ServerView.
Up to 64 bytes can be entered.
Enter the administrator name and press the [Enter] key. Go to the steps below.
If 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 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 Server View modules for 2.4.21-32.EL
copa(Ok) ipmi(Ok) smbus(Ok) [  OK  ]
Loading Server View modules: copa ipmi smbus [  OK  ]
1807

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

install srvmagt-agents, please wait...
Stopping snmpd: [  OK  ]
Starting snmpd: [  OK  ]
Starting snmpd: [  OK  ]
Starting agent scagt[  OK  ]
Starting agent sc2agt[  OK  ]
Starting agent busagt[  OK  ]
Starting agent hdagt[  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 thragt[  OK  ]
Starting agent vvagt[  OK  ]

Collecting Inventory data, please wait...
Executing...                #################################### [done]

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

● Checking the 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.
```

If the above message is not displayed, see "A.1 Troubleshooting of Installation Script" (→pg.388). When the above message is displayed, execute the following commands to unmount and eject the PRIMERGY Document & Tool CD, and then follow the steps in "2.4.7 [Linux] Setting Each Service (When Installing Only ServerView Linux Agent on the Server to Be Monitored)" (→pg.76).

- For Red Hat Linux

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

- For SUSE Linux

```
# cd
# umount /media/cdrom/ or /media/dvd/
```

Remove the PRIMERGY Documents & Tools CD and follow the steps in "2.4.6 [Linux] Setting Each Service (for Servers to Be Monitored)" (→pg.70).

■ Installing ServerView Linux Agent 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.

Referring to "1.3 System requirements" (→pg.19), 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.

- For Red Hat Linux

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
LinuxSVAgent/
# ./chksys
```

- For SUSE Linux

```
# mount /media/cdrom/ or /media/dvd/
# cd /media/cdrom/ or /media/dvd/Svmanage/LinuxSVAgent/
# ./chksys
```

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

```
RPMs check [OK]
```

If an error message about a missing RPM package is displayed, install the package from the Red Hat Linux or SUSE Linux CD-ROM.

3 If the ServerView Linux Agent is already installed, uninstall ServerView.

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

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

4 Create a backup file of snmpd.conf.

Execute the following command.

- For Red Hat Linux

```
# ls /etc/snmp/
```

- For SUSE Linux

```
# ls /etc/
```

Only execute the following command if the file snmpd.conf.org does not exist.

- For Red Hat Linux

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

- For SUSE Linux

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

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

From the CD-ROM, copy snmpd.conf in which the default values have been set.
Execute the following commands.

- For Red Hat Linux

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

- For SUSE Linux

```
# mount /media/cdrom/ or /media/dvd/
# cd /media/cdrom/ or /media/dvd/Svmanage/LinuxSVAgent/Agent/
snmpd.conf
# chmod 644 /etc/snmpd.conf
```

6 Edit snmpd.conf.

Edit the following items in snmpd.conf.

For details about snmpd.conf, see the comments in snmpd.conf.

table: snmpd Items

Item	Settings
com2sec	Add the setting example below into the item com2sec. • com2sec svSec default public • com2sec svSec localhost public • com2sec svSec *** public Assign one of the following values to ***. • default: Allows access from all servers/clients. • localhost: Allows access from own server. • <IP address>: Allows access from a specific server/client. • <subnet>/<netmask>: Allows access from a specific network.
trapsink	Add the setting example below into the item trapsink. • trapsink 127.0.0.1 public • trapsink <IP address> public Specify the IP address to which you want to send SNMP traps. 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 traps to multiple devices, enter the different IP addresses in multiple lines with the same form.
syslocation	Add the setting example below into the item syslocation. • syslocation computer room L200 Enter the server location (installation location). It will be shown as a "Location" among the server properties in ServerView.
syscontact	Add the setting example below into the item syscontact. • syscontact Your name Enter the server administrator name. It will be shown as an "Administrator" among the server properties in ServerView.

IMPORTANT

- To reflect the changes of snmpd.conf, you need to execute the following command:
  /etc/init.d/snmpd restart

7 Execute the RPM commands.

- For Red Hat Linux

```
# /etc/init.d/snmpd restart
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
LinuxSVAgent/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
(XX indicates the version number.)
```

- For SUSE Linux

```
# /etc/init.d/snmpd restart
# cd /media/cdrom/ or /media/dvd/Svmanage/LinuxSVAgent/Agent
# rpm -i srvmagt-mods_src-X.XXXX.suse.rpm
# rpm -i srvmagt-eecd-X.XXXX.suse.rpm
# rpm -i srvmagt-agents-X.XXXX.suse.rpm
(XX indicates the version number.)
```

8 Verify the execution result of the RPM command.

To verify whether the installation has been properly done, execute the following commands. 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-eecd
srvmagt-eecd-X.XX-XX

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

9 Set the default setting of ServerView Linux Agent.

Execute the following commands.

- For Red Hat Linux

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

- For SUSE Linux

```
# groupadd svuser
# cd /media/cdrom/ or /media/dvd/Svmanage/LinuxSVAgent/Agent/config
/etc/
srvmagt/config
# chmod 644 /etc/srvmagt/config
# cd /
# /etc/init.d/srvmagt stop
# /etc/init.d/eecd stop
# /etc/init.d/eecd start
# /etc/init.d/srvmagt start
```

10 Makes the settings after installation.

Execute the following commands.

- For Red Hat Linux

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

- For SUSE Linux

```
# cd
# umount /media/cdrom/ or /media/dvd/
```

Remove the PRIMERGY Document & Tool CD and follow the steps in "2.4.7 [Linux] Setting Each Service (When Installing Only ServerView Linux Agent on the Server to Be Monitored)" (→pg.76).

■ Checking the RPM Version

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

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

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

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

2.3.5 [Linux] Installing ServerView Linux Console

Install ServerView Linux (ServerView S2/AlarmService) on the Linux server to be monitored.
To install the ServerView S2 and the Linux version of the AlarmService at the same time, perform the following steps.
When ServerView S2/AlarmService is installed on a server in a Linux-only environment, the status of other servers can be monitored.

POINT

- If you want to install only the ServerView Linux Agent (without ServerView S2/AlarmService) on the Linux server to be monitored, see "2.3.4 [Linux] Installing ServerView Linux Agent" (→pg.46).
  If ServerView S2/AlarmService is installed but not used, the following packages (RPM) need not to be installed.
  - Red Hat Linux: httpd, openssl, mod_ssl
  - SUSE Linux: apache2, openssl

IMPORTANT

- When ServerView S2 and AlarmService are installed, atd service needs to be running. Start the atd service before installation, and stop the atd service after installation. Perform the following procedure to confirm whether atd has been started and start the service:
  - For Red Hat Linux

    When not started

```
# /etc/init.d/atd status
atd is stopped
```

Starting

```
# /etc/init.d/atd start
Starting atd :          [OK]
# /etc/init.d/atd status
atd (pid xxxxxx) running....
```

Stopping

```
# /etc/init.d/atd stop
Stopping atd :          [OK]
# /etc/init.d/atd status
atd is stopped
```

- For SUSE Linux

  When not started

```
# /etc/init.d/atd status
Checking for at daemon :      unused
```

Starting

```
# /etc/init.d/atd start
Starting service at daemon    done
# /etc/init.d/atd status
Checking for at daemon :      running
```

Stopping

```
# /etc/init.d/atd stop
Shutting down service at daemon    done
# /etc/init.d/atd status
Checking for at daemon :           unused
```

▶ This document describes how to install the ServerView Linux 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 it to "Disabled" before installation.
Change the following value in the "/etc/selinux/config" file, and restart the server.

- (Before edit) SELINUX=enforcing
- (After edit) SELINUX=disabled

■ Installing ServerView Linux Console with the Installation Script

The installation script on the PRIMERGY Document & Tool CD allows you to install the ServerView S2/AlarmService.

If the installation script terminates with an error message displayed, see "A.1 Troubleshooting of Installation Script" (→pg.388).

POINT

▶ The path to the SNMP service configuration file (snmpd.conf) may vary depending on the OS.

- Red Hat Linux: /etc/snmp/snmpd.conf
- SUSE Linux: /etc/snmpd.conf

▶ The snmpd.conf file can also be edited manually after the installation of ServerView.
If the file is edited manually, execute the following command:
/etc/init.d/snmpd restart

● How to Start the Installation Script

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

- For Red Hat Linux

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

- For SUSE Linux

```
# mount /media/cdrom/ or /media/dvd/
# cd /media/cdrom/ or /media/dvd/Svmanage/Linux/LinuxSVConsole/
# ./inssv
```

The following is an example of the output result.

```
ServerView install / RPM control script version V1.2
Copyright(C) FUJITSU LIMITED 2006

Install in Red Hat Linux system.

checking necessary RPMs ...
RPMs check [OK]

install Alarm Service, please wait...
Stopping trpsrvd:  [OK]

Starting  sv_fwdserver ...
job 118 at 2006-07-20 15:58
Starting snmptrapd:  [OK]
Starting trpsrvd:  [OK]

install ServerView_S2, please wait...

Starting  sv_ainit ...
job 119 at 2006-07-20 15:59
```

● Checking the Execution Result

When the ServerView S2/AlarmService has been successfully installed, the following successful completion message is displayed on the last line.

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

If the above message is not displayed, see "A.1 Troubleshooting of Installation Script" (→pg.388).
When the above message is displayed, execute the following commands to unmount and eject the PRIMERGY Document & Tool CD, and then follow the steps in "2.4.6 [Linux] Setting Each Service (for Servers to Be Monitored)" (→pg.70).

- For Red Hat Linux

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

- For SUSE Linux

```
# cd
# umount /media/cdrom/ or /media/dvd/
```

■ Installing ServerView Linux Console Manually

● For Red Hat Linux

1 Check the operation environment.

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

IMPORTANT

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

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

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

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

```
# rpm -q net-snmp
# rpm -q net-snmp-utils
# rpm -q compat-libstdc++
# rpm -q httpd
# rpm -q gnome-libs
# rpm -q rpm
# rpm -q gawk
# rpm -q openssl
# rpm -q mod_ssl
# rpm -q at
```

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 the Red Hat Linux CD-ROM.

3 Execute the RPM commands.

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
LinuxSVConsole/Console
# ./InstallAlarmService.sh AlarmServiceStarter-X.X-X.i386.rpm
# ./InstallServerView_S2.sh ServerView_S2Starter-X.X-X.i386.rpm
(XX indicates the version number.)
```

4 Verify the execution result of the RPM command.

To verify whether the installation has been done correctly, execute the following commands. 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 indicates the version number.)
```

5 Edit the httpd service configuration file.

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

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

IMPORTANT

- When ServerView S2/Alarm Service is used under Linux, use Apache provided on the Red Hat CD-ROM as the Web Server and use the default settings for DocumentRoot/ServerRoot.
If 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 http.conf.

The above step is not required when only ServerView Linux Agent is 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>
#
```

6 Restart the httpd service.

Enter the following command and restart the httpd service.

```
# /etc/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, see "● Auto-Start Setting of the SNMP and httpd Services" (→pg.71).

8 Set the firewall.

See "■ Configuring the Firewall" (→pg.76).

● For SUSE Linux

1 Check the operation environment.

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

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

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

```
# rpm -q net-snmp
# rpm -q apache2
# rpm -q rpm
# rpm -q gnome-libs
# rpm -q gawk
# rpm -q openssl
# rpm -q at
```

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 SUSE Linux CD-ROM.

3 Execute the RPM commands.

```
# mount /media/cdrom/ or /media/dvd/
# cd /media/cdrom/ or /media/dvd/Svmanage/LinuxSVConsole/Console
# ./InstallAlarmService.sh AlarmServiceStarter-X.X-X.i386.rpm
# ./InstallServerView_S2.sh ServerView_S2Starter-X.X-X.i386.rpm
(XX indicates the version number.)
```

4 Verify the execution result of the RPM command.

To verify whether the installation has been properly done, execute the following commands. 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 indicates the version number.)
```

5 Restart the apache2 service.

Enter the following command and restart the apache2 service.

```
# /etc/init.d/apache2 restart
```

6 Set the auto start of the apache2 service.

Use the chkconfig command to set the auto start of the apache2 service.

For details about the chkconfig command, see "● Auto-Start Setting of the SNMP and apache2 Services" (→pg.75).

7 Set the firewall.

See "■ Configuring the Firewall" (→pg.76).

2.4 Checking after Installation

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

The settings vary depending on the OS.

- For Windows:
  - Installing Microsoft Internet Explorer (→pg.62)
  - Installing Java™ 2 Runtime Environment Standard Edition (→pg.63)
  - Setting an administrative user (→pg.65)
  - Registering the interrupt information of optional devices (→pg.67)
  - Extending Web service (when IIS is selected as the Web Server on Windows 2003, →pg.69)
- For Linux:
  - Installing Mozilla 1.3 or later, or Mozilla FireFox 1.0.4 or later (→pg.62)
  - Installing Java™ 2 Runtime Environment Standard Edition (→pg.63)
  - Registering the interrupt information of optional devices (→pg.67)
  - Setting each service (for the server to be monitored, →pg.70)
  - Setting each service (when installing only the ServerView Linux Agent on the server to be monitored, →pg.76)

POINT

- If the server's computer name or IP address has been changed after the installation, make these settings referring to "2.4.8 Changing Computer Information after Installation" (→pg.80).
- 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 where ServerView is to be used.

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

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

- The server or PC on which the ServerView Console is installed
- The server or PC that shows the server monitoring window of ServerView S2
- The server or PC that shows the RSB Web interface window

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

1 Launch Microsoft Internet Explorer.

2 Select [Internet Options...] from the [Tools] menu.

3 Click the [Security] tab and select [Local intranet] or [Trusted sites].

4 Click [Sites] to add the following URLs (http:// server IP address).

For the server where the ServerView Console is installed:

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

For the server that shows the server monitoring window of ServerView S2:

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

For the server that shows the RSB Web interface window:

- The URL set in 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.

- The server on which ServerView Linux is installed
- The server or PC that shows the server monitoring window of ServerView S2
- The server or PC that shows 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 where ServerView is to be used.
The installer of Java™ 2 Runtime Environment Standard Edition is included on the PRIMERGY Document & Tool CD. However, the stored Java version may be incompatible with the Web browser depending on the browser version. The following method for setting the Linux browser (Mozilla) plugin is provided as an example, however, the setting contents (the Java Plugin directory path) vary depending on the browser version. Please check the compatibility of your browser and OS in advance.

● **For Windows:**

- The server or PC on which the ServerView Console is installed
- The server or PC that uses the Web browser to show the server monitoring window of ServerView S2
- The server or PC that shows the RSB Web interface window

● **For Linux**

- The server on which ServerView Linux is installed
- The server or PC that uses the Web browser to show the server monitoring window of ServerView S2
- The server or PC that shows the RSB Web interface window

■ Installation Steps

● **For Windows:**

1 Insert the PRIMERGY Document & Tool CD and start the either one of the following installers (xx indicates the version number.)
[CD-ROM drive]:\Svmanage\WinSVConsole\Tools\Jre\j2re-x_x_x_xx-windows-i586-p.exe
[CD-ROM drive]:\Svmanage\WinSVConsole\Tools?jre-x_x_x_xx-windows-i586-p.exe

● For Linux

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

For Red Hat Linux

POINT

- Below are examples of the folder name for "your browser's folder" in the following procedure.
  •Mozilla: /usr/lib/mozilla-x.x.x
  •Firefox: /usr/lib/firefox-x.x.x

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder
# cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
LinuxSVConsole/Tools/Jre/
# rpm -iv j2re-x_x_x_xx-linux-i586.rpm
Or... # rpm -iv jre-x_x_x_xx-linux-i586.rpm
# cd /your browser's folder/plugins
# ls

When the file libjavaplugin_oji.so already exists:
# rm -fr /your browser's folder/plugins/libjavaplugin_oji.so
If your browser is Mozilla:or Mozilla FireFox:
# ln -s /usr/java/j2re1.x.x_xx/plugin/i386/ns610-gcc32/
libjavaplugin_oji.so
Or... # ln -s /usr/java/jre1.x.x_xx/plugin/i386/ns7/
libjavaplugin_oji.so
# cd
# umount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder
(XX indicates the version number.)
```

IMPORTANT

- The java (jre) plugin for EM64T is not provided.
  For this reason, java cannot be plugged in to Firefox or Mozilla. Use another PC browser to display the ServerView S2 screen or the alarm setting screen of AlarmService.
- When using Java™ 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 procedure.

```
# mount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/
# cp /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/
LinuxSVConsole/Tools/Font/font.properties.ja_JP /usr/java/
j2re1.4.2_08/lib
# umount /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder
```

For SUSE Linux

POINT

- Below are examples of the folder name for "your browser's folder" in the following procedure.
  •Mozilla: /opt/mozilla/lib/

```
# mount /media/cdrom/ or /media/dvd
# cd /media/cdrom/ or /media/dvd/Svmanage/LinuxSVConsole/Tools/
Jre/
# rpm -iv j2re-x_x_x_xx-linux-i586.rpm
Or... # rpm -iv jre-x_x_x_xx-linux-i586.rpm
# cd /your browser's folder/plugins
# ls

When the file libjavaplugin_oji.so already exists:
# rm -fr /your browser's folder/plugins/libjavaplugin_oji.so
# ln -s /usr/java/j2re1.x.x_xx/plugin/i386/ns610-gcc32/
libjavaplugin_oji.so
Or... # ln -s /usr/java/jre1.x.x_xx/plugin/i386/ns7/
libjavaplugin_oji.so
# cd
# umount /media/cdrom/ or /media/dvd
(XX indicates the version number.)
```

2.4.3 Setting an Administrative User

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

POINT

- An administrative user in ServerView means a user who belongs to the "FUJITSU SVUSER" group.
- In Windows 2003, Administrative privileges are not given if the password is not set for the administrative user account. Be sure to set the password.
- Even when a "global" group is added to the FUJITSU SVUSER group, administrative privileges are not given to the users in the added group. Add only users to the FUJITSU SVUSER group.
- If an administrative user is set for another group than SVUSER, the logon immediately after starting the program may fail. In this case, click [Cancel] to exit the logon window. Then, set the logon settings again on 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 settings 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 user 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 the "Administrators" and "FUJITSU SVUSER" groups, and click [OK].

Hold down the [Ctrl] key for multiple selections.
The [Select Groups] window appears again.

14 Click [OK].

The display returns to the user [Properties] window.
Confirm that "Administrators" and "FUJITSU SVUSER" are added to [Member of], and click [OK].

15 Click [OK].

Close the [Computer Management] window.

■ For Linux:

See "■ Settings for Enabling ASR Configuration, Shutdown, and Restart from the ServerView Console" (→pg.79) for the settings.

2.4.4 Registering the Interrupt (MIB) Information of Optional Devices

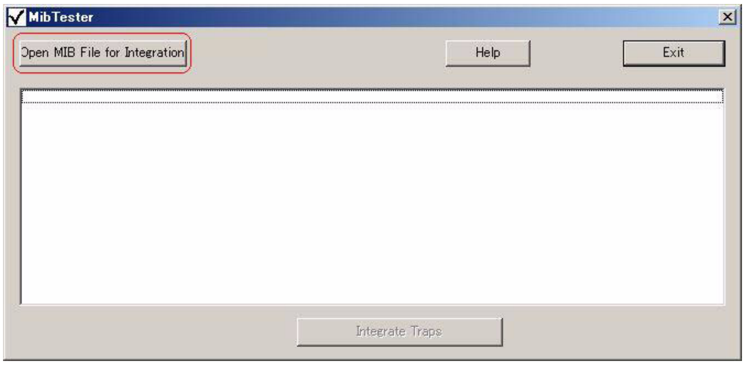
Register the interrupt (MIB) information of optional devices on the management server or PC.

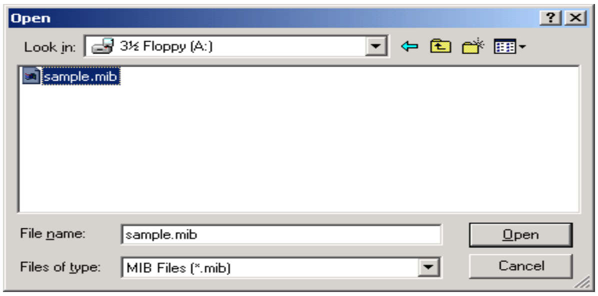
■ For Windows:

1 Click [Start] → [Programs] → [Fujitsu ServerView] → [MIB Integrator].

The process of interrupt information registration starts, and the [Mib Tester] window opens.

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

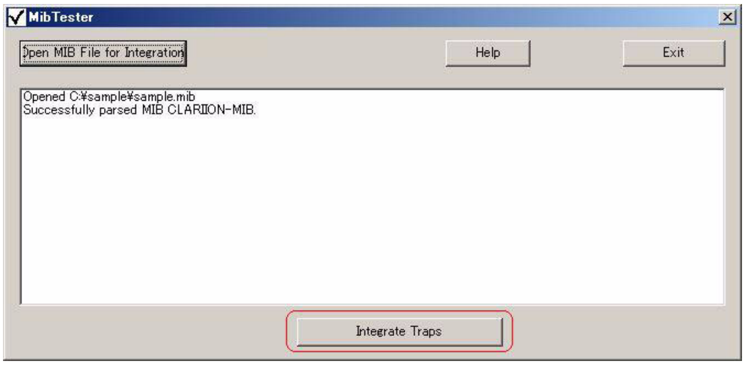




File name: sample.mib

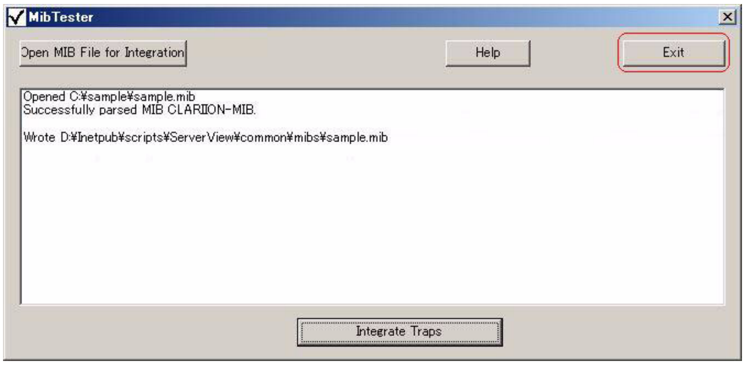
Files of type: MIB Files (*.mib)

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



Opened C:¥sample¥sample.mib
Successfully parsed MIB CLARIION-MIB.

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



Opened C:¥sample¥sample.mib
Successfully parsed MIB CLARIION-MIB.

Wrote D:¥Inetpub¥scripts¥ServerView¥common¥mibs¥sample.mib

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.

For Red Hat Linux

/var/www/cgi-bin/ServerView/SnmpTrap/mibs

For SUSE Linux

/srv/www/cgi-bin/ServerView/SnmpTrap/mibs

2 Enter the following command and restart the Fujitsu Alarm Service.

```
#/etc/init.d/sv_fwdserver restart
```

IMPORTANT

- When replacing the currently registered mib file, pay attention to the difference between upper and lower case in the mib file name. If the file is improperly registered, it will be registered as a new mib file.

■ When Using ServerView S2

For details on operation, see "3.1.5 Registering MIB (MIB INTEGRATION)" (→pg.95).

IMPORTANT

- For ServerView S2 running under Linux, MIB registration is not supported.
  When using Linux, perform the procedure to copy the MIB file (See "■ For Linux:" (→pg.68)).

2.4.5 Extending the Web Service

If the ServerView Console has been installed on Windows 2003 and IIS has been selected as 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 [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 When all files have been added, 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 Servers to Be Monitored)

■ For Red Hat Linux

● Editing the httpd Service Configuration File

1 Edit /etc/httpd/conf/httpd.conf.

Edit the ServerName directive in the file /etc/httpd/conf/httpd.conf (the Apache HTTP server configuration file).
For details about the ServerName directive, see the Red Hat Linux manuals and the comments in httpd.conf.

IMPORTANT

- When ServerView S2/Alarm Service is used in Linux, use Apache provided on the Red Hat CD-ROM as a Web Server and use the default settings for DocumentRoot/ServerRoot.
If 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 http.conf.

The above step is not required when only ServerView Linux Agent is installed.

```
# "/var/www/cgi-bin" should be changed to whatever your Scrip-
tAliased
# 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>
#
```

2 Restart the httpd service.

Enter the following command and restart the httpd service.

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

● Auto-Start Setting of the SNMP and httpd Services

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
```

● Configuring the Firewall

POINT

- Firewall settings are only necessary if you use a firewall.
  If no firewall is used, the following settings are not required.

The firewall is configured when installing Linux or by using the setup command.
This section describes the configuration using the setup command.
The windows are different when setting the firewall during the Linux installation and when executing the setup command; the setting items, however, are the same. For details about how to configure the firewall during the Linux installation, see the Red Hat Linux manuals and the following set up method.

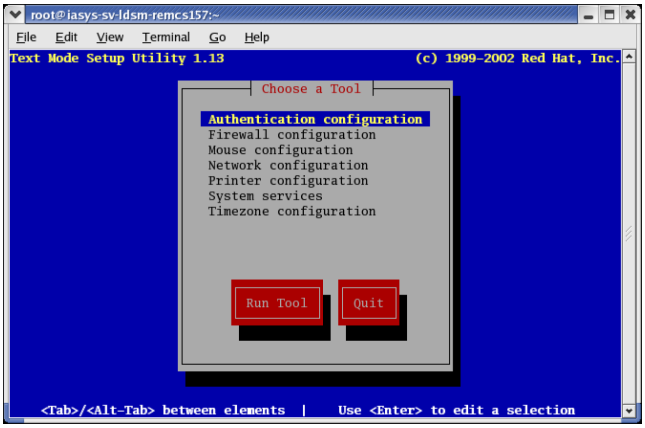
IMPORTANT

- The firewall setting below is required in order for ServerView to operate.
  For details about the firewall settings, see the Red Hat Linux manuals.

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

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

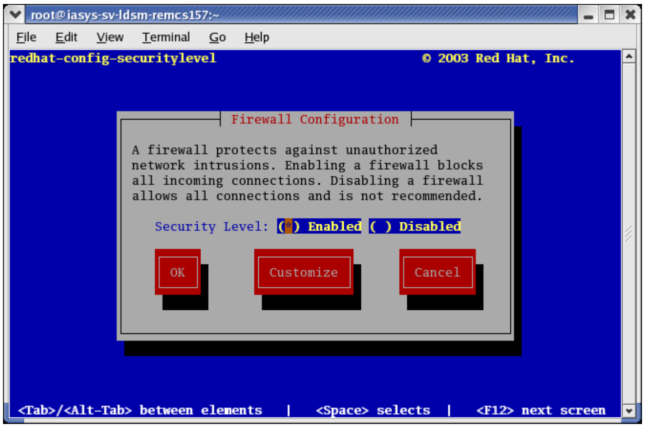
The menu window appears.


root@iasys-sv-ldsm-remcs157:~
File Edit View Terminal Go Help
Run Tool
Quit

```
Text Mode Setup Utility 1.13                    (c) 1999-2002 Red Hat, Inc.

                   Choose a Tool

             Authentication configuration
             Firewall configuration
             Mouse configuration
             Network configuration
             Printer configuration
             System services
             Timezone configuration

  <Tab>/<Alt-Tab> between elements   |   Use <Enter> to edit a selection
```

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

The [Firewall Configuration] window appears.


root@iasys-sv-ldsm-remcs157:~
File Edit View Terminal Go Help
OK
Customize
Cancel

```
redhat-config-securitylevel                      © 2003 Red Hat, Inc.

                   Firewall Configuration

        A firewall protects against unauthorized
        network intrusions. Enabling a firewall blocks
        all incoming connections. Disabling a firewall
        allows all connections and is not recommended.

           Security Level: (*) Enabled ( ) Disabled

 <Tab>/<Alt-Tab> between elements   |   <Space> selects   |   <F12> next screen
```

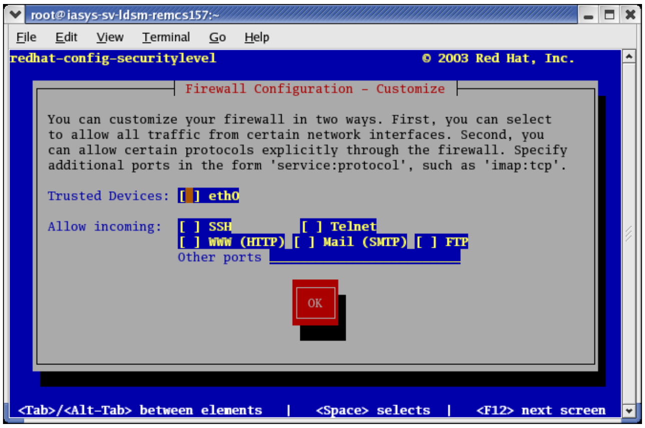
3 Add a [*] mark to "Enabled", use the [Tab] key to move the cursor to [Customize], and then press the [Enter] key.

The [Firewall Configuration - Customize] window appears.

IMPORTANT

- When "Disabled" is selected here, the settings below are not required.

4 Set the protocols to use.


root@iasys-sv-ldsm-remcs157:~
File Edit View Terminal Go Help

```
redhat-config-securitylevel                          © 2003 Red Hat, Inc.

        ┤ Firewall Configuration - Customize ├

  You can customize your firewall in two ways. First, you can select
  to allow all traffic from certain network interfaces. Second, you
  can allow certain protocols explicitly through the firewall. Specify
  additional ports in the form 'service:protocol', such as 'imap:tcp'.

  Trusted Devices: [ ] eth0

  Allow incoming:  [ ] SSH          [ ] Telnet
                   [ ] WWW (HTTP) [ ] Mail (SMTP) [ ] FTP
                   Other ports ________________________

                              OK

 <Tab>/<Alt-Tab> between elements   |   <Space> selects   |   <F12> next screen
```

Set the protocols below.

1. Select "WWW (HTTP)".

   Add a [*] 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 move the cursor to [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 move the cursor to [OK] and press the [Enter] key.

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

7 Edit the packet filtering setting.

Edit /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
```

8 Reflect the packet filtering setting.

Execute the following command.

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

● Settings for Enabling ASR Configuration, Shutdown, and Restart from the ServerView Console

To perform ASR (Automatic Server Reconfiguration & Restart) settings, including fan/temperature/restart, or to turn the power on/off from the Management Console, you will be asked to enter the user name and the password of an administrative user.
Follow the steps below to set an administrative user.

IMPORTANT

- An administrative user in ServerView means a user who belongs to the "svuser" group.
  The "svuser" group is automatically created when ServerView is installed with the 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 in the G option of the useradd command.
  For <user name>, specify a name for 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 newly created user name is enabled when the password is set.
- For details about each command, see the useradd (8) and passwd (1) man page.

2 Set the existing user as an administrative user.

Contact the system administrator to check whether the existing user to be set belongs to multiple groups and then 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,<user group,...> <user name>
```

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

For SUSE Linux

Auto-Start Setting of the SNMP and apache2 Services

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

```
# /sbin/chkconfig apache2 on
# /sbin/chkconfig snmpd on
```

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

```
#/sbin/chkconfig --list |grep apache2
  apache2 0:off 1:off 2:off 3:on 4:off 5:on 6:off
#/sbin/chkconfig --list |grep snmpd
  snmpd 0:off 1:off 2:on 3:on 4:off 5:on 6:off
```

Configuring the Firewall

Open the SuSE Firewall2 configuration window in the following sequence and configure the settings.
[YaST2 Control Center] → [Security and Users] → [Firewall]
However, leave ports 161 and 162 open for the udp communication.

Settings for Enabling ASR Configuration, Shutdown, and Restart from the ServerView Console

To perform ASR (Automatic Server Reconfiguration & Restart) settings, including fan/temperature/restart, or to turn the power on/off from the Management Console, you will be asked to enter the user name and the password of an administrative user.
Follow the steps below to set an administrative user.

IMPORTANT

- An administrative user in ServerView means a 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 commands.

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

- Specify the "svuser" group in the G option of the useradd command.
  For <user name>, specify a name for 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 newly created user name is enabled when the password is set.
- For details about each command, see the useradd (8) and passwd (1) man page.

2 Set the existing user as an administrative user.

Contact the system administrator to check whether the existing user to be set belongs to multiple groups and then 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,<user group,...> <user name>
```

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

2.4.7 [Linux] Setting Each Service (When Installing Only ServerView Linux Agent on the Server to Be Monitored)

■ Auto-Start Setting of the SNMP Service

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

```
# /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
```

■ Configuring the Firewall

● For Red Hat Linux

POINT

- Firewall settings are only necessary if you use a firewall.
  If no firewall is used, the following settings are not required.

The firewall is configured when installing Linux or by using the setup command.
This section describes the configuration when using the setup command.
The windows are different when setting the firewall during the Linux installation and when executing the setup command; the setting items, however, are the same. For details about how to configure the firewall during the Linux installation, see the Red Hat Linux manuals and the following set up method.
The window for the setup command varies depending on the Red Hat distribution, but the setting items are the same.

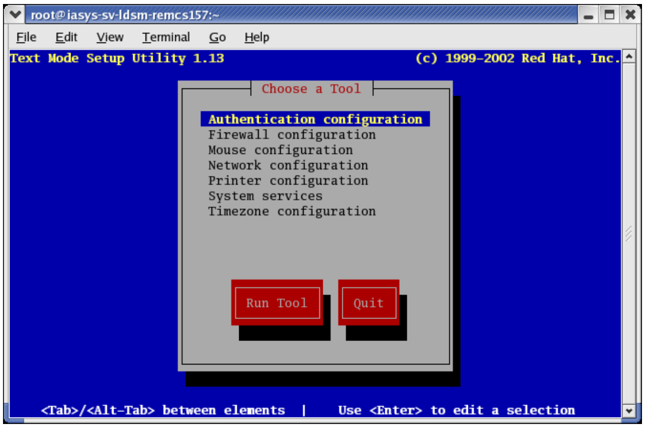
IMPORTANT

- The firewall setting below is required in order for ServerView to operate.
  For details about the firewall settings, see the Red Hat Linux manuals.

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

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

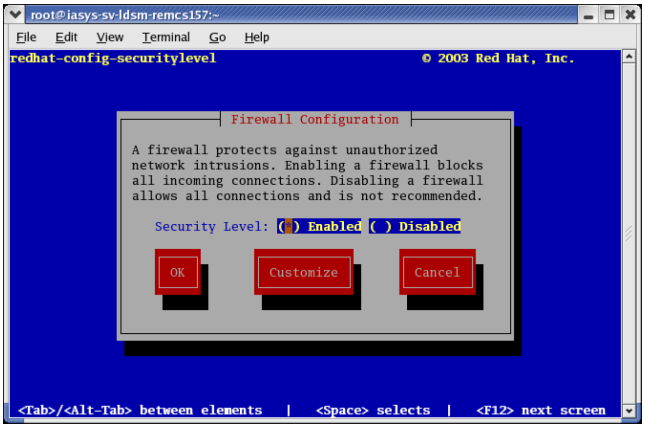
The menu window appears.


root@iasys-sv-ldsm-remcs157:~
File Edit View Terminal Go Help
Run Tool
Quit

```
Text Mode Setup Utility 1.13                    (c) 1999-2002 Red Hat, Inc.

                 Choose a Tool

              Authentication configuration
              Firewall configuration
              Mouse configuration
              Network configuration
              Printer configuration
              System services
              Timezone configuration

  <Tab>/<Alt-Tab> between elements   |    Use <Enter> to edit a selection
```

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

The [Firewall Configuration] window appears.


root@iasys-sv-ldsm-remcs157:~
File Edit View Terminal Go Help
OK
Customize
Cancel

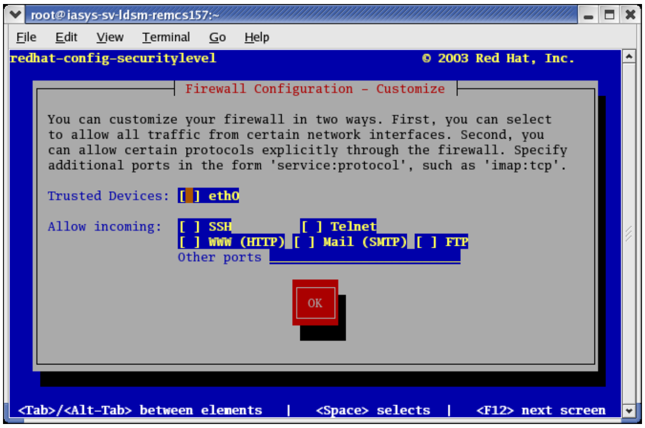
```
redhat-config-securitylevel                          © 2003 Red Hat, Inc.

                  Firewall Configuration

        A firewall protects against unauthorized
        network intrusions. Enabling a firewall blocks
        all incoming connections. Disabling a firewall
        allows all connections and is not recommended.

           Security Level: (*) Enabled ( ) Disabled

 <Tab>/<Alt-Tab> between elements   |  <Space> selects  |  <F12> next screen
```

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

IMPORTANT

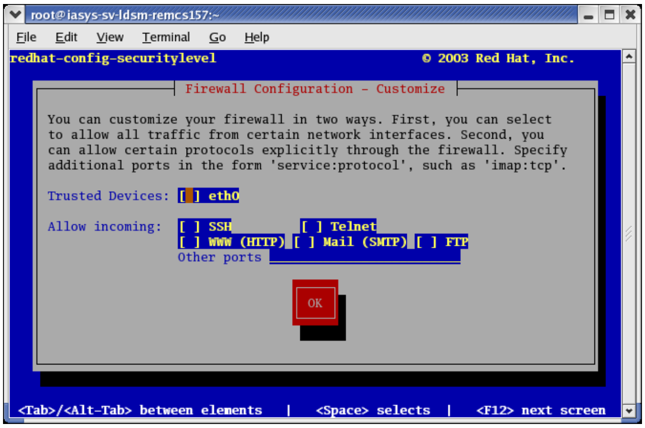
- When "Disabled" is selected here, the settings below are not required.

The [Firewall Configuration - Customize] window appears.



```
redhat-config-securitylevel                          © 2003 Red Hat, Inc.

                  Firewall Configuration - Customize

  You can customize your firewall in two ways. First, you can select
  to allow all traffic from certain network interfaces. Second, you
  can allow certain protocols explicitly through the firewall. Specify
  additional ports in the form 'service:protocol', such as 'imap:tcp'.

  Trusted Devices:  [ ] eth0

  Allow incoming:   [ ] SSH         [ ] Telnet
                    [ ] WWW (HTTP)  [ ] Mail (SMTP) [ ] FTP
                    Other ports

                                 OK

 <Tab>/<Alt-Tab> between elements   |   <Space> selects   |   <F12> next screen
```

4 Set the protocols to use.


root@iasys-sv-ldsm-remcs157:~
File Edit View Terminal Go Help

redhat-config-securitylevel © 2003 Red Hat, Inc.

Firewall Configuration - Customize

You can customize your firewall in two ways. First, you can select to allow all traffic from certain network interfaces. Second, you can allow certain protocols explicitly through the firewall. Specify additional ports in the form 'service:protocol', such as 'imap:tcp'.

Trusted Devices: [ ] eth0

Allow incoming: [ ] SSH [ ] Telnet [ ] WWW (HTTP) [ ] Mail (SMTP) [ ] FTP Other ports

OK

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Set the protocols below.

1. Select "WWW (HTTP)".

   Add a [*] 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 move the cursor to [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 move the cursor to [OK] and press the [Enter] key.

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

- **For SUSE Linux**

Open the SuSE Firewall2 configuration window in the following sequence and configure the settings.
[YaST2 Control Center] → [Security and Users] → [Firewall]
However, leave ports 161 and 162 open for the udp communication.

■ Settings for Enabling ASR Configuration, Shutdown, and Restart from the ServerView Console

To perform ASR (Automatic Server Reconfiguration & Restart) settings, including fan/temperature/restart, or to turn the power on/off from the Management Console, you will be asked to enter the user name and the password of an administrative user.
Follow the steps below to set an administrative user.

POINT

- An administrative user in ServerView means a user who belongs to the "svuser" group.
  The "svuser" group is automatically created when ServerView is installed with the 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 in the G option of the useradd command.
  For <user name>, specify a name for 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 newly created user name is enabled when the password is set.
- For details about each command, see the useradd (8) and passwd (1) man page.

2 Set the existing user as an administrative user.

Contact the system administrator to check whether the existing user to be set belongs to multiple groups and then 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,<user group,...> <user name>
```

- Specify the "svuser" group in the G option of the usermod command. To specify multiple groups, specify the groups separated with a comma ",". If the group to which the user previously belonged is not specified, the user is deleted from that group. Specify all groups to which the user should belong. For <user name>, specify the user name as an administrative user.
  For details about the usermod command, see the usermod (8) man page.

- You can also set the groups directly by using the vigr command or set the groups by using GUI tools. For details, see the vigr (8) man page or the Red Hat/SUSE Linux manuals.

■ Output Format of the System Log (/var/log/messages) by ServerView Linux Agent

ServerView Linux Agent outputs logs to the system log (/var/log/messages) in the following format: “Specific Number” , “Severity” , and “Detailed Message” are the same as those in the trap lists. For detailed information, see the trap list section.

Format: Date Host Name Serverview: [Specific Number][Severity] Detailed Message Host Name
example:

```
Sep 19 20:13:44 host01 Serverview: [1100][INFORMATIONAL] System status has
changed at server host01.
```

● To Switch to the Format without [Specific Number][Severity]

1 Open the file /etc/init.d/srvmagt using an editor such as vi.

2 Search the line with “export …” from the top of the file.

3 Add “export SRVMAGT_OLDTRAPLOG=1” after the “export …” line.

example:

```
export LD_LIBRARY_PATH=/usr/lib:/usr/lib/srvmagt
export SRVMAGT_OLDTRAPLOG=1
```

4 Save the file and close the editor.

5 Restart ServerView Linux Agent.

```
# /etc/init.d/srvmagt stop
# /etc/init.d/srvmagt start
```

2.4.8 Changing Computer Information after Installation

If the name or IP address of the computer is changed after the ServerView installation, perform the steps below.

● For Windows

1 If ServerView and AlarmService are running, 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 changed IP address.
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, see "3.9.2 Adding the Monitored Server (Object)" (→pg.219).

● For Linux

No operation is required.

Chapter 3

How to Use ServerView

This chapter explains how to use the ServerView functions.

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.215).

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/

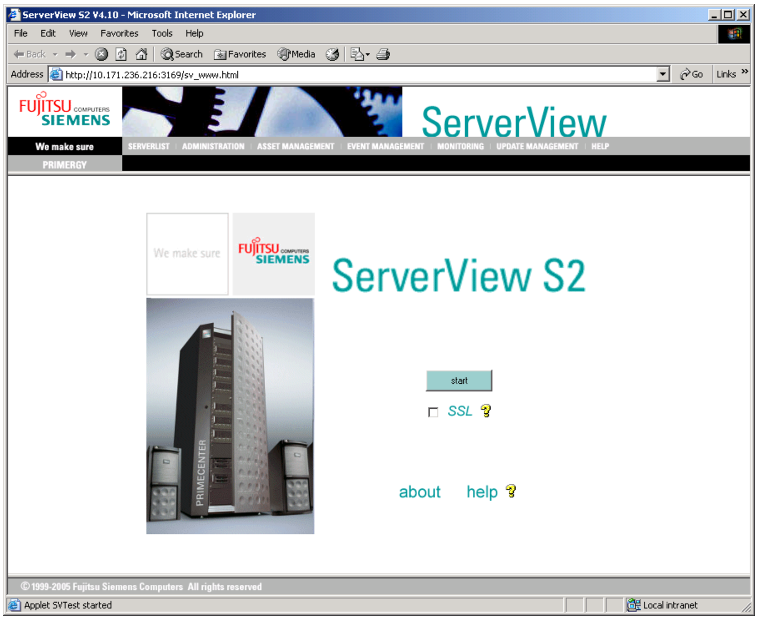
http://<server name or server IP address>:3169/sv_www.html

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

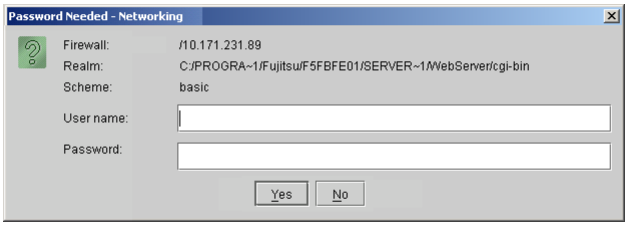
The window of ServerView S2 appears.


ServerView S2 V4.10 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.171.236.216:3169/sv_www.html
Go Links
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SERVERLIST ADMINISTRATION ASSET MANAGEMENT EVENT MANAGEMENT MONITORING UPDATE MANAGEMENT HELP
We make sure
ServerView S2
start
SSL
about
help
PRIMECENTER
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Applet SVTest started
Local intranet

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:



Password Needed - Networking

Firewall: /10.171.231.89

Realm: C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/WebServer/cgi-bin

Scheme: basic

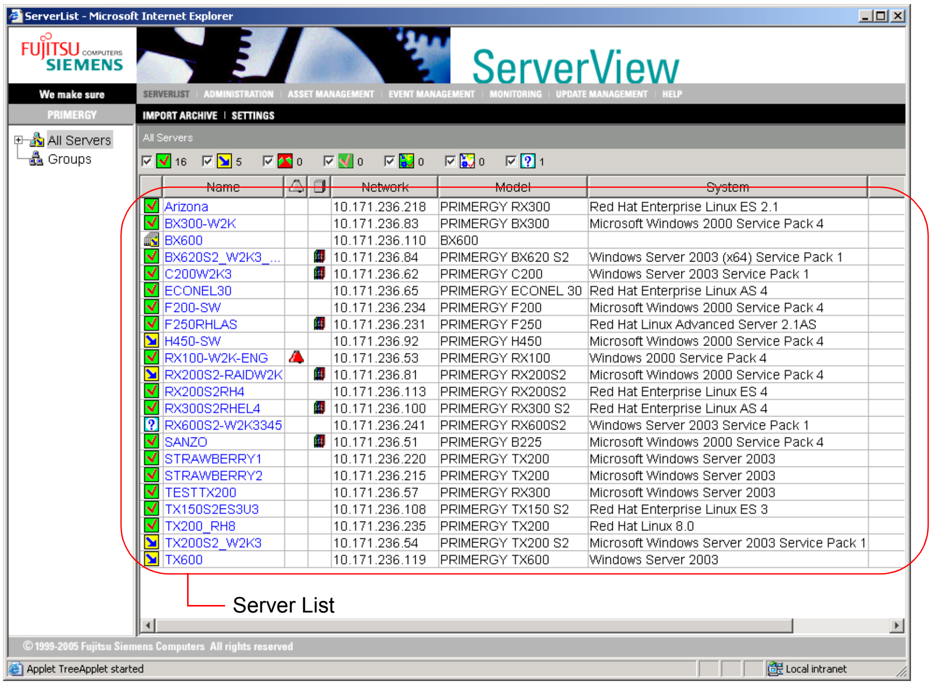
User name:

Password:

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.408).

3 Click [Start].

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


ServerList - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | UPDATE MANAGEMENT | HELP
IMPORT ARCHIVE | SETTINGS
All Servers
Groups
All Servers
☑ 16 ☑ 5 ☑ 0 ☑ 0 ☑ 0 ☑ 0 ☑ 1
Server List
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Applet TreeApplet started
Local intranet

Name	Network	Model	System
Arizona	10.171.236.218	PRIMERGY RX300	Red Hat Enterprise Linux ES 2.1
BX300-W2K	10.171.236.83	PRIMERGY BX300	Microsoft Windows 2000 Service Pack 4
BX600	10.171.236.110	BX600	
BX620S2_W2K3_...	10.171.236.84	PRIMERGY BX620 S2	Windows Server 2003 (x64) Service Pack 1
C200W2K3	10.171.236.62	PRIMERGY C200	Windows Server 2003 Service Pack 1
ECONEL30	10.171.236.65	PRIMERGY ECONEL 30	Red Hat Enterprise Linux AS 4
F200-SW	10.171.236.234	PRIMERGY F200	Microsoft Windows 2000 Service Pack 4
F250RHLAS	10.171.236.231	PRIMERGY F250	Red Hat Linux Advanced Server 2.1AS
H450-SW	10.171.236.92	PRIMERGY H450	Microsoft Windows 2000 Service Pack 4
RX100-W2K-ENG	10.171.236.53	PRIMERGY RX100	Windows 2000 Service Pack 4
RX200S2-RAIDW2K	10.171.236.81	PRIMERGY RX200S2	Microsoft Windows 2000 Service Pack 4
RX200S2RH4	10.171.236.113	PRIMERGY RX200S2	Red Hat Enterprise Linux ES 4
RX300S2RHEL4	10.171.236.100	PRIMERGY RX300 S2	Red Hat Enterprise Linux AS 4
RX600S2-W2K3345	10.171.236.241	PRIMERGY RX600S2	Windows Server 2003 Service Pack 1
SANZO	10.171.236.51	PRIMERGY B225	Microsoft Windows 2000 Service Pack 4
STRAWBERRY1	10.171.236.220	PRIMERGY TX200	Microsoft Windows Server 2003
STRAWBERRY2	10.171.236.215	PRIMERGY TX200	Microsoft Windows Server 2003
TESTTX200	10.171.236.57	PRIMERGY RX300	Microsoft Windows Server 2003
TX150S2ES3U3	10.171.236.108	PRIMERGY TX150 S2	Red Hat Enterprise Linux ES 3
TX200_RH8	10.171.236.235	PRIMERGY TX200	Red Hat Linux 8.0
TX200S2_W2K3	10.171.236.54	PRIMERGY TX200 S2	Microsoft Windows Server 2003 Service Pack 1
TX600	10.171.236.119	PRIMERGY TX600	Windows Server 2003

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 service configuration file of the monitored Linux server. (Check the httpd service configuration file If you are using Red Hat Linux, or check the apache2 service configuration file If you are using SUSE Linux.

     For details, refer to step 5 in "■ Installing ServerView Linux Console Manually" (→pg.57).
  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.206)
	SETTINGS	Sets the interval for updating the server list. →"■ Setting the Update Interval for the Server List" (pg.99)
ADMINISTRATION		
	SERVERBROWSER	Adds servers to be monitored to the server list. →"3.1.3 Registering the Monitored Servers" (pg.89)
	MIB INTEGRATION	Adds MIB files.→"3.1.5 Registering MIB (MIB INTEGRATION)" (pg.95)
ASSET MANAGEMENT		
	ARCHIVE MANAGER	Retrieves and manages archive data. "3.7.1 Starting the Archive Manager" (→pg.198)
	EXPORT MANAGER	Retrieves export data on the servers and saves them on the file. →"3.8 Export Manager" (pg.207)
EVENT MANAGEMENT		
	ALARM MONITOR	Displays received alarms. →"3.5.1 Alarm Monitor" (pg.139).
	ALARM MANAGER	Manages received alarms. →"3.5.2 Alarm Manager" (pg.146).
	ALARM SETTINGS	Configures alarm settings. →"3.5.3 Alarm Settings" (pg.149).
MONITORING		
	PERFORMANCE MANAGER	Configures, monitors, and displays threshold values and/or reports. →"3.6 Performance Manager" (pg.178)
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

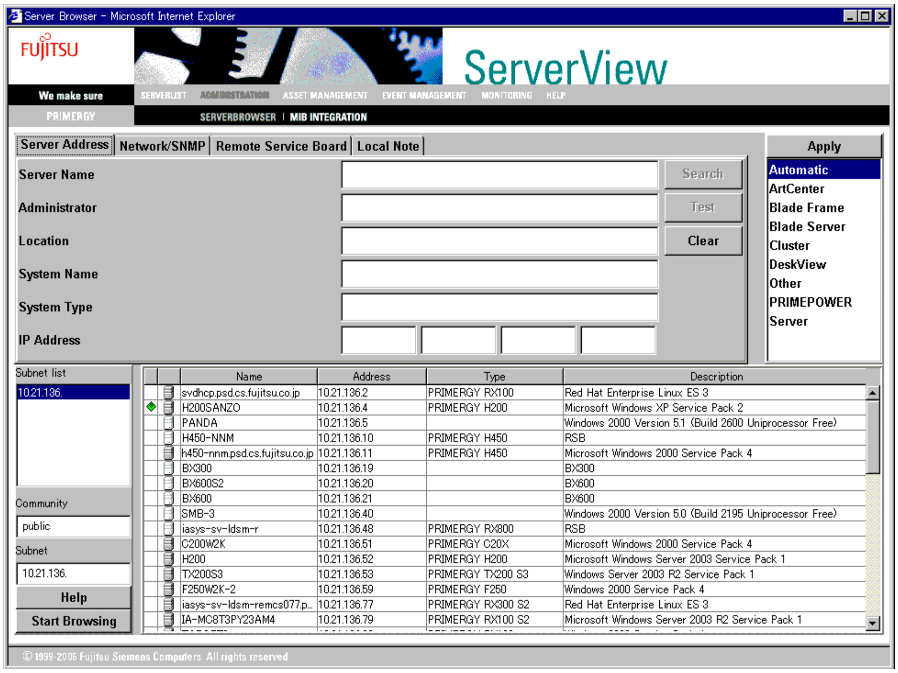
Menu Item	Description
New Server	Opens the [ServerBrowser] window where you can add servers to monitor. →"3.1.3 Registering the Monitored Servers" (pg.89)
New Group	Creates a new group. A new group will be created under the selected group. You cannot create a group under [all server].
Move to group...	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.92)
ASR Properties	Displays the ASR window where you can configure responses to failures. →"3.4 Serious Error Handling (ASR)" (pg.130)
Test Connection	Tests the connection to the server. →"■ Verification of Server Connections" (pg.97)
Redetect servers	Redetects the server status. →"■ Redetect Server/Redetect All Servers" (pg.99)
Redetect All Servers	Redetects the status of all servers. →"■ Redetect Server/Redetect All Servers" (pg.99)
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.



Subnet list: 10.21.136.

Community: public

Subnet: 10.21.136.

		Name	Address	Type	Description
		svdhcp.psd.cs.fujitsu.co.jp	10.21.136.2	PRIMERGY RX100	Red Hat Enterprise Linux ES 3
◆		H200SANZO	10.21.136.4	PRIMERGY H200	Microsoft Windows XP Service Pack 2
		PANDA	10.21.136.5		Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)
		H450-NNM	10.21.136.10	PRIMERGY H450	RSB
		h450-nnm.psd.cs.fujitsu.co.jp	10.21.136.11	PRIMERGY H450	Microsoft Windows 2000 Service Pack 4
		BX300	10.21.136.19		BX300
		BX600S2	10.21.136.20		BX600
		BX600	10.21.136.21		BX600
		SMB-3	10.21.136.40		Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)
		iasys-sv-ldsm-r	10.21.136.48	PRIMERGY RX800	RSB
		C200W2K	10.21.136.51	PRIMERGY C20X	Microsoft Windows 2000 Service Pack 4
		H200	10.21.136.52	PRIMERGY H200	Microsoft Windows Server 2003 Service Pack 1
		TX200S3	10.21.136.53	PRIMERGY TX200 S3	Windows Server 2003 R2 Service Pack 1
		F250W2K-2	10.21.136.59	PRIMERGY F250	Windows 2000 Service Pack 4
		iasys-sv-ldsm-remcs077.p...	10.21.136.77	PRIMERGY RX300 S2	Red Hat Enterprise Linux ES 3
		IA-MC8T3PY23AM4	10.21.136.79	PRIMERGY RX100 S2	Microsoft Windows Server 2003 R2 Service Pack 1

2 Enter the IP address for the server to be registered in the [IP Address] field, and click [Search].

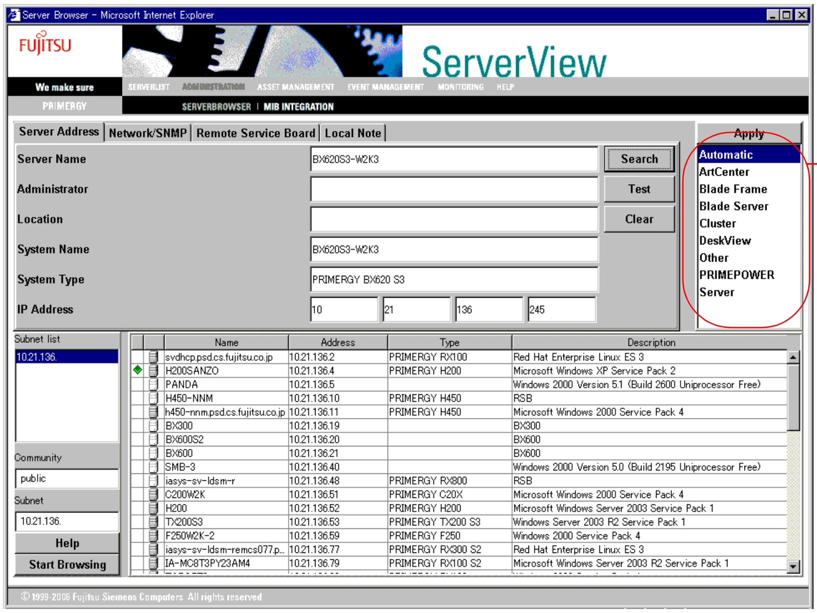
Information for the server, such as the DNS name, is automatically collected and displayed in the other fields.

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.



Server Name: BX620S3-W2K3

Administrator:

Location:

System Name: BX620S3-W2K3

System Type: PRIMERGY BX620 S3

IP Address: 10 21 136 245

Subnet list: 10.21.136.

Community: public

Subnet: 10.21.136.

Name	Address	Type	Description
svdhcp.psd.cs.fujitsu.co.jp	10.21.136.2	PRIMERGY RX100	Red Hat Enterprise Linux ES 3
H200SANZO	10.21.136.4	PRIMERGY H200	Microsoft Windows XP Service Pack 2
PANDA	10.21.136.5		Windows 2000 Version 5.1 (Build 2600 Uniprocessor Free)
H450-NNM	10.21.136.10	PRIMERGY H450	RSB
h450-nnm.psd.cs.fujitsu.co.jp	10.21.136.11	PRIMERGY H450	Microsoft Windows 2000 Service Pack 4
BX300	10.21.136.19		BX300
BX600S2	10.21.136.20		BX600
BX600	10.21.136.21		BX600
SMB-3	10.21.136.40		Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)
iasys-sv-ldsm-r	10.21.136.48	PRIMERGY RX800	RSB
C200W2K	10.21.136.51	PRIMERGY C20X	Microsoft Windows 2000 Service Pack 4
H200	10.21.136.52	PRIMERGY H200	Microsoft Windows Server 2003 Service Pack 1
TX200S3	10.21.136.53	PRIMERGY TX200 S3	Windows Server 2003 R2 Service Pack 1
F250W2K-2	10.21.136.59	PRIMERGY F250	Windows 2000 Service Pack 4
iasys-sv-ldsm-remcs077.p...	10.21.136.77	PRIMERGY RX300 S2	Red Hat Enterprise Linux ES 3
IA-MC8T3PY23AM4	10.21.136.79	PRIMERGY RX100 S2	Microsoft Windows Server 2003 R2 Service Pack 1

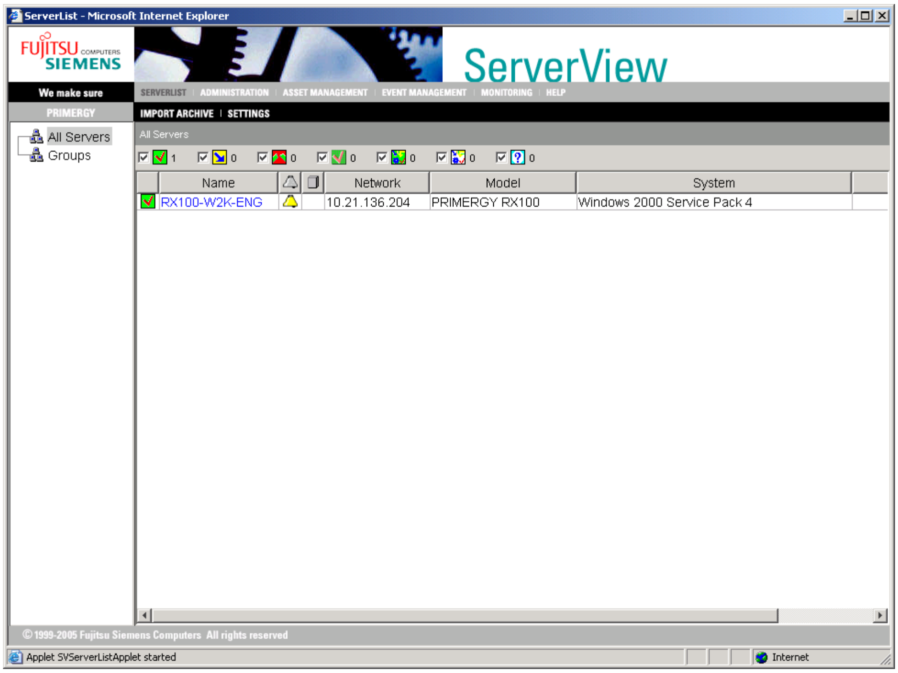
Server type list

table: Server Types

Type Name	Description
Automatic	Auto-detects the type of the server to be added.
ArtCenter	Not supported.
Blade Frame	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.
PRIMEPOWER	Select this to add a PRIMEPOWER system. Not supported.
Server	Adds a server to be monitored by ServerView Agent.

4 Click [Apply].

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


ServerList - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
PRIMERGY
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
IMPORT ARCHIVE | SETTINGS
All Servers
Groups
All Servers
☑ 1 ☑ 0 ☑ 0 ☑ 0 ☑ 0 ☑ 0 ☑ 0
Internet

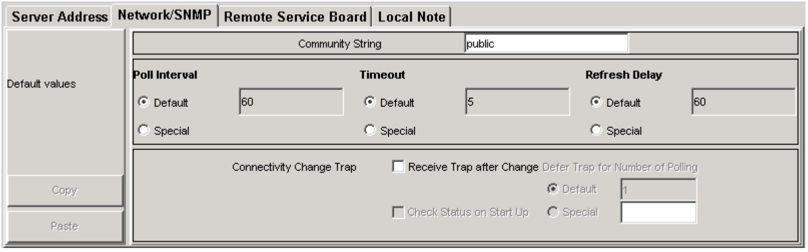
Name			Network	Model	System
RX100-W2K-ENG	△		10.21.136.204	PRIMERGY RX100	Windows 2000 Service Pack 4

©1999-2005 Fujitsu Siemens Computers All rights reserved

Applet SVServerListApplet started

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].



Community String: public

Poll Interval: ● Default 60 ○ Special

Timeout: ● Default 5 ○ Special

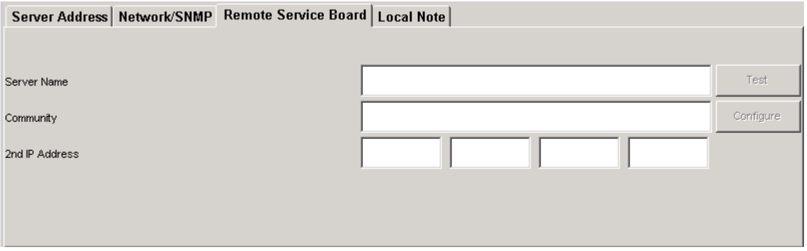
Refresh Delay: ● Default 60 ○ Special

Connectivity Change Trap: □ Receive Trap after Change

Defer Trap for Number of Polling: ● Default 1 ○ Special

□ Check Status on Start Up

  - [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.



Server Name

Community

2nd IP Address

- [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.

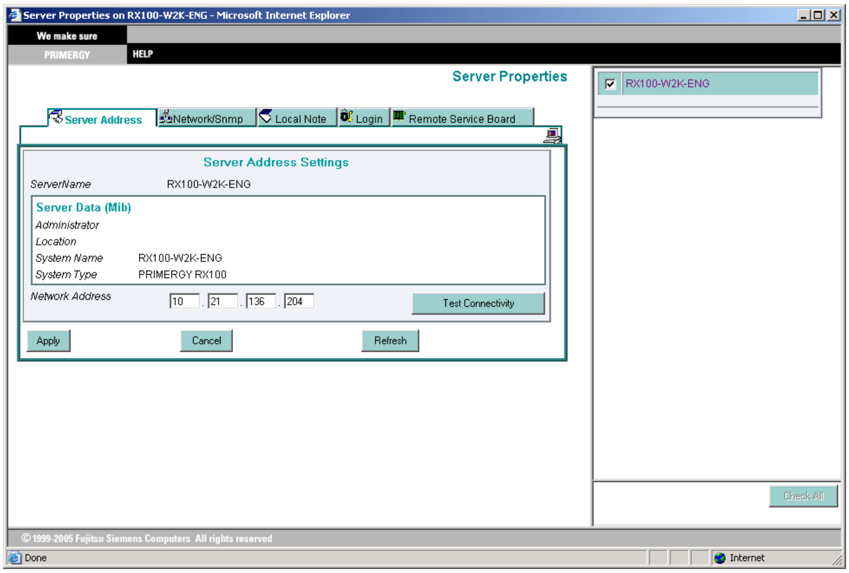
You cannot add a server with the same name or network address as an already registered server.

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.



Server Address Settings

ServerName RX100-W2K-ENG

Server Data (Mib)

Administrator

Location

System Name RX100-W2K-ENG

System Type PRIMERGY RX100

Network Address 10 . 21 . 136 . 204

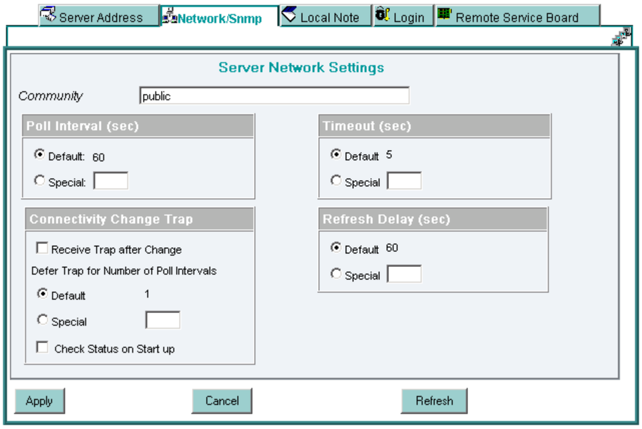
2 Verify/change the settings in each tab window.

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



Server Network Settings

Community: public

Poll Interval (sec)
● Default: 60
○ Special:

Timeout (sec)
● Default 5
○ Special

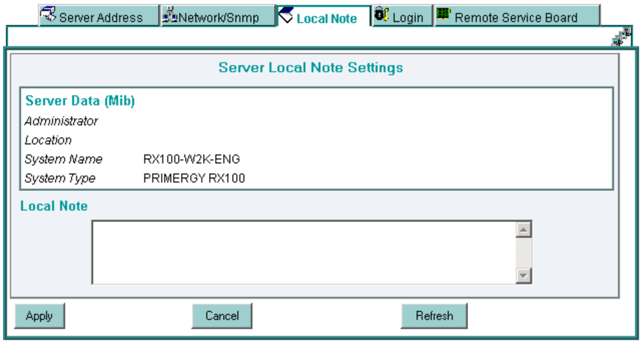
Connectivity Change Trap
□ Receive Trap after Change
Defer Trap for Number of Poll Intervals
● Default 1
○ Special
□ Check Status on Start up

Refresh Delay (sec)
● Default 60
○ Special

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



Server Local Note Settings

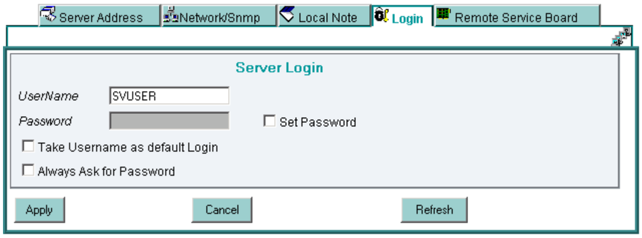
Server Data (Mib)

Administrator	
Location	
System Name	RX100-W2K-ENG
System Type	PRIMERGY RX100

Local Note

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



Server Login

UserName: SVUSER

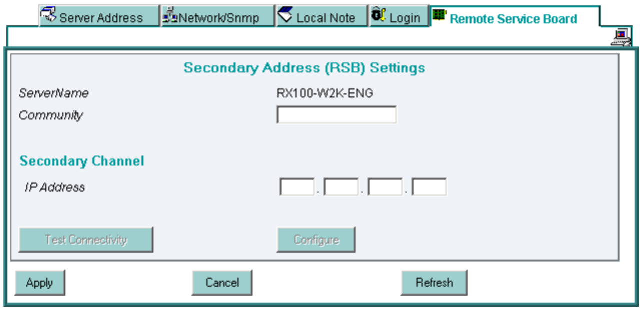
Password: □ Set Password

□ Take Username as default Login

□ Always Ask for Password

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



Secondary Address (RSB) Settings

ServerName RX100-W2K-ENG

Community

Secondary Channel

IP Address

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 "6.3.1 Starting the Web Interface" (→pg.303).

[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)

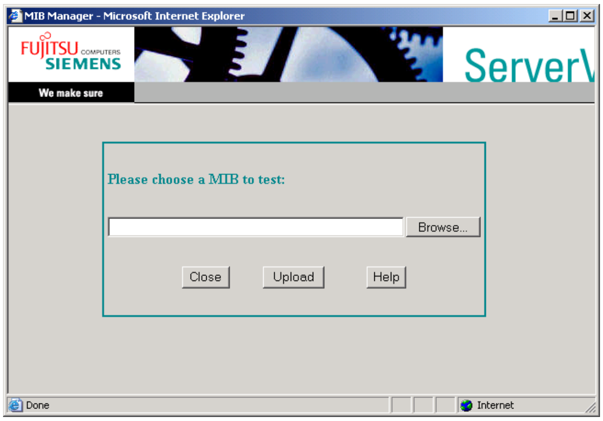
This function is used to register a MIB file in ServerView S2.

IMPORTANT

- For ServerView S2 running under Linux, MIB registration is not supported.
  When using Linux, perform the procedure to copy the MIB file. For details, see "2.4.4 Registering the Interrupt (MIB) Information of Optional Devices" (→pg.67).

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

The MIB file registration window appears.


MIB Manager - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
ServerV
Please choose a MIB to test:
Browse...
Close
Upload
Help
Done
Internet

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.
⚙ i	The DiskInfo tool can start. This is not supported.
🌐	The advanced server manager can be activated.
LDSM	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.

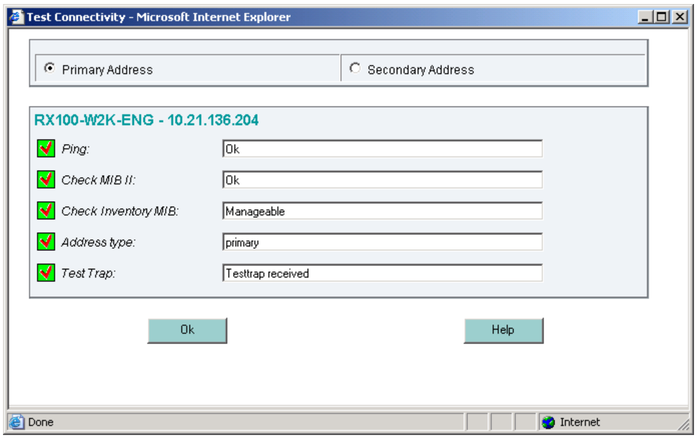
IMPORTANT

- 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.



● Primary Address ○ Secondary Address

RX100-W2K-ENG - 10.21.136.204

✓ Ping:	Ok
✓ Check MIB II:	Ok
✓ Check Inventory MIB:	Manageable
✓ Address type:	primary
✓ Test Trap:	Testtrap received

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.

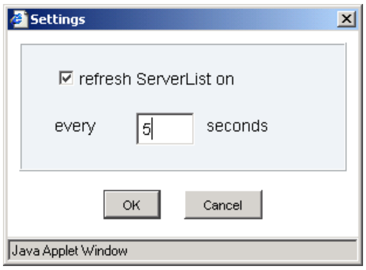
The status check starts for all the servers registered in the server list.

■ 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].



Settings

☑ refresh ServerList on

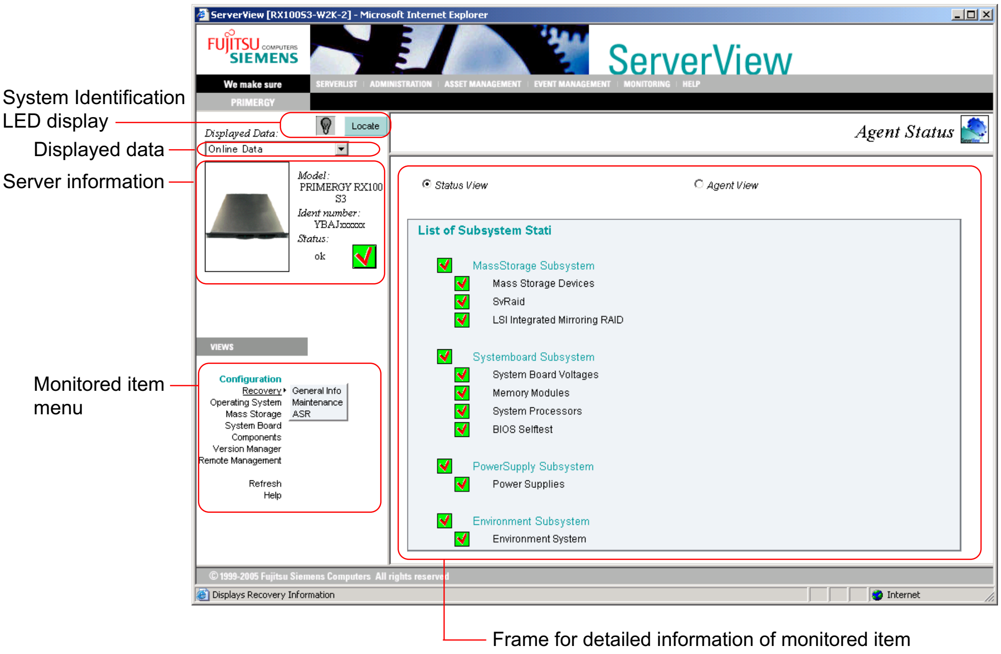
every 5 seconds

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.


System Identification LED display
Displayed data
Server information
Monitored item menu
Frame for detailed information of monitored item
ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
PRIMERGY
Locate
Agent Status
VIEWS
Configuration
Recovery
Operating System
Mass Storage
System Board
Components
Version Manager
Remote Management
Refresh
Help
General Info
Maintenance
ASR
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Displays Recovery Information
Internet

Displayed Data: Online Data

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok ✓

● Status View ○ Agent View

List of Subsystem Stati

- ✓ MassStorage Subsystem
  - ✓ Mass Storage Devices
  - ✓ SvRaid
  - ✓ LSI Integrated Mirroring RAID
- ✓ Systemboard Subsystem
  - ✓ System Board Voltages
  - ✓ Memory Modules
  - ✓ System Processors
  - ✓ BIOS Selftest
- ✓ PowerSupply Subsystem
  - ✓ Power Supplies
- ✓ Environment Subsystem
  - ✓ Environment System

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.126).

● 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.198).

● 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.96).

● 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.103) • 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.104)
Mass Storage	Displays the Mass Storage connected to the server and their file systems. →"■ Mass Storage" (pg.105)
Network Interfaces	Displays the Network Interface installed in the server. →"■ Network Interfaces" (pg.105)
Expansion Boards	Displays the server buses and Expansion Boards. →"■ Expansion Boards" (pg.106)
Recovery	Displays information about the server operation, such as the event log and the error log. →"■ Recovery" (pg.106)
Others	Displays information about fans and temperature sensors. →"■ Others" (pg.107)
MB II	Displays MIB II. →"■ MIB II" (pg.107)
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.108)
Maintenance	Displays the usage time for the internal CMOS battery and information about the fans. →"■ Maintenance" (pg.110)
ASR	You can configure the Automatic Server Reconfiguration & Restart (ASR) function. →"3.4 Serious Error Handling (ASR)" (pg.130)

table: Monitored Item

Item	Description
Operating System	Displays information about the OS installed in the server. →"3.2.5 Displaying Operating System Information" (pg.110)
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.111)
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.116)
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.120)
Power Supply	Displays the configuration and status of the server's power supply. →"■ Power Supply" (pg.121)
Network Interfaces	Lists the I/F, Status, Type, and Description for the Network Interfaces installed in the server. →"■ Network Interfaces" (pg.123)
Resources	Displays the system resources. →"■ Resources" (pg.123)
Version Manager	
Inventory View	Displays the server Inventory information (the hardware and software configuration information). →"3.2.9 Version Manager (Inventory)" (pg.124)
Remote Management	Displays the remote management information. →"3.2.10 Remote Management" (pg.125)
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

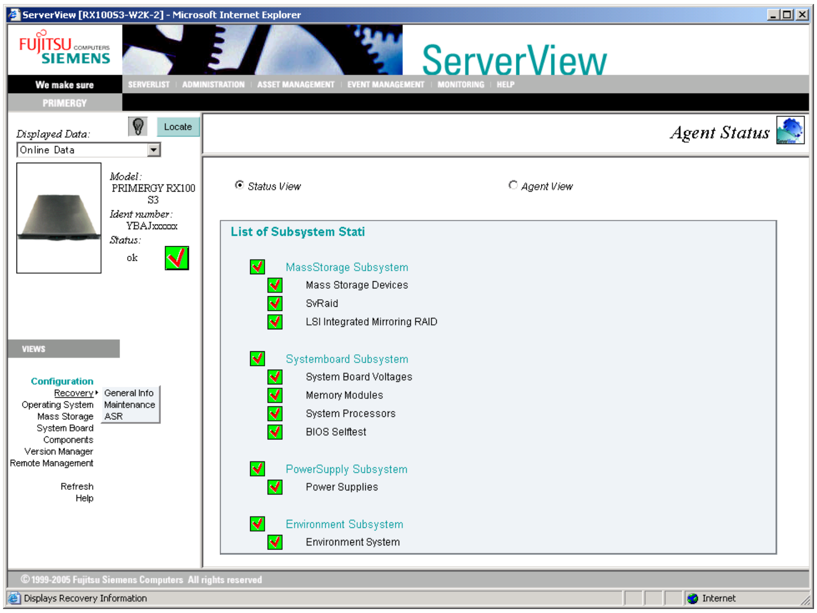
Here, various information about the server configuration is displayed.

■ 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.



Displayed Data: Online Data

Model: PRIMERGY RX100 S3

Ident number: YBAJxxxxxx

Status: ok ✓

Agent Status

● Status View ○ Agent View

List of Subsystem Stati

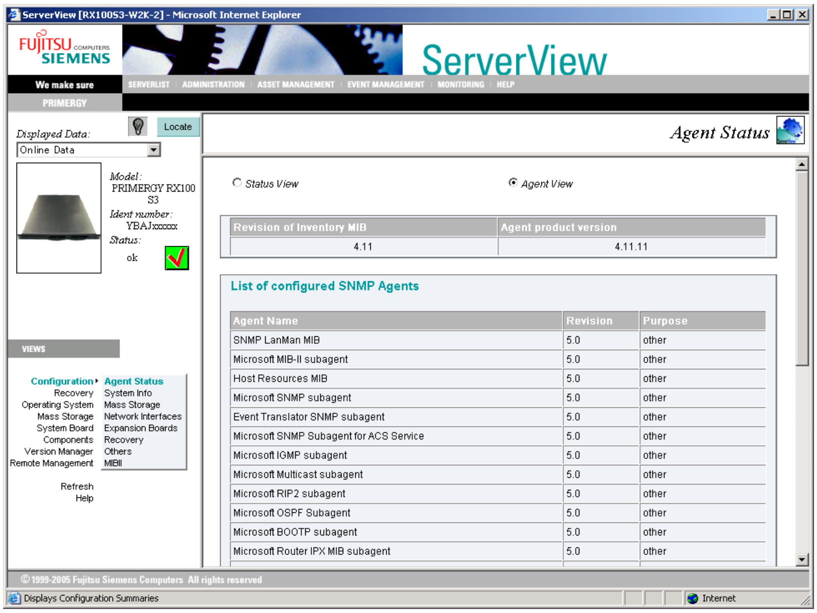
- ✓ MassStorage Subsystem
  - ✓ Mass Storage Devices
  - ✓ SvRaid
  - ✓ LSI Integrated Mirroring RAID
- ✓ Systemboard Subsystem
  - ✓ System Board Voltages
  - ✓ Memory Modules
  - ✓ System Processors
  - ✓ BIOS Selftest
- ✓ PowerSupply Subsystem
  - ✓ Power Supplies
- ✓ Environment Subsystem
  - ✓ Environment System

© 1999-2005 Fujitsu Siemens Computers All rights reserved

Displays Recovery Information

- **Agent View**

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



Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

○ Status View ● Agent View

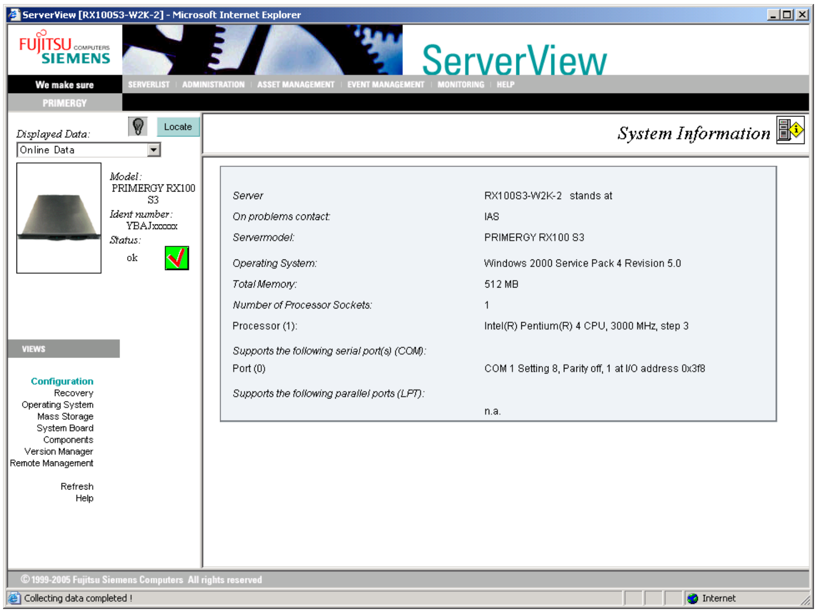
Revision of Inventory MIB	Agent product version
4.11	4.11.11

List of configured SNMP Agents

Agent Name	Revision	Purpose
SNMP LanMan MIB	5.0	other
Microsoft MIB-II subagent	5.0	other
Host Resources MIB	5.0	other
Microsoft SNMP subagent	5.0	other
Event Translator SNMP subagent	5.0	other
Microsoft SNMP Subagent for ACS Service	5.0	other
Microsoft IGMP subagent	5.0	other
Microsoft Multicast subagent	5.0	other
Microsoft RIP2 subagent	5.0	other
Microsoft OSPF Subagent	5.0	other
Microsoft BOOTP subagent	5.0	other
Microsoft Router IPX MIB subagent	5.0	other

■ System Information

Displays system information.

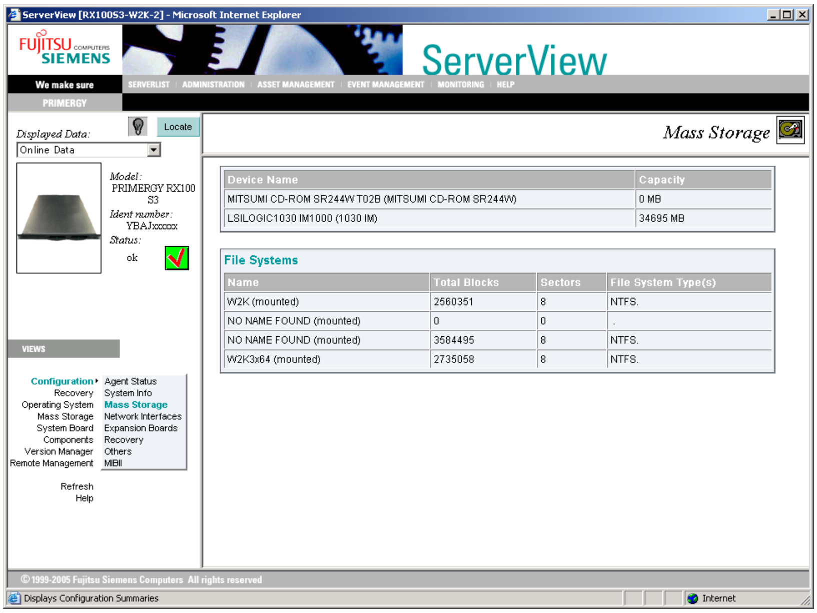

ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
Displayed Data:
Online Data
Locate
VIEWS
Configuration
Recovery
Operating System
Mass Storage
System Board
Components
Version Manager
Remote Management
Refresh
Help
System Information
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Collecting data completed !
Internet

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

Server	RX100S3-W2K-2 stands at
On problems contact:	IAS
Servermodel:	PRIMERGY RX100 S3
Operating System:	Windows 2000 Service Pack 4 Revision 5.0
Total Memory:	512 MB
Number of Processor Sockets:	1
Processor (1):	Intel(R) Pentium(R) 4 CPU, 3000 MHz, step 3
Supports the following serial port(s) (COM):	
Port (0)	COM 1 Setting 8, Parity off, 1 at I/O address 0x3f8
Supports the following parallel ports (LPT):	
	n.a.

■ Mass Storage

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


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
Locate
VIEWS
Configuration ▸
Recovery
Operating System
Mass Storage
System Board
Components
Version Manager
Remote Management
Agent Status
System Info
Mass Storage
Network Interfaces
Expansion Boards
Recovery
Others
MIBII
Refresh
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Displays Configuration Summaries
Internet

Displayed Data: Online Data

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok ✓

Mass Storage

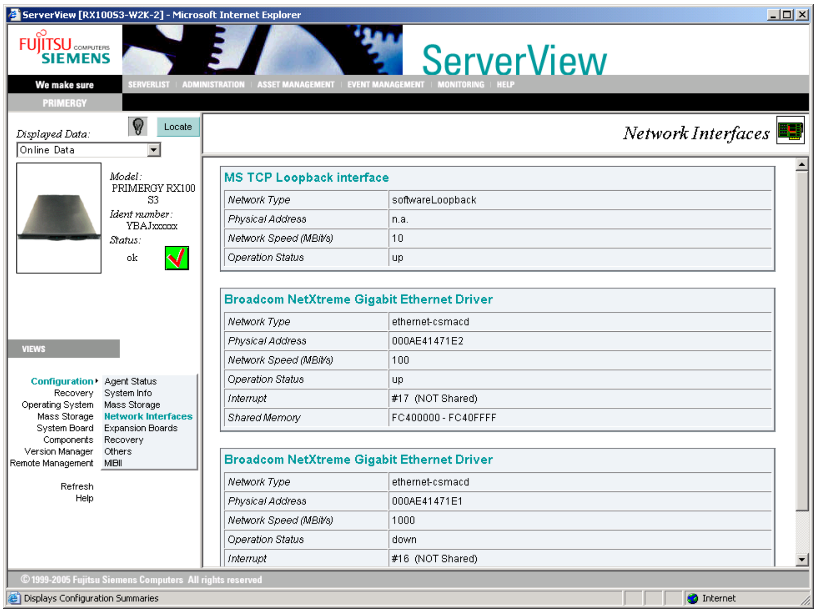
Device Name	Capacity
MITSUMI CD-ROM SR244W T02B (MITSUMI CD-ROM SR244W)	0 MB
LSILOGIC1030 IM1000 (1030 IM)	34695 MB

File Systems

Name	Total Blocks	Sectors	File System Type(s)
W2K (mounted)	2560351	8	NTFS.
NO NAME FOUND (mounted)	0	0	.
NO NAME FOUND (mounted)	3584495	8	NTFS.
W2K3x64 (mounted)	2735058	8	NTFS.

■ Network Interfaces

Displays information about the Network Interfaces installed in the server.


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
Locate
VIEWS
Configuration ▸
Recovery
Operating System
Mass Storage
System Board
Components
Version Manager
Remote Management
Agent Status
System Info
Mass Storage
Network Interfaces
Expansion Boards
Recovery
Others
MIBII
Refresh
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Displays Configuration Summaries
Internet

Displayed Data: Online Data

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok ✓

Network Interfaces

MS TCP Loopback interface

Network Type	softwareLoopback
Physical Address	n.a.
Network Speed (MBit/s)	10
Operation Status	up

Broadcom NetXtreme Gigabit Ethernet Driver

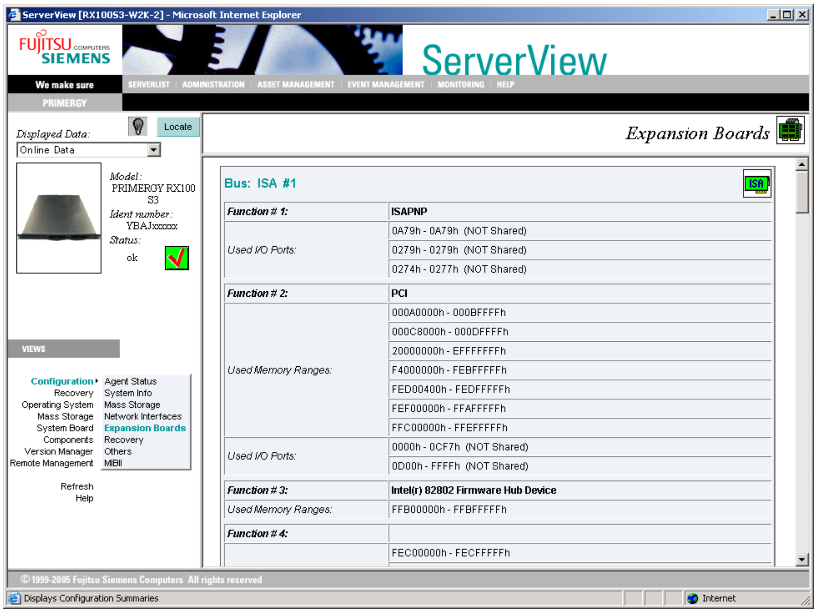
Network Type	ethernet-csmacd
Physical Address	000AE41471E2
Network Speed (MBit/s)	100
Operation Status	up
Interrupt	#17 (NOT Shared)
Shared Memory	FC400000 - FC40FFFF

Broadcom NetXtreme Gigabit Ethernet Driver

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

■ Expansion Boards

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



Displayed Data: Online Data

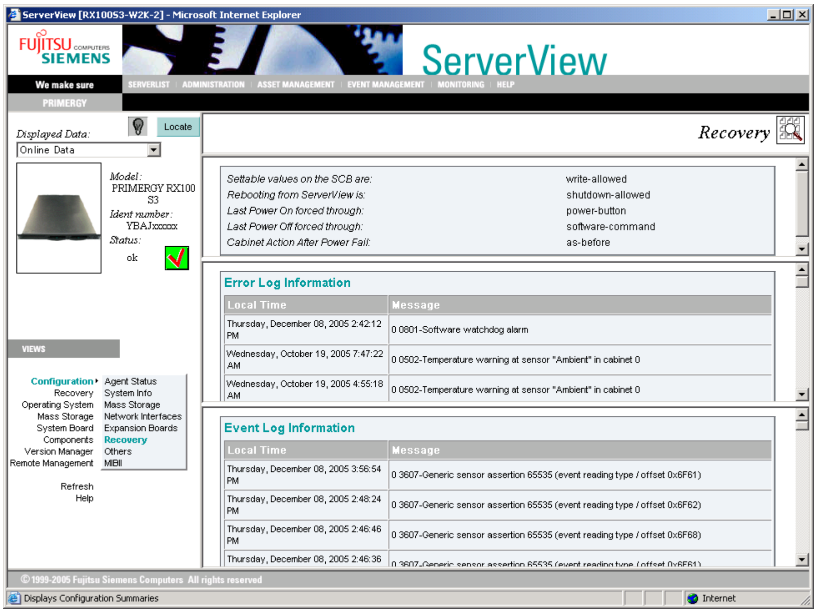
Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

Bus: ISA #1

Function # 1:	**ISAPNP**
Used I/O Ports:	0A79h - 0A79h (NOT Shared) 0279h - 0279h (NOT Shared) 0274h - 0277h (NOT Shared)
Function # 2:	**PCI**
Used Memory Ranges:	000A0000h - 000BFFFFh 000C8000h - 000DFFFFh 20000000h - EFFFFFFFh F4000000h - FEBFFFFFh FED00400h - FEDFFFFFh FEF00000h - FFAFFFFFh FFC00000h - FFEFFFFFh
Used I/O Ports:	0000h - 0CF7h (NOT Shared) 0D00h - FFFFh (NOT Shared)
Function # 3:	**Intel(r) 82802 Firmware Hub Device**
Used Memory Ranges:	FFB00000h - FFBFFFFFh
Function # 4:	
	FEC00000h - FECFFFFFh

■ Recovery

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



Displayed Data: Online Data

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

Settable values on the SCB are:	write-allowed
Rebooting from ServerView is:	shutdown-allowed
Last Power On forced through:	power-button
Last Power Off forced through:	software-command
Cabinet Action After Power Fail:	as-before

Error Log Information

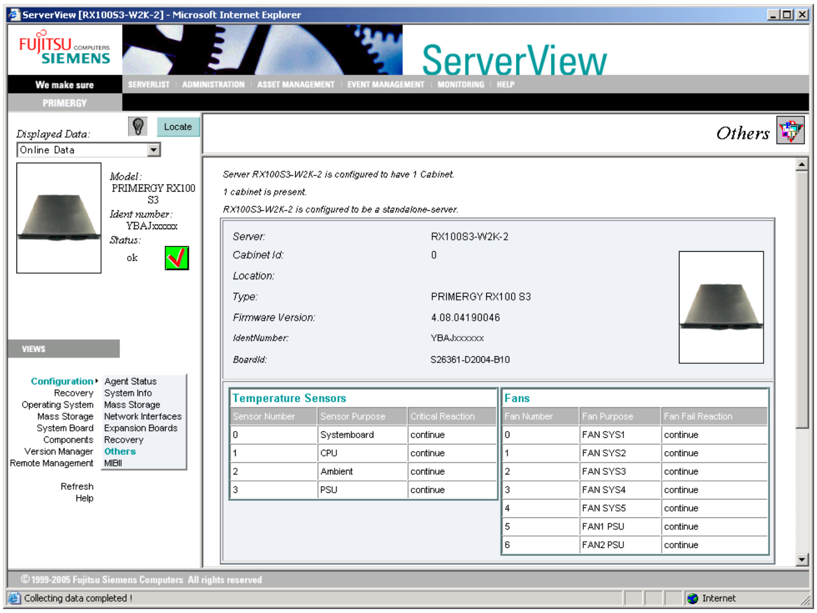
Local Time	Message
Thursday, December 08, 2005 2:42:12 PM	0 0801-Software watchdog alarm
Wednesday, October 19, 2005 7:47:22 AM	0 0502-Temperature warning at sensor "Ambient" in cabinet 0
Wednesday, October 19, 2005 4:55:18 AM	0 0502-Temperature warning at sensor "Ambient" in cabinet 0

Event Log Information

Local Time	Message
Thursday, December 08, 2005 3:56:54 PM	0 3607-Generic sensor assertion 65535 (event reading type / offset 0x6F61)
Thursday, December 08, 2005 2:48:24 PM	0 3607-Generic sensor assertion 65535 (event reading type / offset 0x6F62)
Thursday, December 08, 2005 2:46:46 PM	0 3607-Generic sensor assertion 65535 (event reading type / offset 0x6F68)
Thursday, December 08, 2005 2:46:36	0 3607-Generic sensor assertion 65535 (event reading type / offset 0x6F61)

■ Others

Displays information about fans and temperature sensors.



Displayed Data: Online Data

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

Others

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:	4.08.04190046
IdentNumber:	YBAJxxxxxx
BoardId:	S26361-D2004-B10

Temperature Sensors

Sensor Number	Sensor Purpose	Critical Reaction
0	Systemboard	continue
1	CPU	continue
2	Ambient	continue
3	PSU	continue

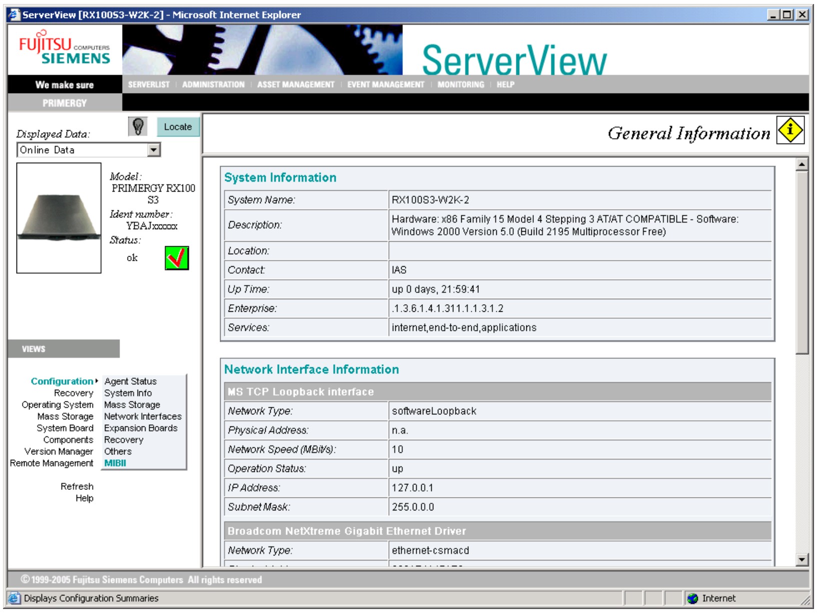
Fans

Fan Number	Fan Purpose	Fan Fail Reaction
0	FAN SYS1	continue
1	FAN SYS2	continue
2	FAN SYS3	continue
3	FAN SYS4	continue
4	FAN SYS5	continue
5	FAN1 PSU	continue
6	FAN2 PSU	continue

Collecting data completed !

■ MIB II

Displays MIB II information.



Displayed Data: Online Data

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

General Information

System Information

System Name:	RX100S3-W2K-2
Description:	Hardware: x86 Family 15 Model 4 Stepping 3 AT/AT 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

MS TCP Loopback interface	
Network Type:	softwareLoopback
Physical Address:	n.a.
Network Speed (MBit/s):	10
Operation Status:	up
IP Address:	127.0.0.1
Subnet Mask:	255.0.0.0
Broadcom NetXtreme Gigabit Ethernet Driver	
Network Type:	ethernet-csmacd

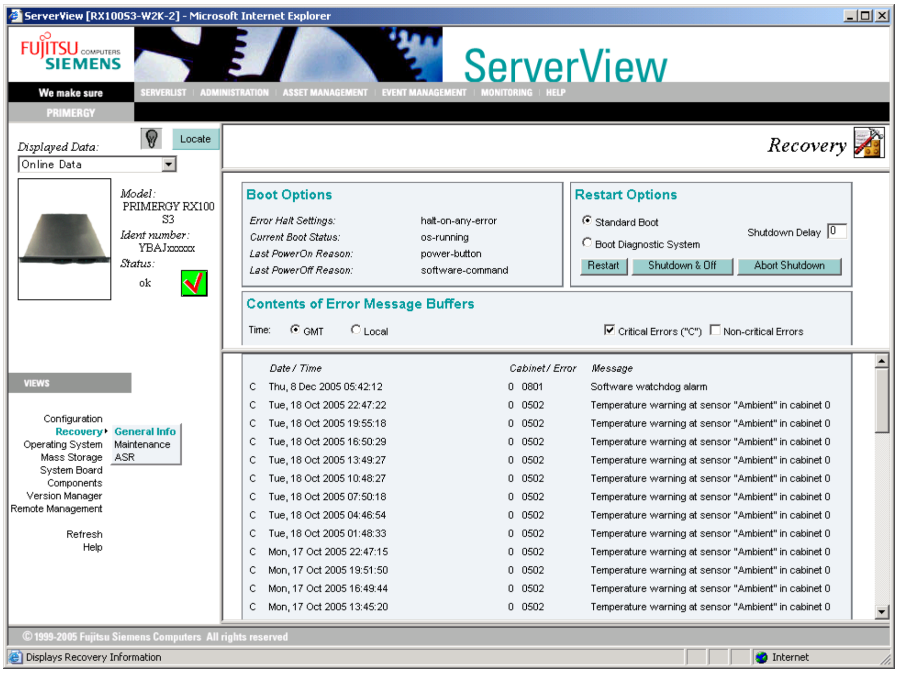
Displays Configuration Summaries

3.2.4 Recovery

In [Recovery], there are three menu items: "■ Recovery" (→pg.108), "■ Maintenance" (→pg.110) and "3.4 Serious Error Handling (ASR)" (→pg.130).

■ Recovery

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


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
PRIMERGY
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
Locate
Recovery
VIEWS
Configuration
Recovery
General Info
Maintenance
ASR
Operating System
Mass Storage
System Board
Components
Version Manager
Remote Management
Refresh
Help
Restart
Shutdown & Off
Abort Shutdown
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Displays Recovery Information
Internet

Displayed Data: Online Data

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

Boot Options

Error Halt Settings:	halt-on-any-error
Current Boot Status:	os-running
Last PowerOn Reason:	power-button
Last PowerOff Reason:	software-command

Restart Options

● Standard Boot
○ Boot Diagnostic System
Shutdown Delay 0

Contents of Error Message Buffers

Time: ● GMT ○ Local ☑ Critical Errors ("C") □ Non-critical Errors

	Date / Time	*Cabinet / Error*		*Message*
C	Thu, 8 Dec 2005 05:42:12	0	0801	Software watchdog alarm
C	Tue, 18 Oct 2005 22:47:22	0	0502	Temperature warning at sensor "Ambient" in cabinet 0
C	Tue, 18 Oct 2005 19:55:18	0	0502	Temperature warning at sensor "Ambient" in cabinet 0
C	Tue, 18 Oct 2005 16:50:29	0	0502	Temperature warning at sensor "Ambient" in cabinet 0
C	Tue, 18 Oct 2005 13:49:27	0	0502	Temperature warning at sensor "Ambient" in cabinet 0
C	Tue, 18 Oct 2005 10:48:27	0	0502	Temperature warning at sensor "Ambient" in cabinet 0
C	Tue, 18 Oct 2005 07:50:18	0	0502	Temperature warning at sensor "Ambient" in cabinet 0
C	Tue, 18 Oct 2005 04:46:54	0	0502	Temperature warning at sensor "Ambient" in cabinet 0
C	Tue, 18 Oct 2005 01:48:33	0	0502	Temperature warning at sensor "Ambient" in cabinet 0
C	Mon, 17 Oct 2005 22:47:15	0	0502	Temperature warning at sensor "Ambient" in cabinet 0
C	Mon, 17 Oct 2005 19:51:50	0	0502	Temperature warning at sensor "Ambient" in cabinet 0
C	Mon, 17 Oct 2005 16:49:44	0	0502	Temperature warning at sensor "Ambient" in cabinet 0
C	Mon, 17 Oct 2005 13:45:20	0	0502	Temperature warning at sensor "Ambient" in cabinet 0

● 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.92).
- ▶ [Boot Diagnostic System] is not supported. Do not select this option.

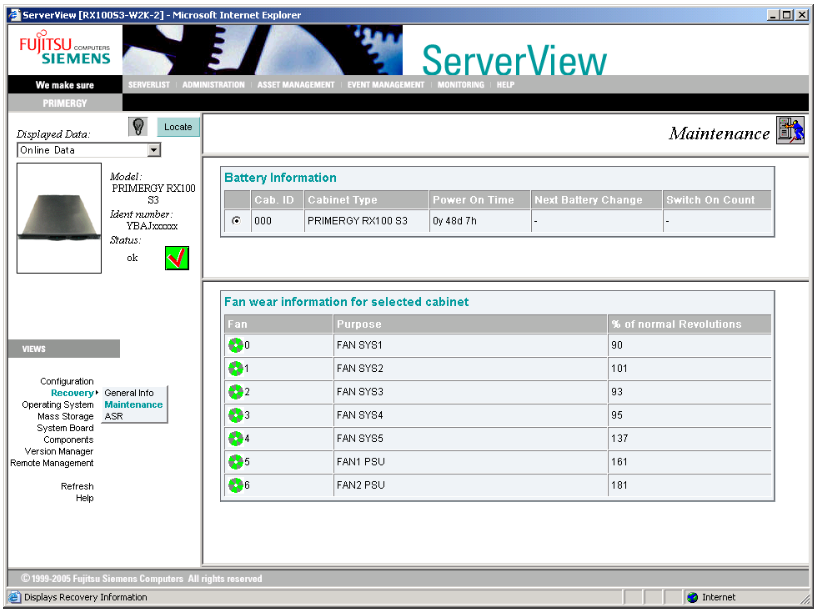
● Contents of Error Message Buffers

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.



Maintenance

Battery Information

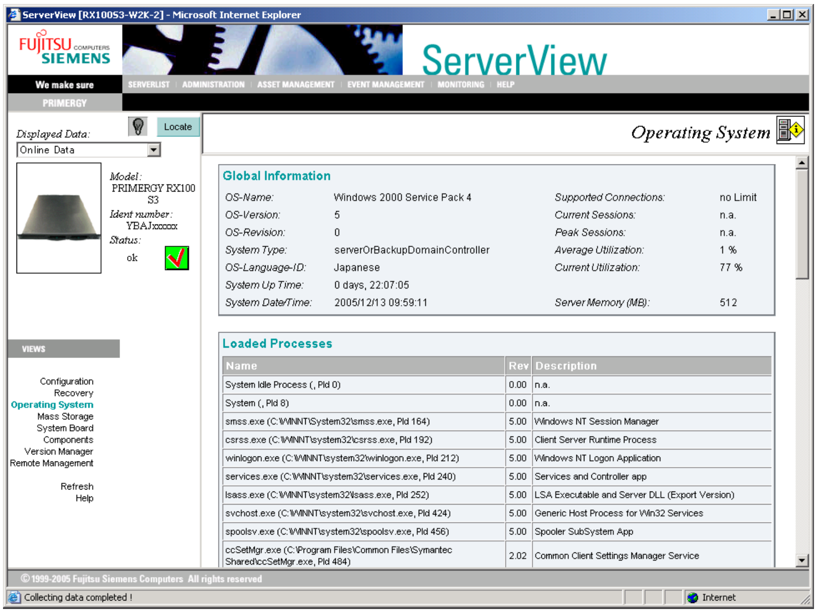
	Cab. ID	Cabinet Type	Power On Time	Next Battery Change	Switch On Count
●	000	PRIMERGY RX100 S3	0y 48d 7h	-	-

Fan wear information for selected cabinet

Fan	Purpose	% of normal Revolutions
0	FAN SYS1	90
1	FAN SYS2	101
2	FAN SYS3	93
3	FAN SYS4	95
4	FAN SYS5	137
5	FAN1 PSU	161
6	FAN2 PSU	181

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.


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
PRIMERGY
Locate
Displayed Data:
Online Data
Model:
PRIMERGY RX100 S3
Ident number:
YBAJxxxxxx
Status:
ok
VIEWS
Configuration
Recovery
Operating System
Mass Storage
System Board
Components
Version Manager
Remote Management
Refresh
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Collecting data completed !
Internet

Operating System

Global Information

OS-Name:	Windows 2000 Service Pack 4	Supported Connections:	no Limit
OS-Version:	5	Current Sessions:	n.a.
OS-Revision:	0	Peak Sessions:	n.a.
System Type:	serverOrBackupDomainController	Average Utilization:	1 %
OS-Language-ID:	Japanese	Current Utilization:	77 %
System Up Time:	0 days, 22:07:05		
System Date/Time:	2005/12/13 09:59:11	Server Memory (MB):	512

Loaded Processes

Name	Rev	Description
System Idle Process (, PId 0)	0.00	n.a.
System (, PId 8)	0.00	n.a.
smss.exe (C:\WINNT\System32\smss.exe, PId 164)	5.00	Windows NT Session Manager
csrss.exe (C:\WINNT\system32\csrss.exe, PId 192)	5.00	Client Server Runtime Process
winlogon.exe (C:\WINNT\system32\winlogon.exe, PId 212)	5.00	Windows NT Logon Application
services.exe (C:\WINNT\system32\services.exe, PId 240)	5.00	Services and Controller app
lsass.exe (C:\WINNT\system32\lsass.exe, PId 252)	5.00	LSA Executable and Server DLL (Export Version)
svchost.exe (C:\WINNT\system32\svchost.exe, PId 424)	5.00	Generic Host Process for Win32 Services
spoolsv.exe (C:\WINNT\system32\spoolsv.exe, PId 456)	5.00	Spooler SubSystem App
ccSetMgr.exe (C:\Program Files\Common Files\Symantec Shared\ccSetMgr.exe, PId 484)	2.02	Common Client Settings Manager Service

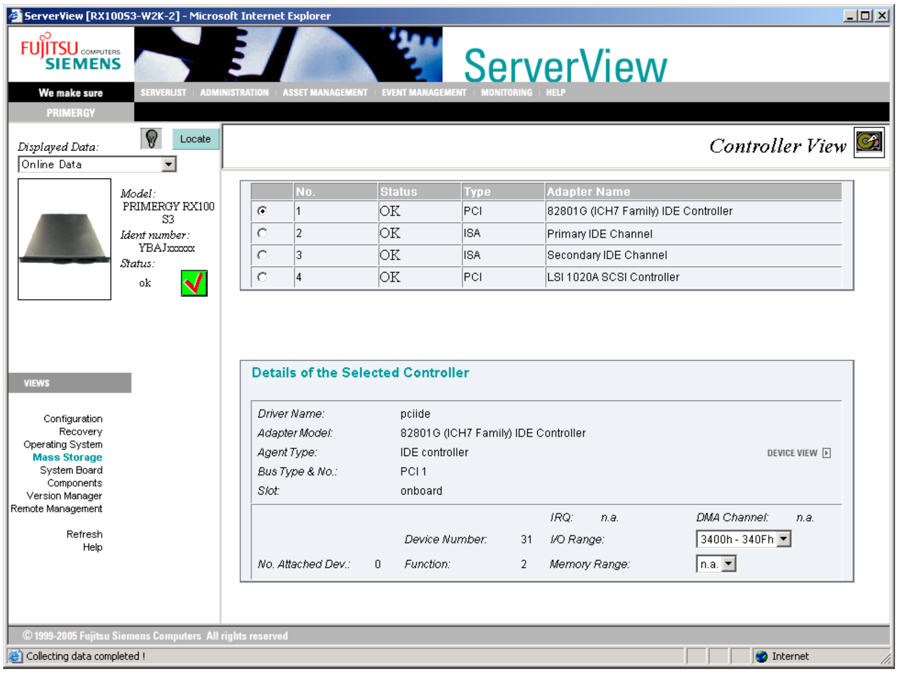
3.2.6 Verifying the Status of Mass Storage

For Mass Storage, you can verify the following states:

- Verifying the device controllers and device status. →"■ Controller View" (pg.111)
- Verifying information about the system files in the logical drives. →"■ Logical View" (pg.115)
- Verifying detailed information about the partitions. →"■ Partition View" (pg.115)

■ Controller View

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


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
PRIMERGY
Locate
VIEWS
Configuration
Recovery
Operating System
Mass Storage
System Board
Components
Version Manager
Remote Management
Refresh
Help
DEVICE VIEW
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Internet

Controller View

Displayed Data: Online Data

Model: PRIMERGY RX100 S3

Ident number: YBAJxxxxxx

Status: ok

	No.	Status	Type	Adapter Name
●	1	OK	PCI	82801G (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: 82801G (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.

Collecting data completed !

● 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

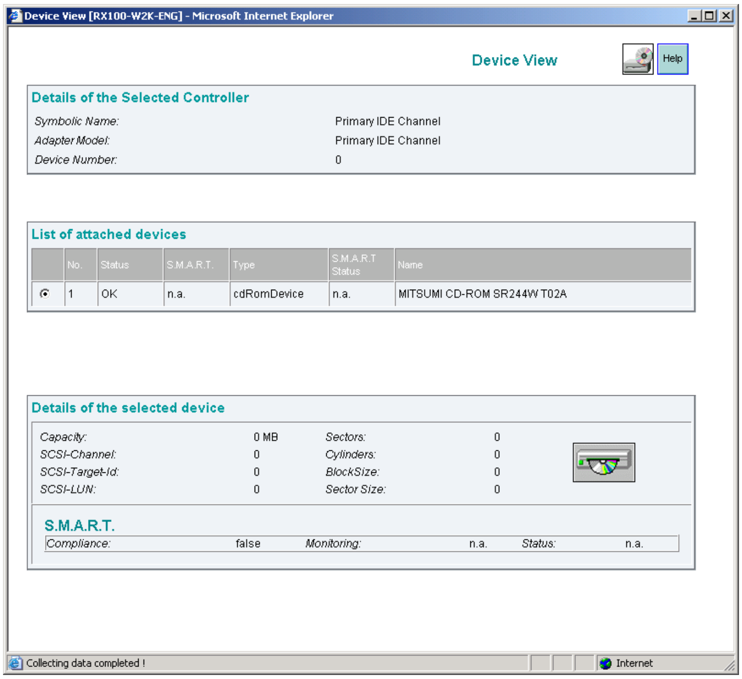
Detailed information about the controller selected in the controller list is displayed. The links to [MULTIPATH VIEW ▸] and [DEVICE VIEW ▸] are displayed to the right. When you click these links, a detailed information window opens. (→"● Device View" (pg.112)) The links shown here and the detailed information 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 [Devise View] window opens and detailed information about the devices connected to the controller is displayed.


Device View [RX100-W2K-ENG] - Microsoft Internet Explorer
Device View
Help
Collecting data completed !
Internet

Details of the Selected Controller

Symbolic Name:	Primary IDE Channel
Adapter Model:	Primary IDE Channel
Device Number:	0

List of attached devices

	No.	Status	S.M.A.R.T.	Type	S.M.A.R.T Status	Name
●	1	OK	n.a.	cdRomDevice	n.a.	MITSUMI CD-ROM SR244W T02A

Details of the selected device

Capacity:	0 MB	*Sectors:*	0
SCSI-Channel:	0	*Cylinders:*	0
SCSI-Target-Id:	0	*BlockSize:*	0
SCSI-LUN:	0	*Sector Size:*	0

S.M.A.R.T.

Compliance:	false	*Monitoring:*	n.a.	*Status:*	n.a.

- 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)" (pg.113)

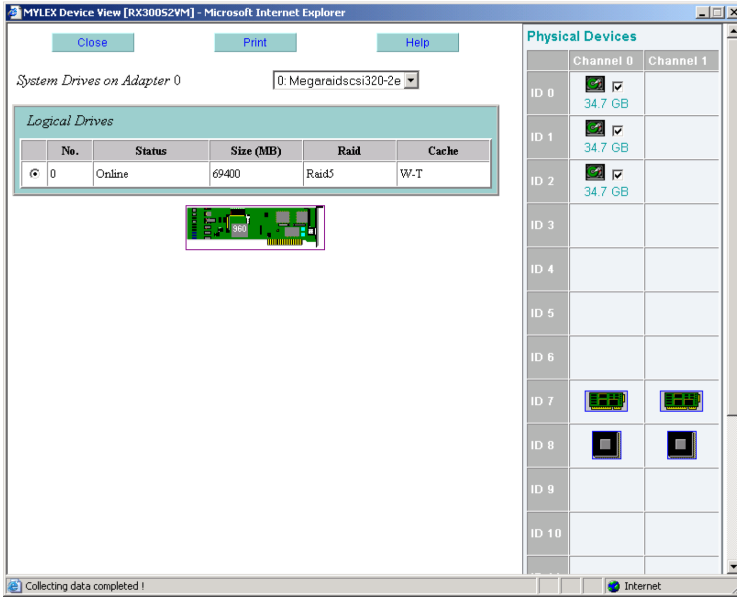
POINT

- ▸ 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 Devise View (View RAID)

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

When you click [DEVICE VIEW], the [Devise 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 [Devise View] window, the following window is displayed.



System Drives on Adapter 0 — 0: Megaraidscsi320-2e

Logical Drives

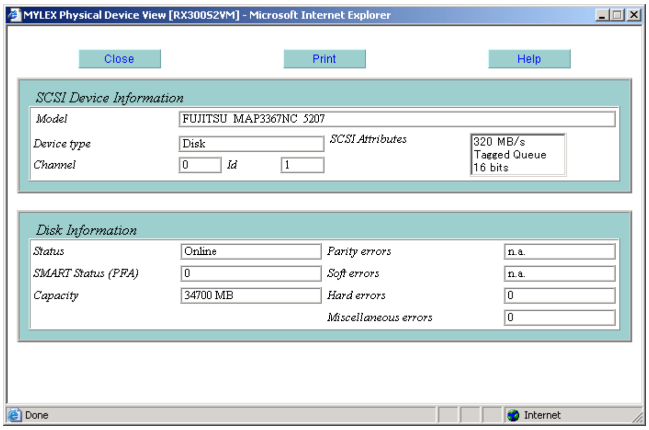
	No.	Status	Size (MB)	Raid	Cache
◉	0	Online	69400	Raid5	W-T

Physical Devices

	Channel 0	Channel 1
ID 0	☑ 34.7 GB	
ID 1	☑ 34.7 GB	
ID 2	☑ 34.7 GB	
ID 3		
ID 4		
ID 5		
ID 6		
ID 7		
ID 8		
ID 9		
ID 10		

Collecting data completed !

- 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.


MYLEX Physical Device View [RX30052VM] - Microsoft Internet Explorer
Close
Print
Help
Internet

SCSI Device Information

Model	FUJITSU MAP3367NC 5207		
Device type	Disk	SCSI Attributes	320 MB/s Tagged Queue 16 bits
Channel	0	Id	1

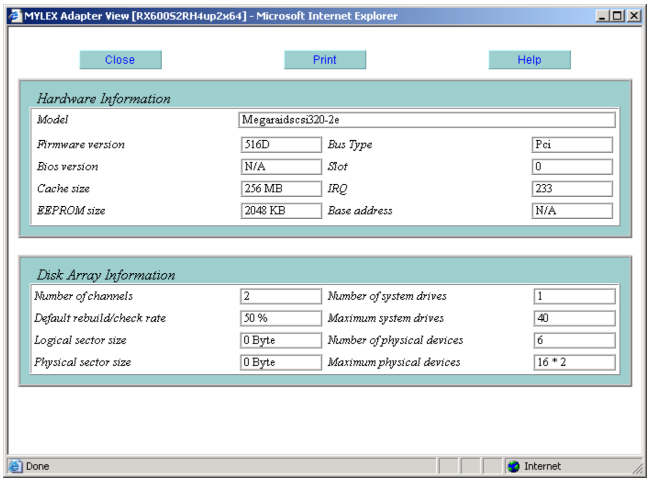
Disk Information

Status	Online	Parity errors	n.a.
SMART Status (PFA)	0	Soft errors	n.a.
Capacity	34700 MB	Hard errors	0
		Miscellaneous errors	0

Done

- 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.


MYLEX Adapter View [RX600S2RH4up2x64] - Microsoft Internet Explorer
Close
Print
Help
Done
Internet

Hardware Information

Model	Megaraidscsi320-2e		
Firmware version	516D	*Bus Type*	Pci
Bios version	N/A	*Slot*	0
Cache size	256 MB	*IRQ*	233
EEPROM size	2048 KB	*Base address*	N/A

Disk Array Information

Number of channels	2	*Number of system drives*	1
Default rebuild/check rate	50 %	*Maximum system drives*	40
Logical sector size	0 Byte	*Number of physical devices*	6
Physical sector size	0 Byte	*Maximum physical devices*	16 * 2

POINT

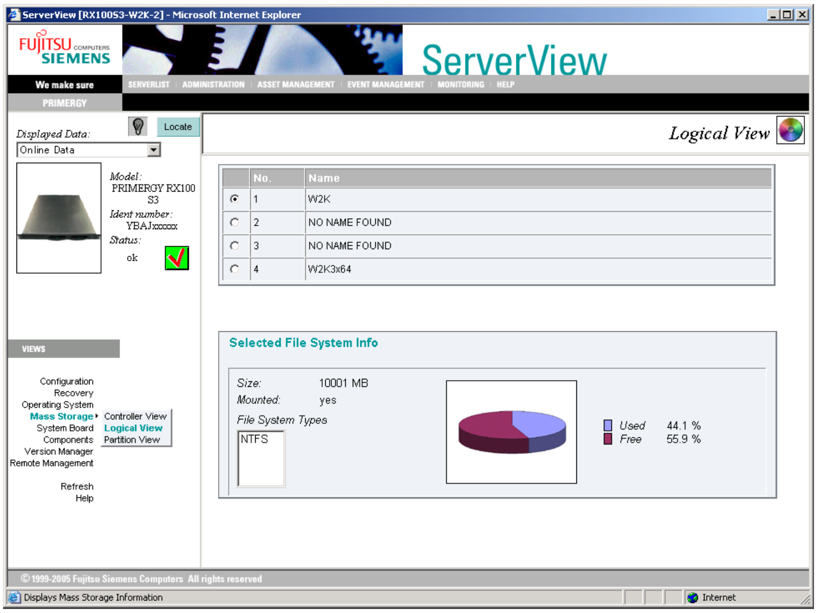
- In order to monitor and display the RAID card, make sure to install the management tool supplied with the card. The Management Console can be notified of information about detected errors.

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.

■ 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.


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
PRIMERGY
Locate
VIEWS
Configuration
Recovery
Operating System
Mass Storage
Controller View
Logical View
Partition View
System Board
Components
Version Manager
Remote Management
Refresh
Help
©1999-2005 Fujitsu Siemens Computers All rights reserved
Displays Mass Storage Information
Internet

Displayed Data: Online Data

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

Logical View

	No.	Name
●	1	W2K
○	2	NO NAME FOUND
○	3	NO NAME FOUND
○	4	W2K3x64

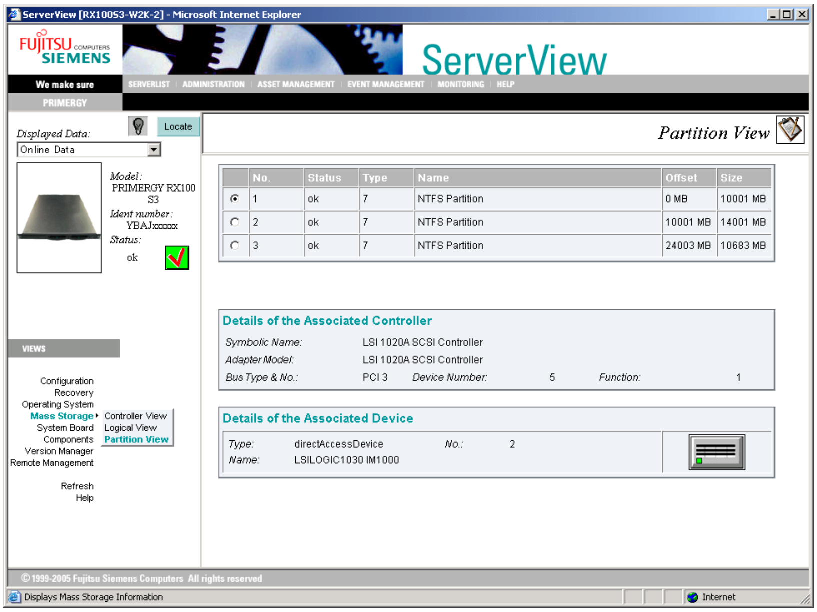
Selected File System Info

Size: 10001 MB
Mounted: yes
File System Types
NTFS

▨	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.


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
PRIMERGY
Locate
VIEWS
Configuration
Recovery
Operating System
Mass Storage
Controller View
Logical View
Partition View
System Board
Components
Version Manager
Remote Management
Refresh
Help
©1999-2005 Fujitsu Siemens Computers All rights reserved
Displays Mass Storage Information
Internet

Displayed Data: Online Data

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

Partition View

	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: LSILOGIC1030 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.

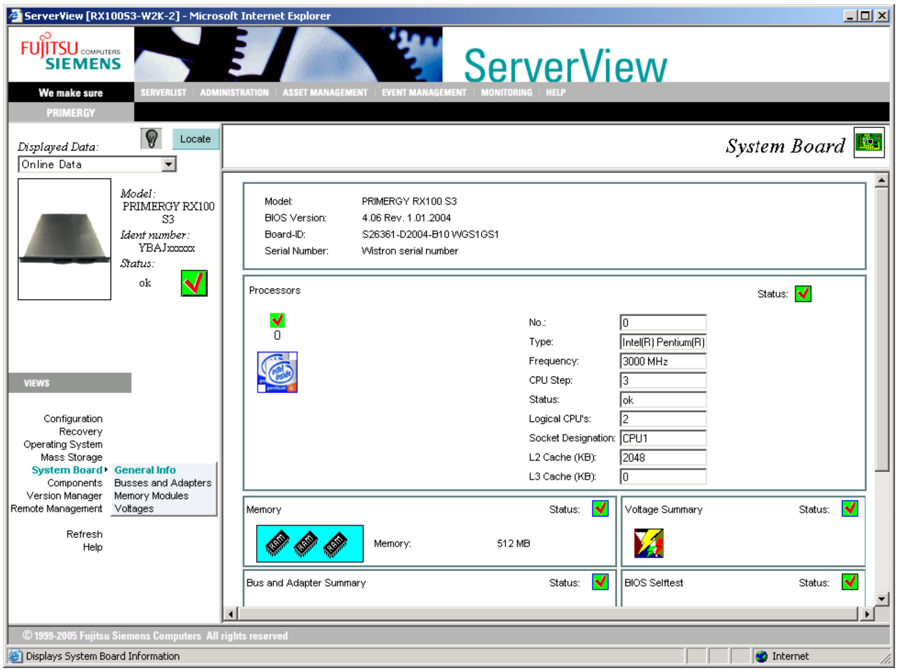
3.2.7 Verifying the Baseboard Status

You can verify the following states for the baseboard:

- Verifying the baseboard status. →"■ System Board" (pg.116)
- Verifying information about the adaptors connected to the server bus. →"■ Busses and Adapters" (pg.118)
- Verifying the status of the memory modules installed in the server. →"■ Memory Modules" (pg.118)
- Verifying the voltage states at certain points of the baseboard.→"■ Voltages" (pg.119)

■ 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.


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
PRIMERGY
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
Locate
VIEWS
Configuration
Recovery
Operating System
Mass Storage
System Board
Components
Version Manager
Remote Management
General Info
Busses and Adapters
Memory Modules
Voltages
Refresh
Help
System Board
©1999-2005 Fujitsu Siemens Computers All rights reserved
Displays System Board Information
Internet

Displayed Data: Online Data

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

Model: PRIMERGY RX100 S3
BIOS Version: 4.06 Rev. 1.01.2004
Board-ID: S26361-D2004-B10 WGS1GS1
Serial Number: Wistron serial number

Processors Status: ✓
0
No.: 0
Type: Intel(R) Pentium(R)
Frequency: 3000 MHz
CPU Step: 3
Status: ok
Logical CPU's: 2
Socket Designation: CPU1
L2 Cache (KB): 2048
L3 Cache (KB): 0

Memory Status: ✓
Memory: 512 MB

Voltage Summary Status: ✓

Bus and Adapter Summary Status: ✓

BIOS Selftest Status: ✓

● 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.118)] window appears.

● Voltage Summary

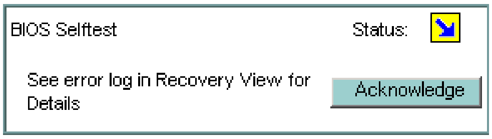
The voltage status is displayed. When you click the status icon, the [Voltages (→ P.119)] window appears.

● Bus and Adapter Summary

The supported bus types and status are displayed. When you click the status icon, the [Busses and Adapters (→ P.118)] window appears.

● BIOS Selftest

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



BIOS Selftest

Status:

See error log in Recovery View for Details

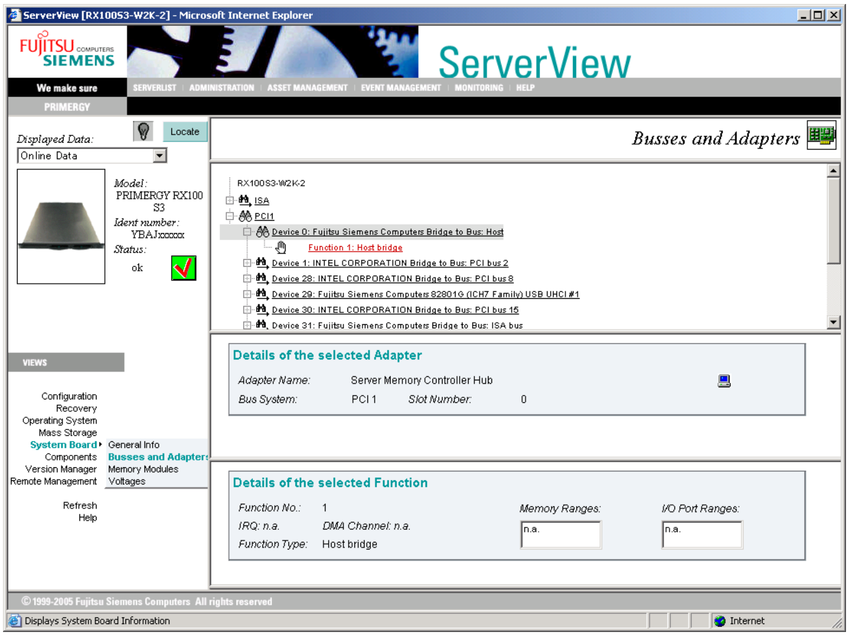
If the [degraded] icon is displayed as the status, you can revert the icon to [OK] by clicking [Acknowledge]. Verify the detailed [degraded] information in the [Contents of Error Message Buffers] in the [Recovery (→ P.108)] window.
However, if the BIOS (version) does not have a self-test notification 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 buses 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.


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
Locate
VIEWS
Configuration
Recovery
Operating System
Mass Storage
System Board
Components
Version Manager
Remote Management
General Info
Busses and Adapters
Memory Modules
Voltages
Refresh
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Displays System Board Information
Internet

Displayed Data: Online Data

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

Busses and Adapters

RX100S3-W2K-2
- ISA
- PCI1
  - Device 0: Fujitsu Siemens Computers Bridge to Bus: Host
    - Function 1: Host bridge
  - Device 1: INTEL CORPORATION Bridge to Bus: PCI bus 2
  - Device 28: INTEL CORPORATION Bridge to Bus: PCI bus 8
  - Device 29: Fujitsu Siemens Computers 82801G (ICH7 Family) USB UHCI #1
  - Device 30: INTEL CORPORATION Bridge to Bus: PCI bus 15
  - Device 31: Fujitsu Siemens Computers Bridge to Bus: ISA bus

Details of the selected Adapter

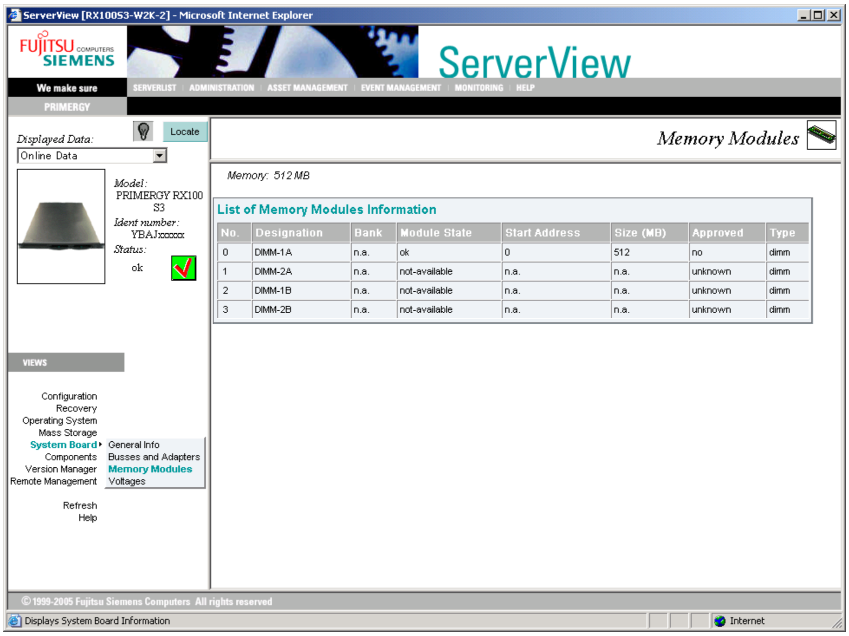
Adapter Name: Server Memory Controller Hub
Bus System: PCI 1 Slot Number: 0

Details of the selected Function

Function No.: 1
IRQ: n.a. DMA Channel: n.a.
Function Type: Host bridge
Memory Ranges: n.a.
I/O Port Ranges: n.a.

■ 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.


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
Locate
VIEWS
Configuration
Recovery
Operating System
Mass Storage
System Board
Components
Version Manager
Remote Management
General Info
Busses and Adapters
Memory Modules
Voltages
Refresh
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Displays System Board Information
Internet

Displayed Data: Online Data

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

Memory Modules

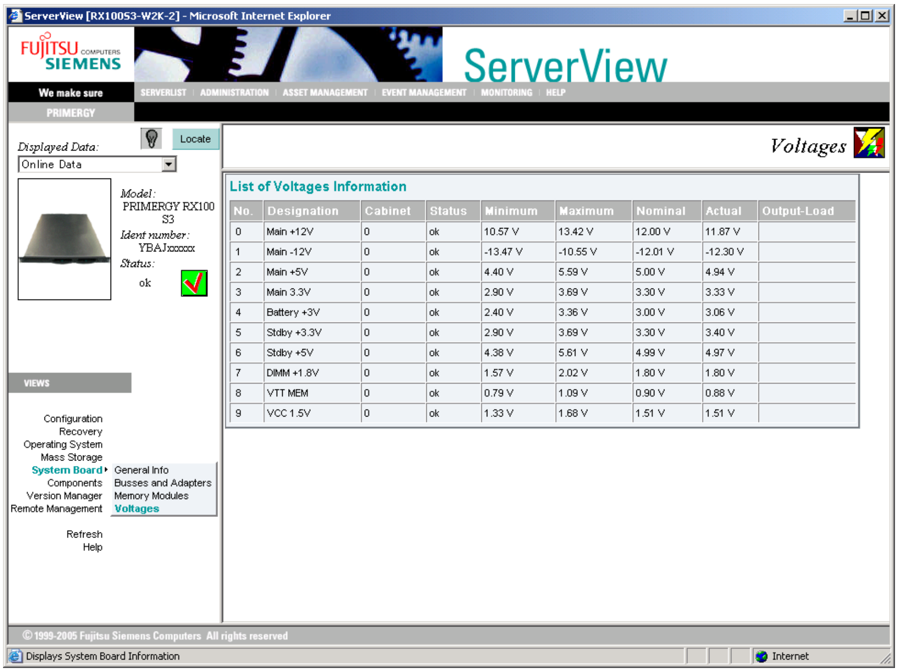
Memory: 512 MB

List of Memory Modules Information

No.	Designation	Bank	Module State	Start Address	Size (MB)	Approved	Type
0	DIMM-1A	n.a.	ok	0	512	no	dimm
1	DIMM-2A	n.a.	not-available	n.a.	n.a.	unknown	dimm
2	DIMM-1B	n.a.	not-available	n.a.	n.a.	unknown	dimm
3	DIMM-2B	n.a.	not-available	n.a.	n.a.	unknown	dimm

■ 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.


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
PRIMERGY
Locate
VIEWS
Configuration
Recovery
Operating System
Mass Storage
System Board
Components
Version Manager
Remote Management
General Info
Busses and Adapters
Memory Modules
Voltages
Refresh
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Internet

Displayed Data: Online Data

Model: PRIMERGY RX100 S3

Ident number: YBAJxxxxxx

Status: ok ✓

Voltages

List of Voltages Information

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	Stdby +3.3V	0	ok	2.90 V	3.69 V	3.30 V	3.40 V	
6	Stdby +5V	0	ok	4.38 V	5.61 V	4.99 V	4.97 V	
7	DIMM +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	

Displays System Board Information

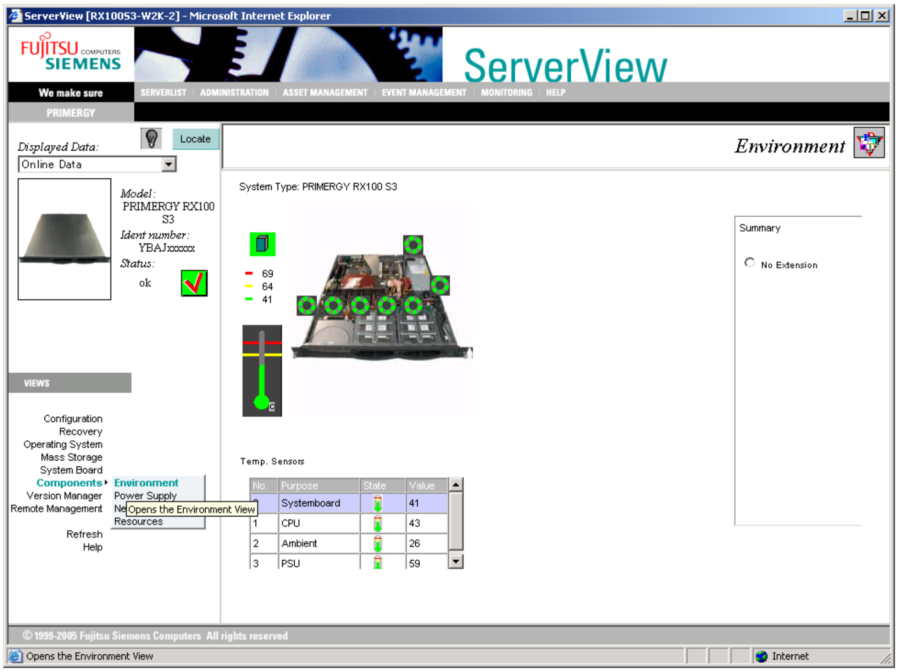
3.2.8 Verifying the Component Status

For the components, you can verify the following states:

- Verifying the server temperature and the fan status. →"■ Verifying the Environment Status" (pg.247)
- Verifying the server power supply information. →"■ Verifying the Power Supply Status" (pg.245)
- Verifying information about the Network Interfaces installed in the server. →"■ Network Interfaces" (pg.123)
- Verifying the system resources.→"■ Resources" (pg.123)

■ Environment

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


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
PRIMERGY
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
Locate
Environment
VIEWS
Configuration
Recovery
Operating System
Mass Storage
System Board
Components
Version Manager
Remote Management
Refresh
Help
Environment
Power Supply
Ne
Resources
Opens the Environment View
69
64
41
C
Summary
○ No Extension
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Internet

Displayed Data: Online Data

Model: PRIMERGY RX100 S3

Ident number: YBAJxxxxxx

Status: ok

System Type: PRIMERGY RX100 S3

Temp. Sensors

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

Opens the Environment View

● 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.

IMPORTANT

- 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

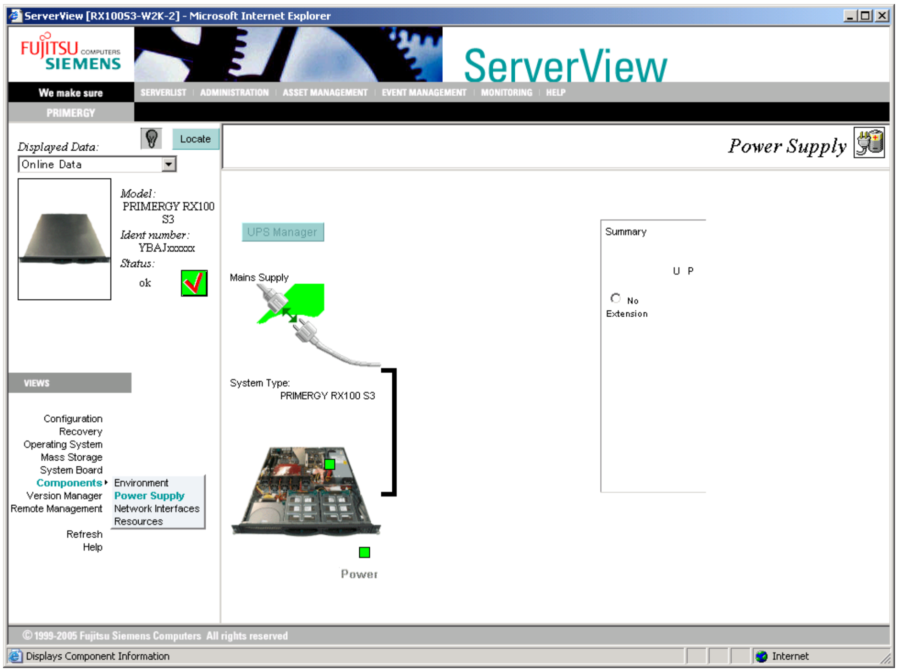
Item	Shutdown	Danger	OK	Sensor Failure	Cannot Verify
Temperature	Red	Yellow	Green	Blue	Gray
Fan	Red	Yellow	Green	---	Gray

● 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.



ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer

Displayed Data: Online Data

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

System Type: PRIMERGY RX100 S3

©1999-2005 Fujitsu Siemens Computers All rights reserved

Displays Component Information

● 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

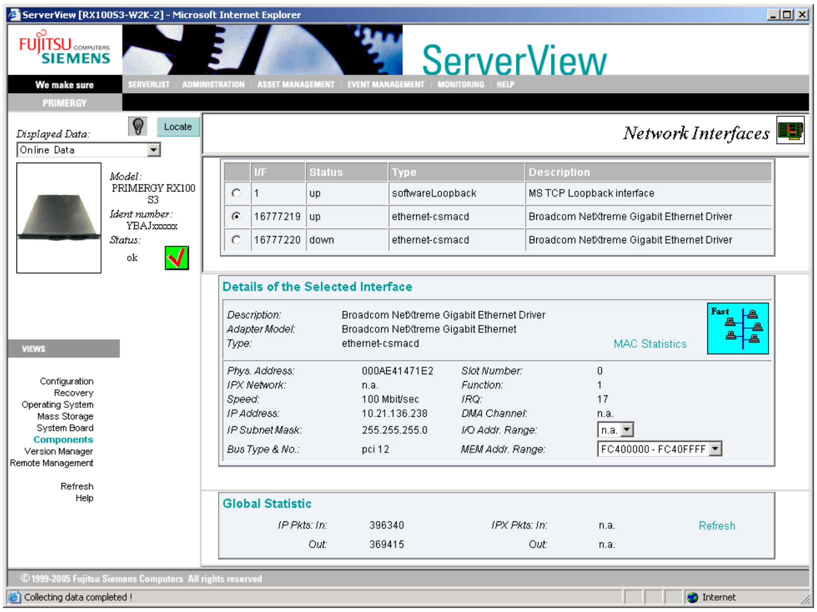
When you select an extension storage device, its status is displayed just like the server status.

● 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.


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
Locate
VIEWS
Configuration
Recovery
Operating System
Mass Storage
System Board
Components
Version Manager
Remote Management
Refresh
Help
Fast
MAC Statistics
Refresh
©1999-2005 Fujitsu Siemens Computers All rights reserved
Internet

Displayed Data: Online Data

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

Network Interfaces

	I/F	Status	Type	Description
○	1	up	softwareLoopback	MS TCP Loopback interface
●	16777219	up	ethernet-csmacd	Broadcom NetXtreme Gigabit Ethernet Driver
○	16777220	down	ethernet-csmacd	Broadcom NetXtreme Gigabit Ethernet Driver

Details of the Selected Interface

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

Phys. Address:	000AE41471E2	Slot Number:	0
IPX Network:	n.a.	Function:	1
Speed:	100 Mbit/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

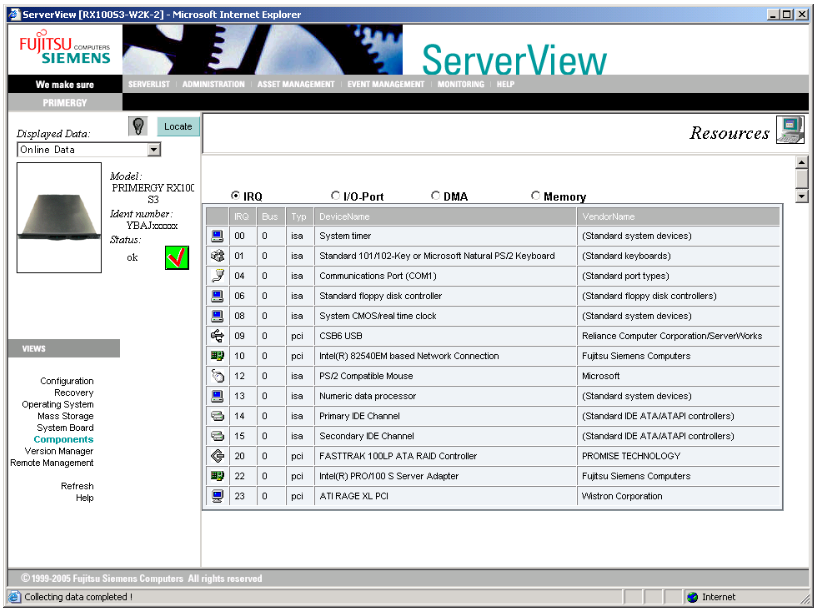
Global Statistic

IP Pkts: In:	396340	IPX Pkts: In:	n.a.
Out:	369415	Out:	n.a.

Collecting data completed !

■ 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.


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
Locate
VIEWS
Configuration
Recovery
Operating System
Mass Storage
System Board
Components
Version Manager
Remote Management
Refresh
Help
©1999-2005 Fujitsu Siemens Computers All rights reserved
Internet

Displayed Data: Online Data

Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

Resources

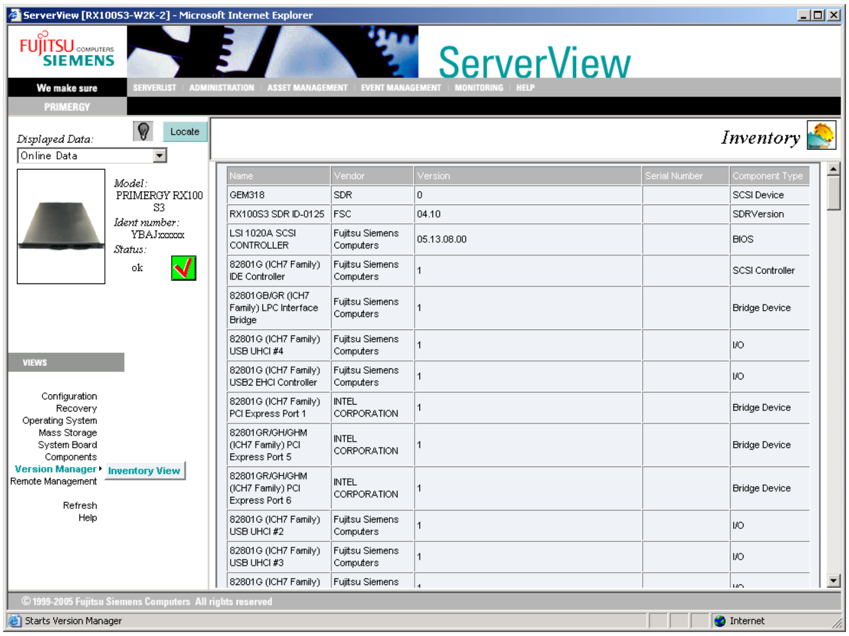
● IRQ ○ I/O-Port ○ DMA ○ Memory

	IRQ	Bus	Typ	DeviceName	VendorName
	00	0	isa	System timer	(Standard system devices)
	01	0	isa	Standard 101/102-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	CSB6 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	FASTTRAK 100LP ATA RAID Controller	PROMISE TECHNOLOGY
	22	0	pci	Intel(R) PRO/100 S Server Adapter	Fujitsu Siemens Computers
	23	0	pci	ATI RAGE XL PCI	Wistron Corporation

Collecting data completed !

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.


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
Locate
Inventory
VIEWS
Configuration
Recovery
Operating System
Mass Storage
System Board
Components
Version Manager
Inventory View
Remote Management
Refresh
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Starts Version Manager
Internet

Displayed Data: Online Data

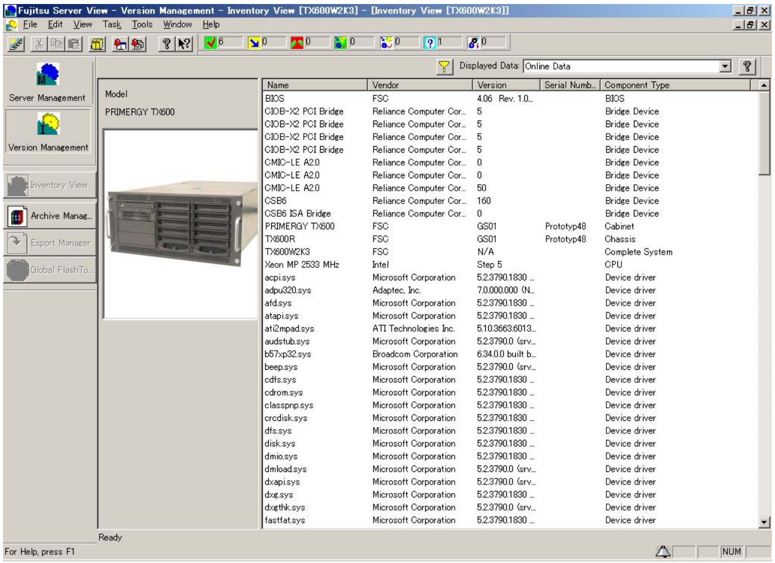
Model: PRIMERGY RX100 S3
Ident number: YBAJxxxxxx
Status: ok

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.


Fujitsu Server View - Version Management - Inventory View [TX600W2K3] - [Inventory View [TX600W2K3]]
File Edit View Task Tools Window Help
6
0
0
0
0
1
0
Server Management
Version Management
Inventory View
Archive Manag...
Export Manager
Global FlashTo...
Ready
For Help, press F1
NUM

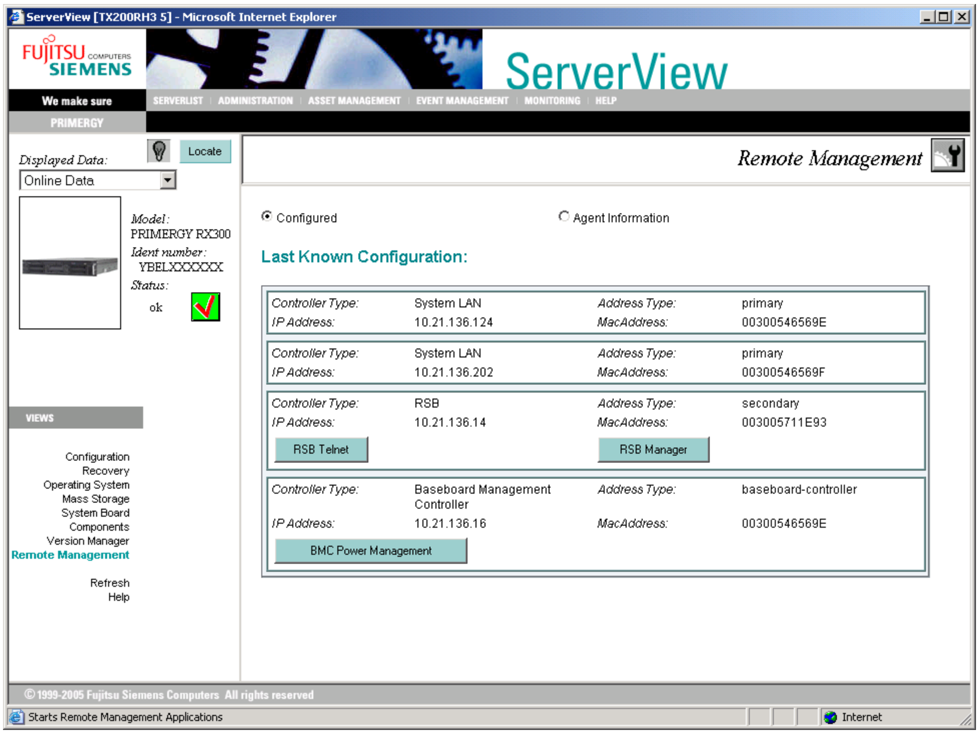
Displayed Data: Online Data

Model
PRIMERGY TX600

Name	Vendor	Version	Serial Numb...	Component Type
BIOS	FSC	4.06 Rev. 1.0...		BIOS
CIOB-X2 PCI Bridge	Reliance Computer Cor...	5		Bridge Device
CIOB-X2 PCI Bridge	Reliance Computer Cor...	5		Bridge Device
CIOB-X2 PCI Bridge	Reliance Computer Cor...	5		Bridge Device
CIOB-X2 PCI Bridge	Reliance Computer Cor...	5		Bridge Device
CMIC-LE A2.0	Reliance Computer Cor...	0		Bridge Device
CMIC-LE A2.0	Reliance Computer Cor...	0		Bridge Device
CMIC-LE A2.0	Reliance Computer Cor...	50		Bridge Device
CSB6	Reliance Computer Cor...	160		Bridge Device
CSB6 ISA Bridge	Reliance Computer Cor...	0		Bridge Device
PRIMERGY TX600	FSC	GS01	Prototyp48	Cabinet
TX600R	FSC	GS01	Prototyp48	Chassis
TX600W2K3	FSC	N/A		Complete System
Xeon MP 2533 MHz	Intel	Step 5		CPU
acpi.sys	Microsoft Corporation	5.2.3790.1830 ...		Device driver
adpu320.sys	Adaptec, Inc.	7.0.000.000 (N...		Device driver
afd.sys	Microsoft Corporation	5.2.3790.1830 ...		Device driver
atapi.sys	Microsoft Corporation	5.2.3790.1830 ...		Device driver
ati2mpad.sys	ATI Technologies Inc.	5.10.3663.6013...		Device driver
audstub.sys	Microsoft Corporation	5.2.3790.0 (srv...		Device driver
b57xp32.sys	Broadcom Corporation	6.34.0.0 built b...		Device driver
beep.sys	Microsoft Corporation	5.2.3790.0 (srv...		Device driver
cdfs.sys	Microsoft Corporation	5.2.3790.1830 ...		Device driver
cdrom.sys	Microsoft Corporation	5.2.3790.1830 ...		Device driver
classpnp.sys	Microsoft Corporation	5.2.3790.1830 ...		Device driver
crcdisk.sys	Microsoft Corporation	5.2.3790.1830 ...		Device driver
dfs.sys	Microsoft Corporation	5.2.3790.1830 ...		Device driver
disk.sys	Microsoft Corporation	5.2.3790.1830 ...		Device driver
dmio.sys	Microsoft Corporation	5.2.3790.1830 ...		Device driver
dmload.sys	Microsoft Corporation	5.2.3790.0 (srv...		Device driver
dxapi.sys	Microsoft Corporation	5.2.3790.0 (srv...		Device driver
dxg.sys	Microsoft Corporation	5.2.3790.1830 ...		Device driver
dxgthk.sys	Microsoft Corporation	5.2.3790.0 (srv...		Device driver
fastfat.sys	Microsoft Corporation	5.2.3790.1830 ...		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.



Displayed Data: Online Data

Model: PRIMERGY RX300

Ident number: YBELXXXXXX

Status: ok ✓

Remote Management

● Configured ○ Agent Information

Last Known Configuration:

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

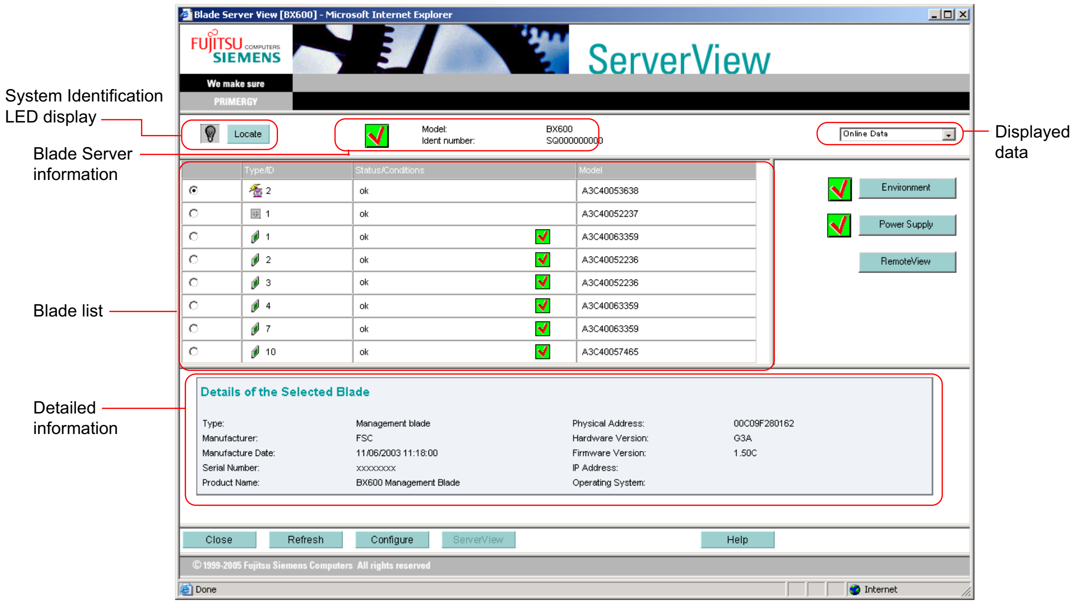
For details, refer to:

- "5.3.2 Start and Exit for RemoteControleService/Web (For iRMC / BMC IPMI connection)" (→pg.275)
- "5.3.3 Start and Exit for RemoteControleService/Web (For RSB connection)" (→pg.278)
- "5.3.1 Start and Exit for RemoteControleService/Web (For iRMC Telnet Connection)" (→pg.273)

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.



Model: BX600
Ident number: SQ000000000

	Type/ID	Status/Conditions	Model
●	2	ok	A3C40053638
○	1	ok	A3C40052237
○	1	ok ✓	A3C40063359
○	2	ok ✓	A3C40052236
○	3	ok ✓	A3C40052236
○	4	ok ✓	A3C40063359
○	7	ok ✓	A3C40063359
○	10	ok ✓	A3C40057465

Details of the Selected Blade

Type:	Management blade	Physical Address:	00C09F280162
Manufacturer:	FSC	Hardware Version:	G3A
Manufacture Date:	11/06/2003 11:18:00	Firmware Version:	1.50C
Serial Number:	xxxxxxxx	IP Address:	
Product Name:	BX600 Management Blade	Operating System:	

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.96).
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 swich blade

: Server blade

● Function Buttons

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

IMPORTANT

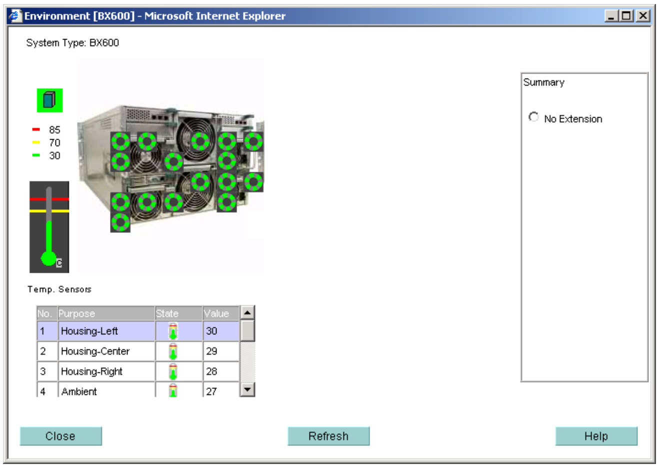
- If the security for the management blade is enabled, the user must log in before operating the function buttons. The user name and password can be configured by accessing the management blade via the Telnet or Web interface.

table: Blade Server Status

Item	Description
Environment	The status for environmental subsystems (fans, temperature) is displayed. →"■ Verifying the Blade Server's Environmental Status" (pg.128)
Power Supply	The status for power supply subsystems is displayed. →"■ Verifying the Blade Server's Power Status" (pg.129)
RemoteView	The [RemoteConsoleService/Web] window appears. "5.3.4 Start and Exit for RemoteControleService/Web (For ManagementBlade connection)" (→pg.280)
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.100). 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.



Environment [BX600] - Microsoft Internet Explorer

System Type: BX600

Temp. Sensors

No.	Purpose	State	Value
1	Housing-Left	🌡	30
2	Housing-Center	🌡	29
3	Housing-Right	🌡	28
4	Ambient	🌡	27

● 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.

IMPORTANT

- 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.

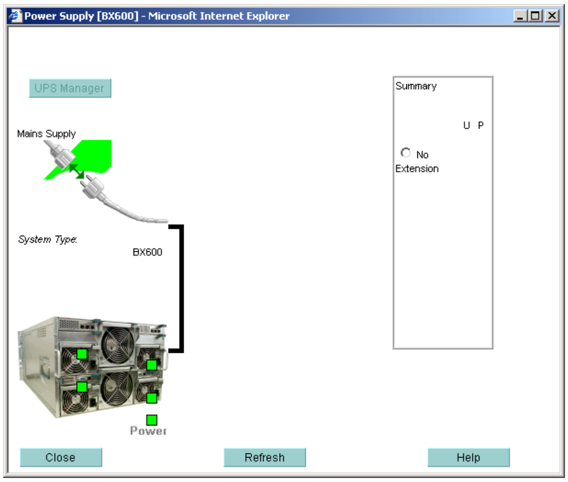
The colors of the fan and temperature sensor icons indicate the following states:

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

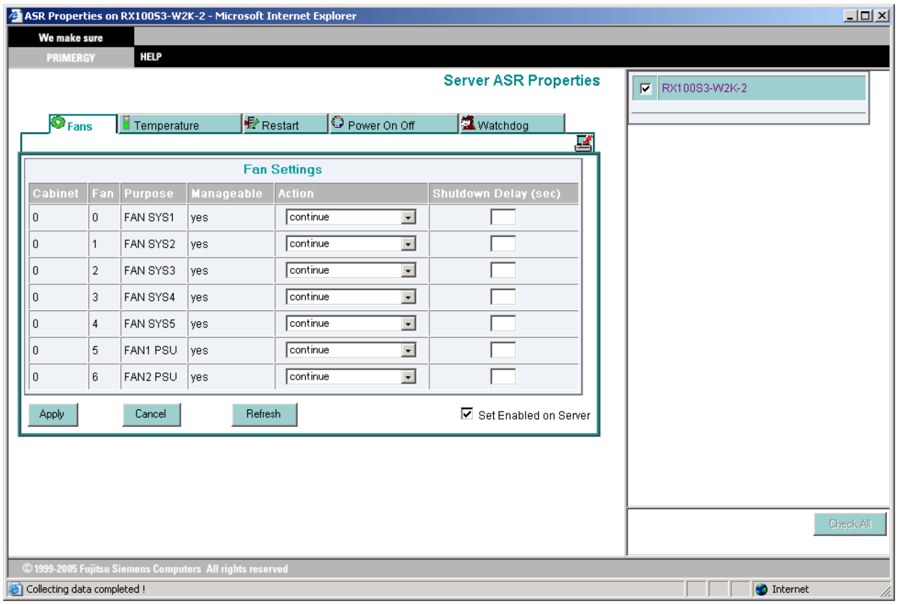
Although the functions are the same between ServerView S2 and Management Console, there are some differences in the item names on the screen. The following describes the screens displayed when operating ServerView S2.

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.


ASR Properties on RX100S3-W2K-2 - Microsoft Internet Explorer
We make sure
PRIMERGY
HELP
Server ASR Properties
Fans
Temperature
Restart
Power On Off
Watchdog
Apply
Cancel
Refresh
RX100S3-W2K-2
Check All
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Collecting data completed !
Internet

Fan Settings

Cabinet	Fan	Purpose	Manageable	Action	Shutdown Delay (sec)
0	0	FAN SYS1	yes	continue	
0	1	FAN SYS2	yes	continue	
0	2	FAN SYS3	yes	continue	
0	3	FAN SYS4	yes	continue	
0	4	FAN SYS5	yes	continue	
0	5	FAN1 PSU	yes	continue	
0	6	FAN2 PSU	yes	continue	

☑ Set Enabled on Server

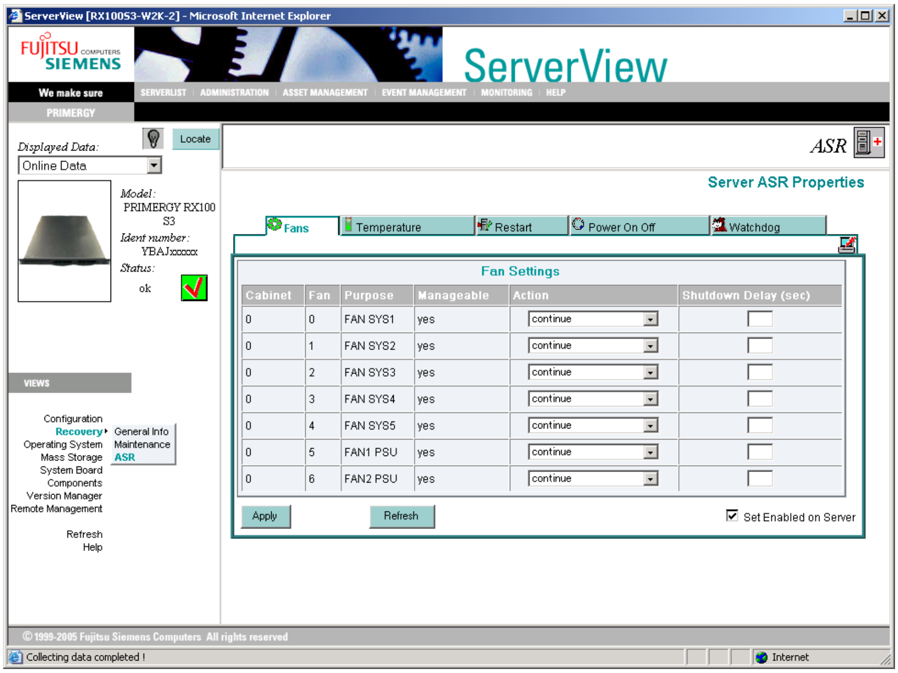
☑ RX100S3-W2K-2

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.


ServerView [RX100S3-W2K-2] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
Locate
ASR
VIEWS
Configuration
Recovery
Operating System
Mass Storage
System Board
Components
Version Manager
Remote Management
General Info
Maintenance
ASR
Refresh
Help
Fans
Temperature
Restart
Power On Off
Watchdog
Apply
Refresh
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Collecting data completed !
Internet

Displayed Data: Online Data

Model: PRIMERGY RX100 S3

Ident number: YBAJxxxxxx

Status: ok

Server ASR Properties

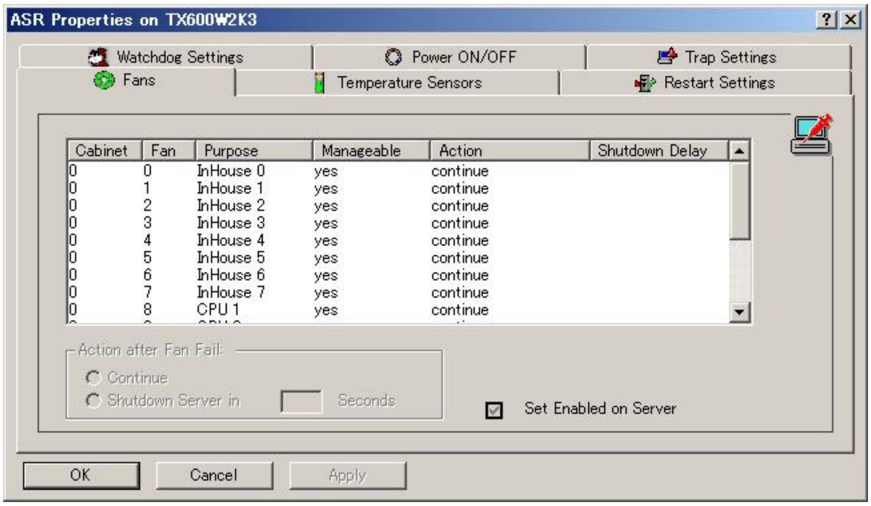
Fan Settings

Cabinet	Fan	Purpose	Manageable	Action	Shutdown Delay (sec)
0	0	FAN SYS1	yes	continue	
0	1	FAN SYS2	yes	continue	
0	2	FAN SYS3	yes	continue	
0	3	FAN SYS4	yes	continue	
0	4	FAN SYS5	yes	continue	
0	5	FAN1 PSU	yes	continue	
0	6	FAN2 PSU	yes	continue	

☑ Set Enabled on Server

Management Console

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



Cabinet	Fan	Purpose	Manageable	Action	Shutdown Delay
0	0	InHouse 0	yes	continue	
0	1	InHouse 1	yes	continue	
0	2	InHouse 2	yes	continue	
0	3	InHouse 3	yes	continue	
0	4	InHouse 4	yes	continue	
0	5	InHouse 5	yes	continue	
0	6	InHouse 6	yes	continue	
0	7	InHouse 7	yes	continue	
0	8	CPU 1	yes	continue	

Action after Fan Fail:
○ Continue
○ Shutdown Server in ☐ Seconds

☑ Set Enabled on Server

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.133)
- [Temperature] tab / [Temperature Sensors] tab (→pg.134)
- [Restart] tab / [Restart Settings] tab (→pg.135)
- [Power On Off] tab / [Power ON/OFF] tab (→pg.136)
- [Watchdog] tab / [Watchdog Settings] tab (→pg.136)
- [Trap Settings] tab (→pg.137)

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 (ServerVew 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.

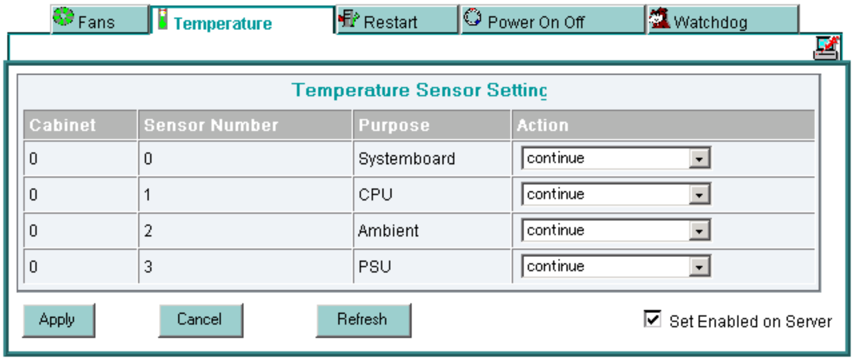
IMPORTANT

- If the redundant fans are installed to the server, set same ASR for both fans that configure redundancy. OS shutdown begins when both fans break down.For the existence of redundant fans and the combination of redundant fans, refer to "User's Guide" supplied with the server.
- 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 (ServerVew S2) / [Temperature Sensors] Tab (Management Console)

Specifies the measures at abnormally high temperature.

Specify [Action] for each temperature sensor monitored.



Temperature Sensor Settinc

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

☑ Set Enabled on Server

table: [Temperature Sensors] Tab

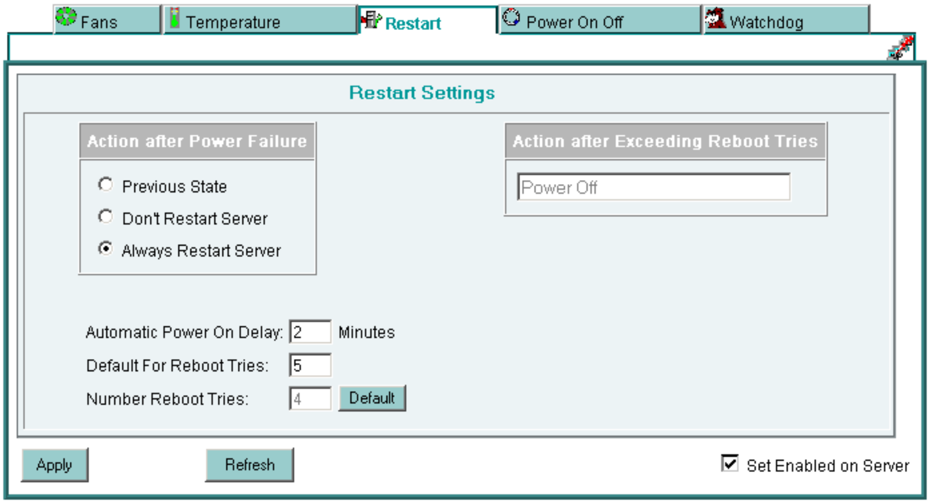
Item	Description
Continue	The server continues to run after abnormal high temperature detection.
Shut down the server now	The server shuts down immediately when temperature reaches the critical value.

IMPORTANT

- 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.



Restart Settings

Action after Power Failure

○ Previous State
○ Don't Restart Server
● Always Restart Server

Action after Exceeding Reboot Tries

Power Off

Automatic Power On Delay: 2 Minutes

Default For Reboot Tries: 5

Number Reboot Tries: 4

☑ Set Enabled on Server

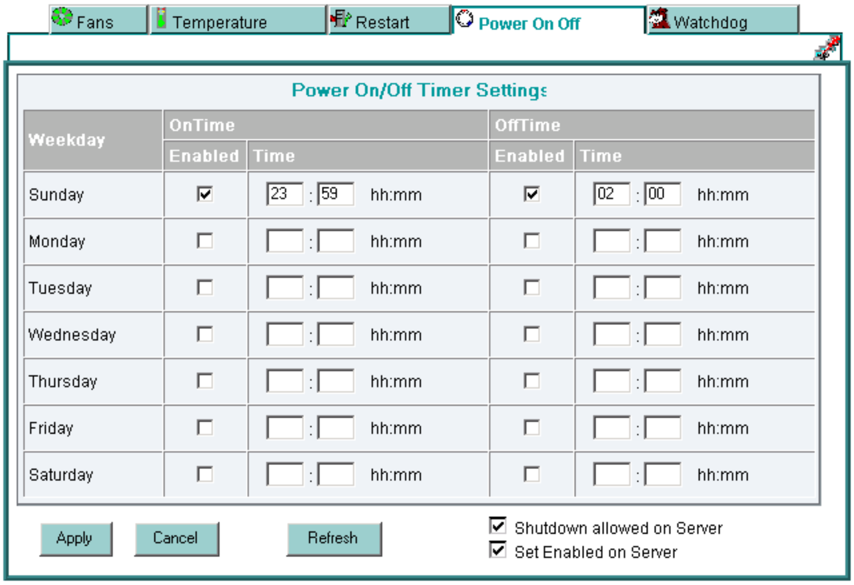
table: [Restart Settings] Tab

Item	Description
Action after Power Failure	Select one of the following items to set restart action after power failure. • Previous State • Don’t Restart Server • Always Restart Server
Action after Exceeding Reboot Tries	An action after exceeding reboot tries that is set by BIOS is displayed.
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.

■ [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.



Power On/Off Timer Settings

Weekday	OnTime			OffTime		
	Enabled	Time		Enabled	Time	
Sunday	☑	23 : 59	hh:mm	☑	02 : 00	hh:mm
Monday	□	:	hh:mm	□	:	hh:mm
Tuesday	□	:	hh:mm	□	:	hh:mm
Wednesday	□	:	hh:mm	□	:	hh:mm
Thursday	□	:	hh:mm	□	:	hh:mm
Friday	□	:	hh:mm	□	:	hh:mm
Saturday	□	:	hh:mm	□	:	hh:mm

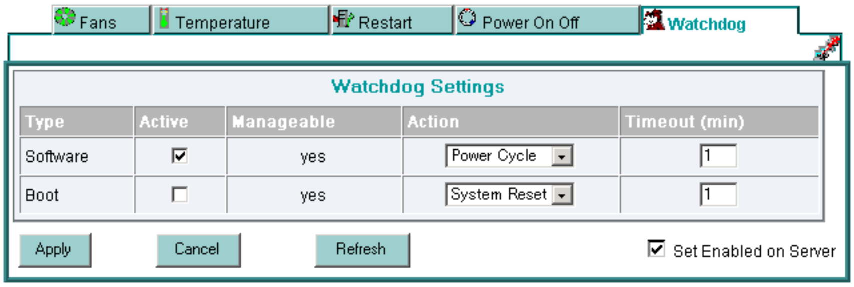
☑ Shutdown allowed on Server
☑ Set Enabled on Server

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".



Watchdog Settings

Type	Active	Manageable	Action	Timeout (min)
Software	☑	yes	Power Cycle	1
Boot	□	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

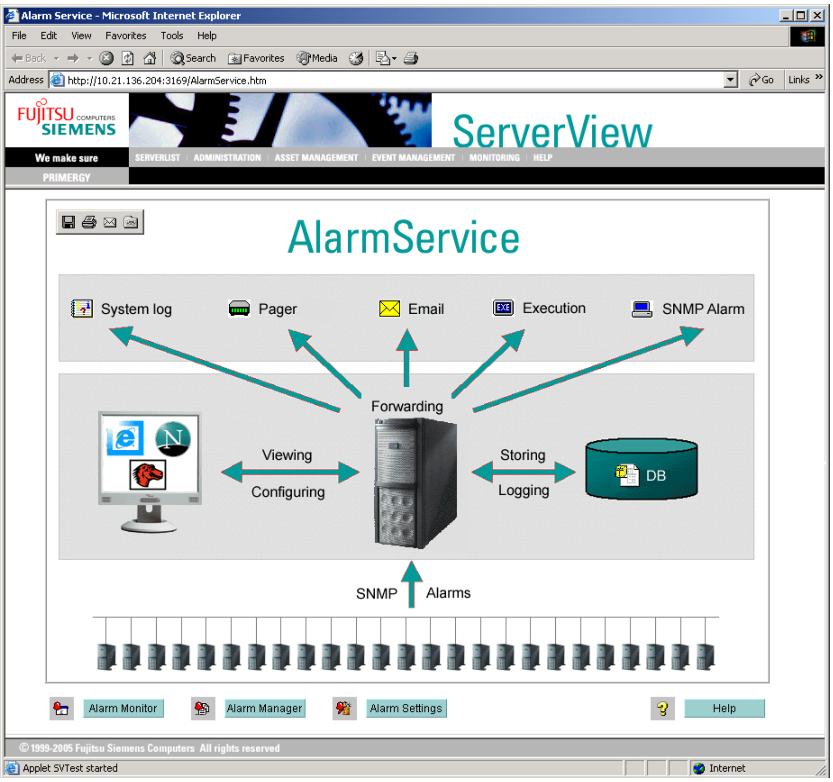
When using ServerView Web-Server (normal connection)

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.


Alarm Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.21.136.204:3169/AlarmService.htm
Go Links
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SERVERLIST ADMINISTRATION ASSET MANAGEMENT EVENT MANAGEMENT MONITORING HELP
AlarmService
System log
Pager
Email
Execution
SNMP Alarm
Forwarding
Viewing
Configuring
Storing
Logging
DB
SNMP
Alarms
Alarm Monitor
Alarm Manager
Alarm Settings
Help
©1999-2005 Fujitsu Siemens Computers All rights reserved
Applet SVTest started
Internet

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.

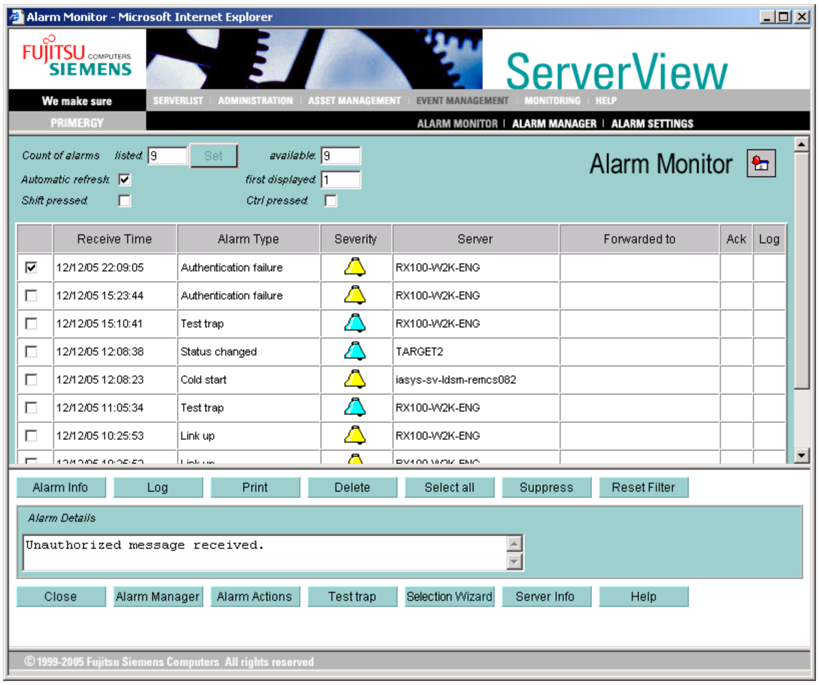
When starting the alarm monitor from Management Console

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.


Alarm Monitor - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
PRIMERGY
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
ALARM MONITOR | ALARM MANAGER | ALARM SETTINGS
Alarm Monitor
Set
Alarm Info
Log
Print
Delete
Select all
Suppress
Reset Filter
Close
Alarm Manager
Alarm Actions
Test trap
Selection Wizard
Server Info
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

Count of alarms listed: 9 available: 9

Automatic refresh ☑ first displayed: 1

Shift pressed □ Ctrl pressed □

	Receive Time	Alarm Type	Severity	Server	Forwarded to	Ack	Log
☑	12/12/05 22:09:05	Authentication failure	🔔	RX100-W2K-ENG			
□	12/12/05 15:23:44	Authentication failure	🔔	RX100-W2K-ENG			
□	12/12/05 15:10:41	Test trap	🔔	RX100-W2K-ENG			
□	12/12/05 12:08:38	Status changed	🔔	TARGET2			
□	12/12/05 12:08:23	Cold start	🔔	iasys-sv-ldsm-remcs082			
□	12/12/05 11:05:34	Test trap	🔔	RX100-W2K-ENG			
□	12/12/05 10:25:53	Link up	🔔	RX100-W2K-ENG			
□	12/12/05 10:25:52	Link up	🔔	RX100-W2K-ENG			

Alarm Details

```
Unauthorized message received.
```

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.

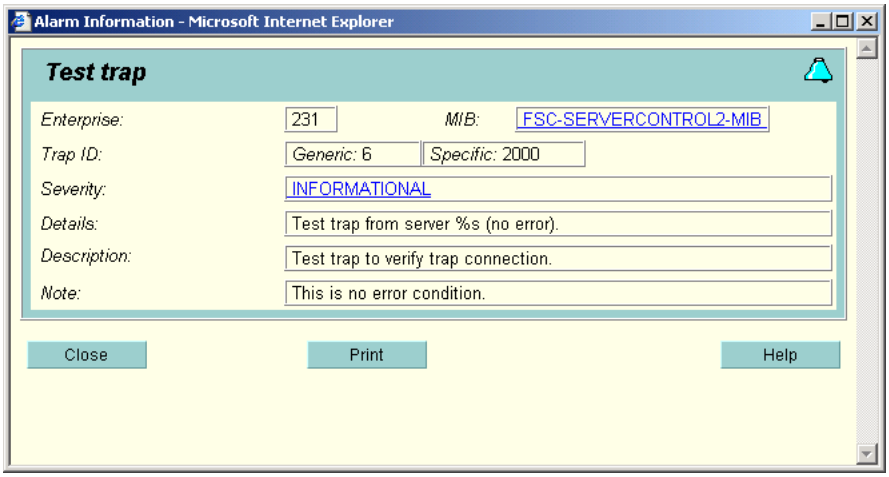
2 After checking the target alarm, select an operation among the following:

table: Alarm Operations

Function Button	Description
Alarm Info	Displays detailed information about the alarm. For details, see "■ The [Alarm Info] Button" (→pg.142).
Log	The selected alarm is logged into Alarm Manager. For details, see "■ The [Log] Button" (→pg.142).
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.142).
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.142).
Alarm Manager	Starts the alarm manager. For details, see "3.5.2 Alarm Manager" (→pg.146).
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.149).
Test trap	Tests transmission of traps. For details, see "■ The [Test trap] Button" (→pg.143).
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.145).
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.



Alarm Information - Microsoft Internet Explorer

Test trap

Enterprise: 231 MIB: FSC-SERVERCONTROL2-MIB

Trap ID: Generic: 6 Specific: 2000

Severity: INFORMATIONAL

Details: Test trap from server %s (no error).

Description: Test trap to verify trap connection.

Note: This is no error condition.

■ 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].)

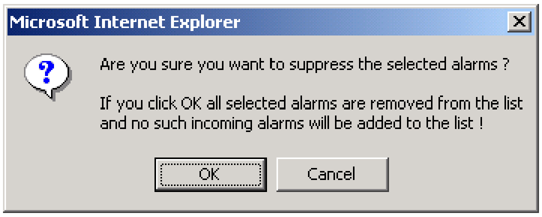
For alarms that have been added to the [Alarm Manager], the icon is displayed in the [Log] field. If alarms are accepted using the [Ack Alarm] button in the [Alarm Manager], the ✓ icon is added. The [Ack Alarm] icon also appears in the [Ack] field of the [Alarm Monitor].

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].

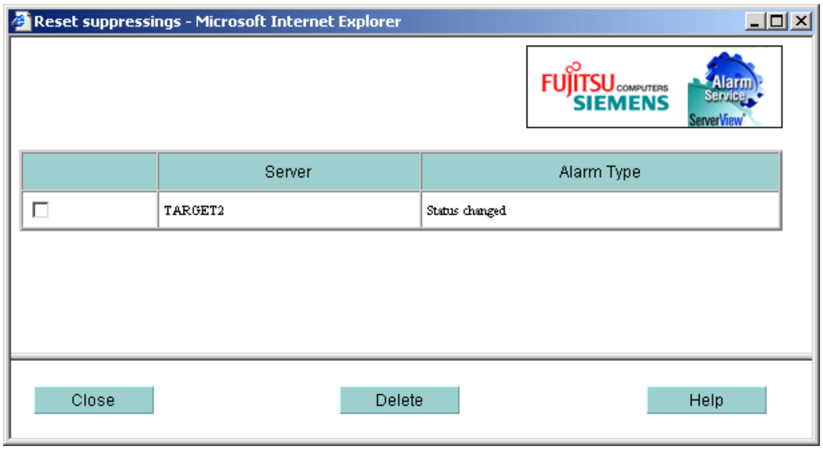


Microsoft Internet Explorer

Are you sure you want to suppress the selected alarms ?

If you click OK all selected alarms are removed from the list and no such incoming alarms will be added to the list !

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].


Reset suppressings - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
Alarm Service
ServerView
Close
Delete
Help

	Server	Alarm Type
□	TARGET2	Status changed

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

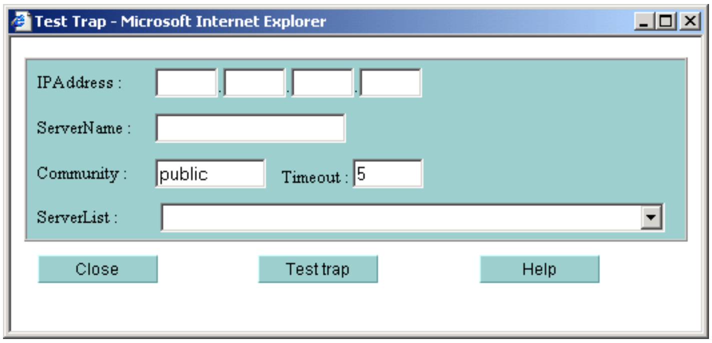
- When the server is starting up, a RAID manager, an Ethernet card, etc. may issue an alarm (SNMP trap) as the start-up notification (e.g. RFC1157LinkUP). To suppress this kind of alarms, configure the alarm exclusion. This blocking function must be specified for each server. If multiple servers are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



IPAddress : . . .

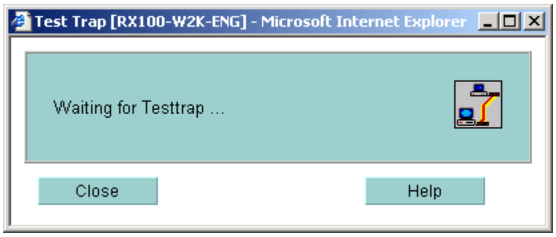
ServerName :

Community : public Timeout : 5

ServerList :

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.

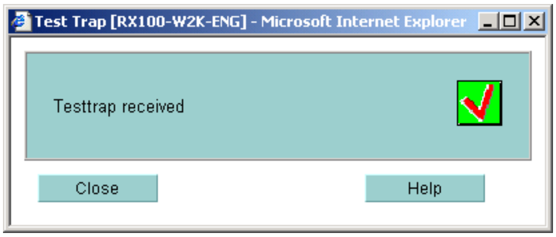


Test Trap [RX100-W2K-ENG] - Microsoft Internet Explorer

Waiting for Testtrap ...

If the transmission/reception succeeds

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

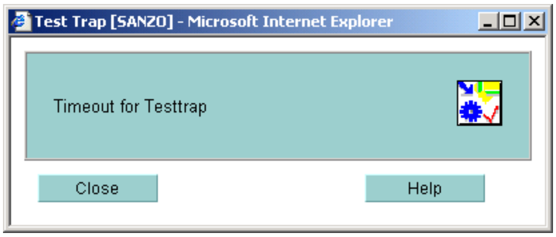


Test Trap [RX100-W2K-ENG] - Microsoft Internet Explorer

Testtrap received

If the transmission/reception fails

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



Test Trap [SANZO] - Microsoft Internet Explorer

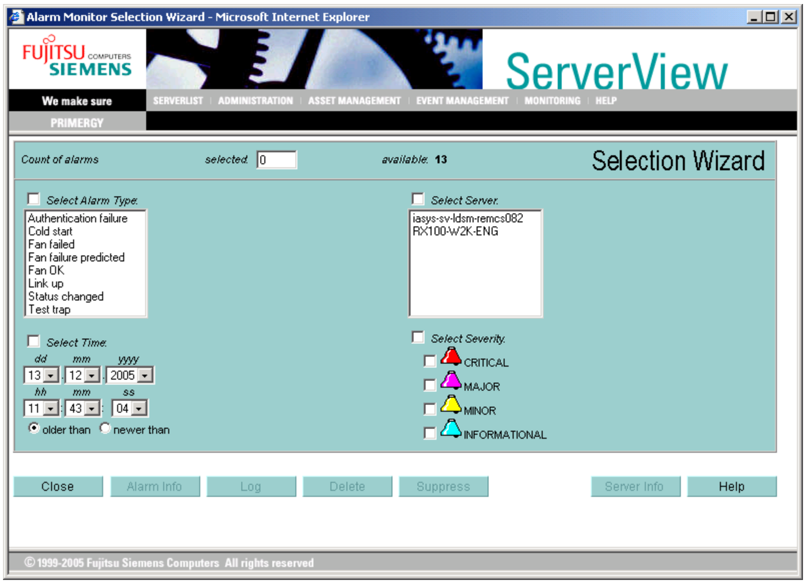
Timeout for Testtrap

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, /etc/snmp/snmpd.conf for Red Hat Linux, or /etc/snmpd.conf for SUSE 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.



Selection Wizard

Count of alarms selected: 0 available: 13

□ Select Alarm Type:
Authentication failure
Cold start
Fan failed
Fan failure predicted
Fan OK
Link up
Status changed
Test trap

□ Select Server:
iasys-sv-ldsm-remcs082
RX100-W2K-ENG

□ Select Time:
dd 13 . mm 12 . yyyy 2005
hh 11 : mm 43 : ss 04
● older than ○ newer than

□ Select Severity:
□ CRITICAL
□ MAJOR
□ MINOR
□ INFORMATIONAL

© 1999-2005 Fujitsu Siemens Computers All rights reserved

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.

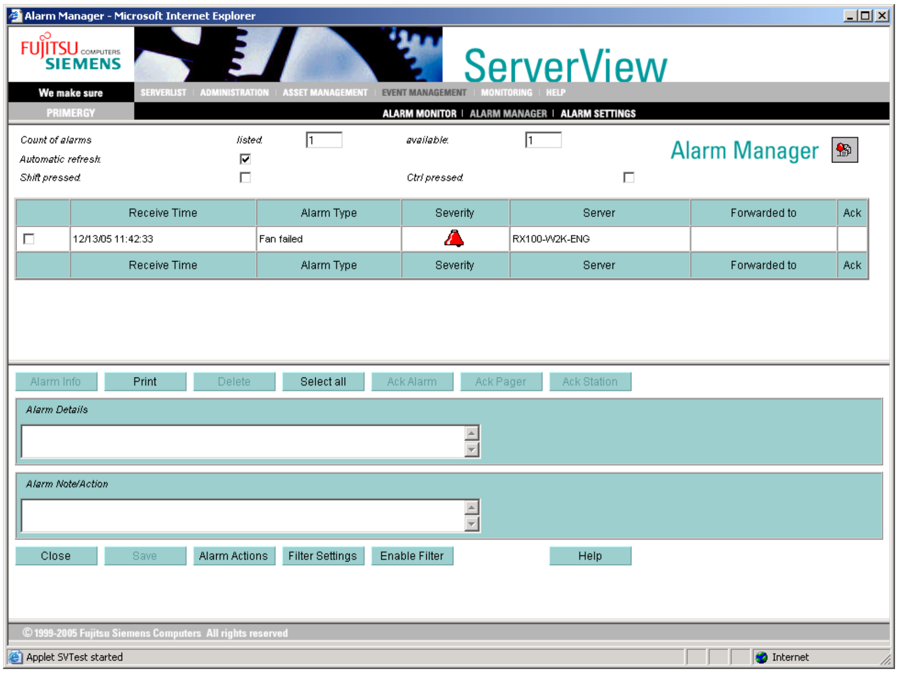
When starting from the Management Console

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.



Count of alarms listed 1 available 1

Automatic refresh ☑

Shift pressed □ Ctrl pressed □

	Receive Time	Alarm Type	Severity	Server	Forwarded to	Ack
□	12/13/05 11:42:33	Fan failed	🔺	RX100-W2K-ENG		
	Receive Time	Alarm Type	Severity	Server	Forwarded to	Ack

Alarm Details

Alarm Note/Action

© 1999-2005 Fujitsu Siemens Computers All rights reserved

Applet SVTest started

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

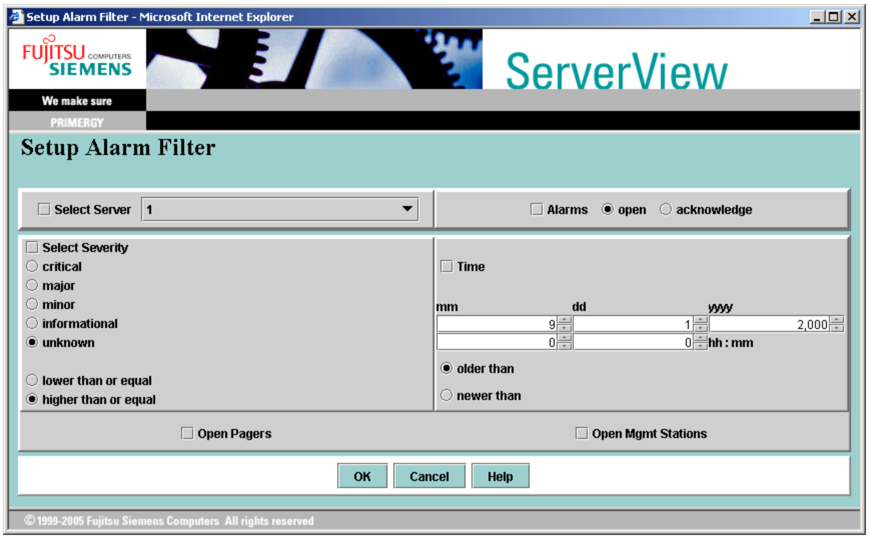
Function Button	Description
Alarm Info	Displays details about the alarm(s).
Print	Prints the selected alarm(s).
Delete	Deletes all selected alarms among the accepted alarms.
Select All	Selects all the alarms.
Ack Alarm	Accepts the selected alarm(s). When an alarm is accepted, the acceptance icon is displayed 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.148）.
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.



Setup Alarm Filter - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView

Setup Alarm Filter

□ Select Server 1

□ Alarms ● open ○ acknowledge

□ Select Severity
○ critical
○ major
○ minor
○ informational
● unknown

○ lower than or equal
● higher than or equal

□ Time

mm 9 dd 1 yyyy 2,000
0 0 hh : mm

● older than
○ newer than

□ Open Pagers □ Open Mgmt Stations

OK
Cancel
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

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".

IMPORTANT

- 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

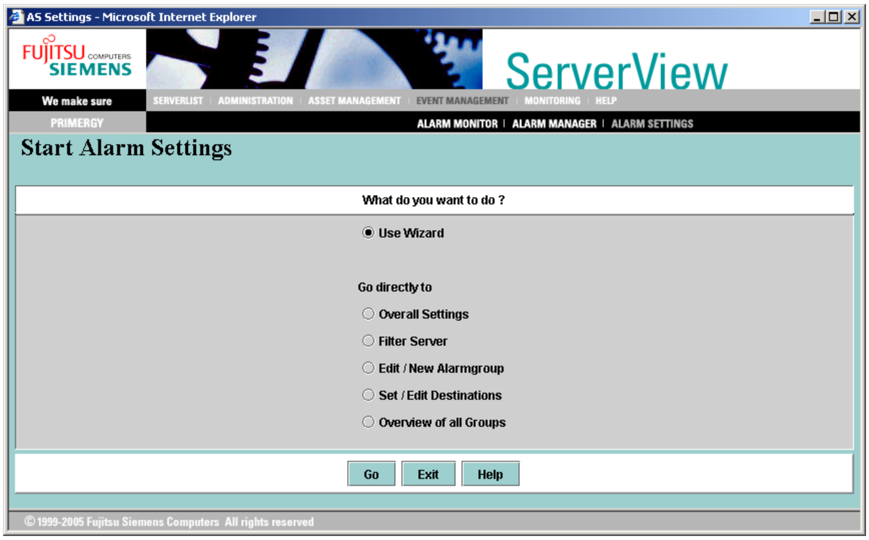
1 Click [EVENT MANAGEMENT] → [ALARM SETTINGS] on the ServerView S2 menu.

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.


AS Settings - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
PRIMERGY
ALARM MONITOR | ALARM MANAGER | ALARM SETTINGS
Go
Exit
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

Start Alarm Settings

What do you want to do ?

● Use Wizard

Go directly to

○ Overall Settings

○ Filter Server

○ Edit / New Alarmgroup

○ Set / Edit Destinations

○ Overview of all Groups

2 Configure the Alarm Settings.

The [ALARM SETTINGS] consists of five settings: "■ Overall Settings" (→pg.150), "■ Filter Server" (→pg.154), "■ Edit / New Alarmgroup" (→pg.154), "■ Set / Edit Destination" (→pg.157), and "■ Overview" (→pg.170).

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:

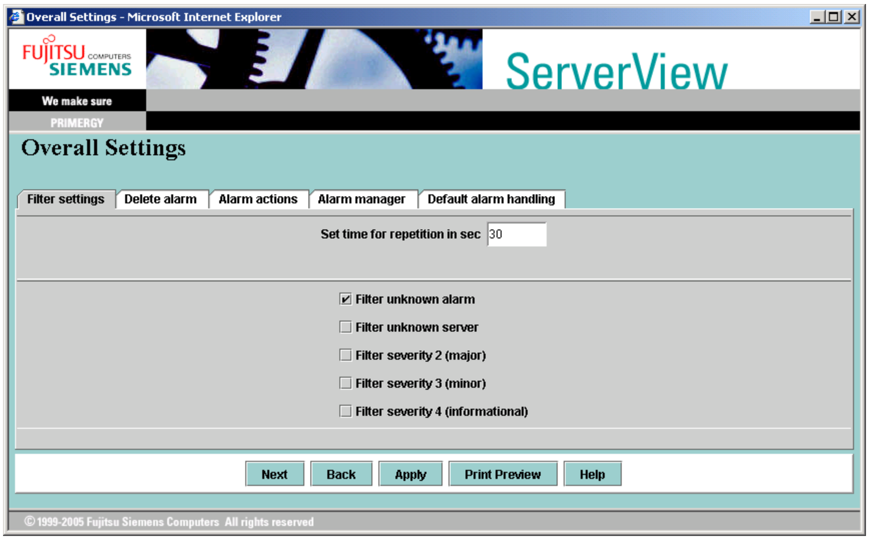
table: Description of the Buttons

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



Set time for repetition in sec 30

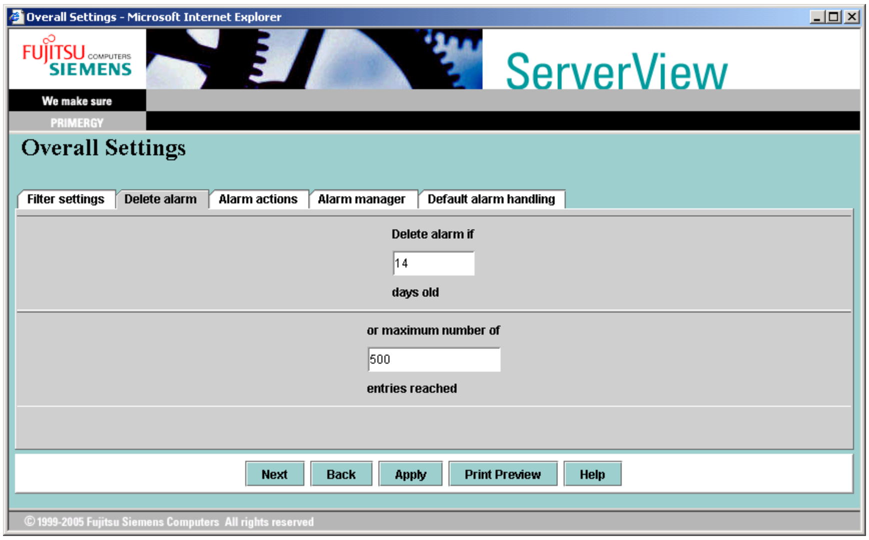
☑ Filter unknown alarm
□ Filter unknown server
□ Filter severity 2 (major)
□ Filter severity 3 (minor)
□ Filter severity 4 (informational)

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



Delete alarm if

14

days old

or maximum number of

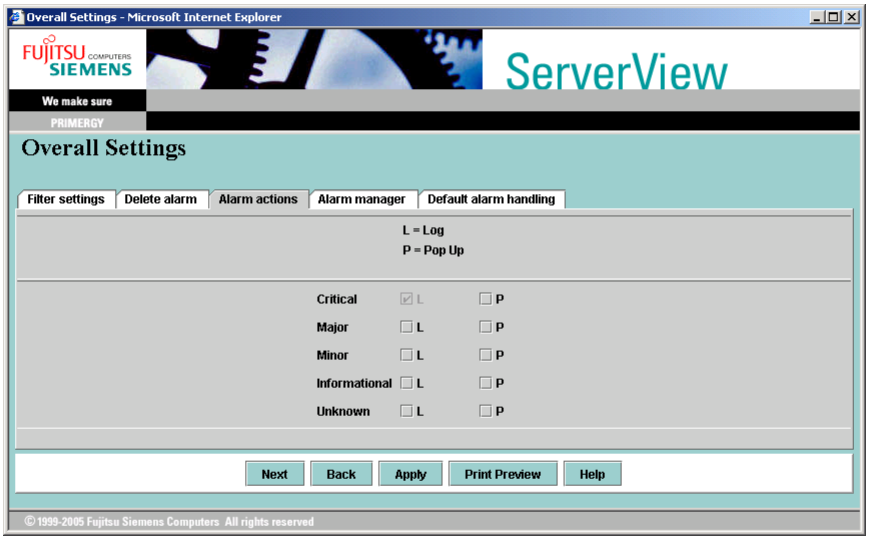
500

entries reached

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



Overall Settings

L = Log
P = Pop Up

Critical ☑ L □ P
Major □ L □ P
Minor □ L □ P
Informational □ L □ P
Unknown □ L □ P

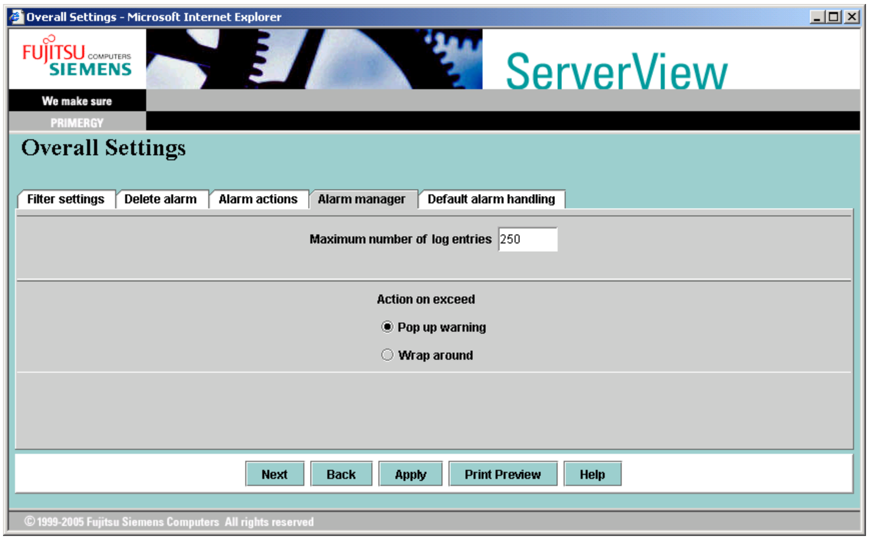
Specifies the action to be executed when receiving an alarm.

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



Overall Settings

Maximum number of log entries 250

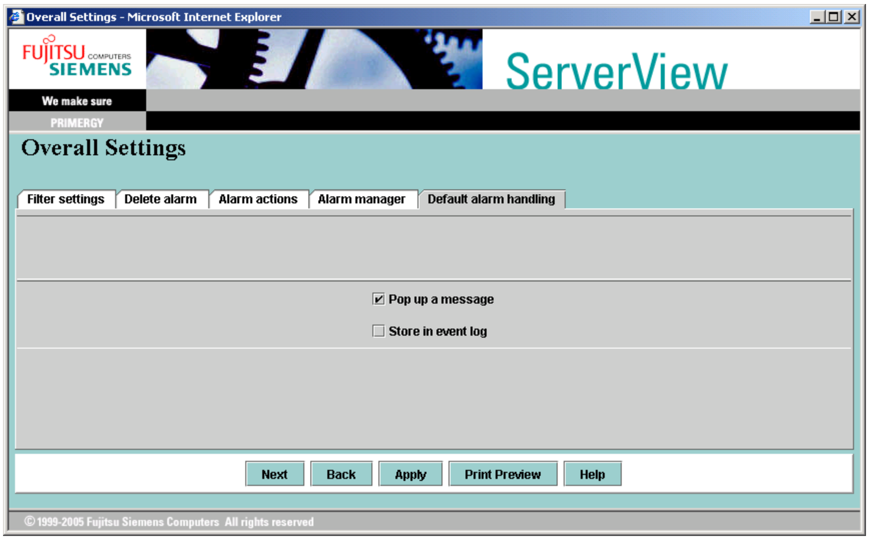
Action on exceed
● Pop up warning
○ Wrap around

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]. • Pop up warning Displays a message to warn the user. • Wrap around Deletes the entries from the oldest one.

● The [Default alarm handling] Tab



☑ Pop up a message

□ Store in event log

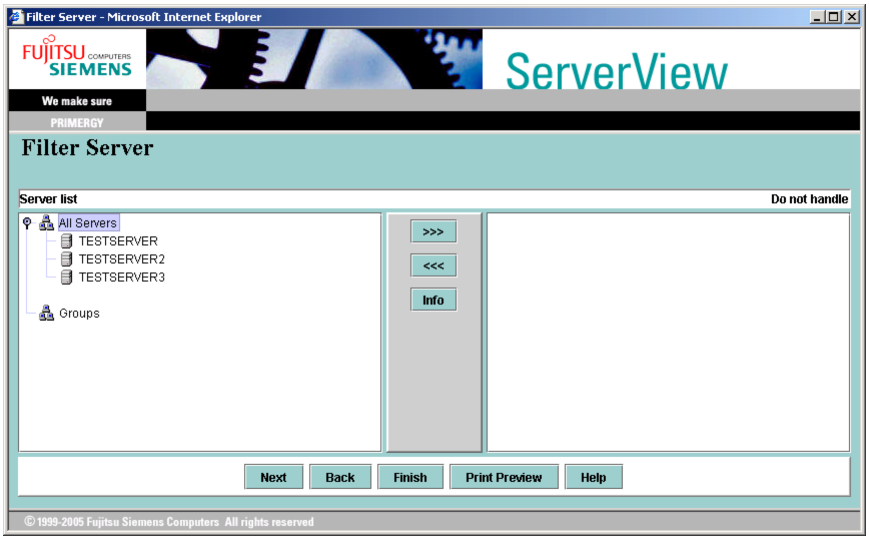
Configures the default action. The action is always executed when an alarm is issued, regardless of the settings for the alarm group.

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.

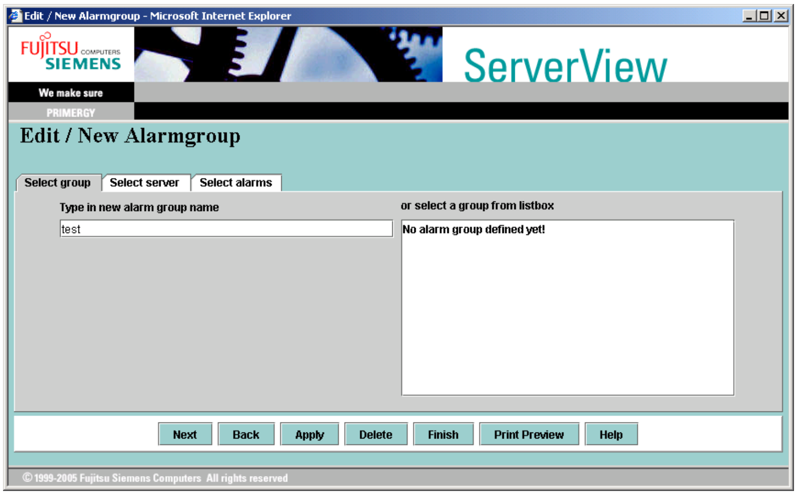
● Alarm Group

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 a alarm group name and click [Apply].

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



Edit / New Alarmgroup - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
PRIMERGY
Select group
Select server
Select alarms
Next
Back
Apply
Delete
Finish
Print Preview
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

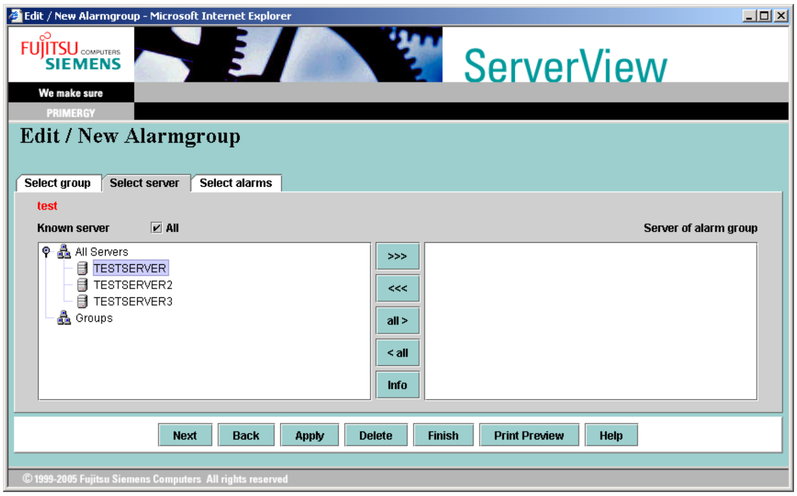
Edit / New Alarmgroup

Type in new alarm group name: test

or select a group from listbox: No alarm group defined yet!

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

In the example below, "TESTSERVER" is selected.



Edit / New Alarmgroup - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
PRIMERGY
Select group
Select server
Select alarms
>>>
<<<
all >
< all
Info
Next
Back
Apply
Delete
Finish
Print Preview
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

Edit / New Alarmgroup

test

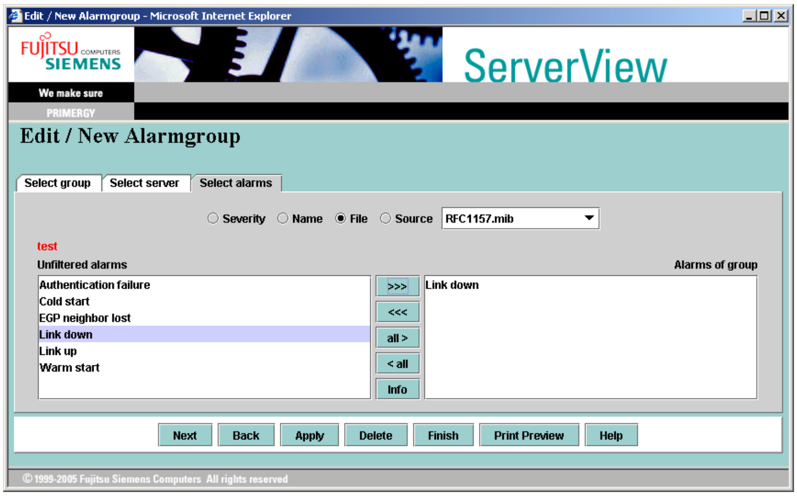
Known server ☑ All

All Servers
TESTSERVER
TESTSERVER2
TESTSERVER3
Groups

Server of alarm group

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 "RCF1157.Mib", click [File], select [RCF1157.Mib] from the combo box, select [LinkDown], and click [>>>].



Edit / New Alarmgroup - Microsoft Internet Explorer

Edit / New Alarmgroup

○ Severity ○ Name ● File ○ Source RFC1157.mib

test

Unfiltered alarms

Authentication failure
Cold start
EGP neighbor lost
Link down
Link up
Warm start

Alarms of group

Link down

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

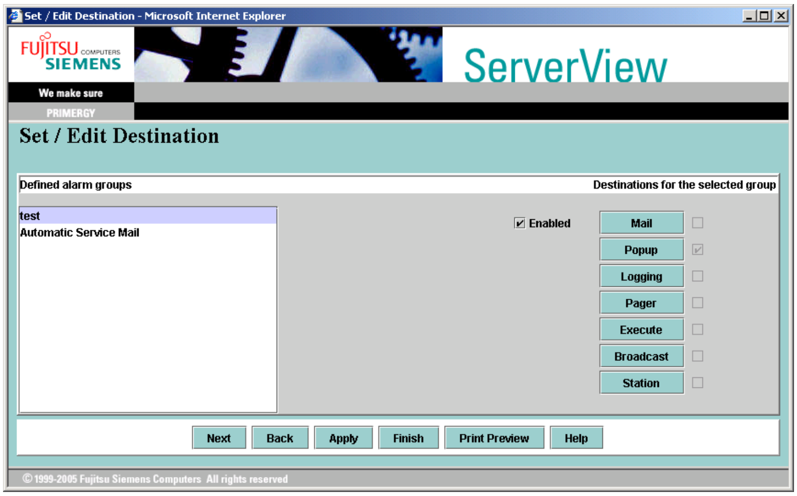
- To delete an alarm group, perform the following procedure:
  1. Select an alarm group from listbox.
  2. Click [Delete].

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.



Set / Edit Destination - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView

Set / Edit Destination

Defined alarm groups

test
Automatic Service Mail

Destinations for the selected group

☑ Enabled

Mail	☐
Popup	☑
Logging	☐
Pager	☐
Execute	☐
Broadcast	☐
Station	☐

Next
Back
Apply
Finish
Print Preview
Help

©1999-2005 Fujitsu Siemens Computers All rights reserved

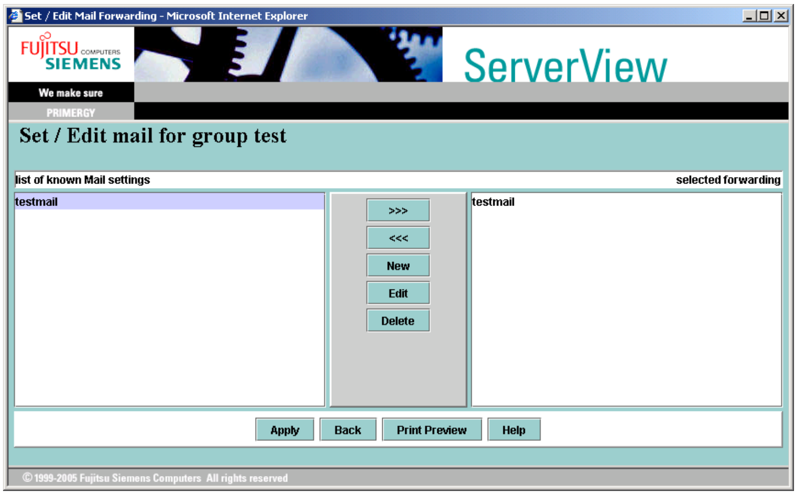
On the left side, the existing alarm groups are listed.

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.158
- Display a message →pg.161
- Write in the log →pg.163
- Execute a command →pg.164
- Broadcast a notification →pg.166
- Send to the station →pg.168

● Mail

When you click [Mail], the [Set / Edit mail for group test] window appears.



Set / Edit Mail Forwarding - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
>>>
<<<
New
Edit
Delete
Apply
Back
Print Preview
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

Set / Edit mail for group test

list of known Mail settings: testmail

selected forwarding: testmail

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.159).

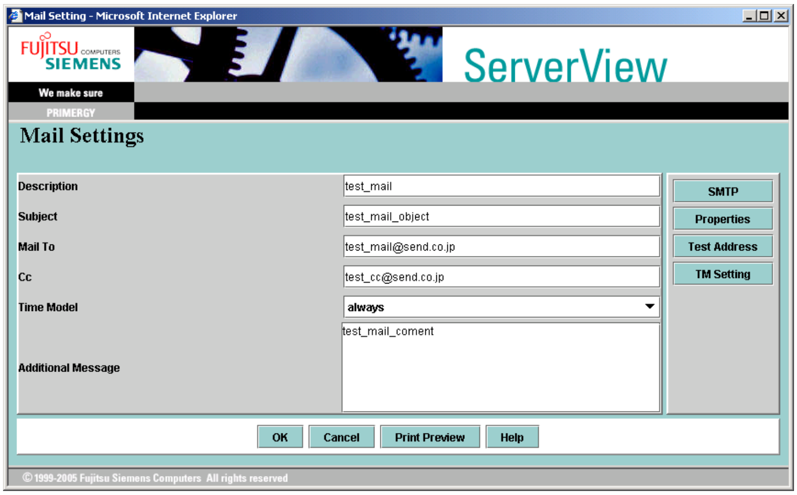
Removing Settings

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.


Mail Setting - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SMTP
Properties
Test Address
TM Setting
OK
Cancel
Print Preview
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

Mail Settings

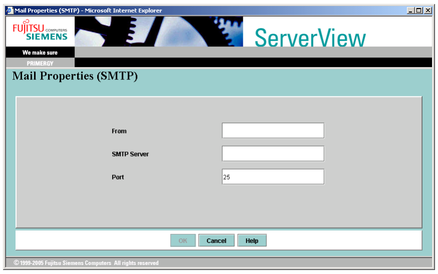
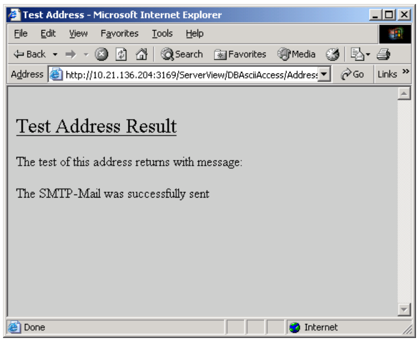
Description: test_mail
Subject: test_mail_object
Mail To: test_mail@send.co.jp
Cc: test_cc@send.co.jp
Time Model: always
Additional Message: test_mail_coment

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	The [Mail Properties (SMTP)] window appears.  Mail Properties (SMTP) - Microsoft Internet Explorer FUJITSU SIEMENS We make sure PRIMERGY ServerView OK Cancel Help Mail Properties (SMTP) From SMTP Server Port 25 © 1999-2005 Fujitsu Siemens Computers All rights reserved Configure [From], [SMTP Server] and [Port], and click [OK].
[Test Address] button	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.  Test Address - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Media Address Go Links Done Internet http://10.21.136.204:3169/ServerView/DBAsciiAccess/Addres: Test Address Result The test of this address returns with message: The SMTP-Mail was successfully sent
[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.

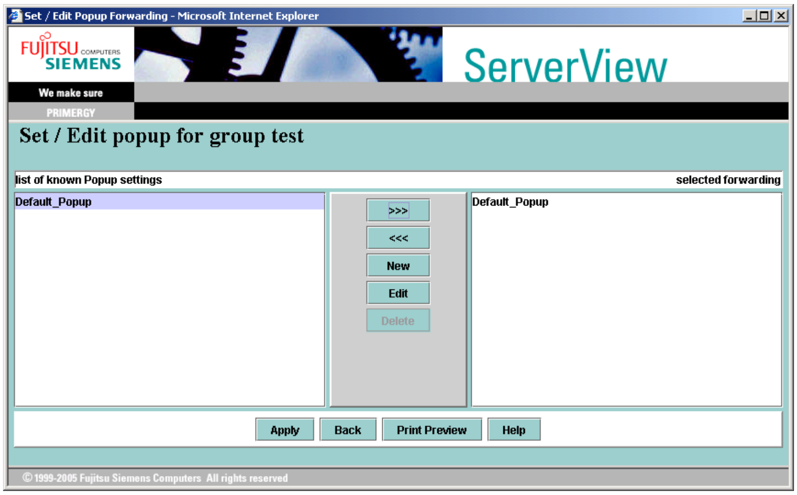
3 Confirm the settings, and click [OK].

The display returns to the [Set / Edit 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.


Set / Edit Popup Forwarding - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
Set / Edit popup for group test
list of known Popup settings
selected forwarding
Default_Popup
>>>
<<<
New
Edit
Delete
Default_Popup
Apply
Back
Print Preview
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

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.162).

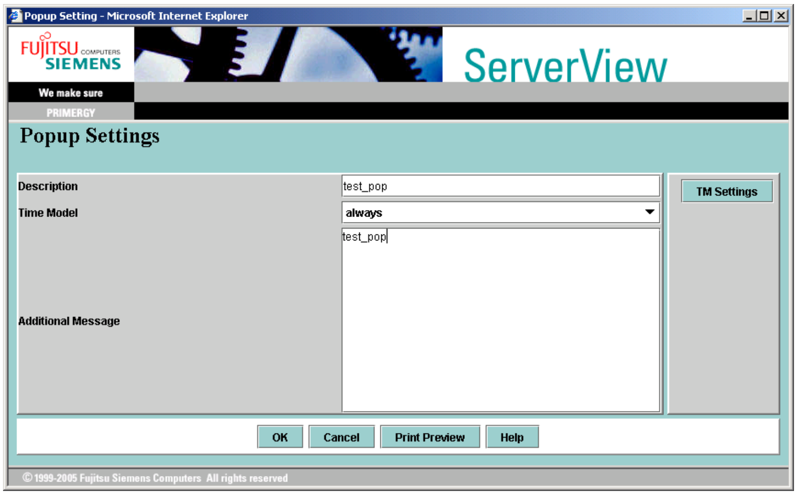
Removing Settings

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.



Popup Settings

Description: test_pop

Time Model: always

Additional Message: test_pop

Popup Setting - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
TM Settings
OK
Cancel
Print Preview
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

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.

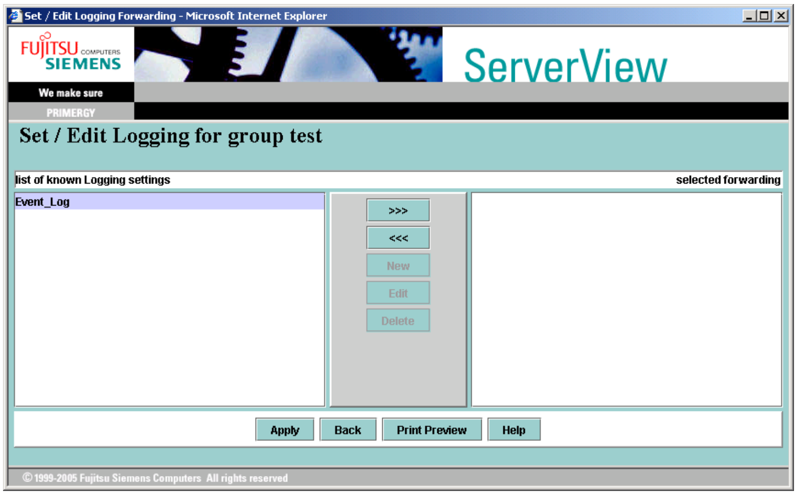
3 Confirm the settings, and click [OK].

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.



Set / Edit Logging Forwarding - Microsoft Internet Explorer

Set / Edit Logging for group test

list of known Logging settings

selected forwarding

Event_Log

© 1999-2005 Fujitsu Siemens Computers All rights reserved

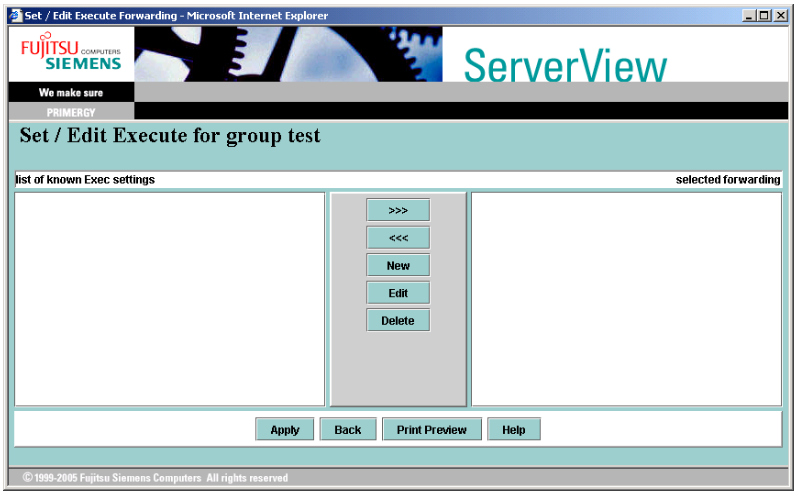
The existing logging settings are displayed in the list. If you have made any changes, do not forget to click [Apply]. When you click [Back], the display returns to the [Set / Edit Destination] window.
You cannot create new logging settings. It is only possible to apply the existing settings.

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.



Set / Edit Execute Forwarding - Microsoft Internet Explorer

Set / Edit Execute for group test

list of known Exec settings

selected forwarding

© 1999-2005 Fujitsu Siemens Computers All rights reserved

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.165).

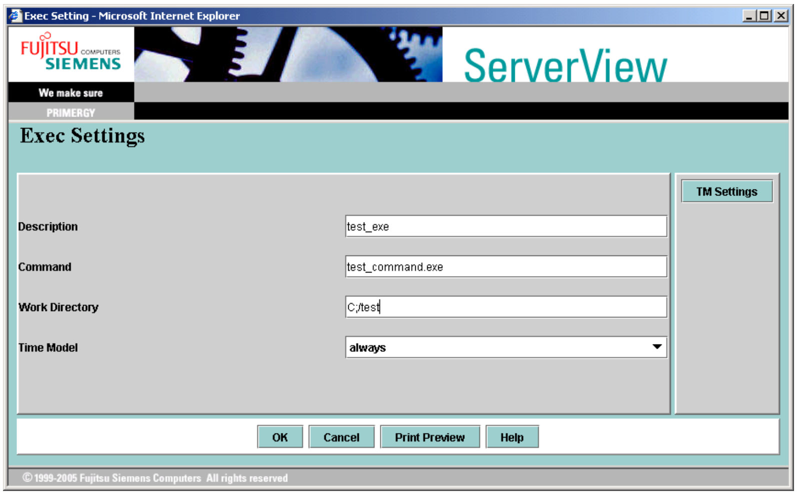
Removing Settings

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.


Exec Setting - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
Exec Settings
TM Settings
OK
Cancel
Print Preview
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

Description: test_exe

Command: test_command.exe

Work Directory: C:/test

Time Model: always

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.

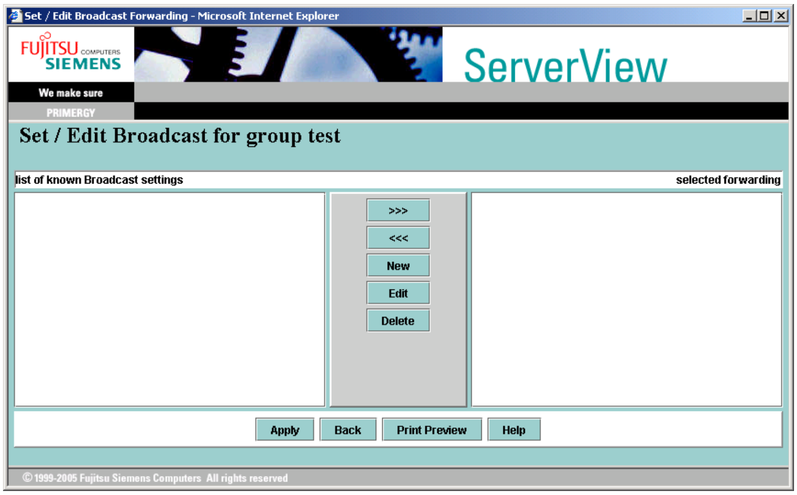
3 Confirm the settings, and click [OK].

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.


Set / Edit Broadcast Forwarding - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
Set / Edit Broadcast for group test
list of known Broadcast settings
selected forwarding
>>>
<<<
New
Edit
Delete
Apply
Back
Print Preview
Help
©1999-2005 Fujitsu Siemens Computers All rights reserved

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.167).

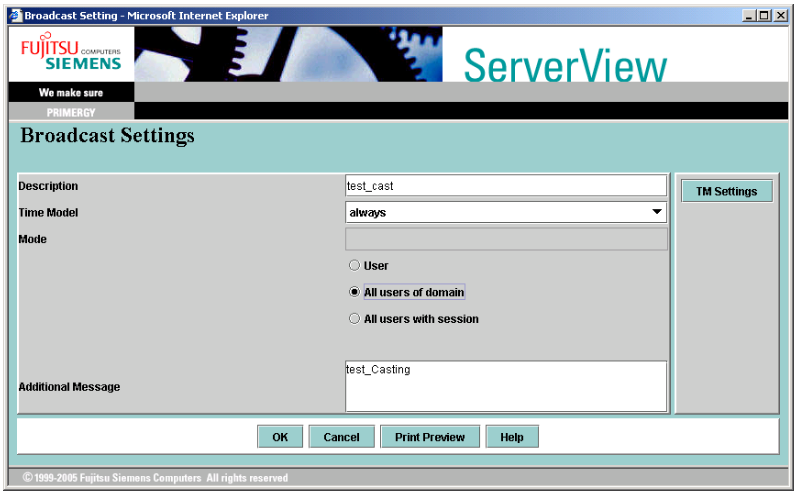
Removing Settings

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.


Broadcast Setting - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
TM Settings
OK
Cancel
Print Preview
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

Broadcast Settings

Description: test_cast

Time Model: always

Mode:
○ User
● All users of domain
○ All users with session

Additional Message: test_Casting

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. • 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.

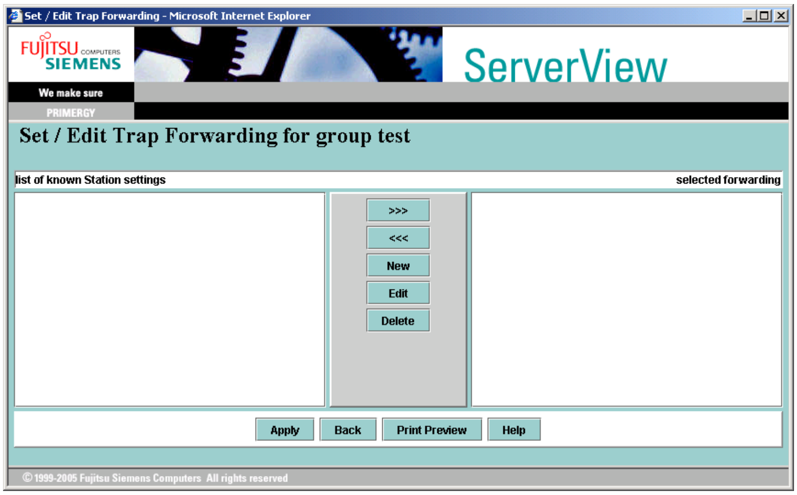
3 Confirm the settings, and click [OK].

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.


Set / Edit Trap Forwarding - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
Set / Edit Trap Forwarding for group test
list of known Station settings
selected forwarding
>>>
<<<
New
Edit
Delete
Apply
Back
Print Preview
Help
©1999-2005 Fujitsu Siemens Computers All rights reserved

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.169).

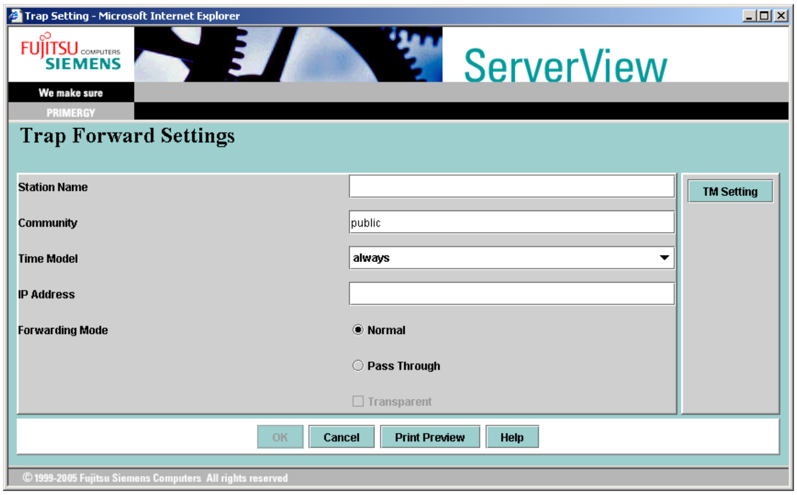
Removing Settings

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.



Trap Forward Settings

Station Name:

Community: public

Time Model: always

IP Address:

Forwarding Mode: ● Normal ○ Pass Through □ Transparent

Trap Setting - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
TM Setting
OK
Cancel
Print Preview
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

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.

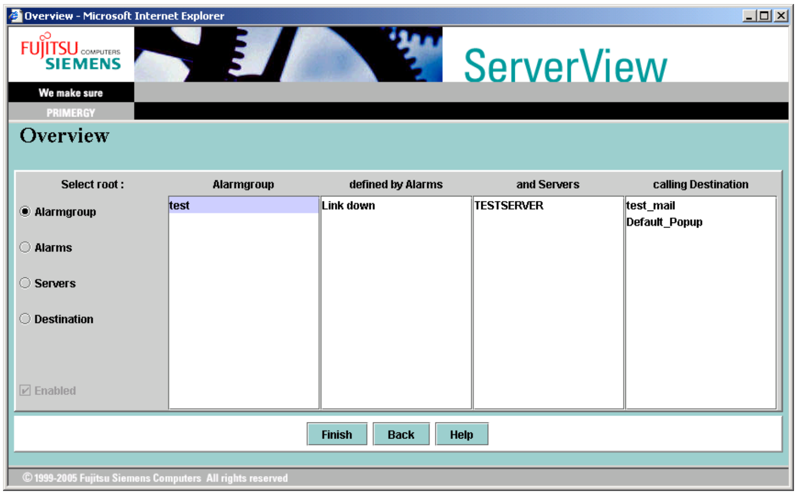
3 Confirm the settings, and click [OK].

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.


Overview - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
PRIMERGY
Finish
Back
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

Overview

Select root :

● Alarmgroup

○ Alarms

○ Servers

○ Destination

☑ Enabled

Alarmgroup	defined by Alarms	and Servers	calling Destination
test	Link down	TESTSERVER	test_mail Default_Popup

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).

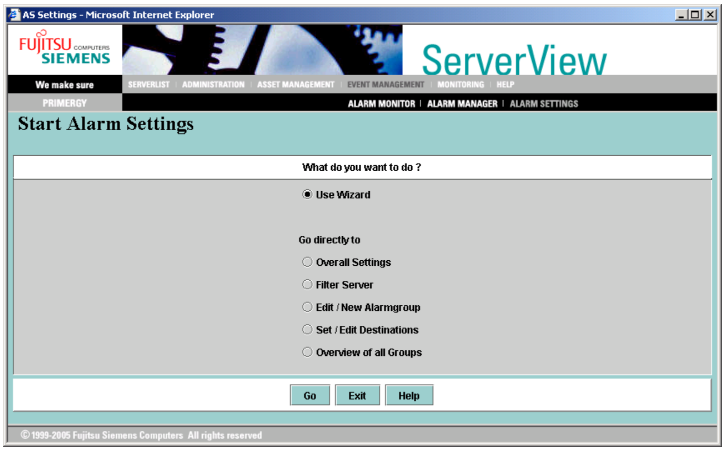
● Premises

- 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.


AS Settings - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
ALARM MONITOR | ALARM MANAGER | ALARM SETTINGS

Start Alarm Settings

What do you want to do ?

● Use Wizard

Go directly to

○ Overall Settings

○ Filter Server

○ Edit / New Alarmgroup

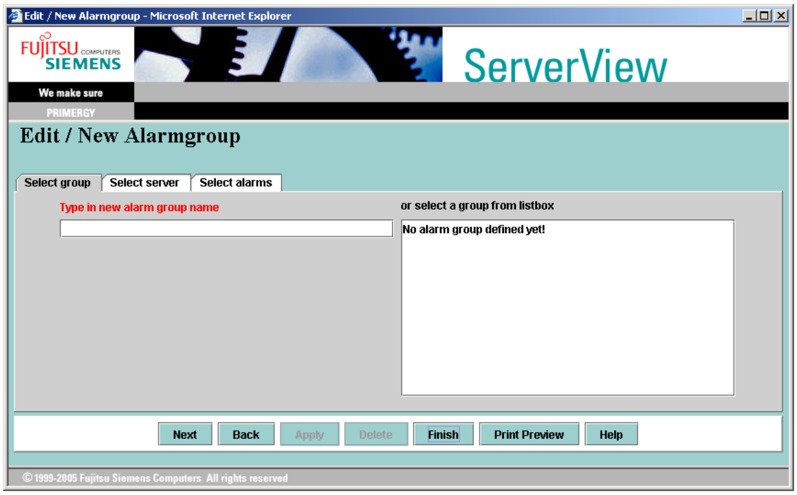
○ Set / Edit Destinations

○ Overview of all Groups

Go
Exit
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

2 Select [Set / New Alarmgroup] and click [Next].

The [Set / New Alarmgroup] window appears.


Edit / New Alarmgroup - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView

Edit / New Alarmgroup

Select group
Select server
Select alarms

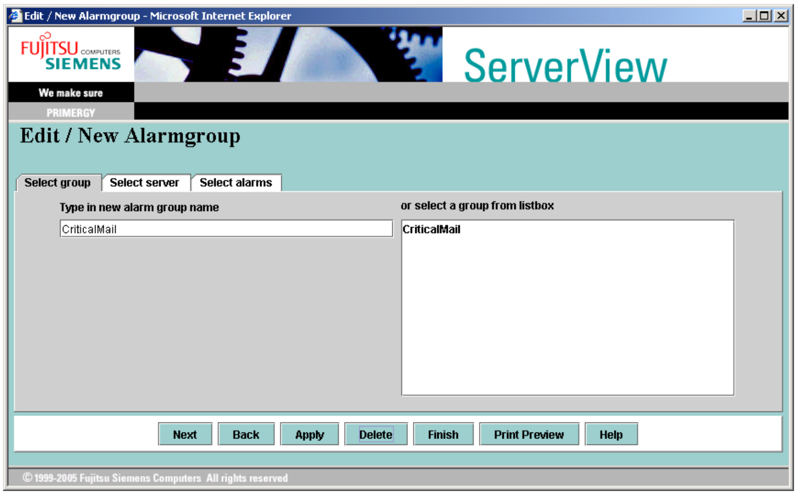
Type in new alarm group name

or select a group from listbox

No alarm group defined yet!

Next
Back
Apply
Delete
Finish
Print Preview
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

3 Enter "CriticalMail" as the alarm group name and click [Apply].

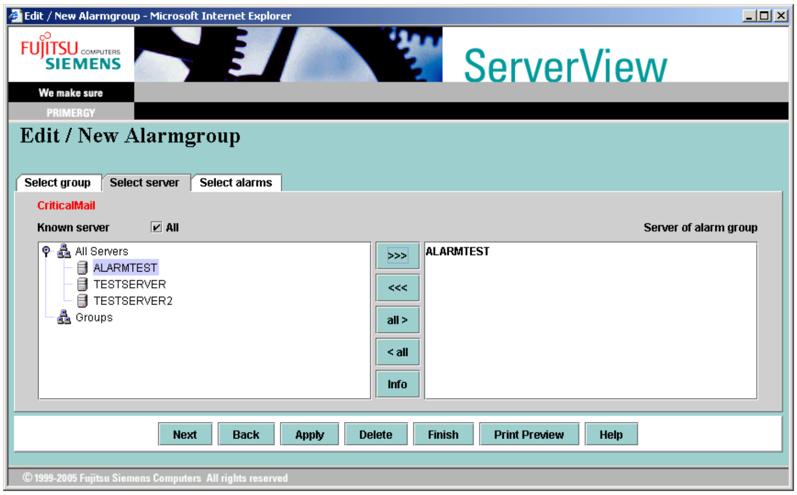

Edit / New Alarmgroup - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
Select group
Select server
Select alarms
Next
Back
Apply
Delete
Finish
Print Preview
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

Edit / New Alarmgroup

Type in new alarm group name: CriticalMail

or select a group from listbox: CriticalMail

4 Click the [Select server] tab, select "ALARMTEST" from the server list, and click [>>>] to add the server to the alarm group.



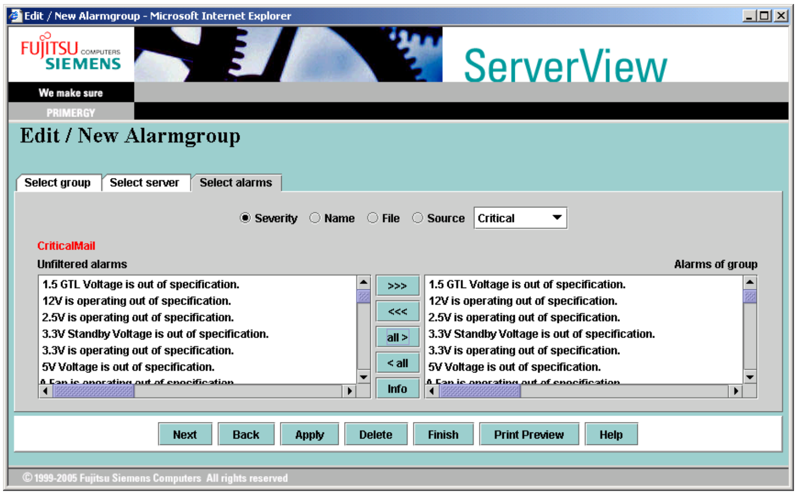
Edit / New Alarmgroup

CriticalMail

Known server ☑ All

Server of alarm group: ALARMTEST

5 Click the [Select alarms] tab, select [Critical] in [Severity], and click [all>] to add all the displayed alarms to the alarm group.


Edit / New Alarmgroup - Microsoft Internet Explorer

Edit / New Alarmgroup

Select group | Select server | Select alarms

● Severity ○ Name ○ File ○ Source Critical

CriticalMail

Unfiltered alarms

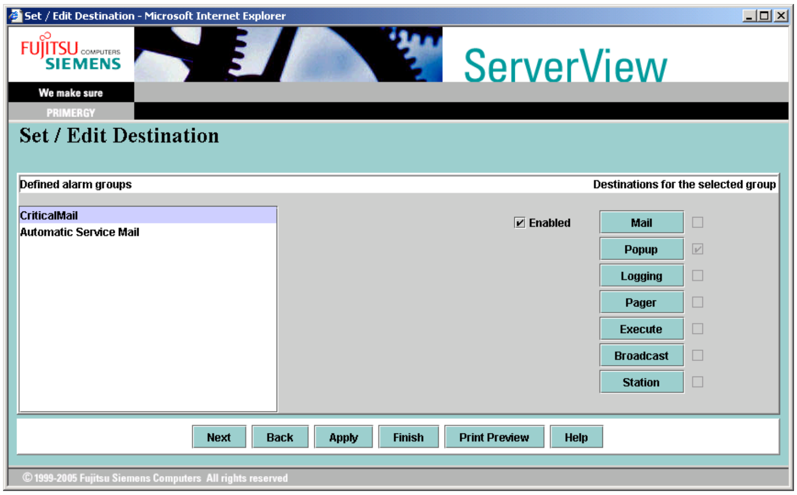
1.5 GTL Voltage is out of specification.
12V is operating out of specification.
2.5V is operating out of specification.
3.3V Standby Voltage is out of specification.
3.3V is operating out of specification.
5V Voltage is out of specification.
A Fan is operating out of specification.

Alarms of group

1.5 GTL Voltage is out of specification.
12V is operating out of specification.
2.5V is operating out of specification.
3.3V Standby Voltage is out of specification.
3.3V is operating out of specification.
5V Voltage is out of specification.
A Fan is operating out of specification.

© 1999-2005 Fujitsu Siemens Computers All rights reserved

6 Click [Apply], and then [Next].


Set / Edit Destination - Microsoft Internet Explorer

Set / Edit Destination

Defined alarm groups

CriticalMail
Automatic Service Mail

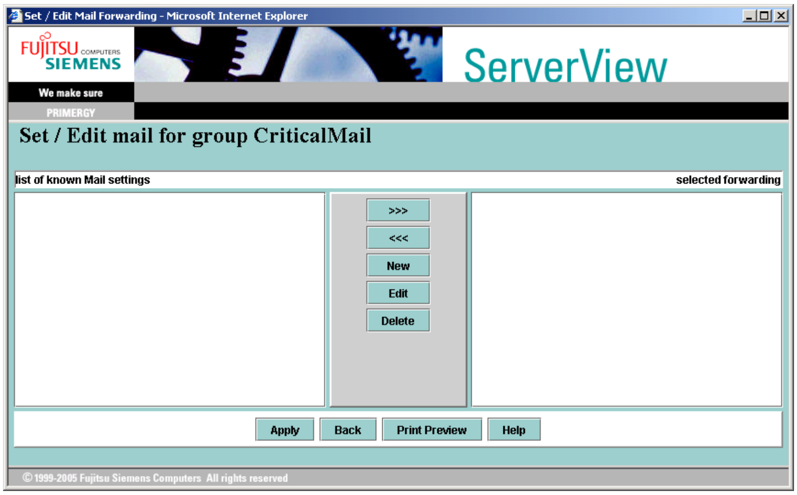
Destinations for the selected group

☑ Enabled

Mail	□
Popup	☑
Logging	□
Pager	□
Execute	□
Broadcast	□
Station	□

© 1999-2005 Fujitsu Siemens Computers All rights reserved

7 Verify that the newly created "CriticalMail" is selected in the alarm group list and click [Mail].



Set / Edit Mail Forwarding - Microsoft Internet Explorer

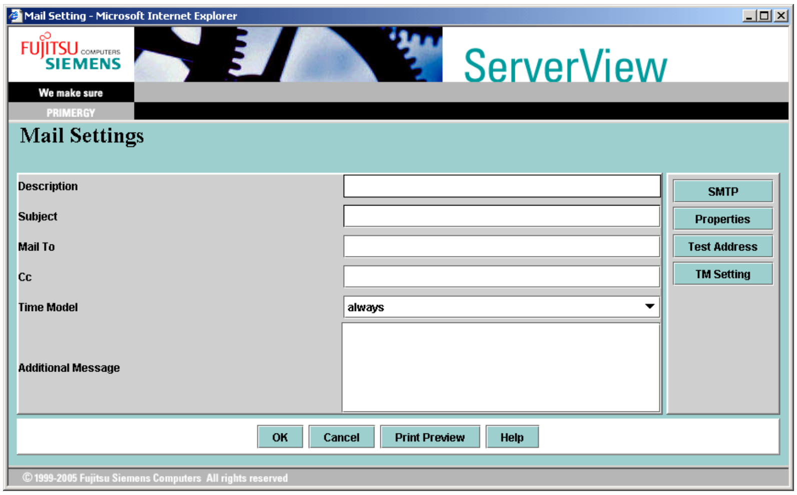
Set / Edit mail for group CriticalMail

list of known Mail settings

selected forwarding

FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
>>>
<<<
New
Edit
Delete
Apply
Back
Print Preview
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

8 Click [New].



Mail Setting - Microsoft Internet Explorer

Mail Settings

Description

Subject

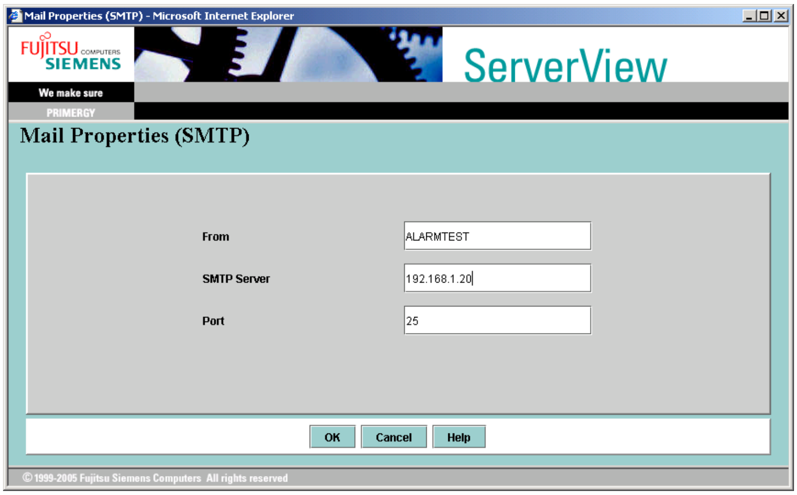
Mail To

Cc

Time Model: always

Additional Message

9 Click [Properties] and enter the required value in each field.


Mail Properties (SMTP) - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
OK
Cancel
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

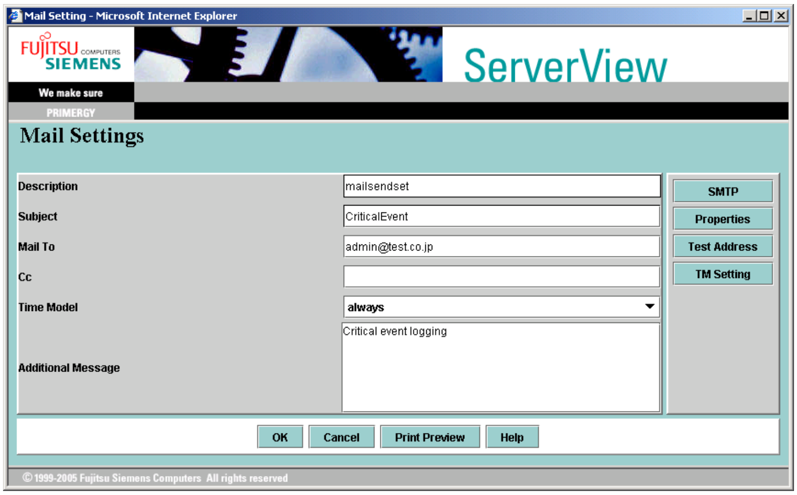
Mail Properties (SMTP)

From: ALARMTEST

SMTP Server: 192.168.1.20

Port: 25

10 Click [OK] to return to the [Mail Settings] window and enter the required value in each field.


Mail Setting - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SMTP
Properties
Test Address
TM Setting
OK
Cancel
Print Preview
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

Mail Settings

Description: mailsendset

Subject: CriticalEvent

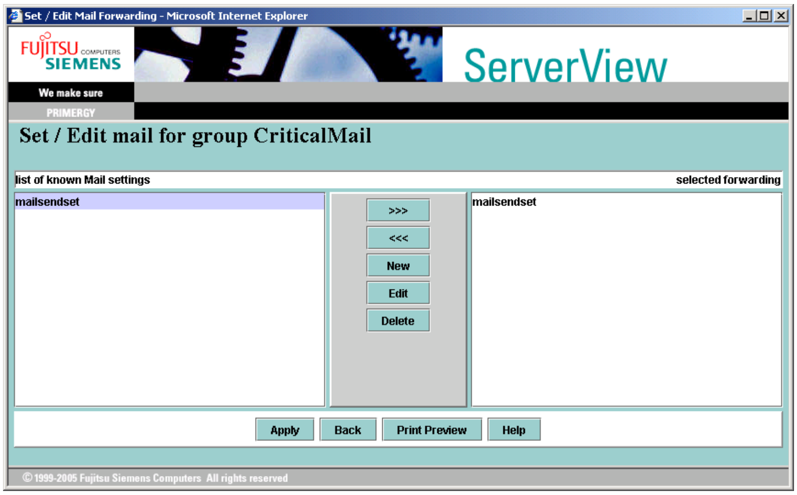
Mail To: admin@test.co.jp

Cc:

Time Model: always

Additional Message: Critical event logging

11 Click [OK] to return to the [Set / Edit mail for group Critical Mail] window, click [Apply] and then [Back].


Set / Edit Mail Forwarding - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
>>>
<<<
New
Edit
Delete
Apply
Back
Print Preview
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

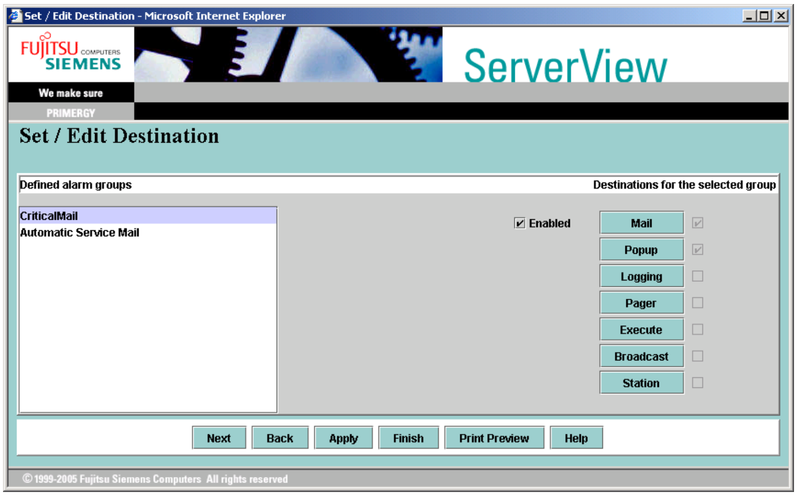
Set / Edit mail for group CriticalMail

list of known Mail settings: mailsendset

selected forwarding: mailsendset

The display returns to the [Set / Edit Destination] window. Since the mail settings have been configured, [Mail] has a check mark.

12 Click [Next].

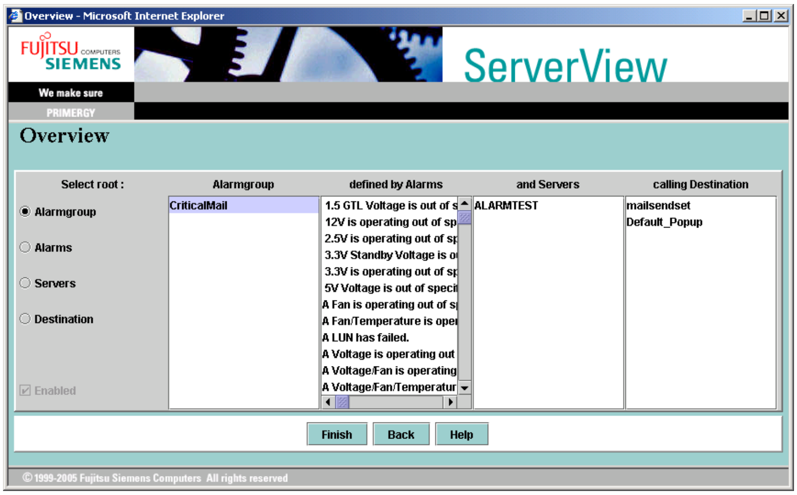

Set / Edit Destination - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
Next
Back
Apply
Finish
Print Preview
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

Set / Edit Destination

Defined alarm groups:
CriticalMail
Automatic Service Mail

Destinations for the selected group:
☑ Enabled
Mail ☑
Popup ☑
Logging ☐
Pager ☐
Execute ☐
Broadcast ☐
Station ☐

13 Confirm the configuration, and click [Finish] to exit.



Overview - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
Finish
Back
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved

Overview

Select root :

● Alarmgroup

○ Alarms

○ Servers

○ Destination

☑ Enabled

Alarmgroup	defined by Alarms	and Servers	calling Destination
CriticalMail	1.5 GTL Voltage is out of s	ALARMTEST	mailsendset
	12V is operating out of sp		Default_Popup
	2.5V is operating out of sp		
	3.3V Standby Voltage is o		
	3.3V is operating out of sp		
	5V Voltage is out of speci		
	A Fan is operating out of s		
	A Fan/Temperature is oper		
	A LUN has failed.		
	A Voltage is operating out		
	A Voltage/Fan is operating		
	A Voltage/Fan/Temperatur		

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

- To use the Performance Manager's function, the following versions are required.
  - For Windows NT: NT Agent V4.00.05 (or later)
  - For Linux: Linux Agent V4.30 (or later)

  See Agent View in "■ Agent Status" (→pg.103) check the Agent version.

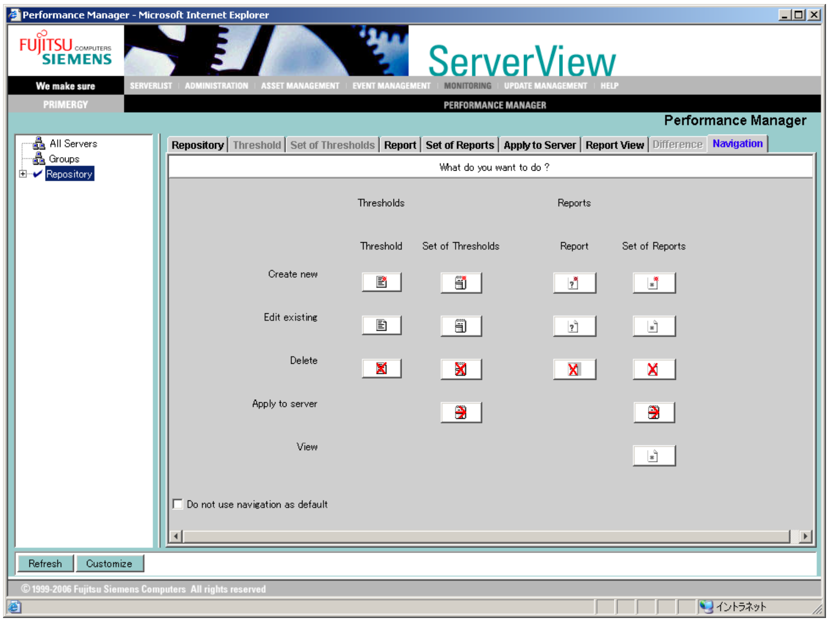
3.6.1 Starting the Performance Manager

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.

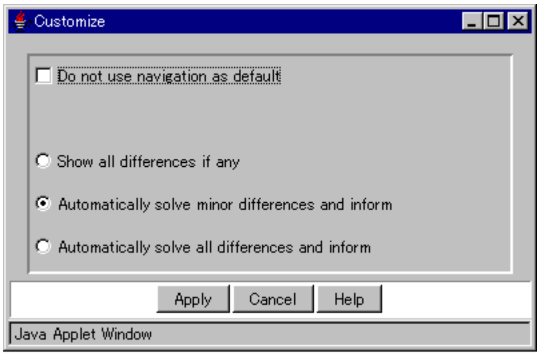

Performance Manager - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | UPDATE MANAGEMENT | HELP
PRIMERGY
PERFORMANCE MANAGER
Performance Manager
All Servers
Groups
Repository
Repository | Threshold | Set of Thresholds | Report | Set of Reports | Apply to Server | Report View | Difference | Navigation
What do you want to do ?
Thresholds
Reports
Threshold
Set of Thresholds
Report
Set of Reports
Create new
Edit existing
Delete
Apply to server
View
Do not use navigation as default
Refresh
Customize
© 1999-2006 Fujitsu Siemens Computers All rights reserved
イントラネット

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.

The following [Customize] window appears by clicking [Customize].



□ Do not use navigation as default

○ Show all differences if any

● Automatically solve minor differences and inform

○ Automatically solve all differences and inform

Check the [Do not use navigation as default] if navigation is not used. Next time the Performance Manager is started, the repository view is opened as initial window.

POINT

- When the settings have been changed by other Performance Manager after getting the latest session, differences may be found between the repository database information of the latest session and the current server settings. All differences are recorded on both database and server with the time-stamp. The followings can be selected.
  - Show all differences if any
  - Automatically solve minor differences and inform
  - Automatically solve all differences and inform

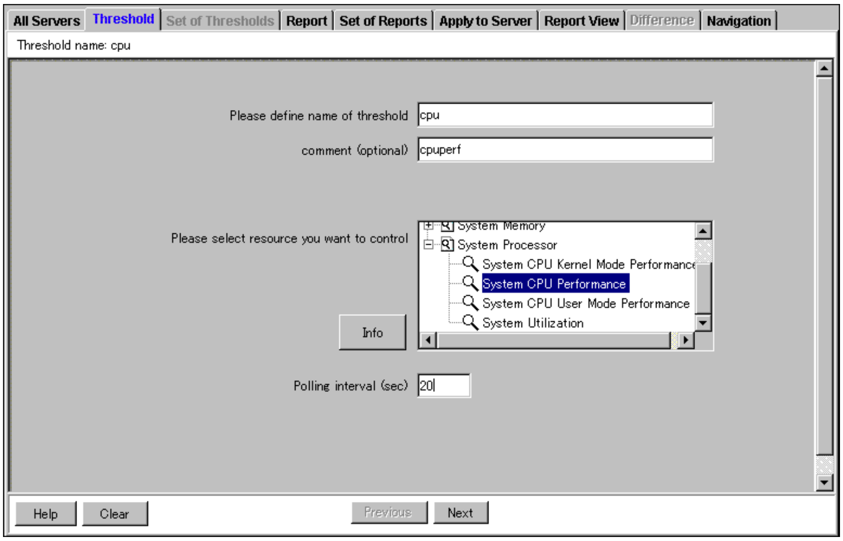
table: Functions on Each Tab

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.
[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.



Threshold name: cpu

Please define name of threshold: cpu

comment (optional): cpuperf

Please select resource you want to control:
- System Memory
- System Processor
  - System CPU Kernel Mode Performanc
  - System CPU Performance
  - System CPU User Mode Performance
  - System Utilization

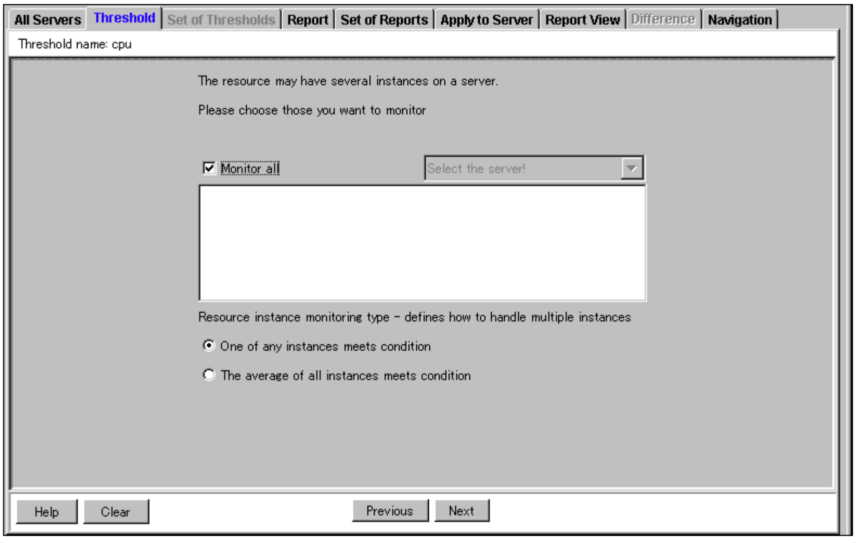
Polling interval (sec): 20

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.
To monitor the resource, select one from the displayed list.
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.



Threshold name: cpu

The resource may have several instances on a server.

Please choose those you want to monitor

☑ Monitor all

Resource instance monitoring type - defines how to handle multiple instances

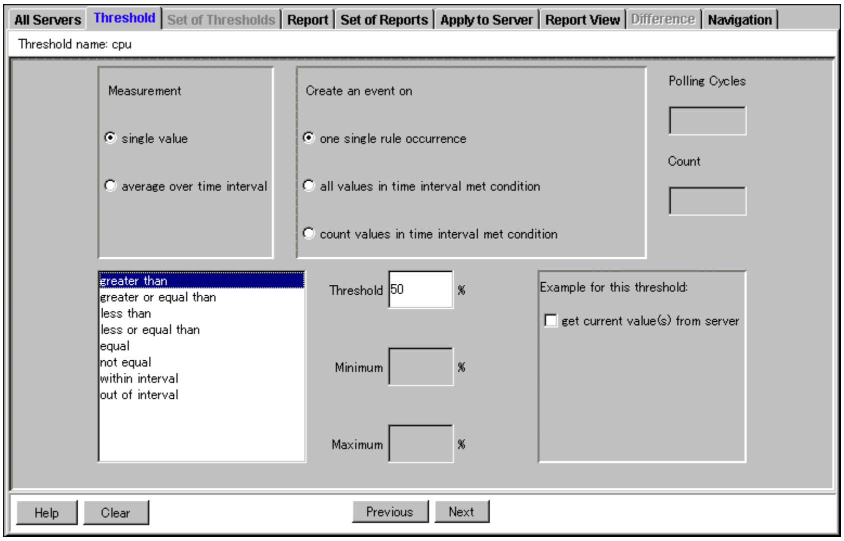
● One of any instances meets condition

○ The average of all instances meets condition

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.



Threshold name: cpu

Measurement

● single value

○ average over time interval

Create an event on

● one single rule occurrence

○ all values in time interval met condition

○ count values in time interval met condition

Polling Cycles

Count

greater than
greater or equal than
less than
less or equal than
equal
not equal
within interval
out of interval

Threshold 50 %

Minimum %

Maximum %

Example for this threshold:

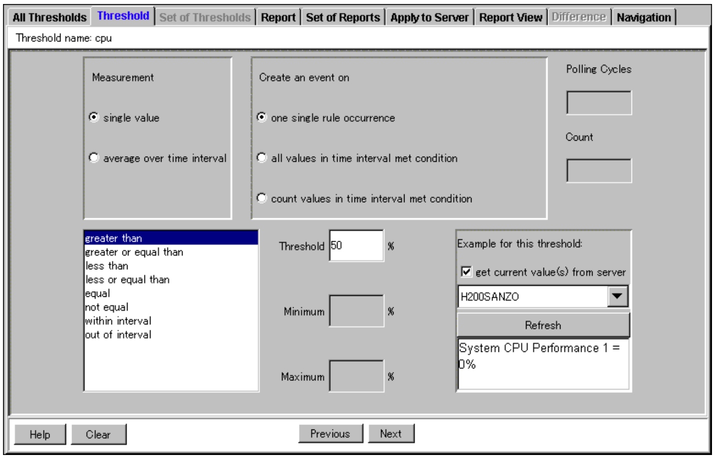
□ get current value(s) from server

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].



Threshold name: cpu

Measurement
● single value
○ average over time interval

Create an event on
● one single rule occurrence
○ all values in time interval met condition
○ count values in time interval met condition

Polling Cycles
Count

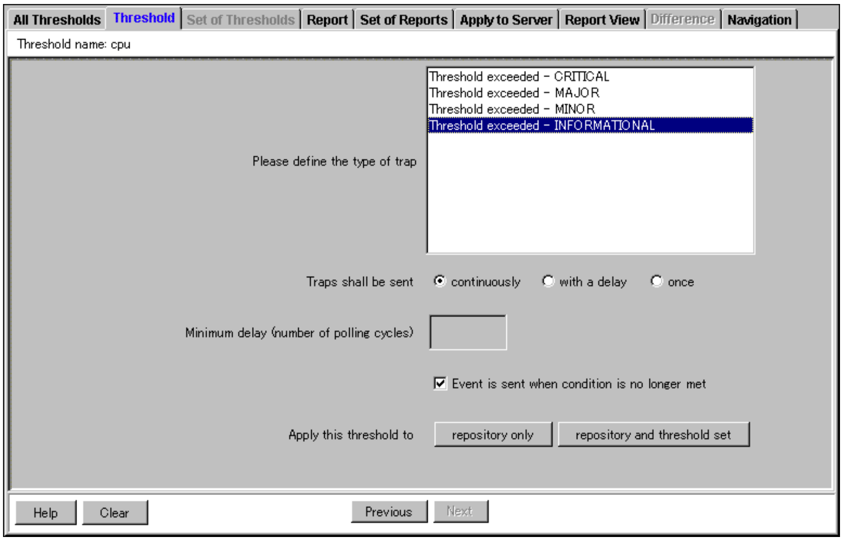
greater than
greater or equal than
less than
less or equal than
equal
not equal
within interval
out of interval

Threshold 50 %
Minimum %
Maximum %

Example for this threshold:
☑ get current value(s) from server
H200SANZO
System CPU Performance 1 = 0%

5 Click [Next].

A screen to select the trap type appears.



Threshold name: cpu

Please define the type of trap
Threshold exceeded - CRITICAL
Threshold exceeded - MAJOR
Threshold exceeded - MINOR
Threshold exceeded - INFORMATIONAL

Traps shall be sent ● continuously ○ with a delay ○ once

Minimum delay (number of polling cycles)

☑ Event is sent when condition is no longer met

Apply this threshold to [repository only] [repository and threshold set]

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.

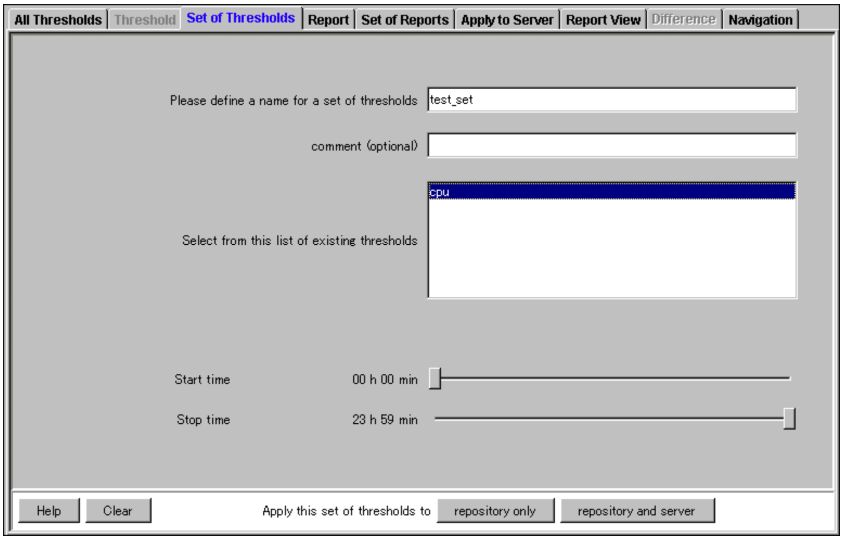
[repository and threshold set]: The threshold is stored in the repository and the [Set of Thresholds] tab appears.

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.



Please define a name for a set of thresholds test_set

comment (optional)

Select from this list of existing thresholds cpu

Start time 00 h 00 min

Stop time 23 h 59 min

Apply this set of thresholds to

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.

Enter comments in the [comment] if needed.

3 Specify the monitoring time (Start time/Stop time) for the Set of Thresholds.

4 Store the Set of Thresholds.

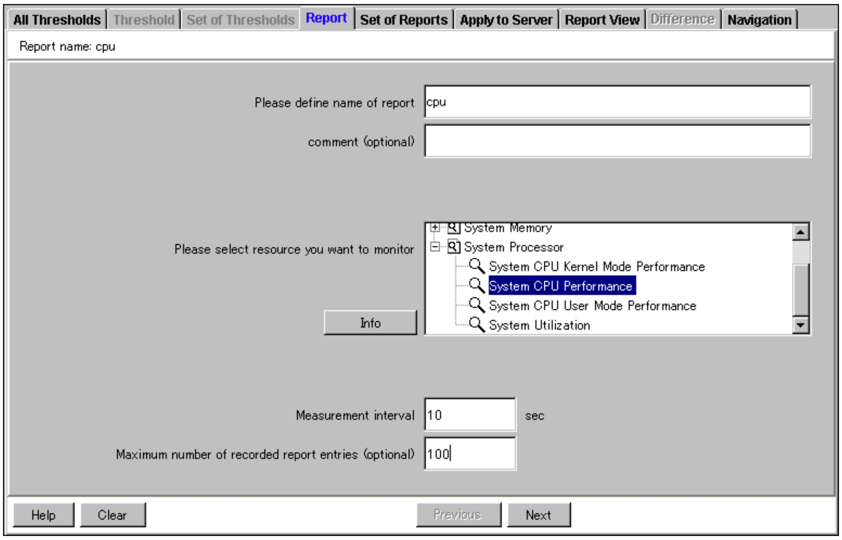
[repository only]: The Set of Thresholds is stored in the repository.

[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.



Report name: cpu

Please define name of report: cpu

comment (optional):

Please select resource you want to monitor:

- System Memory
- System Processor
  - System CPU Kernel Mode Performance
  - System CPU Performance
  - System CPU User Mode Performance
  - System Utilization

Measurement interval: 10 sec

Maximum number of recorded report entries (optional): 100

2 Enter the report name and set the observed resource and poll interval.

table: Setting Items for the Report Definition

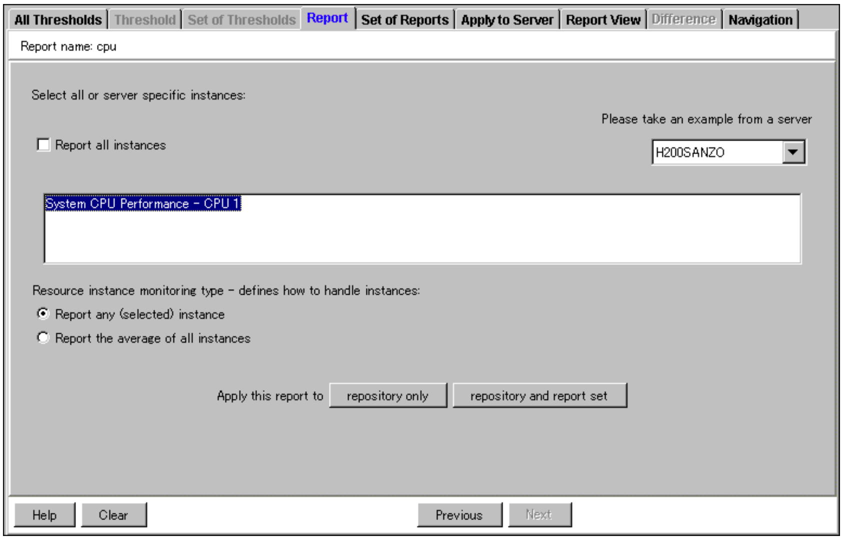
Item	Description
Please define name of report	Enter the report name here.
comment (optional)	Enter a comment for the report here. This item is optional.
Please select resource you want to monitor	Select one resource to be observed.
Measurement interval	Specifies the interval between two reports in seconds.
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.

IMPORTANT

- 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 Click [Next].

The window for setting the instances to be monitored appears.



Report name: cpu

Select all or server specific instances:

Please take an example from a server

□ Report all instances

H200SANZO

System CPU Performance - CPU 1

Resource instance monitoring type - defines how to handle instances:

● Report any (selected) instance

○ Report the average of all instances

Apply this report to [repository only] [repository and report set]

4 Set the instances to be monitored.

To monitor specific instance among selected resources, clear [Report all instances], select the server from the combo box and select the instance to be monitored from the displayed list.
You do not clear [Report all instances] for normal use.
When the [Report all instances] is checked, the average of all instances is reported.

5 Define how to handle instances.

[Report any (selected) instance] or [Report the average of all instances] can be selected.

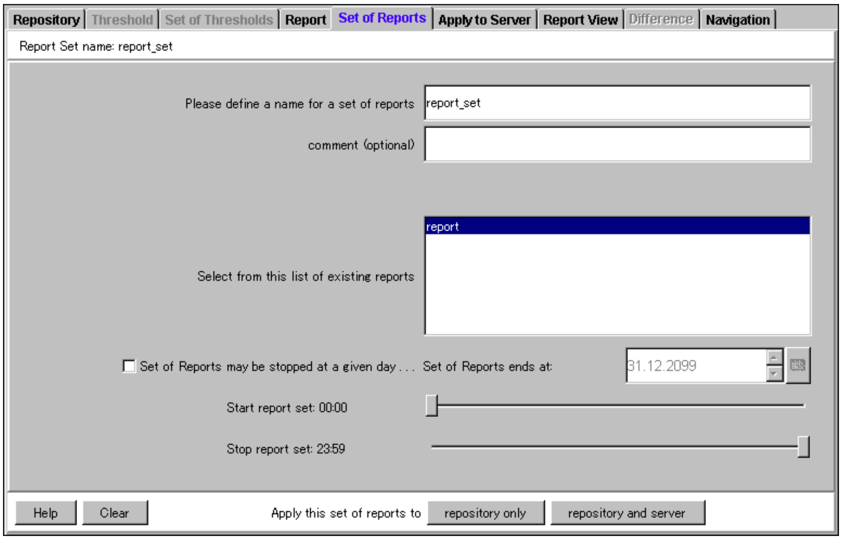
6 Store the reports.

[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.



Repository | Threshold | Set of Thresholds | Report | Set of Reports | Apply to Server | Report View | Difference | Navigation

Report Set name: report_set

Please define a name for a set of reports: report_set

comment (optional):

Select from this list of existing reports: report

□ Set of Reports may be stopped at a given day . . . Set of Reports ends at: 31.12.2099

Start report set: 00:00

Stop report set: 23:59

Help
Clear
Apply this set of reports to
repository only
repository and server

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.

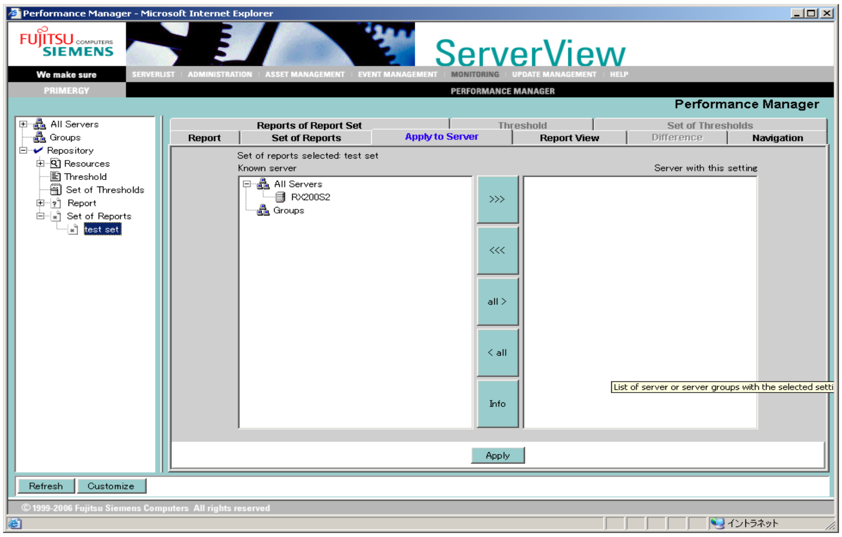
[repository and server]: The Set of Reports is stored in the repository and [Apply to Server] tab appears.

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.



Set of reports selected: test set

The [Known server] 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 login window appears for security. The user name and the password of the ServerView administrator privilege are necessary. After login is authenticated, the settings of [Set of Thresholds] or [Set of Reports] are applied to the servers.

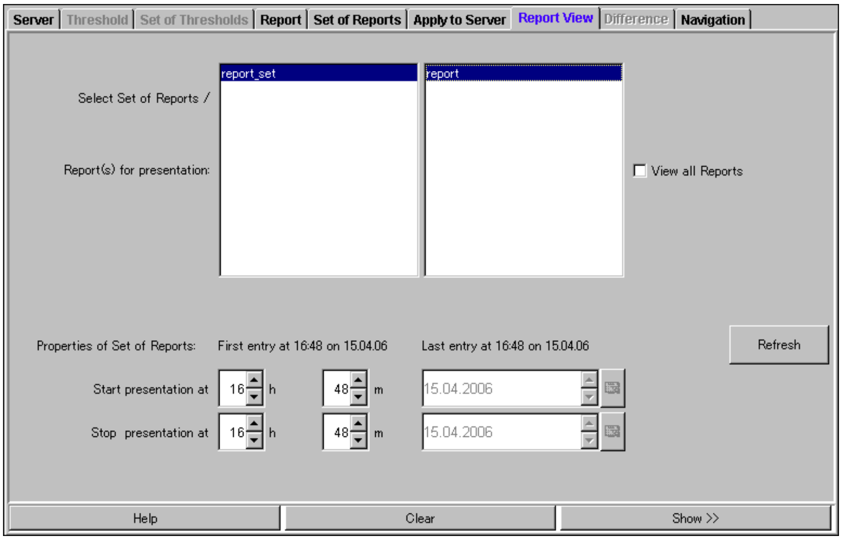
3.6.7 Viewing and Setting Reports

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 window for selecting set of reports appears.



Select Set of Reports / Report(s) for presentation: report_set | report

□ View all Reports

Properties of Set of Reports: First entry at 16:48 on 15.04.06 Last entry at 16:48 on 15.04.06

Start presentation at 16 h 48 m 15.04.2006

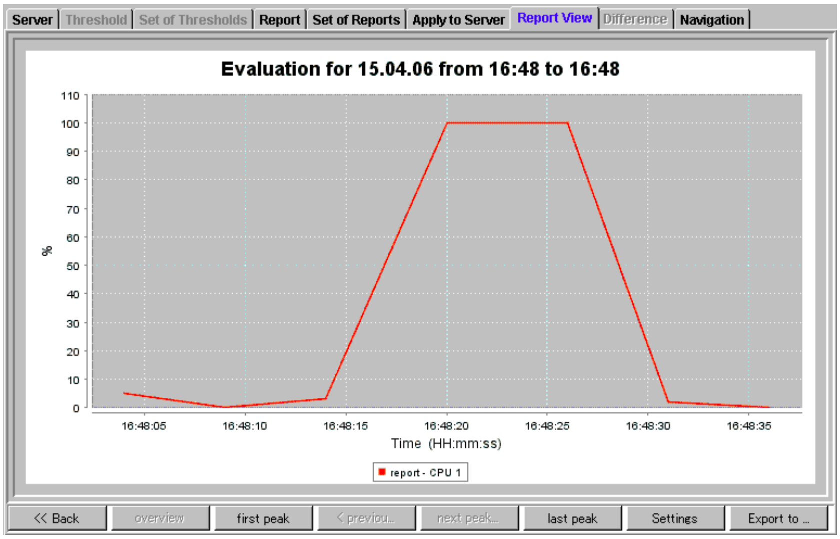
Stop presentation at 16 h 48 m 15.04.2006

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.

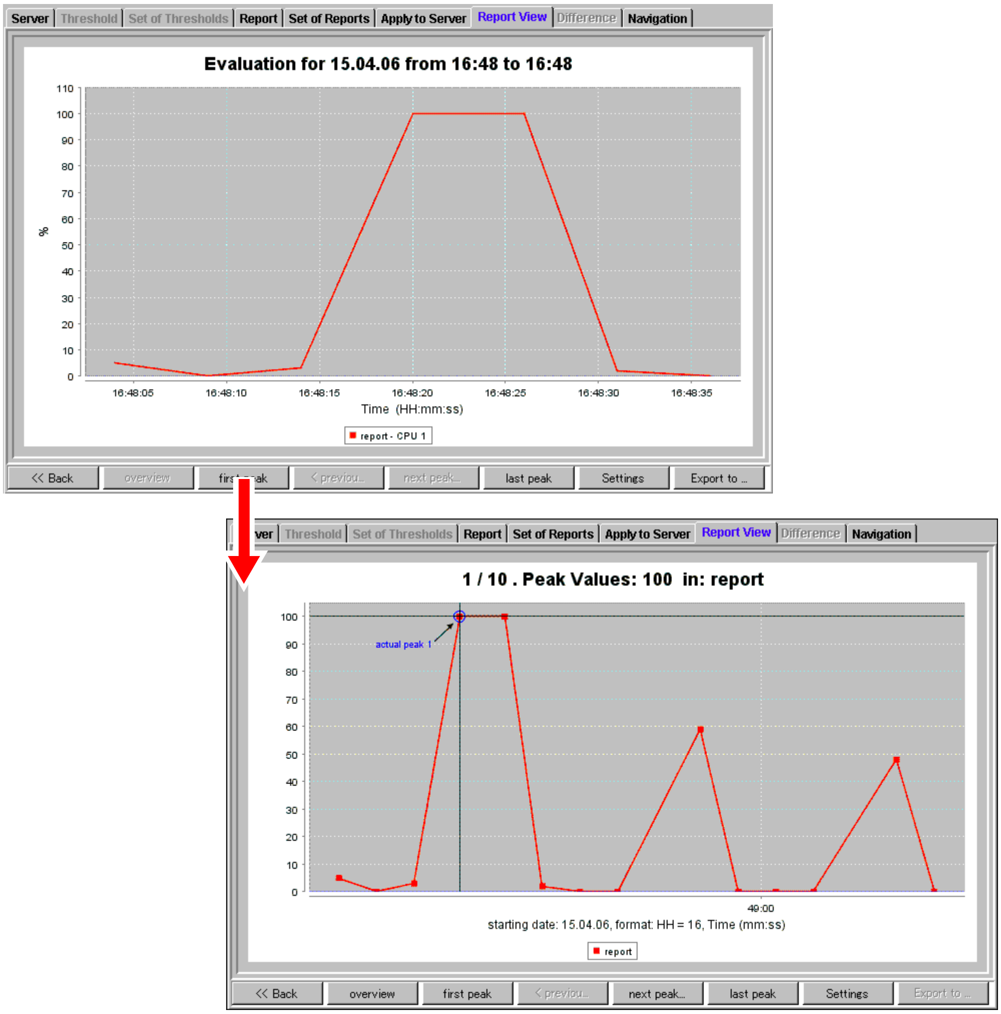
3 Click [Show>>].

The report data is displayed.



For operations for this window, refer to "■ Operations for Report Data" (→pg.191).

■ Operations for Report Data



The following buttons can be used.

table: Buttons of Report Data Window

Button	Description
[<< Back]	Back to the window for selecting set of reports.
[overview]	Back to the report data window from the peak window. This button is available when the peak window is displayed.
[first peak]	Switch s to the peak window and displays the first peak.
[< previous]	Displays the previous peak. This button is always available except when the first peak is displayed.
[next peak]	Displays the next peak. This button is always available except when the last peak is displayed.
[last peak]	Displays the last peak.
[Settings]	Displays the [Settings] window. The settings such as peak values and chart type can be configured.→"● Window for Setting" (pg.192)

table: Buttons of Report Data Window

Button	Description
[Export to...]	Displays the [Export to CSV file] window. →"● Window for Exporting to CSV files" (pg.196)

IMPORTANT

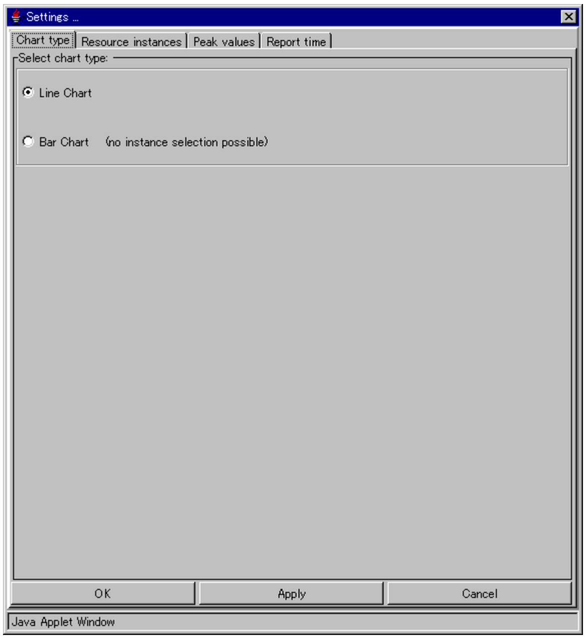
- For Linux, displaying the peak value and the [Export to...] function are not supported.

● Window for Setting

The settings such as peak values and chart type can be configured in this window.
To reflect changes, click [Apply].

- [Chart type] tab

  Select chart type of report data.



Select chart type:

◉ Line Chart

○ Bar Chart (no instance selection possible)

table: Items of [Chart type] tab

Item	Description
Line Chart	Report data is displayed in the line chart.
Bar Chart	Report data is displayed in the bar chart.

- [Resource instances] tab
  Select instances to be displayed.

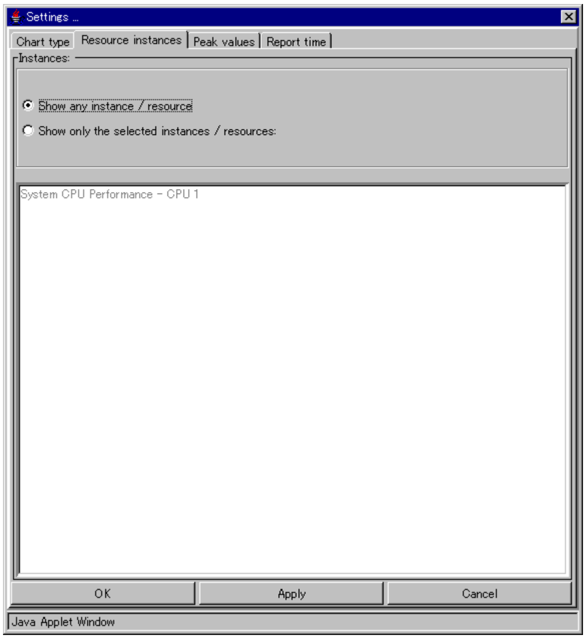
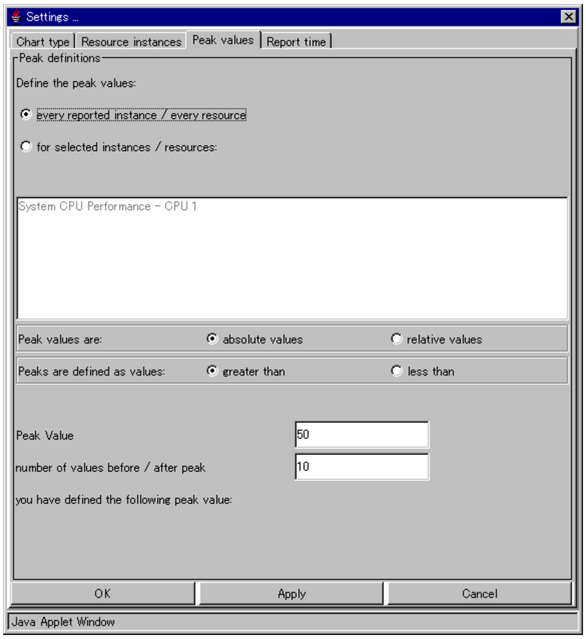

Settings ...
Chart type
Resource instances
Peak values
Report time
Instances:
● Show any instance / resource
○ Show only the selected instances / resources:
System CPU Performance - CPU 1
OK
Apply
Cancel
Java Applet Window

table: Items of [Resource instances] tab

Item	Description
Show any instance / resource	The measured instances of all resources are displayed.
Show only the selected instances / resources	The instances to be displayed can be selected.

- [Peak values] tab

  Configure peak values.



Peak definitions

Define the peak values:

● every reported instance / every resource

○ for selected instances / resources:

System CPU Performance - CPU 1

Peak values are: ● absolute values ○ relative values

Peaks are defined as values: ● greater than ○ less than

Peak Value: 50

number of values before / after peak: 10

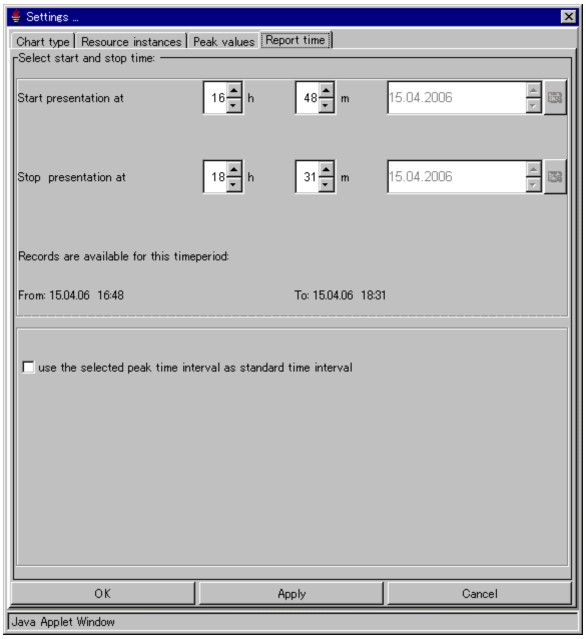
you have defined the following peak value:

table: Items of [Peak values] tab

Item	Description
Define the peak values	Select instances to be searched.
every reported instance / every resource	Searches the peak on all instances.
for selected instances / resources	Searches the peak on instances selected from the list.
Peak values are	Select absolute values or relative values.
Peaks are defined as values	Select intended peak values.
greater than	The values greater than criterial value are intended.
less than	The values less than criterial value are intended.
Peak Value	Configure the criterial peak value.
number of values before / after peak	Configure the number of peak values to be displayed.

- [Report time] tab

  Configure the time of displaying the report.



Select start and stop time:

Start presentation at 16 h 48 m 15.04.2006

Stop presentation at 18 h 31 m 15.04.2006

Records are available for this timeperiod:

From: 15.04.06 16:48 To: 15.04.06 18:31

□ use the selected peak time interval as standard time interval

table: Items of [Rport time] tab

Item	Description
Start presentation at	Displays the presentation that is recorded after specified time.
Stop presentation at	Displays the presentation that is recorded before specified time.
use the selected peak time interval as standard time interval	Check this box if you want to compare peak values between reports.

● Window for Exporting to CSV files

The settings for exporting report data to CSV files can be configured in this window.

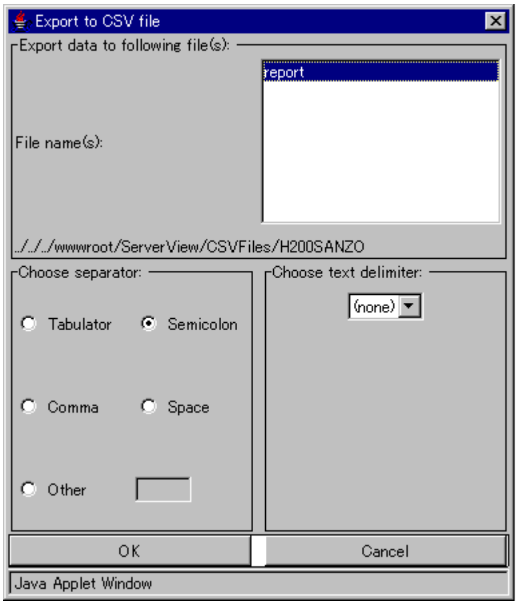


table: Items of [Export to CSV file] window

Item	Description
Export data to following file(s)	Select the file from the list.
Choose separator	Select a mark such as comma and tabulator to use as separator.
Choose text delimiter	Select test delimiter.

The directories where the CSV files are stored are as follows.

- When ServerView Web-Server (Apache for Win32 base) is used
  System Drive:\Program Files\Fujitsu\F5FBFE01\ServerView Services\wwwroot\ServerView\CSVFiles\[server name]\
- When IIS is used
  System Drive:\Inetpub\wwwroot\ServerView\CSVFiles\[server name]\

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.

IMPORTANT

- When ServerView is uninstalled leaving threshold/report settings of the Performance Manager, the configuration will differ between the console and the Agent. Make sure to remove the threshold/report settings before uninstalling ServerView.

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

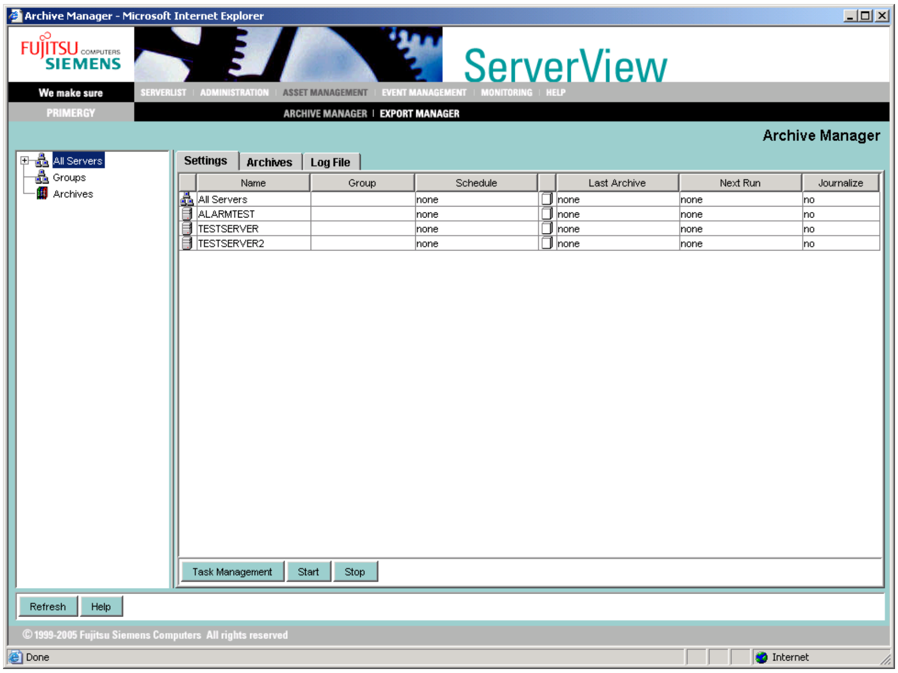
- For details about the archive manager, refer to online help topics.

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.


Archive Manager - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
PRIMERGY
ARCHIVE MANAGER | EXPORT MANAGER
Archive Manager
All Servers
Groups
Archives
Settings
Archives
Log File
Task Management
Start
Stop
Refresh
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Done
Internet

Name	Group	Schedule		Last Archive	Next Run	Journalize
All Servers		none		none	none	no
ALARMTEST		none		none	none	no
TESTSERVER		none		none	none	no
TESTSERVER2		none		none	none	no

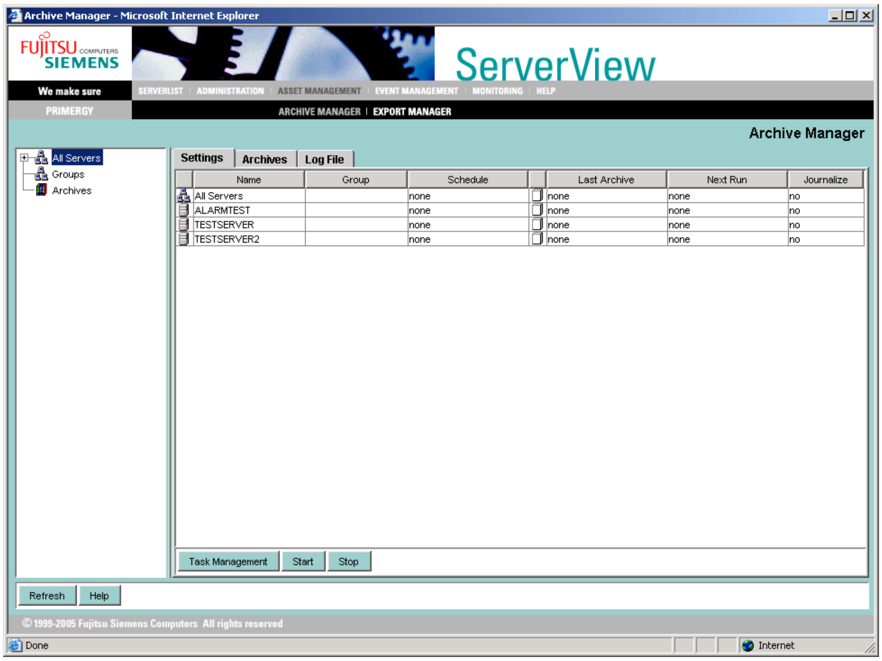
POINT

- 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.


Archive Manager - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
PRIMERGY
ARCHIVE MANAGER | EXPORT MANAGER
Archive Manager
All Servers
Groups
Archives
Settings
Archives
Log File
Task Management
Start
Stop
Refresh
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Done
Internet

Name	Group	Schedule		Last Archive	Next Run	Journalize
All Servers		none	☐	none	none	no
ALARMTEST		none	☐	none	none	no
TESTSERVER		none	☐	none	none	no
TESTSERVER2		none	☐	none	none	no

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]\

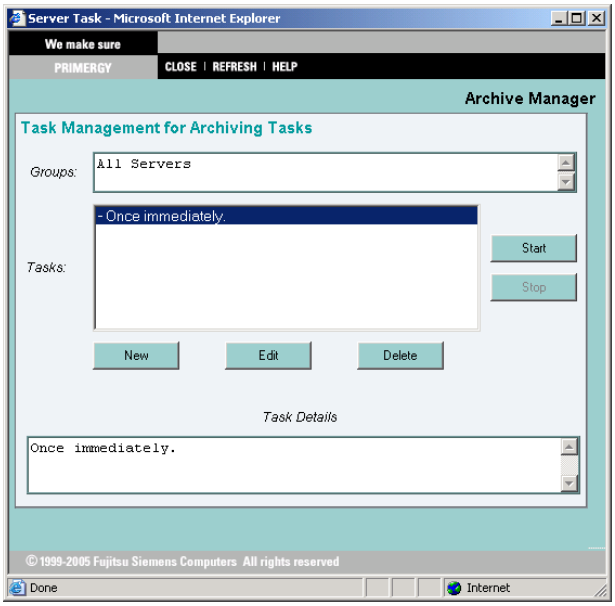
- When Red Hat Linux is used
  \var\www\html\ServerView/Arcive\[server name]\
- When Suse Linux is used
  \srv\www\htdocs\ServerView\Archive\[server name]\

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.


Server Task - Microsoft Internet Explorer
We make sure
PRIMERGY
CLOSE | REFRESH | HELP
Archive Manager
Start
Stop
New
Edit
Delete
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Done
Internet

Task Management for Archiving Tasks

Groups: All Servers

Tasks: - Once immediately.

Task Details

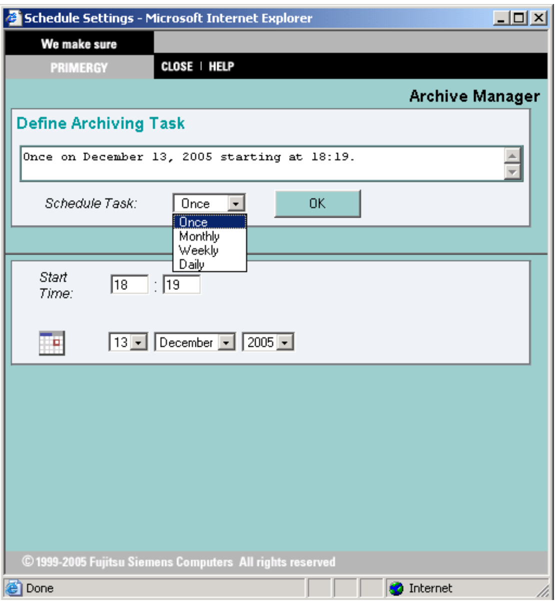
Once immediately.

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.


Schedule Settings - Microsoft Internet Explorer
We make sure
PRIMERGY
CLOSE | HELP
Archive Manager
Once
Monthly
Weekly
Daily
OK
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Done
Internet

Define Archiving Task

```
Once on December 13, 2005 starting at 18:19.
```

Schedule Task: Once

Start Time: 18 : 19

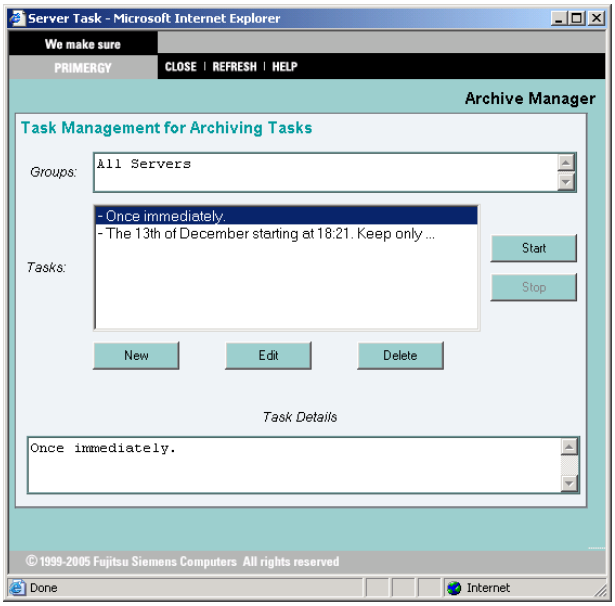
13 December 2005

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.


Server Task - Microsoft Internet Explorer
We make sure
PRIMERGY
CLOSE | REFRESH | HELP
Archive Manager
Task Management for Archiving Tasks
Start
Stop
New
Edit
Delete
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Done
Internet

Groups: All Servers

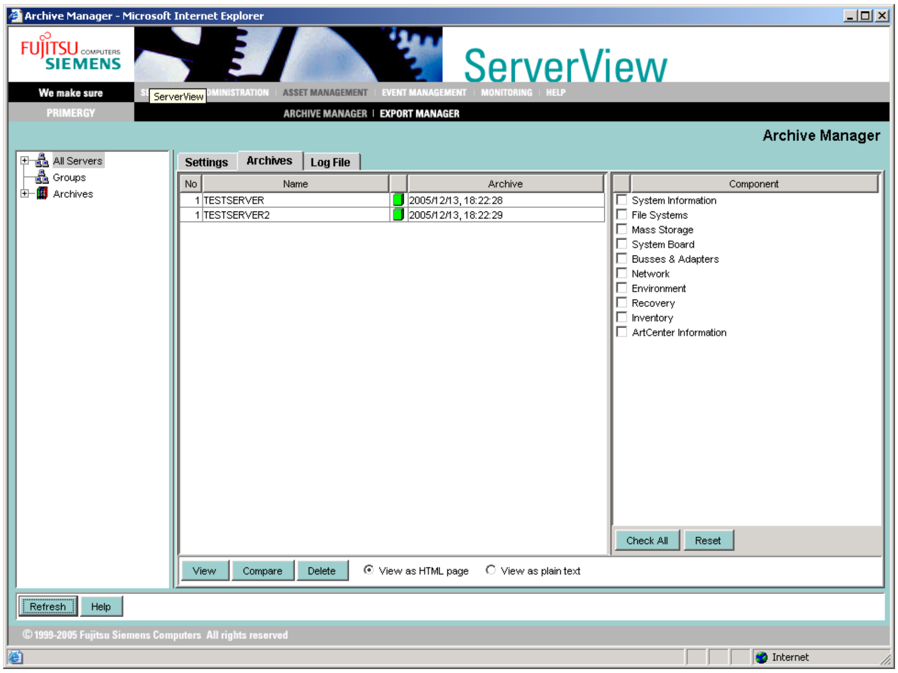
Tasks:
- Once immediately.
- The 13th of December starting at 18:21. Keep only ...

Task Details

Once immediately.

3.7.4 Displaying/Comparing/Deleting Archive Data

Display/compare/delete archive data in the [Archives] tab.


Archive Manager - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
PRIMERGY
ServerView
ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
ARCHIVE MANAGER | EXPORT MANAGER
Archive Manager
All Servers
Groups
Archives
Settings
Archives
Log File
Check All
Reset
View
Compare
Delete
Refresh
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Internet

No	Name		Archive
1	TESTSERVER	🟩	2005/12/13, 18:22:28
1	TESTSERVER2	🟩	2005/12/13, 18:22:29

Component
- □ System Information
- □ File Systems
- □ Mass Storage
- □ System Board
- □ Busses & Adapters
- □ Network
- □ Environment
- □ Recovery
- □ Inventory
- □ ArtCenter Information

● View as HTML page ○ View as plain text

■ Displaying Archive Data

Follow the procedure below to display archive data.

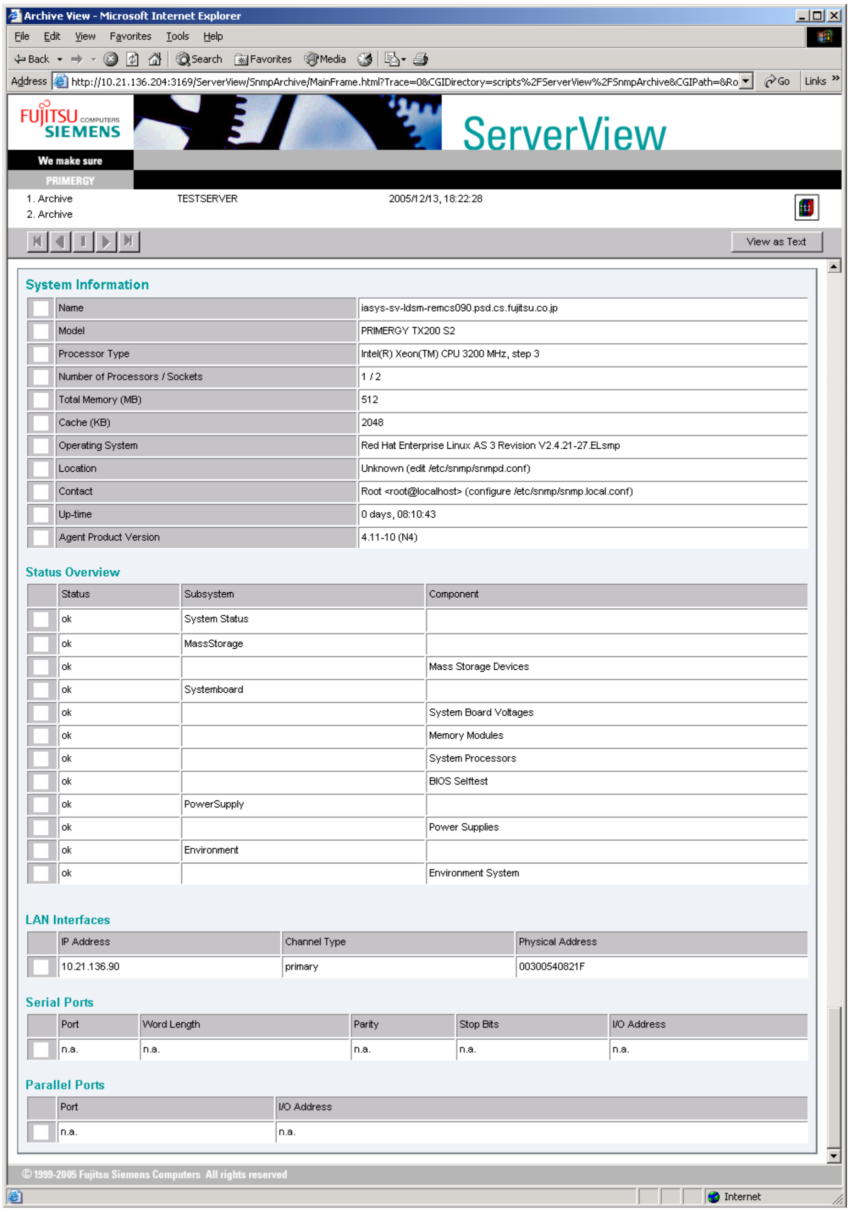
1 Click the [Archives] tab and select the corresponding archive.

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.


Archive View - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.21.136.204:3169/ServerView/SnmpArchive/MainFrame.html?Trace=0&CGIDirectory=scripts%2FServerView%2FSnmpArchive&CGIPath=&Ro
Go Links
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
PRIMERGY
View as Text
Internet

1. Archive TESTSERVER 2005/12/13, 18:22:28
2. Archive

System Information

□	Name	iasys-sv-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 /etc/snmp/snmpd.conf)
□	Contact	Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
□	Up-time	0 days, 08:10:43
□	Agent Product Version	4.11-10 (N4)

Status Overview

	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

	IP Address	Channel Type	Physical Address
□	10.21.136.90	primary	00300540821F

Serial Ports

	Port	Word Length	Parity	Stop Bits	I/O Address
□	n.a.	n.a.	n.a.	n.a.	n.a.

Parallel Ports

	Port	I/O Address
□	n.a.	n.a.

© 1999-2005 Fujitsu Siemens Computers All rights reserved

■ Comparing Archive Data

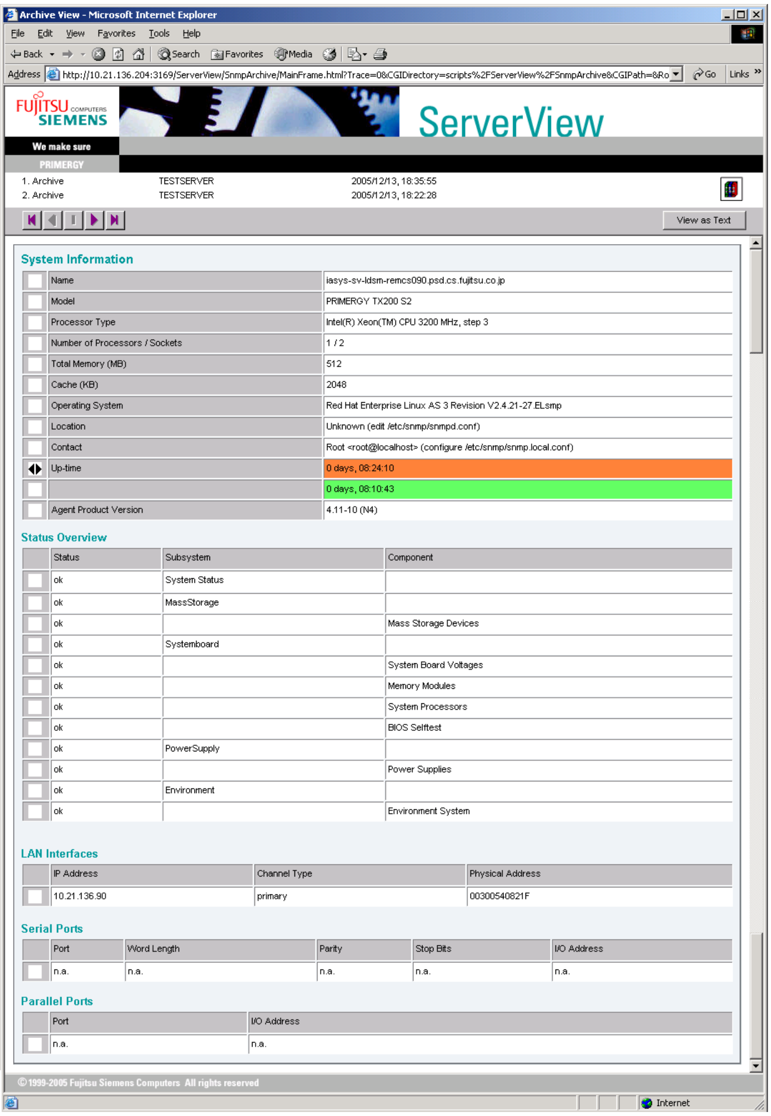
Follow the procedure below to compare archive data in a server.

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.


Archive View - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Links
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
PRIMERGY
View as Text
Internet

http://10.21.136.204:3169/ServerView/SnmpArchive/MainFrame.html?Trace=0&CGIDirectory=scripts%2FServerView%2FSnmpArchive&CGIPath=&Ro

1. Archive	TESTSERVER	2005/12/13, 18:35:55
2. Archive	TESTSERVER	2005/12/13, 18:22:28

System Information

□	Name	iasys-sv-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 /etc/snmp/snmpd.conf)
□	Contact	Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
◀▶	Up-time	0 days, 08:24:10
□		0 days, 08:10:43
□	Agent Product Version	4.11-10 (N4)

Status Overview

	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

	IP Address	Channel Type	Physical Address
□	10.21.136.90	primary	00300540821F

Serial Ports

	Port	Word Length	Parity	Stop Bits	I/O Address
□	n.a.	n.a.	n.a.	n.a.	n.a.

Parallel Ports

	Port	I/O Address
□	n.a.	n.a.

© 1999-2005 Fujitsu Siemens Computers All rights reserved

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]

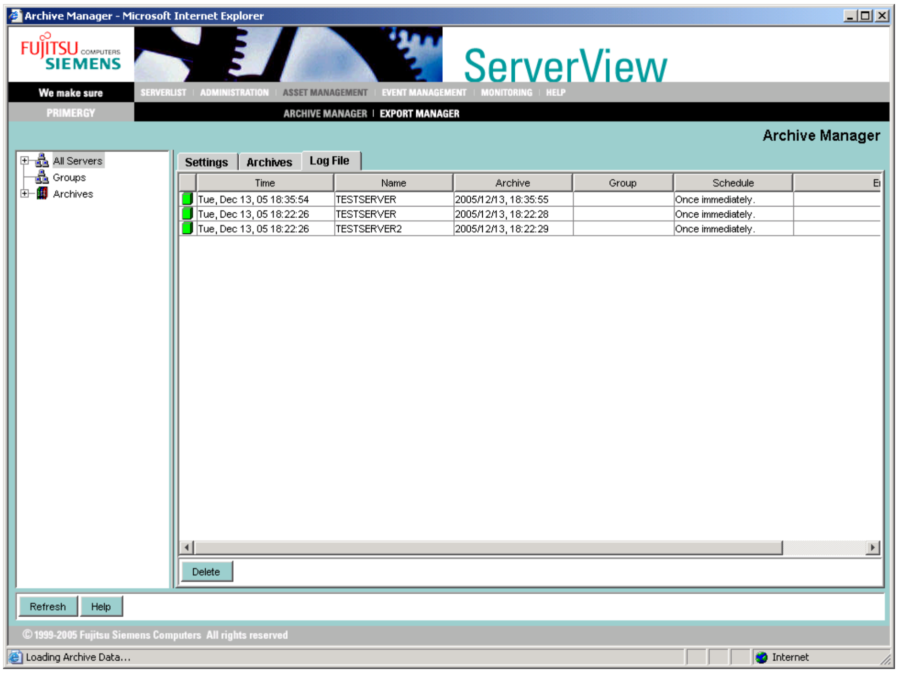
The archive data is deleted.

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.


Archive Manager - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
PRIMERGY
ARCHIVE MANAGER | EXPORT MANAGER
Archive Manager
All Servers
Groups
Archives
Settings
Archives
Log File
Delete
Refresh
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Loading Archive Data...
Internet

	Time	Name	Archive	Group	Schedule	E
🟩	Tue, Dec 13, 05 18:35:54	TESTSERVER	2005/12/13, 18:35:55		Once immediately.	
🟩	Tue, Dec 13, 05 18:22:26	TESTSERVER	2005/12/13, 18:22:28		Once immediately.	
🟩	Tue, Dec 13, 05 18:22:26	TESTSERVER2	2005/12/13, 18:22:29		Once immediately.	

table: Log List in Archive Manager

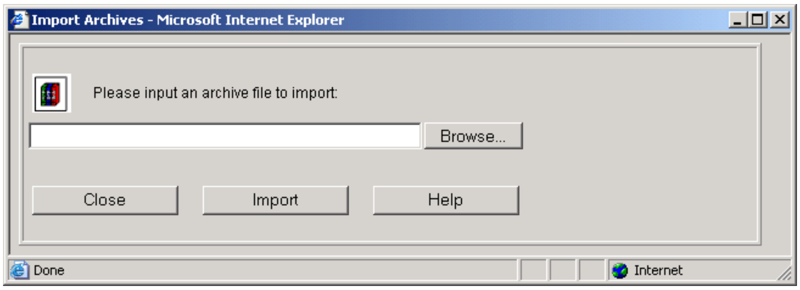
Items	Description
Time	The day and time when archive data is obtained are displayed.
Name	The object name is displayed.
Archive	The archive name is displayed.
Schedule	The format in which the archive is obtained is displayed.

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.

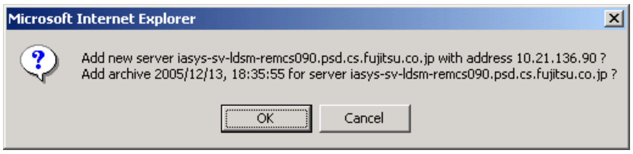


Please input an archive file to import:

2 Click [Browse] and specify the archive file to import.

3 Click [Import].

The confirmation dialog box appears.



Add new server iasys-sv-ldsm-remcs090.psd.cs.fujitsu.co.jp with address 10.21.136.90 ?
Add archive 2005/12/13, 18:35:55 for server iasys-sv-ldsm-remcs090.psd.cs.fujitsu.co.jp ?

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.

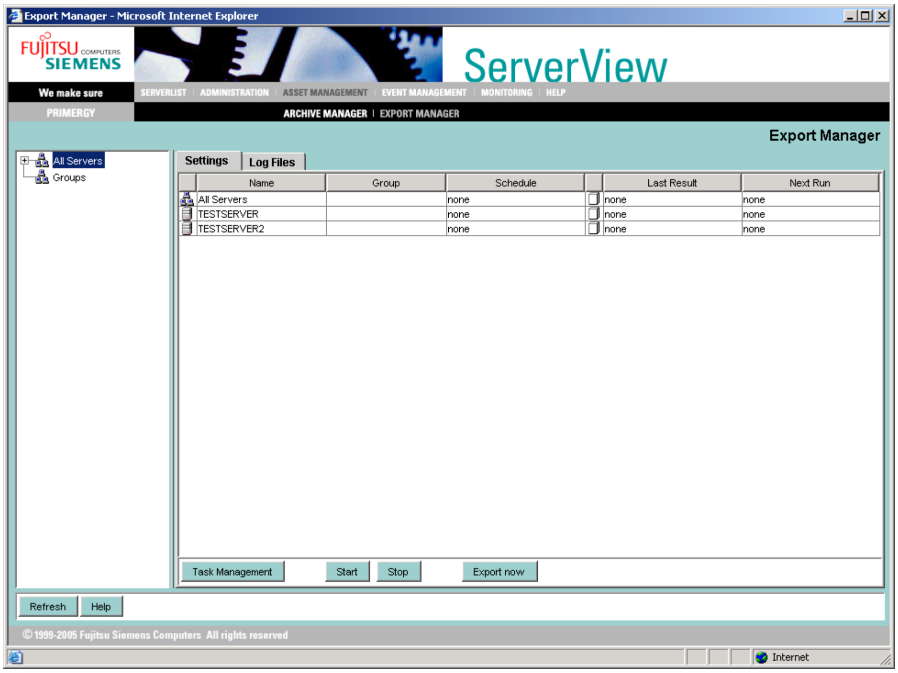
3.8.1 Acquiring Export Data

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.


Export Manager - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
PRIMERGY
ARCHIVE MANAGER | EXPORT MANAGER
Export Manager
All Servers
Groups
Settings
Log Files
Task Management
Start
Stop
Export now
Refresh
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Internet

Name	Group	Schedule	Last Result	Next Run
All Servers		none	none	none
TESTSERVER		none	none	none
TESTSERVER2		none	none	none

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
     ```

     or

     ```
     # rpm -ql jre | grep bin/java
     ```

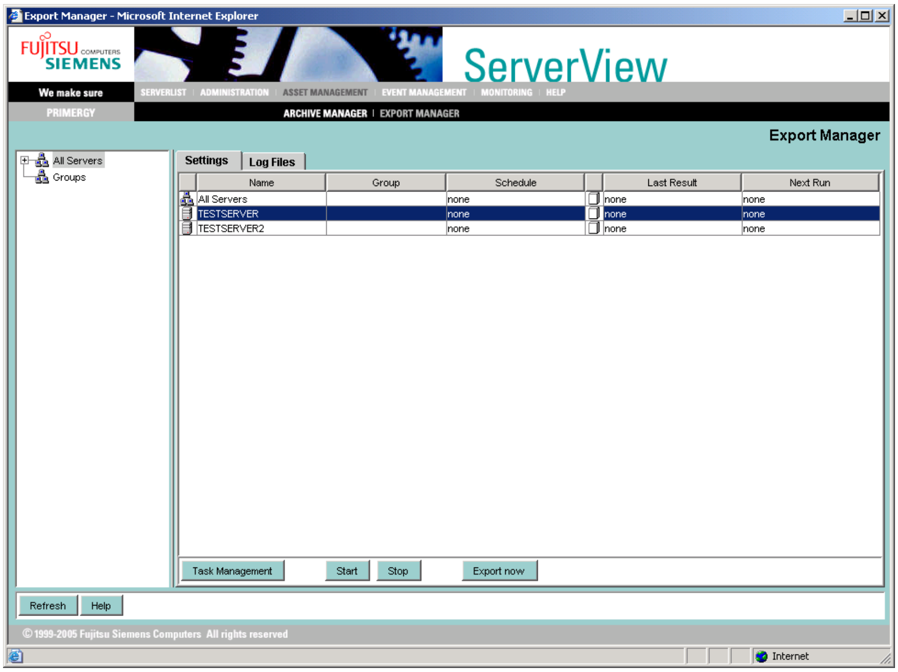
  2. Add following 2 lines to the /etc/profile and log off the OS.
     The following is an example when the Java is install in /usr/lib/···.

     ```
     PATH=/usr/lib/j2rex.x.x_xx/bin:$PATH
     export PATH
     ```

     or

     ```
     PATH=/usr/lib/jrex.x.x_xx/bin:$PATH
     export PATH
     ```

2 Click the [Settings] tab and select the server in which export data is to be created.



Export Manager - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
ServerView
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | HELP
ARCHIVE MANAGER | EXPORT MANAGER
Export Manager
All Servers
Groups
Settings
Log Files
Task Management
Start
Stop
Export now
Refresh
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Internet

Name	Group	Schedule	Last Result	Next Run
All Servers		none	none	none
TESTSERVER		none	none	none
TESTSERVER2		none	none	none

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.

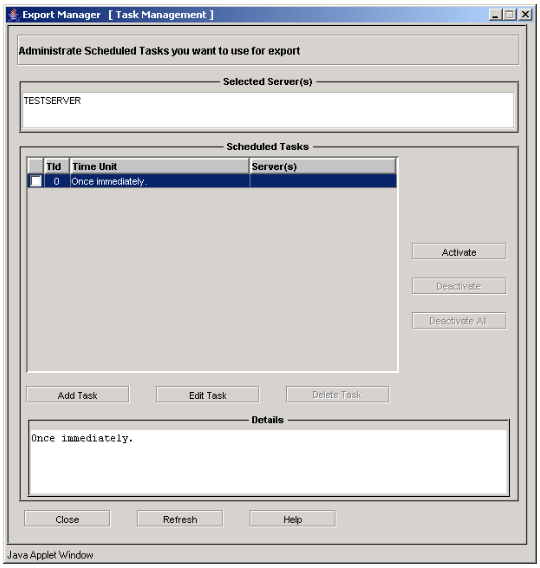
POINT

- 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.210). 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.



Export Manager [Task Management]

Administrate Scheduled Tasks you want to use for export

Selected Server(s)

TESTSERVER

Scheduled Tasks

	TId	Time Unit	Server(s)
□	0	Once immediately.	

Details

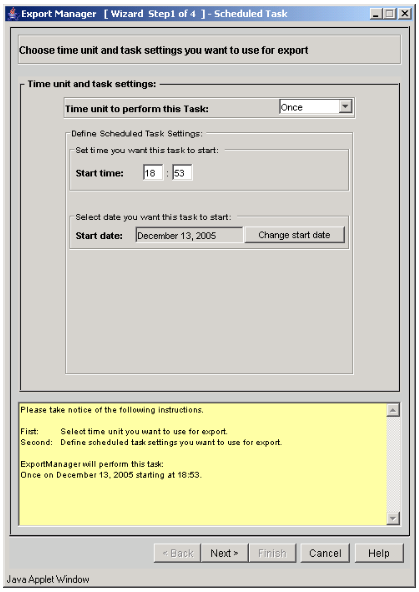
Once immediately.

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.



Export Manager [Wizard Step1 of 4] - Scheduled Task

Choose time unit and task settings you want to use for export

Time unit and task settings:

Time unit to perform this Task: Once

Define Scheduled Task Settings:

Set time you want this task to start:

Start time: 18 : 53

Select date you want this task to start:

Start date: December 13, 2005

Please take notice of the following instructions.

First: Select time unit you want to use for export.
Second: Define scheduled task settings you want to use for export.

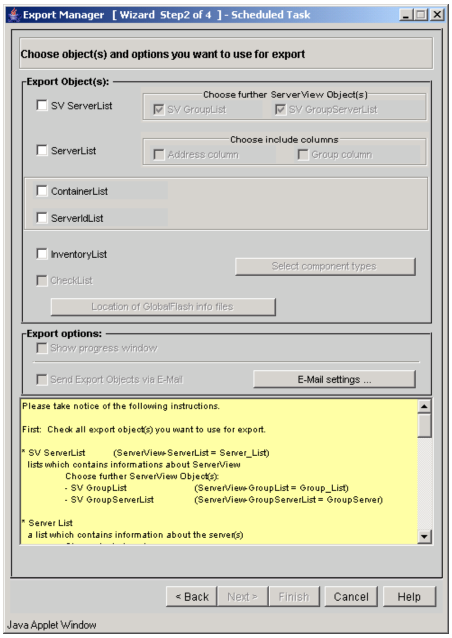
ExportManager will perform this task:
Once on December 13, 2005 starting at 18:53.

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].

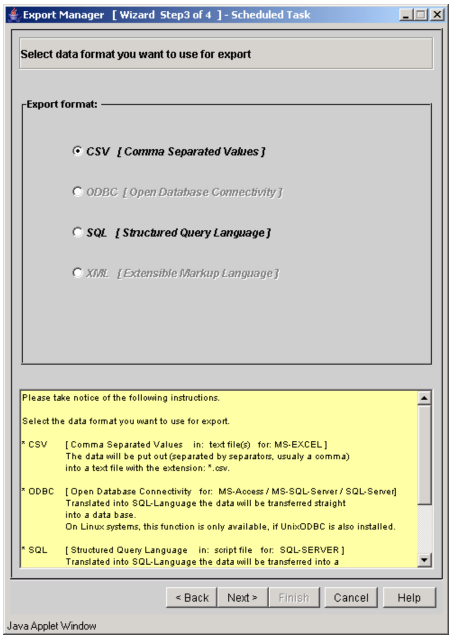
The window for selecting objects appears.



```
Please take notice of the following instructions.

First:  Check all export object(s) you want to use for export.

* SV ServerList         (ServerView-ServerList = Server_List)
  lists which contains informations about ServerView
              Choose further ServerView Object(s):
              - SV GroupList                (ServerView-GroupList = Group_List)
              - SV GroupServerList          (ServerView-GroupServerList = GroupServer)

* Server List
  a list which contains information about the server(s)
```

5 Select an object to export by checking its checkbox and click [Next].

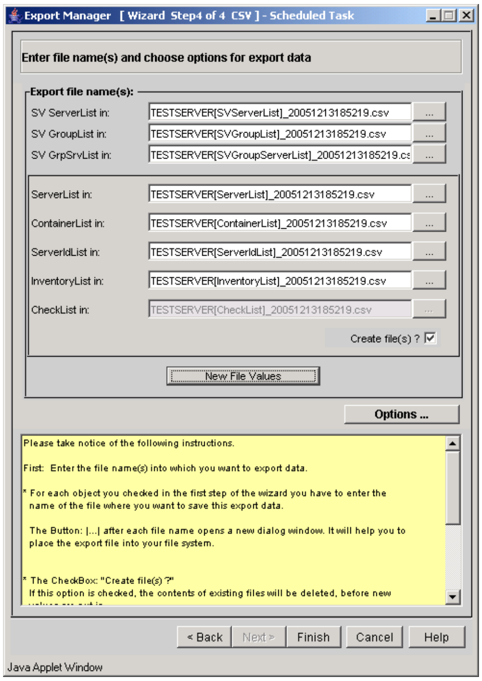
The window for selecting a data type appears.


Export Manager [Wizard Step3 of 4] - Scheduled Task
Select data format you want to use for export
Export format:
● CSV [Comma Separated Values]
○ ODBC [Open Database Connectivity]
○ SQL [Structured Query Language]
○ XML [Extensible Markup Language]
< Back
Next >
Finish
Cancel
Help
Java Applet Window

```
Please take notice of the following instructions.

Select the data format you want to use for export.

* CSV     [ Comma Separated Values    in:  text file(s)   for: MS-EXCEL ]
          The data will be put out (separated by separators, usualy a comma)
          into a text file with the extension: *.csv.

* ODBC    [ Open Database Connectivity   for:  MS-Access / MS-SQL-Server / SQL-Server]
          Translated into SQL-Language the data will be transferred straight
          into a data base.
          On Linux systems, this function is only available, if UnixODBC is also installed.

* SQL     [ Structured Query Language    in:  script file   for:  SQL-SERVER ]
          Translated into SQL-Language the data will be transferred into a
```

6 Select a data type and click [Next].

The window for specifying a file name appears.



Enter file name(s) and choose options for export data

Export file name(s):

SV ServerList in:	TESTSERVER[SVServerList]_20051213185219.csv
SV GroupList in:	TESTSERVER[SVGroupList]_20051213185219.csv
SV GrpSrvList in:	TESTSERVER[SVGroupServerList]_20051213185219.cs
ServerList in:	TESTSERVER[ServerList]_20051213185219.csv
ContainerList in:	TESTSERVER[ContainerList]_20051213185219.csv
ServerIdList in:	TESTSERVER[ServerIdList]_20051213185219.csv
InventoryList in:	TESTSERVER[InventoryList]_20051213185219.csv
CheckList in:	TESTSERVER[CheckList]_20051213185219.csv

Create file(s) ? ☑

Please take notice of the following instructions.

First: Enter the file name(s) into which you want to export data.

* For each object you checked in the first step of the wizard you have to enter the name of the file where you want to save this export data.

The Button: |...| after each file name opens a new dialog window. It will help you to place the export file into your file system.

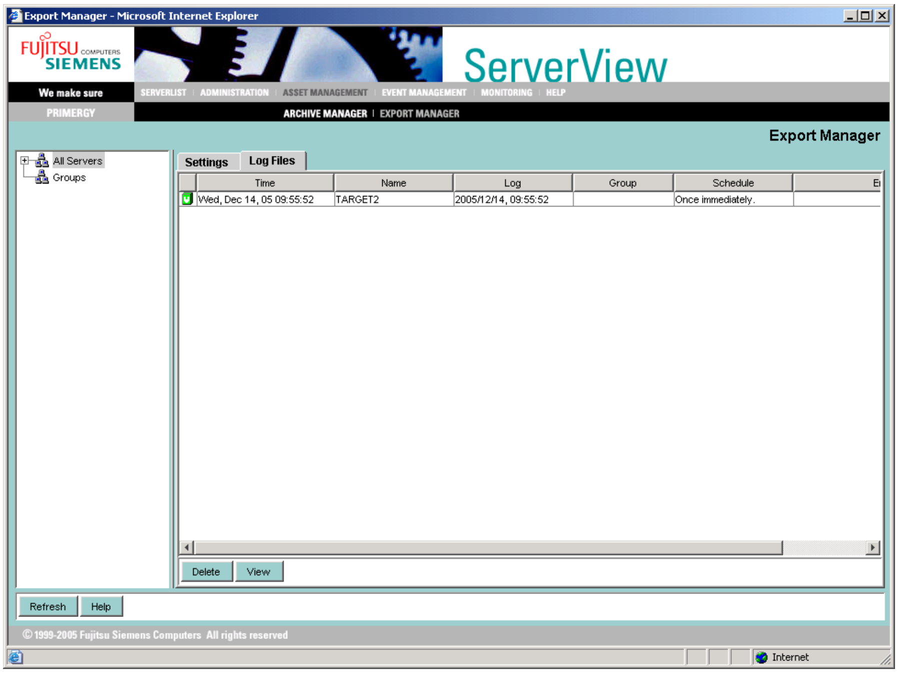
* The CheckBox: "Create file(s) ?"
If this option is checked, the contents of existing files will be deleted, before new

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.



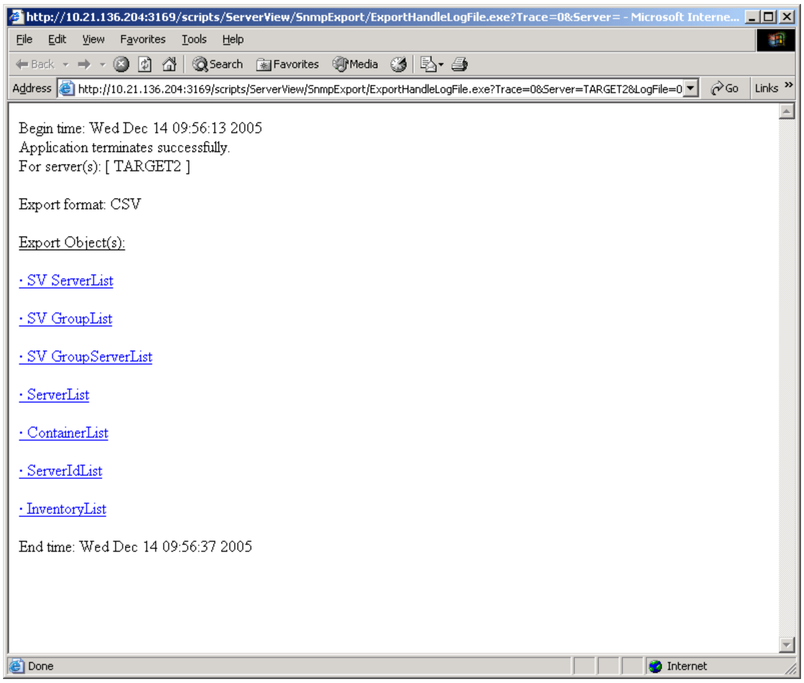
Time	Name	Log	Group	Schedule	E
Wed, Dec 14, 05 09:55:52	TARGET2	2005/12/14, 09:55:52		Once immediately.	

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.


http://10.21.136.204:3169/scripts/ServerView/SnmpExport/ExportHandleLogFile.exe?Trace=0&Server= - Microsoft Interne...
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.21.136.204:3169/scripts/ServerView/SnmpExport/ExportHandleLogFile.exe?Trace=0&Server=TARGET2&LogFile=0
Go Links
Done
Internet

Begin time: Wed Dec 14 09:56:13 2005
Application terminates successfully.
For server(s): [TARGET2]

Export format: CSV

Export Object(s):

· SV ServerList

· SV GroupList

· SV GroupServerList

· ServerList

· ContainerList

· ServerIdList

· InventoryList

End time: Wed Dec 14 09:56:37 2005

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

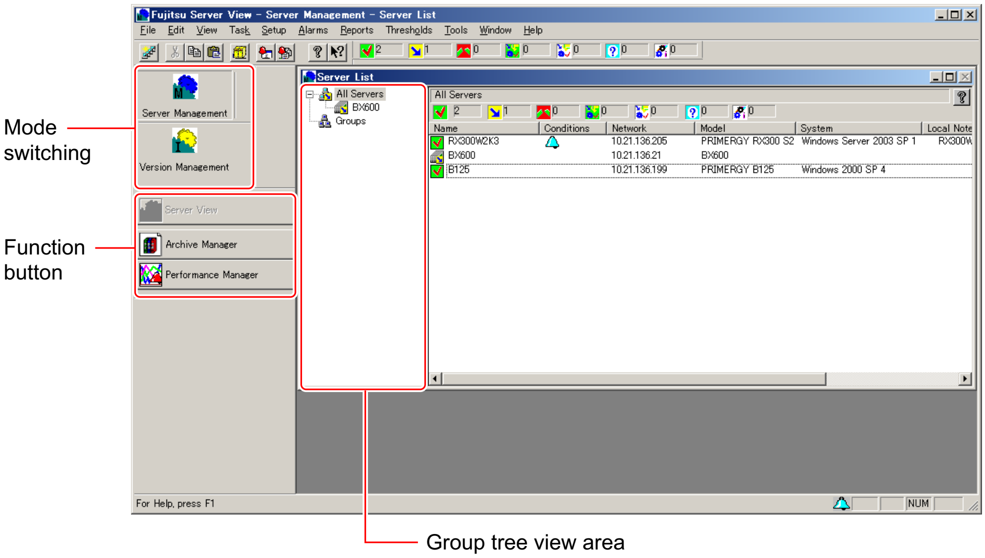
1 Click the [Start] button → [Programs] → [Fujitsu ServerView] → [ServerView(Win32)].

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.



Name	Conditions	Network	Model	System	Local Note
RX300W2K3		10.21.136.205	PRIMERGY RX300 S2	Windows Server 2003 SP 1	RX300W
BX600		10.21.136.21	BX600		
B125		10.21.136.199	PRIMERGY B125	Windows 2000 SP 4	

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.219)
New Group	Creates a new group in the server list. →"■ Creating Groups" (pg.222)
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.124
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.222)
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.231)
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.146)
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.139)
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.149)
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.227)
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.224)
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.198)
Export Manager	Starts the export manager. It is available on the version management mode only. →"3.8 Export Manager" (pg.207)
Performance Manager	Starts the Performance Manager. It is available on the server management mode only. →"3.6 Performance Manager" (pg.178)
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. →"3.9.2 Adding the Monitored Server (Object)" (pg.219)
Open	Starts the "ServerView" for the server management mode or the "Inventory View" (→pg.124) 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 (→pg.207). 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.

table: Pop-up Menu

Menu Item	Description
Server Properties	Starts the server properties. →"3.9.3 Verifying/Changing the Server Information" (pg.223)
ASR Properties	Starts the ASR properties.
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)

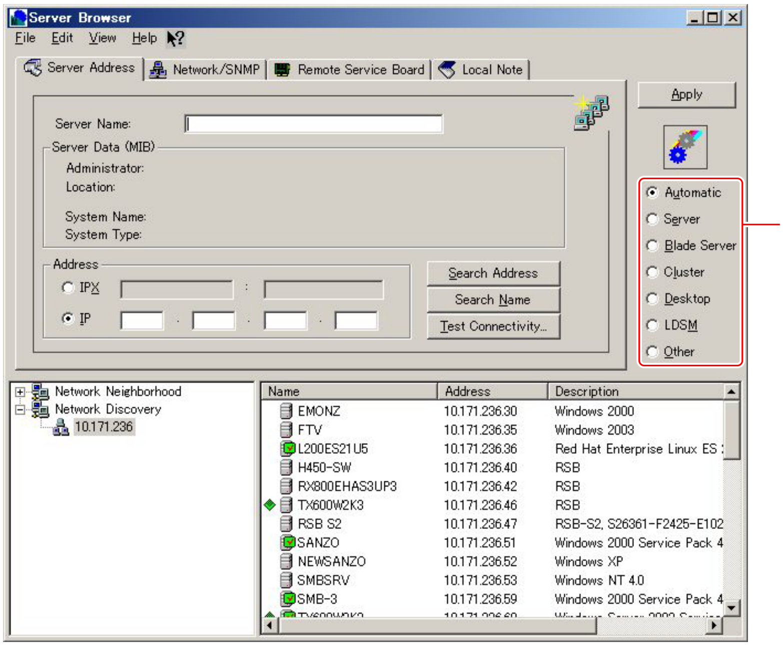
Add the monitored server on your network to the server list.

■ 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.



Address: ● IP

● Automatic

Name	Address	Description
EMONZ	10.171.236.30	Windows 2000
FTV	10.171.236.35	Windows 2003
L200ES21U5	10.171.236.36	Red Hat Enterprise Linux ES :
H450-SW	10.171.236.40	RSB
RX800EHAS3UP3	10.171.236.42	RSB
TX600W2K3	10.171.236.46	RSB
RSB S2	10.171.236.47	RSB-S2, S26361-F2425-E102
SANZO	10.171.236.51	Windows 2000 Service Pack 4
NEWSANZO	10.171.236.52	Windows XP
SMBSRV	10.171.236.53	Windows NT 4.0
SMB-3	10.171.236.59	Windows 2000 Service Pack 4

Server type

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].

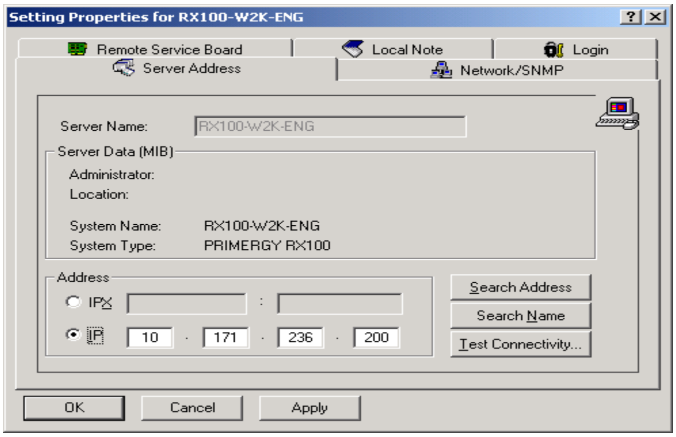
2 Select whether it is displayed or hidden and click [OK].

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.



Setting Properties for RX100-W2K-ENG

Server Name: RX100-W2K-ENG

Server Data (MIB)

Administrator:

Location:

System Name: RX100-W2K-ENG

System Type: PRIMERGY RX100

Address

○ IPX :

● IP 10 . 171 . 236 . 200

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 "6.3.1 Starting the Web Interface" (→pg.303)

[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.425).
- Specifying relative values enables you to detect the variation beyond the relative values from the current value.

IMPORTANT

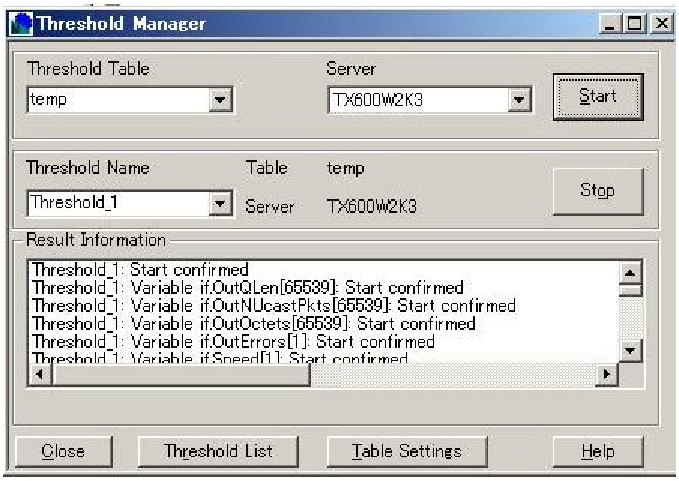
- Even if a threshold value is assigned with the threshold manager, ASR is not available. ASR is available only for the basic threshold assigned to servers (hardware). Additionally the threshold manager cannot change the basic threshold.

■ Specifying Thresholds

1 Select the server to specify a threshold.

2 Click the [Threshold] menu → [Threshold Manager].

The [Threshold Manager] window is displayed.



Threshold Manager

Threshold Table: temp

Server: TX600W2K3

Threshold Name: Threshold_1

Table: temp

Server: TX600W2K3

Result Information

```
Threshold_1: Start confirmed
Threshold_1: Variable if.OutQLen[65539]: Start confirmed
Threshold_1: Variable if.OutNUcastPkts[65539]: Start confirmed
Threshold_1: Variable if.OutOctets[65539]: Start confirmed
Threshold_1: Variable if.OutErrors[1]: Start confirmed
Threshold_1: Variable if.Speed[1]: Start confirmed
```

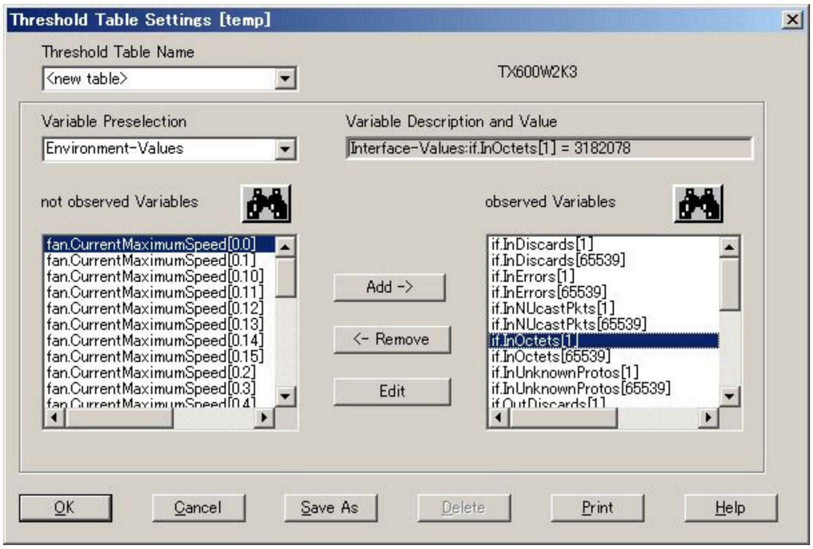
3 Select [Threshold Table] to specify for the server.

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.



Threshold Table Settings [temp]

Threshold Table Name: <new table>

TX600W2K3

Variable Preselection: Environment-Values

Variable Description and Value: Interface-Values:if.InOctets[1] = 3182078

not observed Variables

```
fan.CurrentMaximumSpeed[0.0]
fan.CurrentMaximumSpeed[0.1]
fan.CurrentMaximumSpeed[0.10]
fan.CurrentMaximumSpeed[0.11]
fan.CurrentMaximumSpeed[0.12]
fan.CurrentMaximumSpeed[0.13]
fan.CurrentMaximumSpeed[0.14]
fan.CurrentMaximumSpeed[0.15]
fan.CurrentMaximumSpeed[0.2]
fan.CurrentMaximumSpeed[0.3]
fan.CurrentMaximumSpeed[0.4]
```

observed Variables

```
if.InDiscards[1]
if.InDiscards[65539]
if.InErrors[1]
if.InErrors[65539]
if.InNUcastPkts[1]
if.InNUcastPkts[65539]
if.InOctets[1]
if.InOctets[65539]
if.InUnknownProtos[1]
if.InUnknownProtos[65539]
if.OutDiscards[1]
```

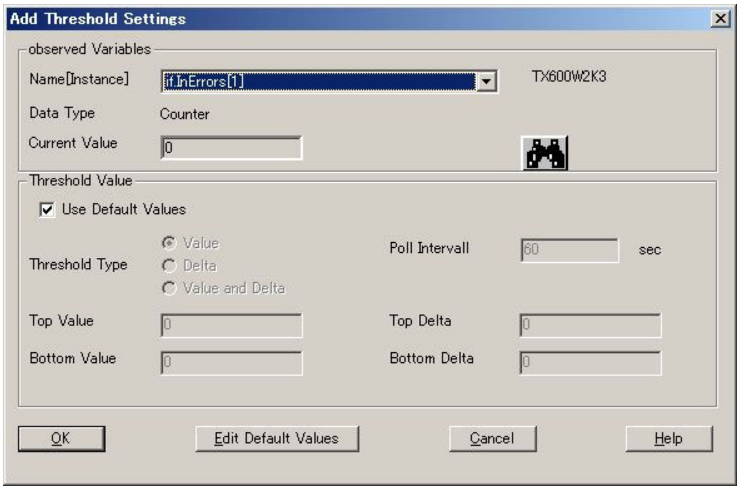
2. Select a category from [Variable Preselection].

   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.



Add Threshold Settings

observed Variables

Name[Instance] ifInErrors[1] TX600W2K3

Data Type Counter

Current Value 0

Threshold Value

☑ Use Default Values

Threshold Type ● Value ○ Delta ○ Value and Delta

Poll Intervall 60 sec

Top Value 0

Top Delta 0

Bottom Value 0

Bottom Delta 0

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 exceededADELTA-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].

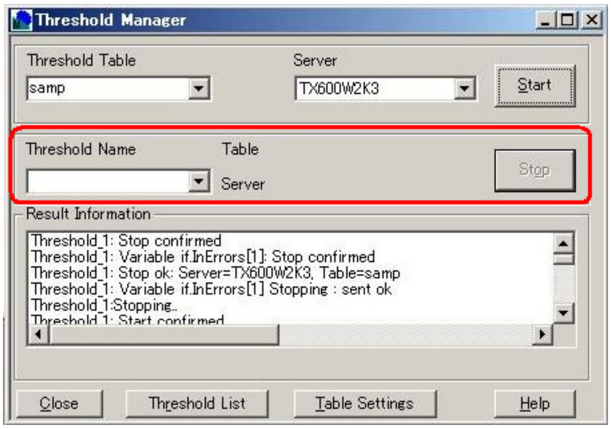
■ Stopping Threshold Monitoring

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_1: Stop confirmed
Threshold_1: Variable if.InErrors[1]: Stop confirmed
Threshold_1: Stop ok: Server=TX600W2K3, Table=samp
Threshold_1: Variable if.InErrors[1] Stopping : sent ok
Threshold_1:Stopping..
Threshold_1: Start confirmed
```

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

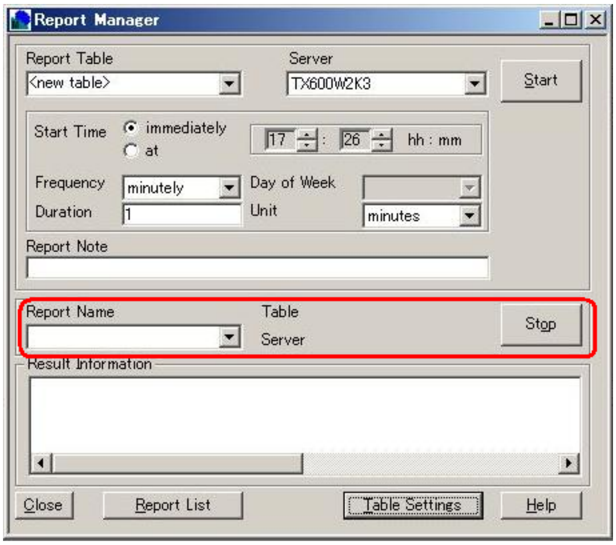
- The report manager settings do not directly relate to each monitoring items that ServerView monitors. Even if the report settings is not assigned, each of monitoring and notification is performed.
- To prevent one variable from being selected in two different tables, a single server can open only one 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.



Report Table: <new table>
Server: TX600W2K3
Start Time: ● immediately ○ at 17 : 26 hh : mm
Frequency: minutely
Day of Week:
Duration: 1
Unit: minutes
Report Note:
Report Name:
Table
Server
Result Information

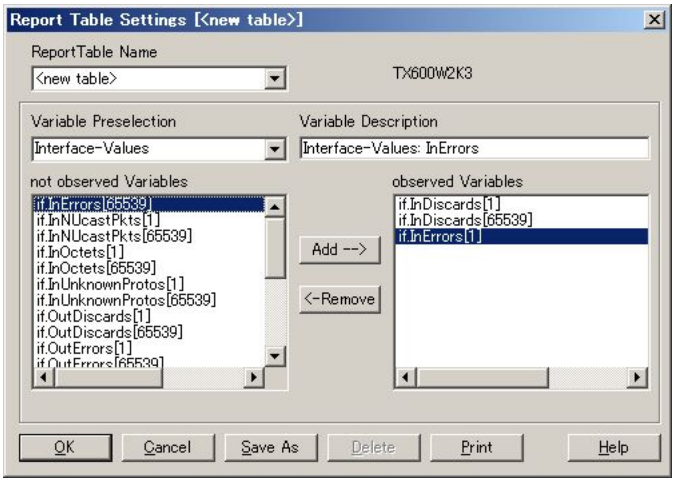
3 Select [Report Table] to specify for the server.

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.



Report Table Settings [<new table>]

ReportTable Name: <new table>

TX600W2K3

Variable Preselection: Interface-Values

Variable Description: Interface-Values: InErrors

not observed Variables:

```
if.InErrors[65539]
if.InNUcastPkts[1]
if.InNUcastPkts[65539]
if.InOctets[1]
if.InOctets[65539]
if.InUnknownProtos[1]
if.InUnknownProtos[65539]
if.OutDiscards[1]
if.OutDiscards[65539]
if.OutErrors[1]
if.OutErrors[65539]
```

observed Variables:

```
if.InDiscards[1]
if.InDiscards[65539]
if.InErrors[1]
```

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

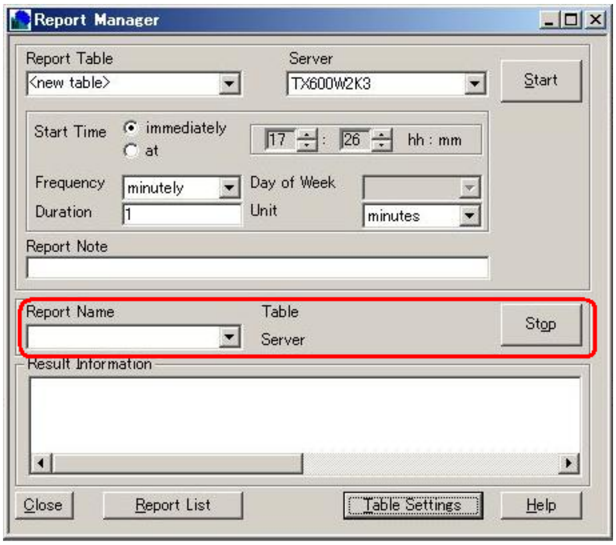
Stop reporting before a period limit expires.

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].



Report Manager

Report Table: <new table>

Server: TX600W2K3

Start Time: ● immediately ○ at 17 : 26 hh : mm

Frequency: minutely

Day of Week:

Duration: 1

Unit: minutes

Report Note:

Report Name:

Table

Server

Result Information

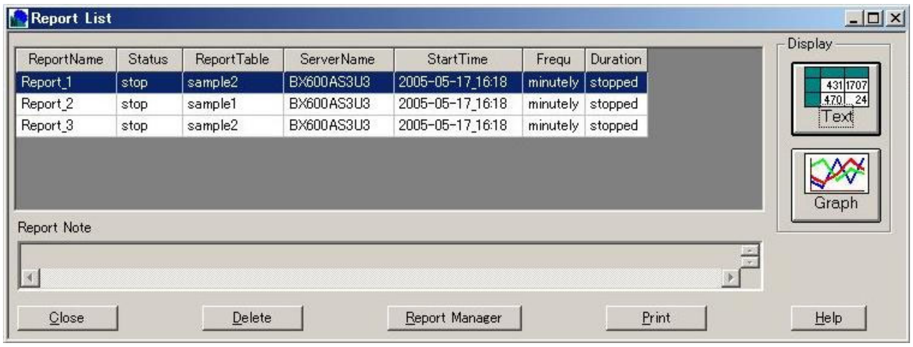
4 Click [Close].

The report manager exits.

■ Reviewing Reports

1 Click the [Reports] menu → [List].

The [Report List] window is displayed.



Report List

ReportName	Status	ReportTable	ServerName	StartTime	Frequ	Duration
Report_1	stop	sample2	BX600AS3U3	2005-05-17 16:18	minutely	stopped
Report_2	stop	sample1	BX600AS3U3	2005-05-17 16:18	minutely	stopped
Report_3	stop	sample2	BX600AS3U3	2005-05-17 16:18	minutely	stopped

Report Note

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

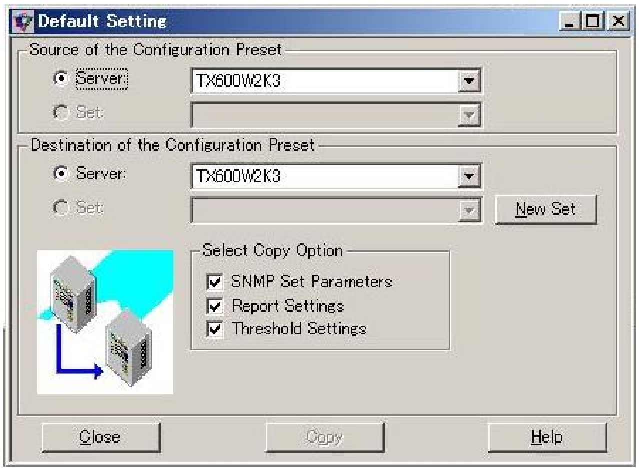
- Reports are created in the ASCII format. The created text file that is named "repnnn.txt" is saved in the "\ServerView_installdir\Reports\server_name" folder.
- This report can be exported to Excel in the following procedure:
  1. Import the report in Excel using the Excel text wizard.
     Note that 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.



Default Setting

Source of the Configuration Preset

● Server: TX600W2K3

○ Set:

Destination of the Configuration Preset

● Server: TX600W2K3

○ Set:

Select Copy Option

☑ SNMP Set Parameters

☑ Report Settings

☑ Threshold Settings

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

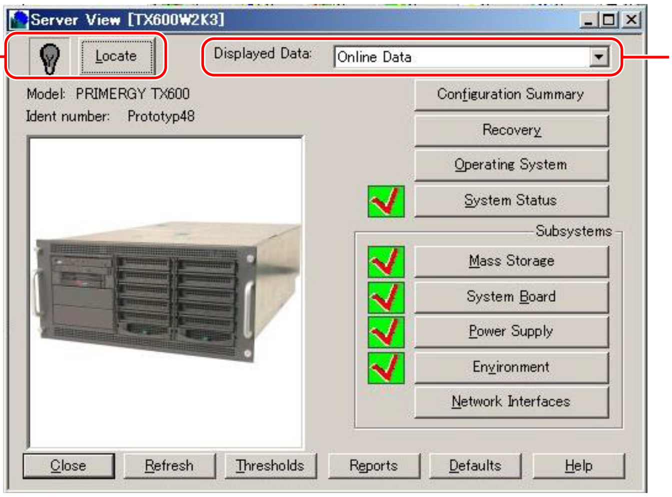
1 Select the server to monitor.

POINT

- For blade servers, refer to "3.9.8 Verifying the Status of the Blade Servers" (→pg.248).

2 Click [ServerView].

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



Server View [TX600W2K3]

Displayed Data: Online Data

Model: PRIMERGY TX600

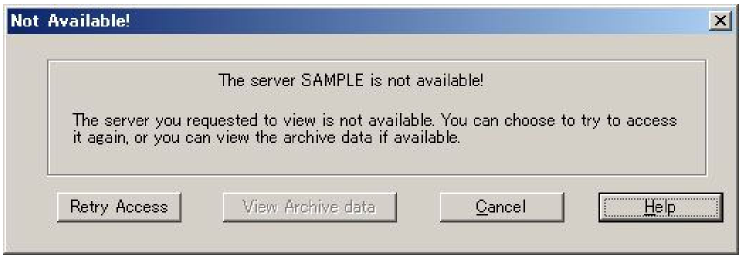
Ident number: Prototyp48

Locate

Displayed Data

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 is installed.
  - Recovery
  - System Board
  - Power Supply
  - Environment
- When the RSB mode is active and the remote service board is installed, the following dialog appears if you select the server to monitor and click [ServerView]. For the Web interface, refer to "6.3.1 Starting the Web Interface" (→pg.303).



Not Available!

The server SAMPLE is not available!

The server you requested to view is not available. You can choose to try to access it again, or you can view the archive data if available.

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.

💡 :LED ON 💡 : LED OFF

💡 :Flashing LED (Indicates a system error)

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: • 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.235).
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.237).
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.244).
Power Supply	Displays the power supply settings and status for servers. For more details, refer to "■ Verifying the Power Supply Status" (→pg.245).
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.247).
Network Interfaces	Data on networks can be obtained. First, click the list entry required to obtain information continuously. • 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.224).

table: Status Verification of Servers

Items	Description
Reports	The report manager starts. For more details, refer to "3.9.5 Report Manager" (→pg.227).
Defaults	The default settings start. For more details, refer to "3.9.6 Copying Settings to the Other Servers" (→pg.231).
Help	Help topics for each item appears.

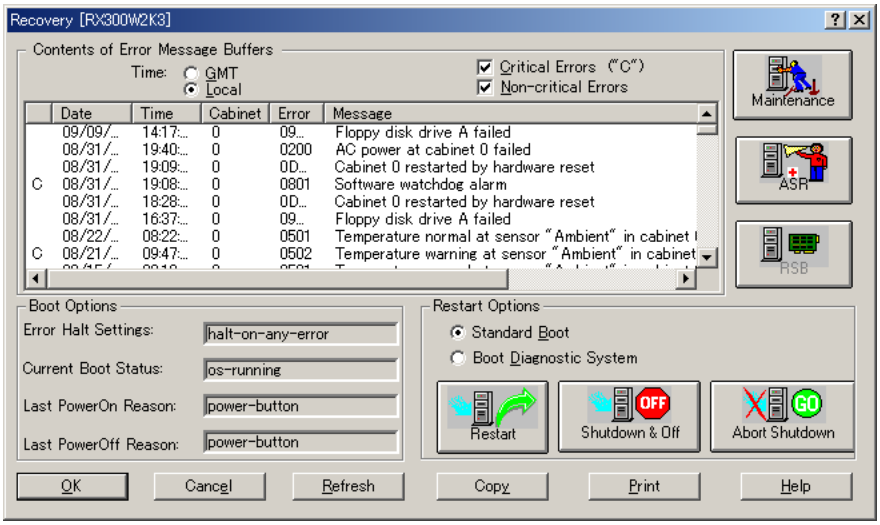
4 After completing verification for each item, click [Close].

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.



Recovery [RX300W2K3]

Contents of Error Message Buffers

Time: ○ GMT ● Local

☑ Critical Errors ("C")
☑ Non-critical Errors

	Date	Time	Cabinet	Error	Message
	09/09/...	14:17:...	0	09...	Floppy disk drive A failed
	08/31/...	19:40:...	0	0200	AC power at cabinet 0 failed
	08/31/...	19:09:...	0	0D...	Cabinet 0 restarted by hardware reset
C	08/31/...	19:08:...	0	0801	Software watchdog alarm
	08/31/...	18:28:...	0	0D...	Cabinet 0 restarted by hardware reset
	08/31/...	16:37:...	0	09...	Floppy disk drive A failed
	08/22/...	08:22:...	0	0501	Temperature normal at sensor "Ambient" in cabinet
C	08/21/...	09:47:...	0	0502	Temperature warning at sensor "Ambient" in cabinet

Boot Options

Error Halt Settings: halt-on-any-error

Current Boot Status: os-running

Last PowerOn Reason: power-button

Last PowerOff Reason: power-button

Restart Options

● Standard Boot
○ Boot Diagnostic System

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.130).

● 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 Options

Shutdown/restart operation of the server can be performed by specifying the option and clicking the operation button. When each button is clicked, the login window appears for security. The user name and the password of the ServerView administrative privileges are required.

- Restart
  Restarts the server. Specify the passed time required for the server to be restarted.
- Shutdows & 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.
- Abort Shutdown
  This button aborts any shutdown that is started by clicking [Restart] or [Shutdown & Off]. 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.223).
- [Boot Diagnostic System] is not supported.

■ Verifying Mass Storage Status

If you click [Mass Storage], the detailed information appears about hard disks and controllers.

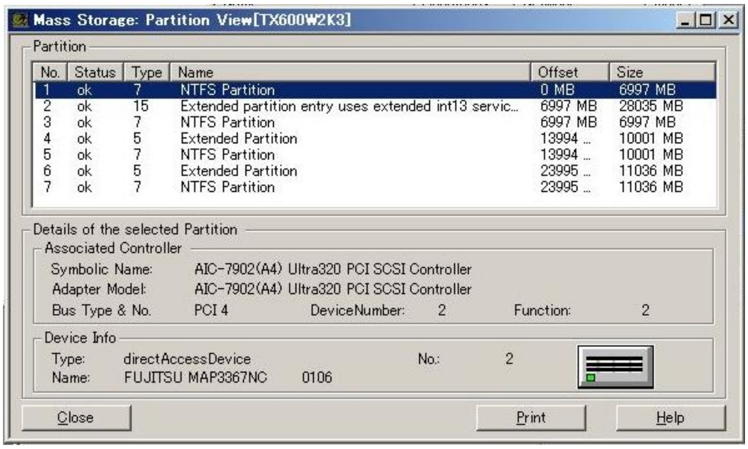
- Controller list
  The critical data, number, status (OK or FAIL), type (EISA, PCI, ISA), slot, and driver name is displayed for controllers.
- Details for Selected Controller
  Data on HD and EISA MIB is displayed.

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.



Mass Storage: Partition View[TX600W2K3]

Partition

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

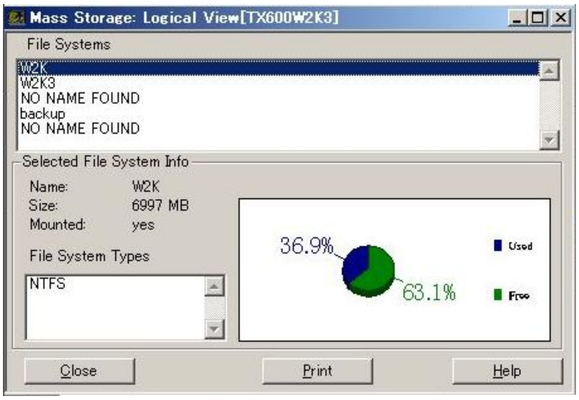
Name: FUJITSU MAP3367NC 0106

[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.



Mass Storage: Logical View[TX600W2K3]

File Systems

W2K
W2K3
NO NAME FOUND
backup
NO NAME FOUND

Selected File System Info

Name: W2K

Size: 6997 MB

Mounted: yes

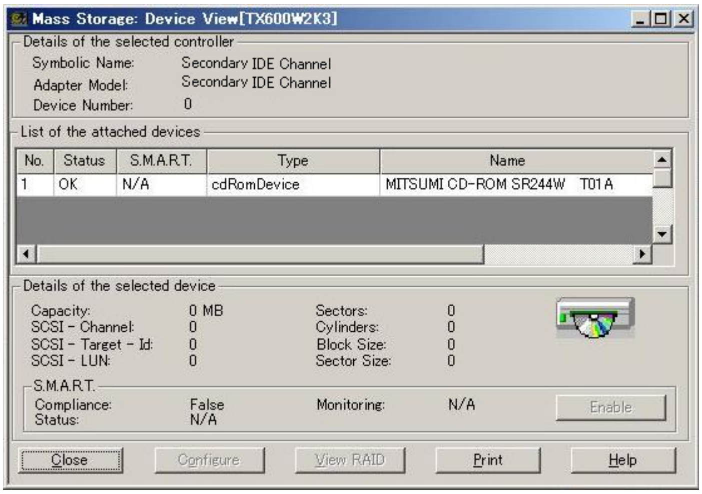
File System Types

NTFS

- 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.



Mass Storage: Device View[TX600W2K3]

Details of the selected controller

Symbolic Name:	Secondary IDE Channel
Adapter Model:	Secondary IDE Channel
Device Number:	0

List of the attached devices

No.	Status	S.M.A.R.T.	Type	Name
1	OK	N/A	cdRomDevice	MITSUMI CD-ROM SR244W T01A

Details of the selected device

Capacity:	0 MB	Sectors:	0
SCSI - Channel:	0	Cylinders:	0
SCSI - Target - Id:	0	Block Size:	0
SCSI - LUN:	0	Sector Size:	0

S.M.A.R.T.

Compliance:	False	Monitoring:	N/A
Status:	N/A		

- 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.

IMPORTANT

- 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.

● 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 SCSIAWide 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].

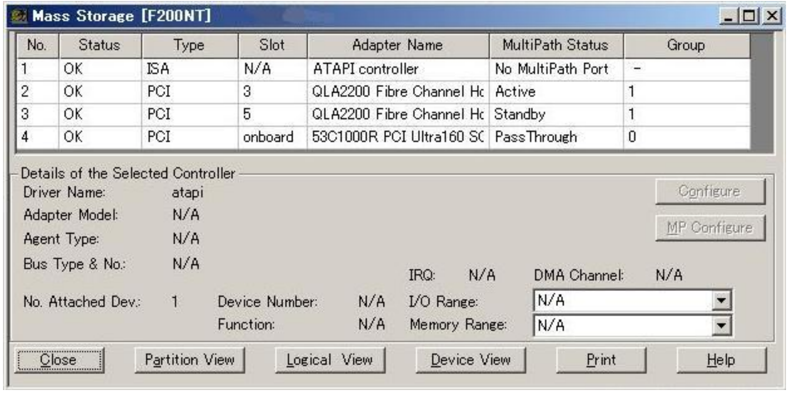
● Details of the Bridge Controller

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].



Mass Storage [F200NT]

No.	Status	Type	Slot	Adapter Name	MultiPath Status	Group
1	OK	ISA	N/A	ATAPI controller	No MultiPath Port	-
2	OK	PCI	3	QLA2200 Fibre Channel Hc	Active	1
3	OK	PCI	5	QLA2200 Fibre Channel Hc	Standby	1
4	OK	PCI	onboard	53C1000R PCI Ultra160 SC	PassThrough	0

Details of the Selected Controller
Driver Name: atapi
Adapter Model: N/A
Agent Type: N/A
Bus Type & No.: N/A
IRQ: N/A
DMA Channel: N/A
No. Attached Dev.: 1
Device Number: N/A
I/O Range: N/A
Function: N/A
Memory Range: N/A

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

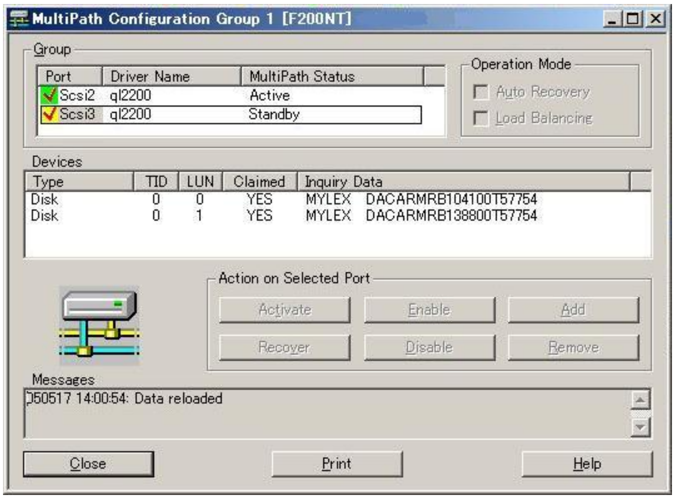
Value	Meaning
Path Through	The second port is not available.
Active	The channel is running. This is user-selected.
Standby (inactive)	Suspending. This is user-selected. When load balancing capability is enabled, this status is not displayed.
Disable	Suspending through maintenance activity.
Error	Any 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.



MultiPath Configuration Group 1 [F200NT]

Group

Port	Driver Name	MultiPath Status
✓ Scsi2	ql2200	Active
✓ Scsi3	ql2200	Standby

Operation Mode

□ Auto Recovery

□ Load Balancing

Devices

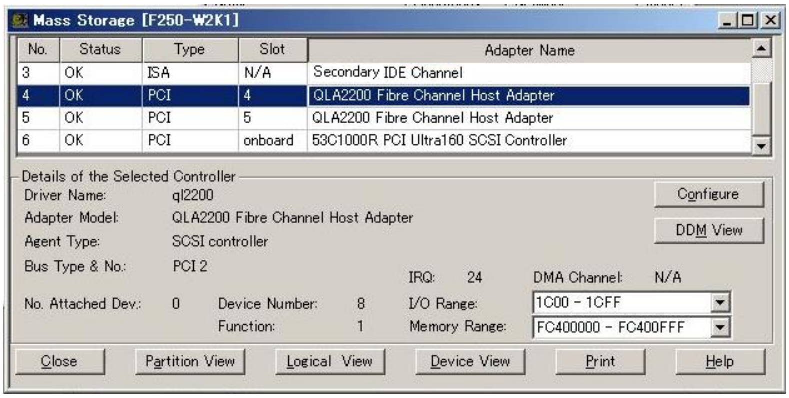
Type	TID	LUN	Claimed	Inquiry Data
Disk	0	0	YES	MYLEX DACARMRB104100T57754
Disk	0	1	YES	MYLEX DACARMRB138800T57754

Messages

```
050517 14:00:54: Data reloaded
```

■ External Storage Devices - DuplexWrite

When DuplexWrite is installed, the information about DuplexWrite is displayed by clicking [Device View].



Mass Storage [F250-W2K1]

No.	Status	Type	Slot	Adapter Name
3	OK	ISA	N/A	Secondary IDE Channel
4	OK	PCI	4	QLA2200 Fibre Channel Host Adapter
5	OK	PCI	5	QLA2200 Fibre Channel Host Adapter
6	OK	PCI	onboard	53C1000R PCI Ultra160 SCSI Controller

Details of the Selected Controller

Driver Name: ql2200

Adapter Model: QLA2200 Fibre Channel Host Adapter

Agent Type: SCSI controller

Bus Type & No.: PCI 2

IRQ: 24 DMA Channel: N/A

No. Attached Dev.: 0 Device Number: 8 I/O Range: 1C00 - 1CFF

Function: 1 Memory Range: FC400000 - FC400FFF

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.

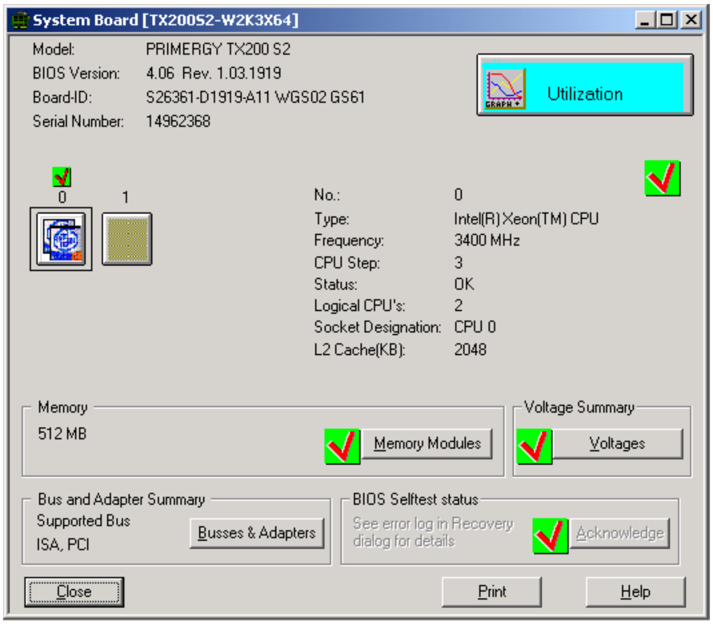
[DW Configure] can be selected when the DuplexWrite agent is installed in the selected server and the DuplexWrite status other than N/A, MultiPath, or <cluster node name> is displayed in the selected entry. For details on each item, refer to help topics.

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.



System Board [TX200S2-W2K3X64]

Model: PRIMERGY TX200 S2
BIOS Version: 4.06 Rev. 1.03.1919
Board-ID: S26361-D1919-A11 WGS02 GS61
Serial Number: 14962368

No.: 0
Type: Intel(R) Xeon(TM) CPU
Frequency: 3400 MHz
CPU Step: 3
Status: OK
Logical CPU's: 2
Socket Designation: CPU 0
L2 Cache(KB): 2048

Memory
512 MB

Bus and Adapter Summary
Supported Bus
ISA, PCI

BIOS Selftest status
See error log in Recovery dialog for details

● 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

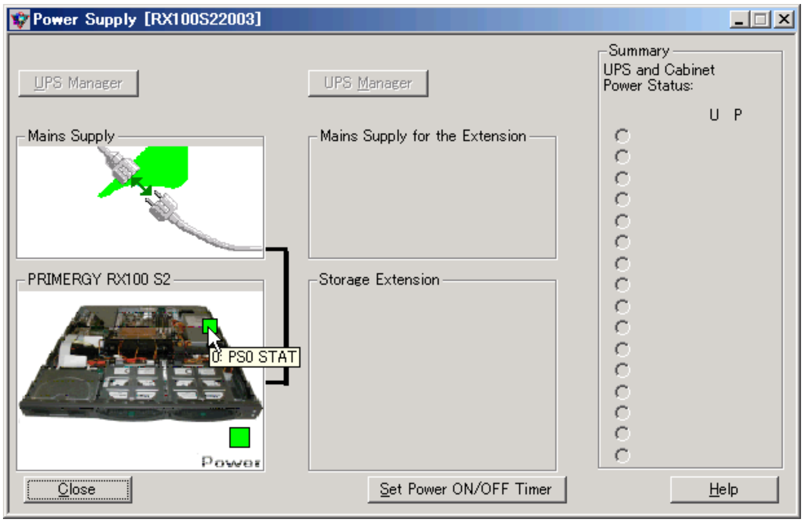
- If you reinstall ServerView Agent in the state where you have restored the "normal" icon by clicking [Acknowledge], the "abnormal" icon may appear again (a trap may occur at the same time). Click [Acknowledge] again to restore the "normal" icon.

■ 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.136).

● UPS Manager

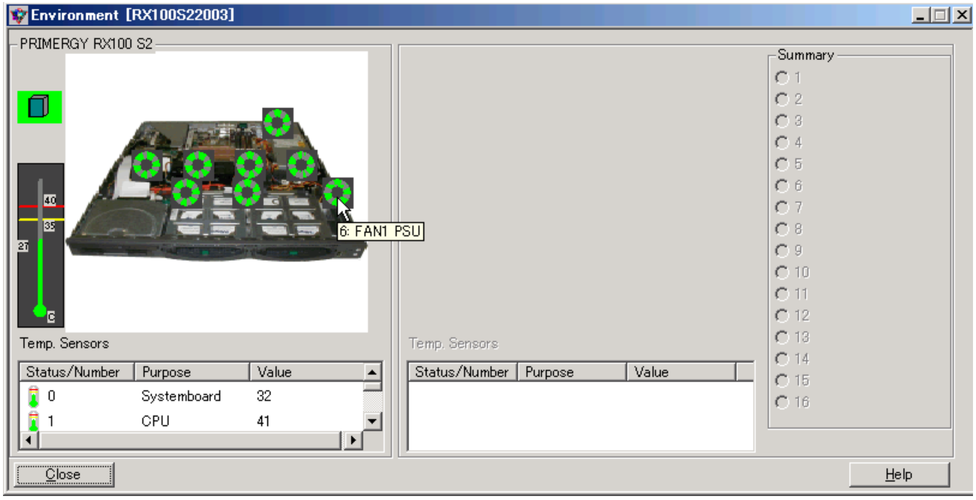
Unsupported.
When the UPS management software is installed and the settings for interaction with the UPS management software are assigned, the [UPS Manager] button is enabled.

■ 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.



Temp. Sensors

Status/Number	Purpose	Value
0	Systemboard	32
1	CPU	41

Temp. Sensors

Status/Number	Purpose	Value

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

Item	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.

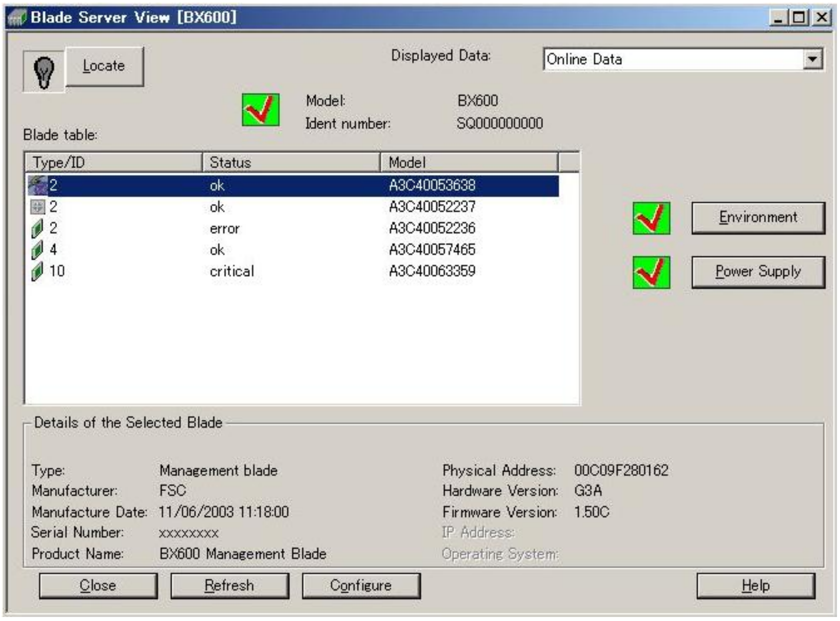
3.9.8 Verifying the Status of the Blade Servers

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.



Displayed Data: Online Data

Model: BX600

Ident number: SQ000000000

Blade table:

Type/ID	Status	Model
2	ok	A3C40053638
2	ok	A3C40052237
2	error	A3C40052236
4	ok	A3C40057465
10	critical	A3C40063359

Details of the Selected Blade

Type: Management blade

Manufacturer: FSC

Manufacture Date: 11/06/2003 11:18:00

Serial Number: xxxxxxxx

Product Name: BX600 Management Blade

Physical Address: 00C09F280162

Hardware Version: G3A

Firmware Version: 1.50C

IP Address:

Operating System:

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.

IMPORTANT

- 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	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. : Management blade (master) : Management blade (slave) : Switch blade : fiber channel path through blade : LAN path through blade : KVM blade : fiber channel swich blade : Server blade
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	When the management blade or the switch blade is selected, the configuration window (Web browser) of each blade appears by clicking [Configure]. For each blade settings windows, refer to the respective manual for the management blade or the switch blade. However when the server blade is selected, this button is disabled.
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 save and restore the settings of ServerView Agent.

3.10.1 Save/Restore Settings (Configuration Tools)

Configuration Tools enables you to save and restore the settings of ServerView Agent.
Servers equipped with a Remote Service Board, including a Remote Service Controller, and servers equipped with a Remote Management Controller can back up and restore these settings.

POINT

- An error may occur during backup or restoration in environments with a different version of ServerView Agent or a different type or version of the Remote Service Board, Remote Management Controller, and BMC. Restore the settings with the same version as the one used for backup.
- Configuration Tools can only be used under Windows.

IMPORTANT

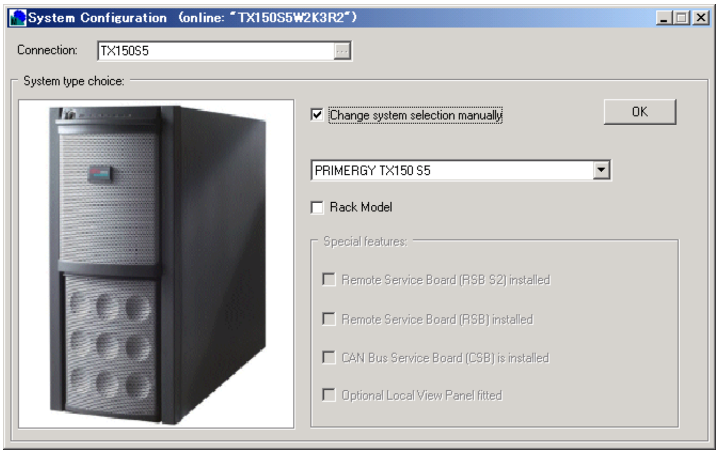
- When performing restoration on a server while another management console configures the settings of that server, the configuration may become inconsistent which may lead to server errors. Confirm that no other management consoles are modifying the settings before starting the restoration.
- Even though the Configuration Tools can modify various settings, when a management console or another web interface tool is running on another PC, this may lead to inconsistencies and server errors. Do not use the Configuration Tools to change the settings. However, the initial IP settings for PG-RSB102 through 105 and the UPS settings can be modified.

■ Configuring the Remote Service Board IP and the UPS Device

When ServerView Agents are installed in the Windows server, the remote service board and UPS 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.



System Configuration (online: "TX150S5W2K3R2")

Connection: TX150S5

System type choice:

☑ Change system selection manually

PRIMERGY TX150 S5

□ Rack Model

Special features:

□ Remote Service Board (RSB S2) installed

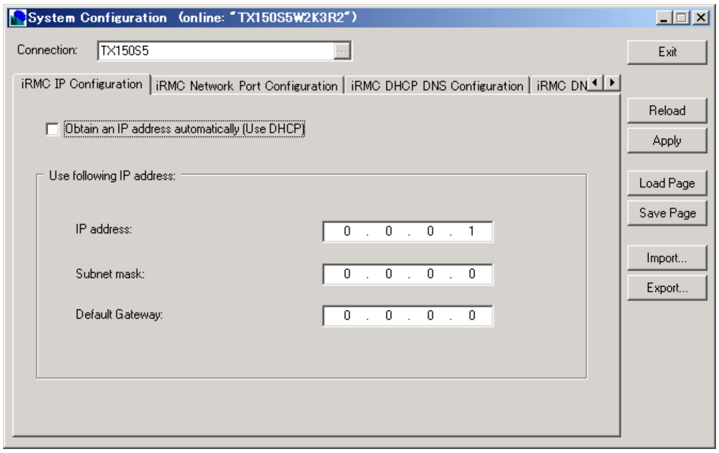
□ Remote Service Board (RSB) installed

□ CAN Bus Service Board (CSB) is installed

□ Optional Local View Panel fitted

2 Select the [Change system selection manually] checkbox and click [OK].

A window appears for specifying items.



System Configuration (online: "TX150S5W2K3R2")

Connection: TX150S5

iRMC IP Configuration | iRMC Network Port Configuration | iRMC DHCP DNS Configuration | iRMC DN

□ Obtain an IP address automatically (Use DHCP)

Use following IP address:

IP address: 0 . 0 . 0 . 1

Subnet mask: 0 . 0 . 0 . 0

Default Gateway: 0 . 0 . 0 . 0

3 Click each Tab and set items if necessary.

The displayable and configurable tabs vary depending on the server components.

If Not Equipped with a Remote Management Controller/Remote Service Board/ Controller

For details about each setting, see "■ [Power On Off] Tab (ServerView S2) / [Power ON/OFF] Tab (Management Console)" (→pg.136) and "■ [Watchdog] Tab (ServerView S2) / [Watchdog Settings] Tab (Management Console)" (→pg.136).

table: System Configuration Settings Window

Tab Window	Contents
Boot Watchdog	The settings are associated with Boot Watchdog.
BMC IP Configuration	The unique IP configuration for the server’ s main firmware.
Software Watchdog	The settings are associated with Software Watchdog.
System Power On/Off Settings	The settings are associated with the power schedule.
Global Settings	The time when to perform a fan test.
UPS Configuration	The settings are associated with UPS.

If Equipped with a Remote Management Controller (iRMC)

For details about settings for the Remote Management Controller, see "7.4 Setting and Referencing User Information" (→pg.352).

table: System Configuration Settings Window

Tab Window	Contents
iRMC IP Configuration	The IP configuration for the Remote Management Controller.
iRMC Network Port Configuration	The port configuration for the Remote Management Controller.
iRMC DHCP DNS Configuration	The DHCP/DNS configuration for the Remote Management Controller.
iRMC DNS Server Configuration	The DHCP server configuration for the Remote Management Controller.
iRMC SMTP Configuration	The SMTP server configuration for the Remote Management Controller.
iRMC eMail Format Configuration	The email format configuration for the Remote Management Controller
iRMC SNMP Configuration	The SNMP configuration for the Remote Management Controller.
iRMC User Configuration [Note1]	The user configuration for the Remote Management Controller.
iRMC Remote Image Server Configuration	The remote storage configuration for the Remote Management Controller.
Boot Watchdog	The settings are associated with Boot Watchdog.
Software Watchdog	The settings are associated with Software Watchdog.
System Power On/Off Settings	The settings are associated with the power schedule.
Global Settings	The time when to perform a fan test.
UPS Configuration	The settings are associated with UPS.

Note 1: Settings in the iRMC User Configuration tab cannot be backed up or restored.

If Equipped with a Remote Service Board (PG-RSB102 through 105)

For details about settings for the Remote Service Board, see "6.3 Displaying Each Monitoring Information" (→pg.303).

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.
UPS Configuration	The settings are associated with UPS.
RSB S2 IP Configuration	The IP configuration for the Remote Service Board.
RSB S2 Network Services [Note1]	Various network settings for the Remote Service Board.
RSB S2 User administration [Note1]	The user configuration for the Remote Service Board.
RSB S2 SNMP Configuration [Note1]	The SNMP configuration for the Remote Service Board.

Note 1: In certain environments with PG-RSB102 or PG-RSB103(L) connected, these items are unsupported and an error may occur. The remaining items are already set, so click [Exit] and exit the Configuration Tool.

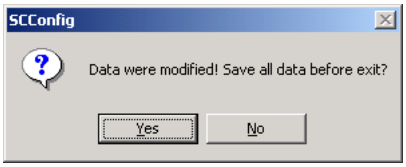
POINT

- If you click [Reload] before saving the settings, the values revert to the previous values.
- If the server is equipped with a front LCD panel, the [LocalView Panel Configuration] tab may be displayed. However, this configuration is not supported.

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.



SCConfig

Data were modified! Save all data before exit?

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).

● For Red Hat Linux

```
# /etc/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/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...
```

● For SUSE Linux

```
# /etc/init.d/srvmagt status
/usr/sbin/scagt:                                            running
/usr/sbin/sc2agt:                                           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/init.d/eecd status
Checking for service eecd: OK
```

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).

For Red Hat Linux

```
# /etc/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/init.d/eecd stop
Shutting down eecd: TERM      [ OK ]
```

For SUSE Linux

```
# /etc/init.d/srvmagt stop
Stopping agents: sc sc2 bus hd unix ether bios secur status inv vv   done
# /etc/init.d/eecd stop
Shutting down eecd: TERM                                             done
```

IMPORTANT

- To start the ServerView Linux agent, login as super user and execute the following command.
  # /etc/init.d/eecd start
  # /etc/init.d/srvmagt start
- When you cannot start /etc/init.d/srvmagt, execute the following command to verify status of the SNMP service. If the SNMP service stops, start it.
  # /etc/init.d/snmpd status
  # /etc/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.84). For the operation procedures of AlarmService, refer to "3.5 AlarmService" (→pg.138).

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, or apache 2 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:
  - For Red Hat Linux
    # /etc/init.d/sv_fwdserver status
    snmptrapd (pid xxxx) is running...
  - For SUSE Linux
    # /etc/init.d/sv_fwdserver status
    Checking for SVFwserver: running

■ System Logs Stored by ServerView Linux Agent

While ServerView Linux Agent is running, log files (log.xxxx) that records the operation status (internal trace) are stored under /var/log.
These log files are cleared when restarting ServerView Linux Agent.

IMPORTANT

- These log files are for maintenance purposes. Do not use the log files for monitoring purposes and do not refer to them. Refer to the server monitoring entries recorded in the system log (/var/log/messages).

A log example is shown below.

```
-rw-r--r--   1 root  root     0 Aug 18 22:35 /var/log/log.SVRemoteConnector
-rw-rw-rw-   1 root  root     83 Aug 18 22:36 /var/log/log.StatusChAction
-rw-r--r--   1 root  root     1213 Aug 18 22:35 /var/log/log.biosagt
-rw-r--r--   1 root  root     767 Aug 18 22:35 /var/log/log.busagt
-rw-r--r--   1 root  root     1788 Aug 18 22:35 /var/log/log.eecd
-rw-r--r--   1 root  root     1833 Aug 18 22:36 /var/log/log.eecd_mods_src
-rw-r--r--   1 root  root     769 Aug 18 22:35 /var/log/log.etheragt
-rw-r--r--   1 root  root     765 Aug 18 22:35 /var/log/log.hdagt
-rw-r--r--   1 root  root     767 Aug 18 22:35 /var/log/log.invagt
-rw-r--r--   1 root  root     63 Aug 18 22:36 /var/log/log.package
-rw-r--r--   1 root  root     1918 Aug 18 22:36 /var/log/log.sc2agt
-rw-r--r--   1 root  root     1499 Aug 18 22:36 /var/log/log.scagt
-rw-r--r--   1 root  root     768 Aug 18 22:35 /var/log/log.securagt
-rw-r--r--   1 root  root     1730 Aug 18 22:36 /var/log/log.statusagt
-rw-r--r--   1 root  root     1808 Aug 18 22:36 /var/log/log.thragt
-rw-r--r--   1 root  root     767 Aug 18 22:35 /var/log/log.unixagt
-rw-r--r--   1 root  root     2320 Aug 19 00:37 /var/log/log.vvagt
```

Chapter 4

RAID Manager Linking

This chapter explains how to link RAID Manager with ServerView S2 or the Management Console.

4.1 Overview of the RAID Manager Linking

To perform the RAID Manager linking, the management software for an array controller must be installed on the server to be monitored. This management software is hereinafter called RAID Manager.
For information on how to install and use RAID Manager, see “User’s Guide” supplied with the array controller or the server.

■ Available RAID Manager

The following RAID Manager can link with ServerView S2 or the Management Console.

- ServerView RAID
- GAM (Global Array Manager)
- Storage Manager
- PROMISE Fasttrak
- PAM (PROMISE ARRAY MANAGEMENT)

■ Functions of the RAID Manager Linking

Functions of the RAID Manager linking are as follows.

● Starting up ServerView RAID Manager (Web Client)

ServerView RAID Manager (Web client) can be started up from ServerView S2 or the Management Console.
For information on how to start up ServerView RAID Manager, see "4.2 Starting up ServerView RAID Manager (Web Client)" (→pg.262).

● Starting up RAID Manager (Client Software other than ServerView RAID Manager)

RAID Manager (client software other than ServerView RAID Manager) can be started up from the Management Console. Note that RAID Manager other than ServerView RAID Manager cannot be started up from ServerView S2.
Also, to start up RAID Manager using the linking function, RAID Manager (client software) must be installed on the management terminal where the Management Console is installed.
For information on how to start up RAID Manager, see "■ Verifying Mass Storage Status" (→pg.237).

● Showing Detailed Information

The detailed information provided by RAID Manager can be displayed on the detailed information window of ServerView S2 and the Management Console. For viewing the detailed information, see the following sections.

- For ServerView S2
  →"● MYLEX Devise View (View RAID)" (pg.113)
- For the Management Console
  →"■ Mass Storage - the RAID controller" (pg.240)

● Monitoring Traps

The Alarm Service can monitor the trap events from RAID Manager.

● Changing Icons

When abnormality is notified from RAID Manager, the status icon of ServerView S2 and the Management Console is changed. So you can recognize the abnormality.

4.2 Starting up ServerView RAID Manager (Web Client)

This section describes how to start up ServerView RAID Manager (Web client).

POINT

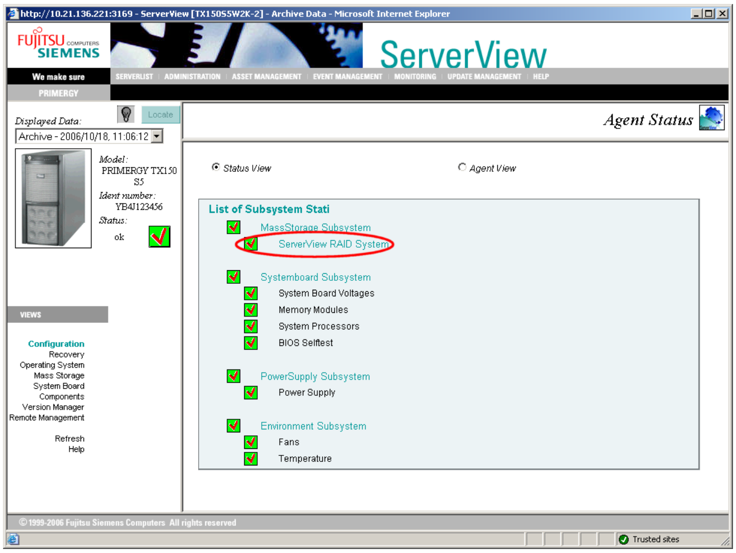
- ServerView S2 and the Management Console of the following version can be used to start up ServerView RAID Manager (Web client).
  - ServerView Console for Windows/Linux V4.20.xx or later

■ Starting up from ServerView S2 (Configuration Information)

Open the [Configuration Information] window of the server to be monitored where RAID Manager is installed from ServerView S2. For details about the configuration information, see "3.2.3 Displaying Configuration Information" (→pg.103).

1 Click [List of Subsystem Stati], [MassStorage Subsystem], and [ServerView RAID System].

If ServerView RAID is not installed, [ServerView RAID System] is not displayed.



Displayed Data: Archive - 2006/10/18, 11:06:12

Model: PRIMERGY TX150 S5
Ident number: YB4J123456
Status: ok ✓

● Status View ○ Agent View

List of Subsystem Stati

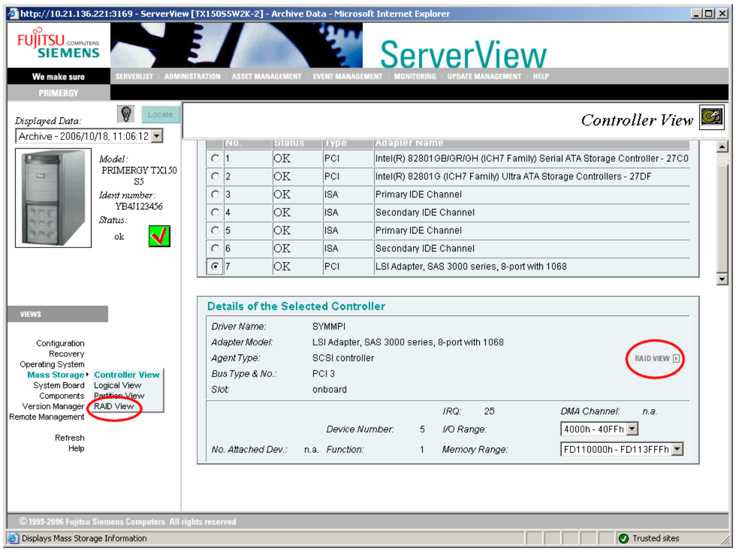
- ✓ MassStorage Subsystem
  - ✓ ServerView RAID System
- ✓ Systemboard Subsystem
  - ✓ System Board Voltages
  - ✓ Memory Modules
  - ✓ System Processors
  - ✓ BIOS Selftest
- ✓ PowerSupply Subsystem
  - ✓ Power Supply
- ✓ Environment Subsystem
  - ✓ Fans
  - ✓ Temperature

■ Starting up from ServerView S2 (Mass Storage)

Open the [Mass Storage] window of the server to be monitored where ServerView RAID is installed from ServerView S2. For details about the mass storage, see "3.2.6 Verifying the Status of Mass Storage" (→pg.111).

1 Click [RAID View] from the [Mass Storage] menu. Or click [RAID VIEW] in [Details of the Selected Controller].

If ServerView RAID is not installed or you select a controller that is not compliant with ServerView RAID, [RAID View]/[RAID VIEW] is not displayed.


http://10.21.136.221:3169 - ServerView [TX150S5W2K-2] - Archive Data - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
SERVERLIST | ADMINISTRATION | ASSET MANAGEMENT | EVENT MANAGEMENT | MONITORING | UPDATE MANAGEMENT | HELP
PRIMERGY
Locate
Controller View
VIEWS
Configuration
Recovery
Operating System
Mass Storage
Controller View
Logical View
Partition View
RAID View
System Board
Components
Version Manager
Remote Management
Refresh
Help
RAID VIEW
© 1999-2006 Fujitsu Siemens Computers All rights reserved
Displays Mass Storage Information
Trusted sites

Displayed Data: Archive - 2006/10/18, 11:06:12

Model: PRIMERGY TX150 S5

Ident number: YB4J123456

Status: ok

	No.	Status	Type	Adapter Name
○	1	OK	PCI	Intel(R) 82801GB/GR/GH (ICH7 Family) Serial ATA Storage Controller - 27C0
○	2	OK	PCI	Intel(R) 82801G (ICH7 Family) Ultra ATA Storage Controllers - 27DF
○	3	OK	ISA	Primary IDE Channel
○	4	OK	ISA	Secondary IDE Channel
○	5	OK	ISA	Primary IDE Channel
○	6	OK	ISA	Secondary IDE Channel
●	7	OK	PCI	LSI Adapter, SAS 3000 series, 8-port with 1068

Details of the Selected Controller

Driver Name: SYMMPI
Adapter Model: LSI Adapter, SAS 3000 series, 8-port with 1068
Agent Type: SCSI controller
Bus Type & No.: PCI 3
Slot: onboard

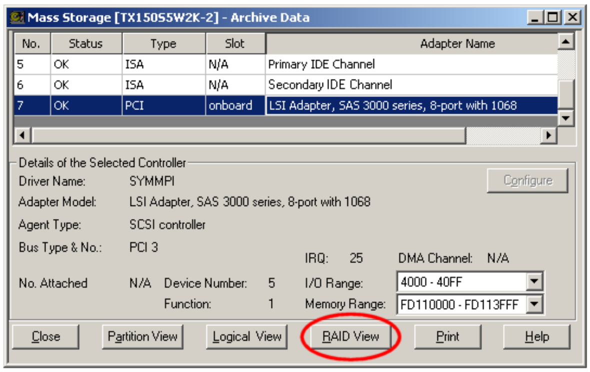
IRQ: 25
DMA Channel: n.a.
Device Number: 5
I/O Range: 4000h - 40FFh
No. Attached Dev.: n.a.
Function: 1
Memory Range: FD110000h - FD113FFFh

■ Starting up from the Management Console (Mass Storage)

Open the [Mass Storage] window of the server to be monitored where ServerView RAID is installed from the Management Console. For details about the mass storage, see "■ Verifying Mass Storage Status" (→pg.237).

1 Click [RAID View] in [Details of the Selected Controller].

If ServerView RAID is not installed or you select a controller that is not compliant with ServerView RAID, [RAID View] is not displayed.



No.	Status	Type	Slot	Adapter Name
5	OK	ISA	N/A	Primary IDE Channel
6	OK	ISA	N/A	Secondary IDE Channel
7	OK	PCI	onboard	LSI Adapter, SAS 3000 series, 8-port with 1068

Details of the Selected Controller

Driver Name: SYMMPI
Adapter Model: LSI Adapter, SAS 3000 series, 8-port with 1068
Agent Type: SCSI controller
Bus Type & No.: PCI 3

IRQ: 25
DMA Channel: N/A
No. Attached: N/A
Device Number: 5
I/O Range: 4000 - 40FF
Function: 1
Memory Range: FD110000 - FD113FFF

Chapter 5

Using RemoteControlService

This chapter explains how to use RemoteControlService.

5.1 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

By using RemoteControlService, the server can be controlled remotely from administration terminal to control the power supply and display current power supply status of the server. Also, text-based console redirection can be displayed.

■ Components of RemoteControlService

RemoteControlService consists of the following two components on the server side and administration terminal side.

● Server side components [iRMC, BMC]

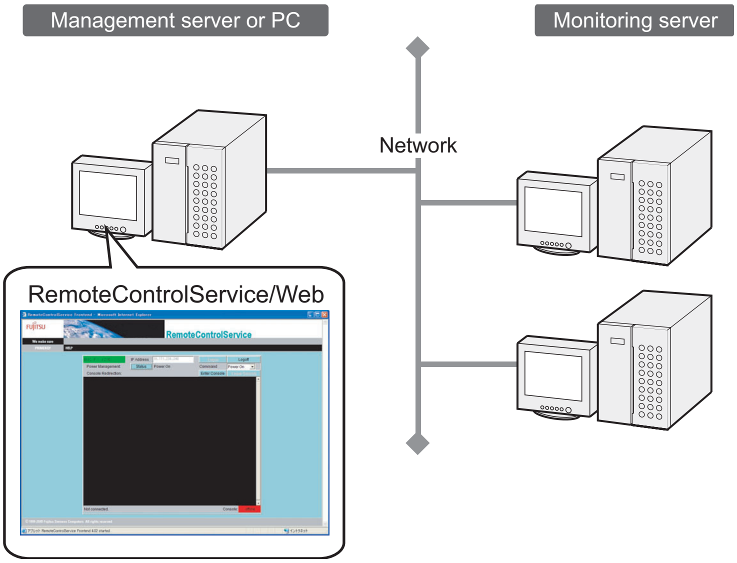
- iRMC (integrated Remote Management Controller)
  This is a server's iRMC function that is equivalent to the function of the onboard RSB.
  The following servers support this function.
  PRIMERGY RX300 S3 / PRIMERGY RX200 S3 / PRIMERGY TX200 S3 / PRIMERGY TX150 S5
- BMC (IPMI over LAN)
  This is a server's BMC (IPMI over LAN) function that provides reset, power OFF/ON, console redirection in text modes and so on.
  The following servers support this function.
  - IPMI 1.5
    PRIMERGY RX100 S3 / PRIMERGY TX150 S4
  - IPMI 2.0
    PRIMERGY RX600 S2 / PRIMERGY RX600 S3

POINT

- For the support of blade servers, refer to "PRIMERGY BX600 Hardware Guide (Management Blades)".

● Administration terminal side component [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.



5.1.1 Functions

RemoteControlService/Web includes the following functions:

- Remote Management by Telnet connection:
  Remote Managemen Controller, Remote Service Board / Remote Service Controller, Management Blade
- Remote Management by IPMI connection: iRMC / BMC (IPMI over LAN)

● Remote Management by Telnet connection

The power supply management function and the text-based console redirection function are provided.

POINT

- The console redirection function cannot be used on the management blade.

● Remote Management by IPMI connection

The power supply management function and the text-based console redirection function are provided.

5.1.2 System Requirements

System requirements for servers and administration terminals are as follows.

■ Server

table: System Requirements for Servers

Hardware	Software
• BMC: BMC firm version 2.xx or later • iRMC: iRMC installed on the server RX300 S3 or later	No particular conditions

■ Administration Terminal

This can be used for the servers (terminals) that ServerView S2 is installed on.

5.1.3 Notes

■ RemoteControlService/LAN

RemoteControlService/Web can not be used together with RemoteControlService/LAN. When using RemoteControlService/Web, uninstall RemoteControlService/LAN first.

■ IPMI (Intelligent Platform Management Interface)

The IPMI function depends on machine type. For support of this function, refer to "RCS_Hints".

● Notes for "QLogic RMCP Filter"

- Some servers require "QLogic RMCP Filter" on the administration terminal to execute the console redirection through IPMI.
- For information on how to install and use "QLogic RMCP Filter", refer to "PCS_Hints".

● 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 opened in a target network.

5.2 Preparation

Set up iRMC and BMC, and install RemoteControleService/Web in preparation for the use of RemoteControleService.

5.2.1 Installing/Uninstalling RemoteControleService/Web

This section describes how to install/uninstall RemoteControleService/Web into an administration terminal.

IMPORTANT

- It is necessary to install ServerView S2 beforehand to install RemoteControlService/Web.
- Do not uninstall ServerView S2 before uninstalling 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\WinSVRcs\SV_Rcs.bat
   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/Svmanage/Linux/
ENGLISH/sv
# ./InstallRCSW.sh RemoteViewFE-X.X-X.i386.rpm
(X.X-X indicates version number.)
```

● Uninstalling

Execute the following command.

```
# rpm -e RemoteViewFE
```

5.2.2 Configuration for iRMC

To use iRMC, the settings on BIOS and Server Management Tools (IPMIview) are required.
The setting method might be different according to the server model or version of firmware/BIOS.
Refer to ”User’s Guide” of your server for details.

■ For PRIMERGY RX300 S3 / PRIMERGY RX200 S3 / PRIMERGY TX200 S3 / PRIMERGY TX150 S5

● 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 Configration]	
Serial 1	Enabled
Serial Multiplexer	System
[Server] - [Console Redirection]	
Console Redirection	Enabled
Port	Serial 1
Baud Rate	9600
Protocol	VT100+
Flow Control	CTS/RTS
Mode	Enhanced

2 Set the IP address, user name and password, referring to "7.2 Preparations" (→pg.346).

5.2.3 Configuration for IPMI

To use IPMI, it is necessary to set up it using Server Management Tools (IPMIview). The setting procedure depends on machine type and BIOS version. For details, refer to "User’s Guide" for your server.

■ Common Setting on the Server Side

1 Select [User Management] from the [Server Management Tools] menu.

2 Specify the password for ID3.

This password is used for connecting IPMI.

3 Select "1" (enable user) for [Operation].

4 Press the [F1] key to store the settings.

5 Select [Channel Configuration] from the [Server Management Tools] menu.

6 Select "#2 802.3_LAN" from [Select Channel] and specify the following items.

table: IP Address Setting

Items	Settings
BMC NIC IP Address / MAC Address	Since the IPMI function is applied only for onboard LAN port, MAC address cannot be changed from the default value.
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.

7 Press the [F1] key to store the settings.

IMPORTANT

- When configuring BIOS and Server Management Tools (IPMIview), use the default values or consult the server’s manual, except for the designated settings.
- BMC IP address for the following servers must be different from that of the server OS.
  PRIMERGY RX100 S3 / PRIMERGY TX150 S4

■ For PRIMERGY RX600 S2 / RX600 S3

1 Configure the console redirection.

When only using power management, configuration is not required.
Start the BIOS Setup Utility and configure the following settings:

table: Setting Items for BIOS Setup Utility

Items	Settings
[Server] - [Console Redirection] - [COM1 Console Redirection]	
Console Redirect Port	Enabled
Flow Control	RTS/CTS + CD
Baud Rate	19.2k
Terminal Type	VT100+

■ For PRIMERGY TX150 S4 / RX100 S3

1 Configure the console redirection.

When only using power management, configuration is not required.
Start the BIOS Setup Utility and configure the following settings:

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

5.3 Starting and Exiting

This section describes how to start and exit RemoteControleService/Web along with its menu.

5.3.1 Start and Exit for RemoteControleService/Web (For iRMC Telnet Connection)

The starting method of RemoteControlService/Web is different in whether or not OS is started.

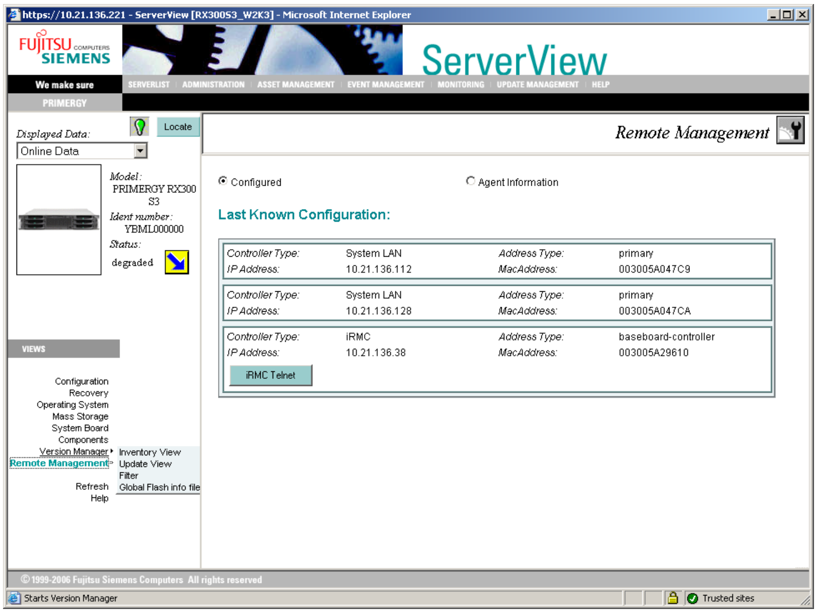
IMPORTANT

- For connecting to the Remote Management Controller (iRMC), you can also use the Web interface, in addition to Telnet. For details, refer to "7.3 Starting and Exiting" (→pg.348).
- When using Telnet to connect to the Remote Management Controller (iRMC), the Telnet port needs to be enabled using the iRMC Web interface before the Telnet connection. For details, refer to "7.4.7 Network Settings" (→pg.368).

● When OS is started

1 ServerView S2 window→[SERVERLIST] → Select of server →[VIEWS] →[Remote Manager].

The following window appears.



https://10.21.136.221 - ServerView [RX300S3_W2K3] - Microsoft Internet Explorer

Remote Management

Displayed Data: Online Data

Model: PRIMERGY RX300 S3

Ident number: YBML000000

Status: degraded

● Configured ○ Agent Information

Last Known Configuration:

Controller Type:	System LAN	Address Type:	primary
IP Address:	10.21.136.112	MacAddress:	003005A047C9
Controller Type:	System LAN	Address Type:	primary
IP Address:	10.21.136.128	MacAddress:	003005A047CA
Controller Type:	iRMC	Address Type:	baseboard-controller
IP Address:	10.21.136.38	MacAddress:	003005A29610

iRMC Telnet

© 1999-2006 Fujitsu Siemens Computers All rights reserved

Starts Version Manager

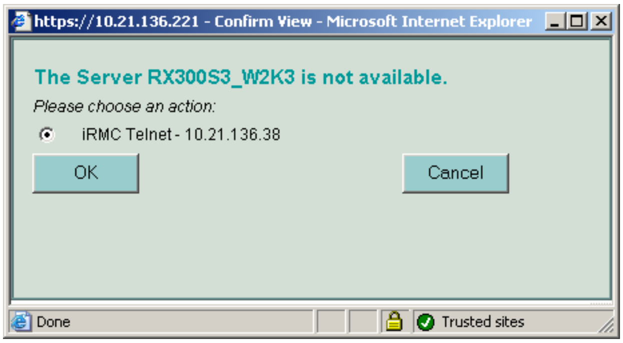
2 Click [iRMC Telnet].

RemoteConsoleService/Web is started.

● When OS is not started

1 The object server is selected from [ServerList] of ServerView S2 windows.

The following window appears.



https://10.21.136.221 - Confirm View - Microsoft Internet Explorer

The Server RX300S3_W2K3 is not available.

Please choose an action:

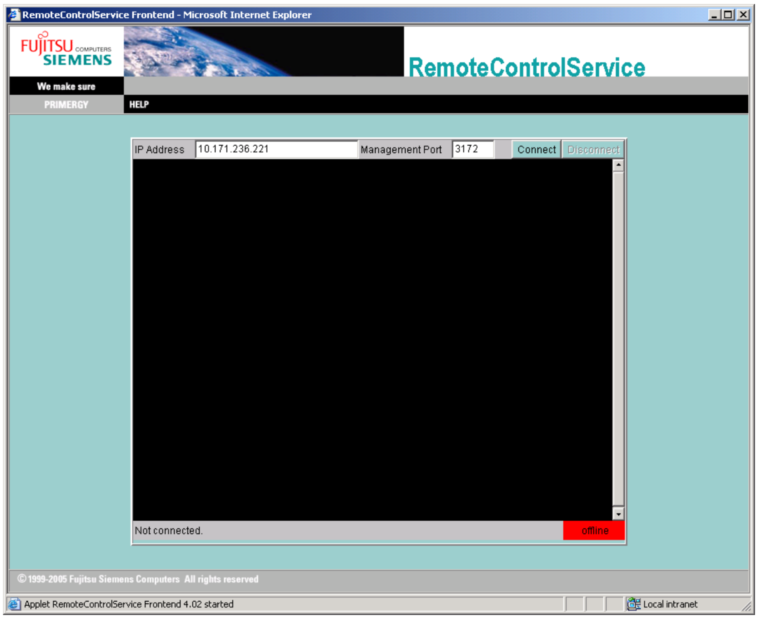
◉ iRMC Telnet - 10.21.136.38

2 Select [iRMC Telnet] and click [OK].

RemoteConsoleService/Web is started.

■ RemoteConsoleService/Web Windows

When RemoteConsoleService/Web starts, the following window appears.



RemoteControlService Frontend - Microsoft Internet Explorer

IP Address: 10.171.236.221 Management Port: 3172

Not connected.

FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
RemoteControlService
HELP
Connect
Disconnect
offline
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Applet RemoteControlService Frontend 4.02 started
Local intranet

After connected iRMC, you can refer and operate the following information.

table: RemoteConsoleService/Web window

Item	Description
IP Address	IP Address connected to iRMC is displayed.
Management Port	Telnet number connected to iRMC is displayed.
[connect]	Logon to iRMC displayed in "IP Address" .
[Disconnect]	Logoff iRMC.

■ How to Use iRMC Telnet

For details about the iRMC Telnet main menu for RemoteControlService/Web, refer to "5.4.1 iRMC Telnet Connection" (→pg.282).

■ Exiting

1 Click [Disconnect], when logon for iRMC.

2 Close RemoteControlService/Web browser.

RemoteControleService/Web exits.

5.3.2 Start and Exit for RemoteControleService/Web (For iRMC / BMC IPMI connection)

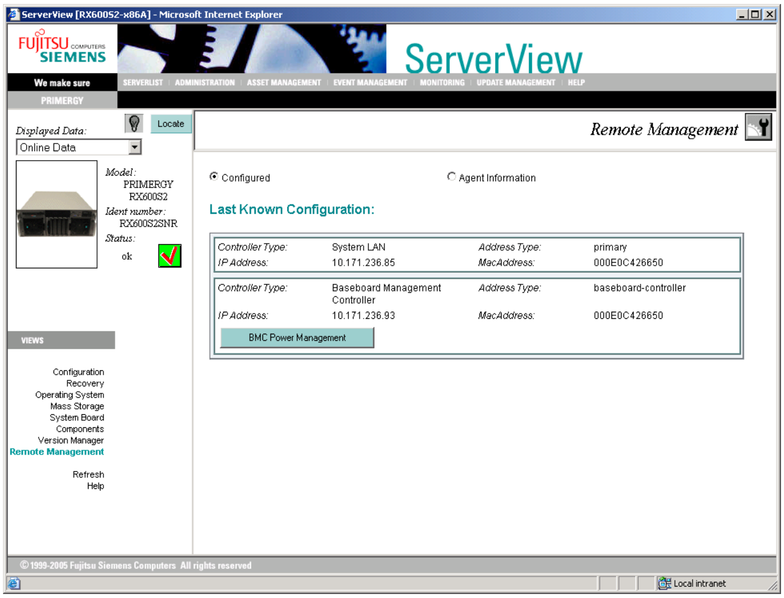
The starting method of RemoteControlService/Web is different in whether or not OS is started.

■ Starting

● When OS is started

1 ServerView S2 window→[SERVERLIST] → Select of server →[VIEWS] →[Remote Manager].

The following window appears.



Remote Management

Displayed Data: Online Data

Model: PRIMERGY RX600S2

Ident number: RX600S2SNR

Status: ok ✓

◉ Configured ○ Agent Information

Last Known Configuration:

Controller Type:	System LAN	*Address Type:*	primary
IP Address:	10.171.236.85	*MacAddress:*	000E0C426650

Controller Type:	Baseboard Management Controller	*Address Type:*	baseboard-controller
IP Address:	10.171.236.93	*MacAddress:*	000E0C426650

BMC Power Management

2 Click [BMC Power Management] or [iRMC Power Management].

RemoteConsoleService/Web is started.

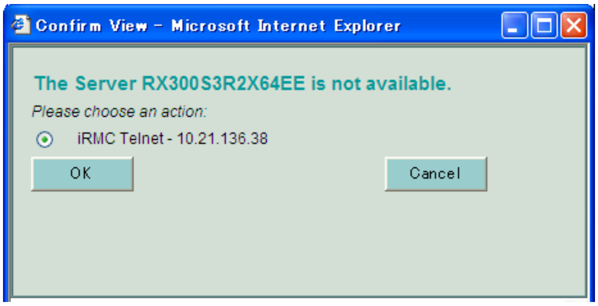
POINT

- When selecting [iRMC Web], the Remote Management Controller Web interface can be started.

● When OS is not started

1 The object server is selected from [ServerList] of ServerView S2 windows.

The following window appears.



Confirm View - Microsoft Internet Explorer

The Server RX300S3R2X64EE is not available.

Please choose an action:

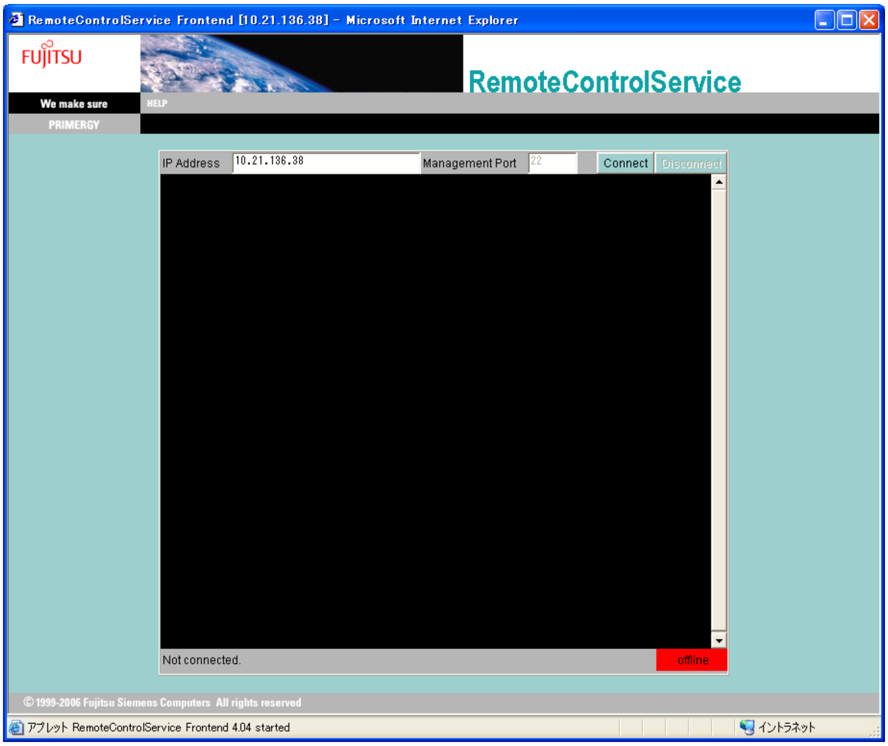
◉ iRMC Telnet - 10.21.136.38

2 Select [BMC Power Management] or [iRMC Power Management], and click [OK].

RemoteConsoleService/Web is started.

■ RemoteConsoleService/Web Window

When RemoteConsoleService/Web starts, the following window appears.



RemoteControlService Frontend [10.21.136.38] - Microsoft Internet Explorer

IP Address 10.21.136.38 Management Port 22

Not connected.

© 1999-2006 Fujitsu Siemens Computers All rights reserved

アプレット RemoteControlService Frontend 4.04 started

The following information can be referred and the following operations can be performed after connecting to iRMC / BMC.

table: RemoteConsoleService/Web window

Item		Description
BMC(FW:)		After logon, the version of the iRMC / BMC firmware is displayed.
IP Address		IP Address set to iRMC / BMC is displayed.
[Loggon]		Logon to iRMC / BMC displayed in "IP Address" .
[Loggoff]		Logoff iRMC / 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.

RemoteControleService/Web exits.

5.3.3 Start and Exit for RemoteControleService/Web (For RSB connection)

The starting method of RemoteControlService/Web is different in whether or not OS is started.

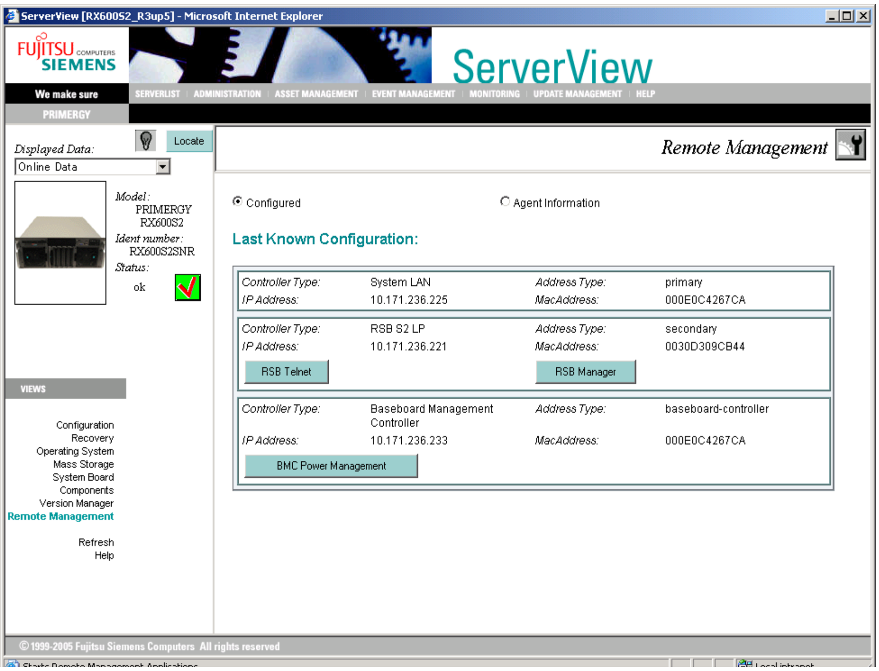
IMPORTANT

- For connecting to the Remote Service Board, you can also use the Web interface, in addition to Telnet. For details, refer to "6.3 Displaying Each Monitoring Information" (→pg.303).
- 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 "6.3.8 [Web/ SSL Config] Page" (→pg.336).

● When OS is started

1 ServerView S2 window→[SERVERLIST] → Select of server →[VIEWS] →[Remote Manager].

The following window appears.



Displayed Data: Online Data

Model: PRIMERGY RX600S2

Ident number: RX600S2SNR

Status: ok

● Configured ○ Agent Information

Last Known Configuration:

Controller Type:	System LAN	Address Type:	primary
IP Address:	10.171.236.225	MacAddress:	000E0C4267CA
Controller Type:	RSB S2 LP	Address Type:	secondary
IP Address:	10.171.236.221	MacAddress:	0030D309CB44
Controller Type:	Baseboard Management Controller	Address Type:	baseboard-controller
IP Address:	10.171.236.233	MacAddress:	000E0C4267CA

2 Click [RSB Telnet].

RemoteConsoleService/Web is started.

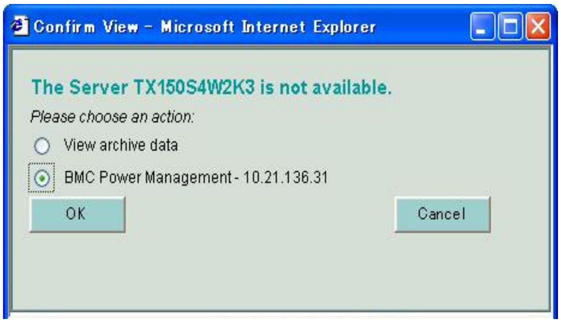
POINT

- 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.



Confirm View - Microsoft Internet Explorer

The Server TX150S4W2K3 is not available.

Please choose an action:

○ View archive data

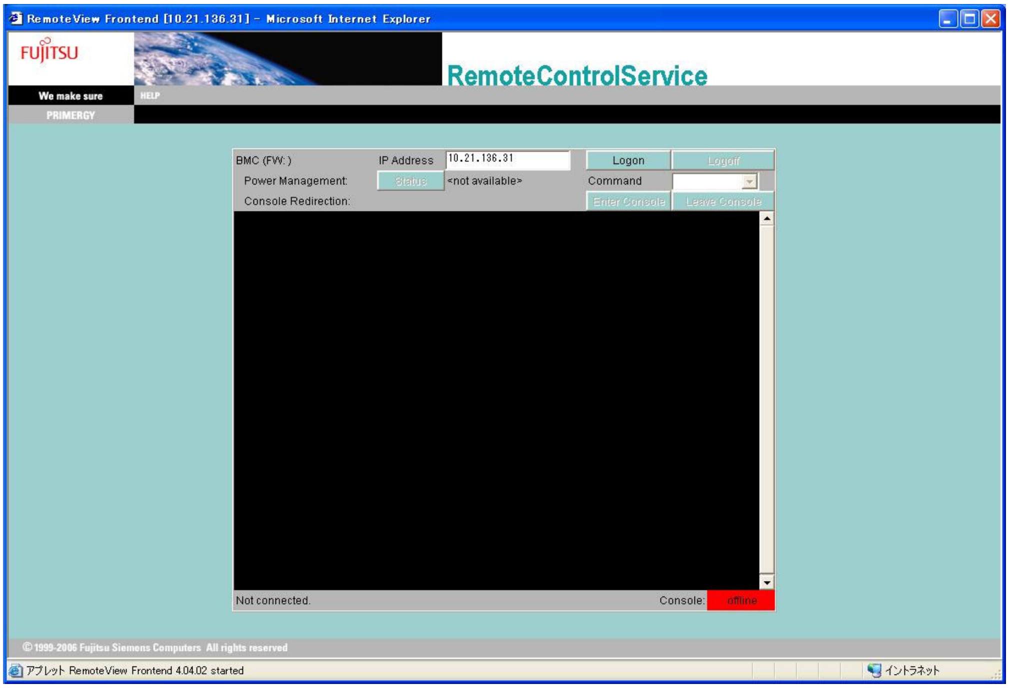
● BMC Power Management - 10.21.136.31

2 Select [Start RSB Telnet], and click [OK].

RemoteConsoleService/Web is started.

■ RemoteConsoleService/Web Windows

When RemoteConsoleService/Web starts, the following window appears.



RemoteView Frontend [10.21.136.31] - Microsoft Internet Explorer

BMC (FW:)

IP Address 10.21.136.31

Power Management: <not available>

Command

Console Redirection:

Not connected.

Console: offline

© 1999-2006 Fujitsu Siemens Computers All rights reserved

アプレット RemoteView Frontend 4.04.02 started

After connected RSB, you can refer and operate the following information.

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.

table: RemoteConsoleService/Web window

Item	Description
[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 "5.4.3 RSB Telnet Connection"-"■ Main Menu" (→pg.285).

■ Exiting

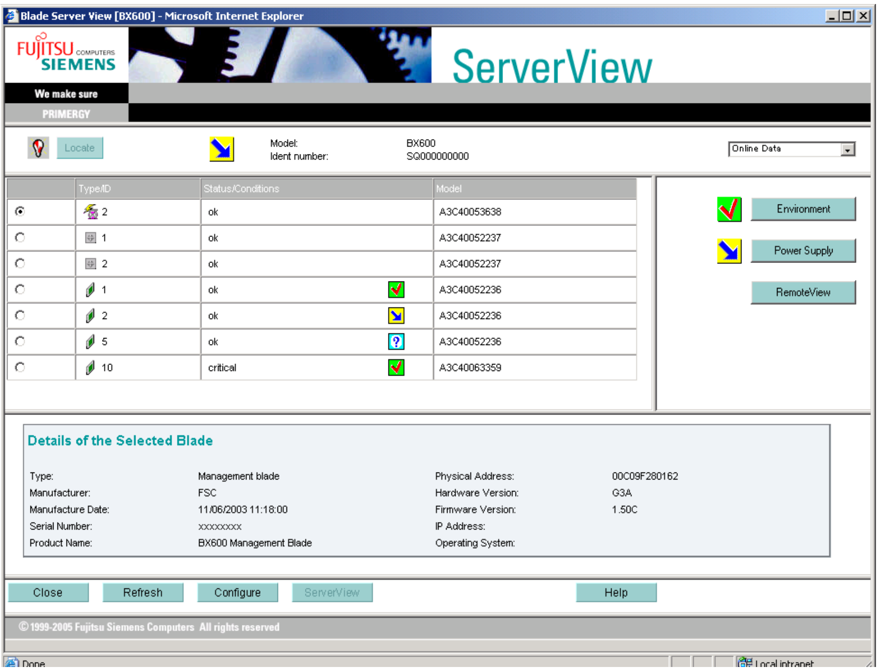
1 Click [Disconnect], when logon for RSB.

2 Close RemoteControlService/Web browser.

RemoteControleService/Web exits.

5.3.4 Start and Exit for RemoteControleService/Web (For ManagementBlade connection)

1 ServerView S2 window→[SERVERLIST] → Select of server →[Blade Server View] →[RemoteView].


Blade Server View [BX600] - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
ServerView
We make sure
PRIMERGY
Locate
Online Data
Environment
Power Supply
RemoteView
Close
Refresh
Configure
ServerView
Help
© 1999-2005 Fujitsu Siemens Computers All rights reserved
Done
Local intranet

Model: BX600
Ident number: SQ000000000

	Type/ID	Status/Conditions		Model
●	2	ok		A3C40053638
○	1	ok		A3C40052237
○	2	ok		A3C40052237
○	1	ok	✓	A3C40052236
○	2	ok	↘	A3C40052236
○	5	ok	?	A3C40052236
○	10	critical	✓	A3C40063359

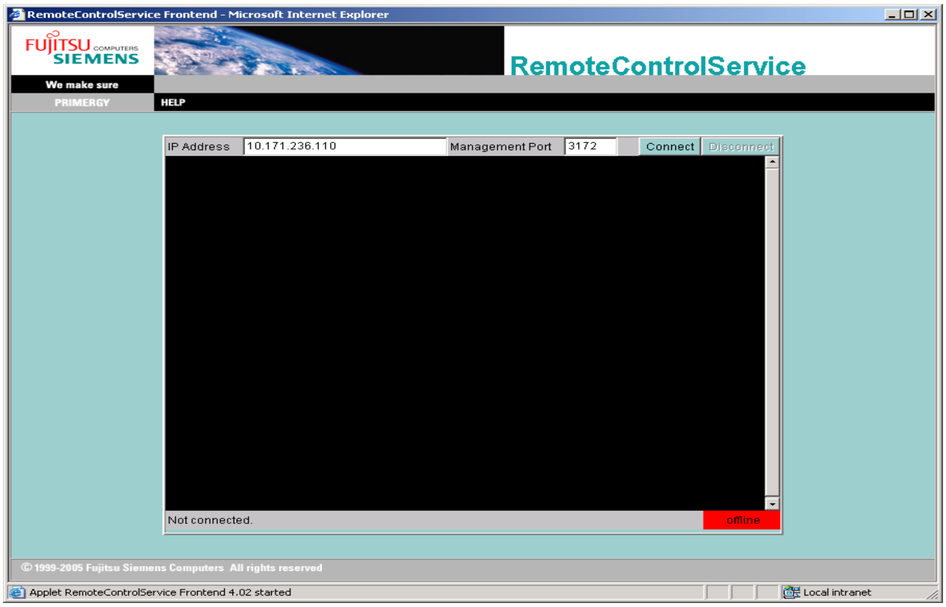
Details of the Selected Blade

Type:	Management blade	Physical Address:	00C09F280162
Manufacturer:	FSC	Hardware Version:	G3A
Manufacture Date:	11/06/2003 11:18:00	Firmware Version:	1.50C
Serial Number:	xxxxxxxx	IP Address:	
Product Name:	BX600 Management Blade	Operating System:	

RemoteConsoleService/Web is started.

■ RemoteConsoleService/Web Window

When RemoteConsoleService/Web starts, the following window appears.


RemoteControlService Frontend - Microsoft Internet Explorer
FUJITSU COMPUTERS SIEMENS
We make sure
PRIMERGY
HELP
RemoteControlService
Connect
Disconnect

IP Address 10.171.236.110

Management Port 3172

Not connected.

offline

© 1999-2005 Fujitsu Siemens Computers All rights reserved

Applet RemoteControlService Frontend 4.02 started

Local intranet

After connected ManagementBlade, you can refer and operate the following information.

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.

RemoteControleService/Web exits.

5.4 How to Use

This section describes how to use RemoteControleService/Web.
For details, refer to the corresponding online help.

5.4.1 iRMC Telnet Connection

This section describes Remote Management Controller support through RemoteControleService/Web.

■ Connecting to Remote Management Controller

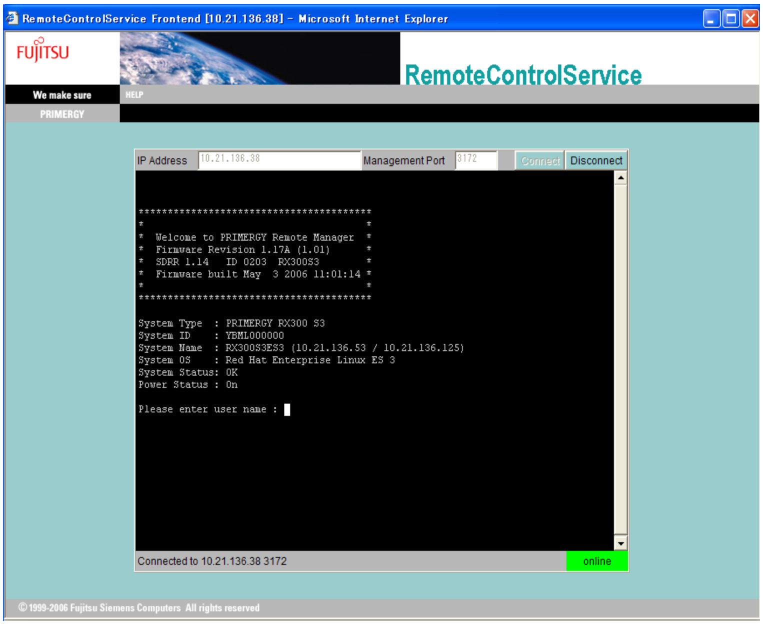
Remote Management Controller has a Telnet interface called Remote Manager, which allows to connect from RemoteControlService/Web. When connecteing to Remote Management Controller using Telnet, only the power supply management of the server and the text-based console redirection function are supported.
Follow the procedures below to connect to Remote Management Controller from RemoteControlService/Web.

IMPORTANT

- The Telnet port should be made effective by using Web interface of Remote Management Controller before the Telnet connection is executed. For details, refer to "7.4.7 Network Settings" (→pg.368).

1 Click [Connect] and login with the account that is set beforehand.

The following window appears.


RemoteControlService Frontend [10.21.136.38] - Microsoft Internet Explorer
FUJITSU
RemoteControlService
We make sure
HELP
PRIMERGY
Connect
Disconnect
online
© 1999-2006 Fujitsu Siemens Computers All rights reserved

IP Address 10.21.136.38 Management Port 3172

```
****************************************
*                                      *
*  Welcome to PRIMERGY Remote Manager  *
*  Firmware Revision 1.17A (1.01)      *
*  SDRR 1.14   ID 0203  RX300S3        *
*  Firmware built May  3 2006 11:01:14 *
*                                      *
****************************************

System Type  : PRIMERGY RX300 S3
System ID    : YBML000000
System Name  : RX300S3ES3 (10.21.136.53 / 10.21.136.125)
System OS    : Red Hat Enterprise Linux ES 3
System Status: OK
Power Status : On

Please enter user name : █
```

Connected to 10.21.136.38 3172

Main Menu

The main menu in the Remote Management Controller is shown as follows.
The menu depends on machine type and an applicable menu will appear.
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.

table: Main Menu of Remote Management Controller

Menu Item	Description
System Information	This function is not supported.
Power Management	Controls the server power supply. If this is selected, the power management menu appears.
Enclosure Information	This function is not supported.
Service Processor	This function is not supported.
Change password	This function is not supported.
Console Redirection (EMS/ASC)	Use this to redirect a console.
Start a Command Line shell	This function is not supported.

● Power Management

table: Power Management Menu

Menu Item	Description
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. Remote Management Controller sends a shutdown request to the ServerView Agent in the server.
Graceful Reset (Reboot)	Reboots the server. Remote Management Controller sends a reset request to the ServerView Agent in the server.

● Console Redirection (EMS/ASC)

The window and keyboard operation of the server can be redirected to the remote console by console redirection of Remote Management controller. When the console redirection is selected, the window of the server is forwarded to the remote manager window. The data which is input from the keyboard is sent to the keyboard controller of the server.
The following operations can be performed by the console redirection.

- Displaying window during POST
- BIOS setup

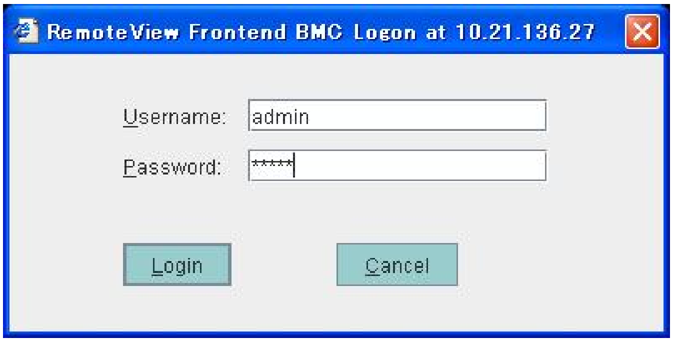
The console redirection closes when entering tilde (~) and period (.), or 'Esc' and '(' within two seconds in quick succession.

5.4.2 BMC Connection

This section describes the support of IPMI over LAN through RemoteControleService/Web.
Follow the procedure below to connect to BMC from RemoteControleService/Web.

■ Connecting to BMC

1 Click [Loggon] from the RemoteConsoleService/Web window. Log in as a set account on the following window.



RemoteView Frontend BMC Logon at 10.21.136.27

Username: admin

Password: *****

2 The following information can be referred and the following operations can be performed after connecting to BMC.

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.

5.4.3 RSB Telnet Connection

This section describes the support of Remote Service Board through RemoteControleService/Web.

■ Connecting to Remote Service Board

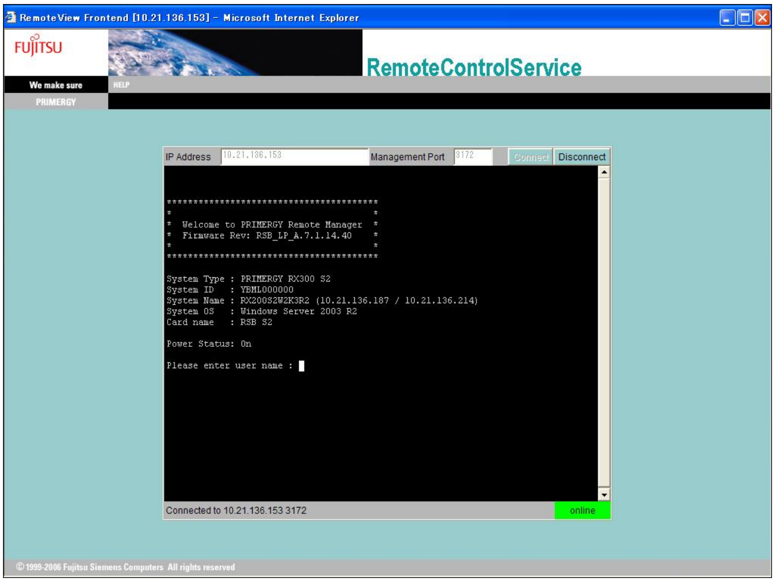
The remote service board includes the Telnet interface called remote manager, which can be connected from RemoteControleService/Web. The remote manager allows you to verify the information about the target server. The information includes items such as a system name which appear only after the ServerView Agent is initially started, or only when the server is properly configured.

Follow the procedure below to connect to the remote service board from RemoteControlService/Web.

IMPORTANT

- Before starting Telnet connection, use a Web interface in the remote service board to enable a Telnet port.

1 Click [connect] from the RemoteConsoleService/Web window. Log in as an account that set for the Remote Service Board.


RemoteView Frontend [10.21.136.153] - Microsoft Internet Explorer
FUJITSU
RemoteControlService
We make sure
HELP
PRIMERGY
IP Address
10.21.136.153
Management Port
3172
Connect
Disconnect
Connected to 10.21.136.153 3172
online
©1999-2006 Fujitsu Siemens Computers All rights reserved

```
****************************************
*                                      *
*  Welcome to PRIMERGY Remote Manager  *
*  Firmware Rev: RSB_LP_A.7.1.14.40    *
*                                      *
****************************************

System Type : PRIMERGY RX300 S2
System ID   : YBML000000
System Name : RX200S2W2K3R2 (10.21.136.187 / 10.21.136.214)
System OS   : Windows Server 2003 R2
Card name   : RSB S2

Power Status: On

Please enter user name :
```

2 The information can be referred and the following operations can be performed after connecting to RSB.

■ Main Menu

The main menu in the remote manager is shown below.

The menu depends on machine type and an applicable menu will appear.

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 (*).

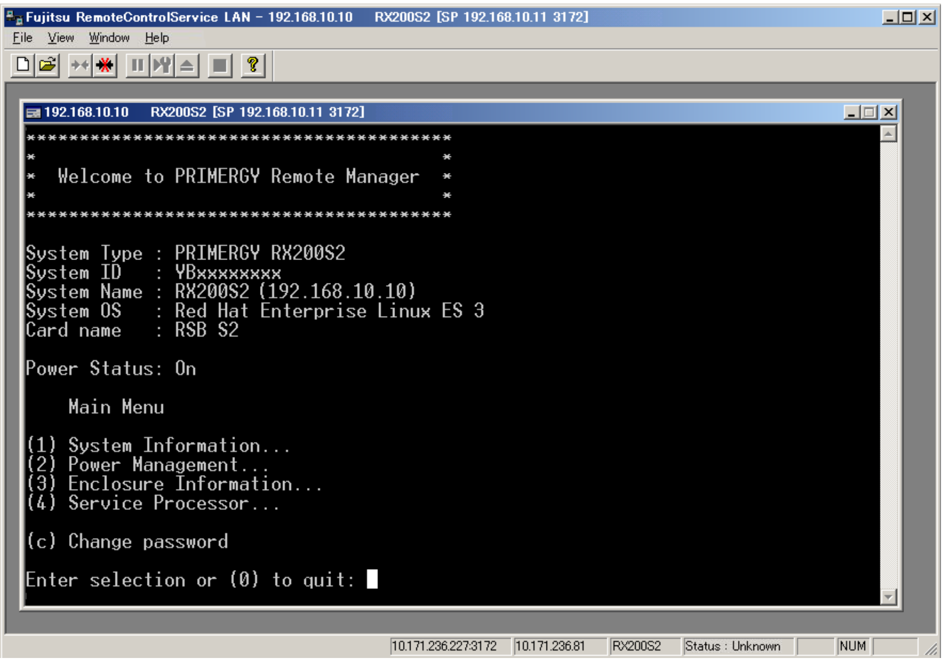
If the [0] key is pressed, the higher menu would appear. If the [0] key is pressed while the main menu is displayed, the remote service board would be disconnected.

POINT

- For details about each item, refer to the manual supplied with the server.

table: Main Menu

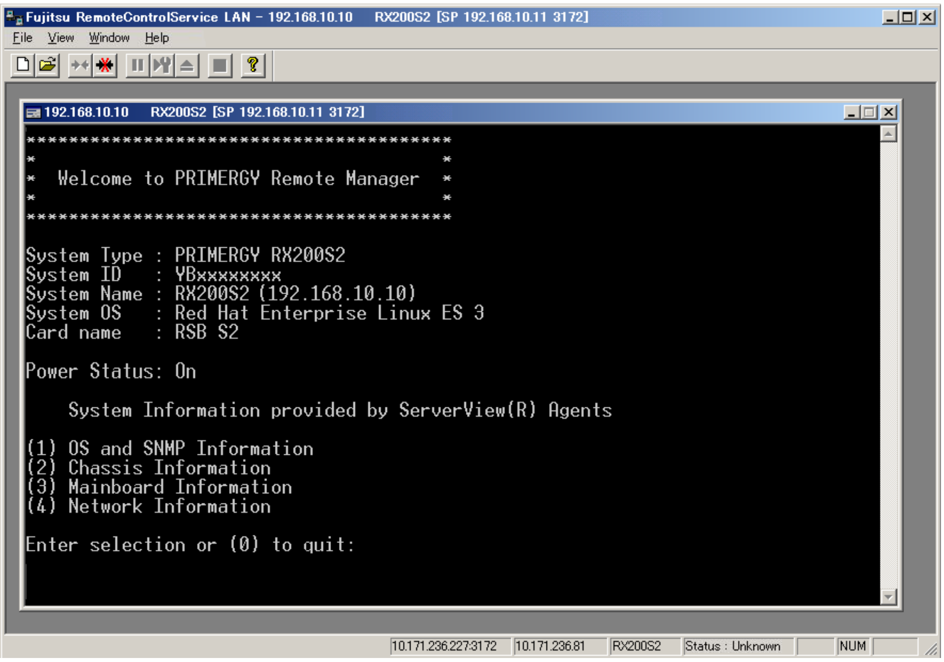
Menu Item	Description
System Information	Displays system information. If this is selected, the system information menu appears.
Power Management	Controls the server power supply. If this is selected, the power management menu appears.
Enclosure Information	Displays server information. If this is selected, 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.


Fujitsu RemoteControlService LAN - 192.168.10.10   RX200S2 [SP 192.168.10.11 3172]
File
View
Window
Help
192.168.10.10   RX200S2 [SP 192.168.10.11 3172]
10.171.236.227:3172
10.171.236.81
RX200S2
Status : Unknown
NUM

```
****************************************
*                                      *
*  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

    Main Menu

(1) System Information...
(2) Power Management...
(3) Enclosure Information...
(4) Service Processor...

(c) Change password

Enter selection or (0) to quit:
```

● System Information

Select [System Information] 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
192.168.10.10 RX200S2 [SP 192.168.10.11 3172]
10.171.236.227:3172
10.171.236.81
RX200S2
Status : Unknown
NUM

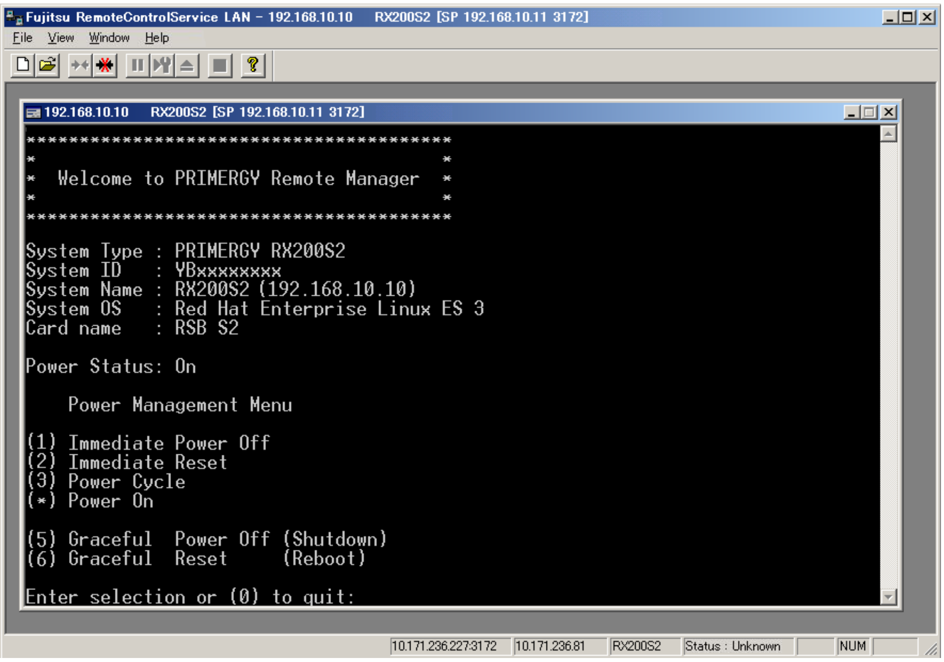
```
****************************************
*                                      *
*  Welcome to PRIMERGY Remote Manager  *
*                                      *
****************************************

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

    System Information provided by ServerView(R) Agents

(1) OS and SNMP Information
(2) Chassis Information
(3) Mainboard Information
(4) Network Information

Enter selection or (0) to quit:
```

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.


Fujitsu RemoteControlService LAN - 192.168.10.10 RX200S2 [SP 192.168.10.11 3172]
File View Window Help
192.168.10.10 RX200S2 [SP 192.168.10.11 3172]
10.171.236.227:3172
10.171.236.81
RX200S2
Status : Unknown
NUM

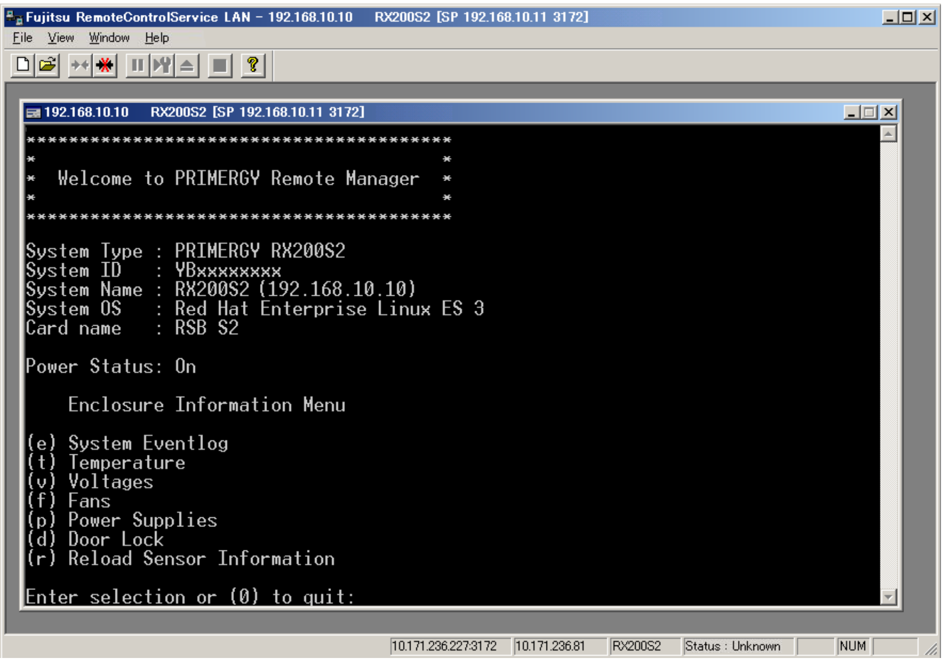
```
****************************************
*                                      *
*  Welcome to PRIMERGY Remote Manager  *
*                                      *
****************************************

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

    Power Management Menu

(1) Immediate Power Off
(2) Immediate Reset
(3) Power Cycle
(*) Power On

(5) Graceful  Power Off (Shutdown)
(6) Graceful  Reset     (Reboot)

Enter selection or (0) to quit:
```

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.


Fujitsu RemoteControlService LAN - 192.168.10.10 RX200S2 [SP 192.168.10.11 3172]
File View Window Help
192.168.10.10 RX200S2 [SP 192.168.10.11 3172]
10.171.236.227:3172
10.171.236.81
RX200S2
Status : Unknown
NUM

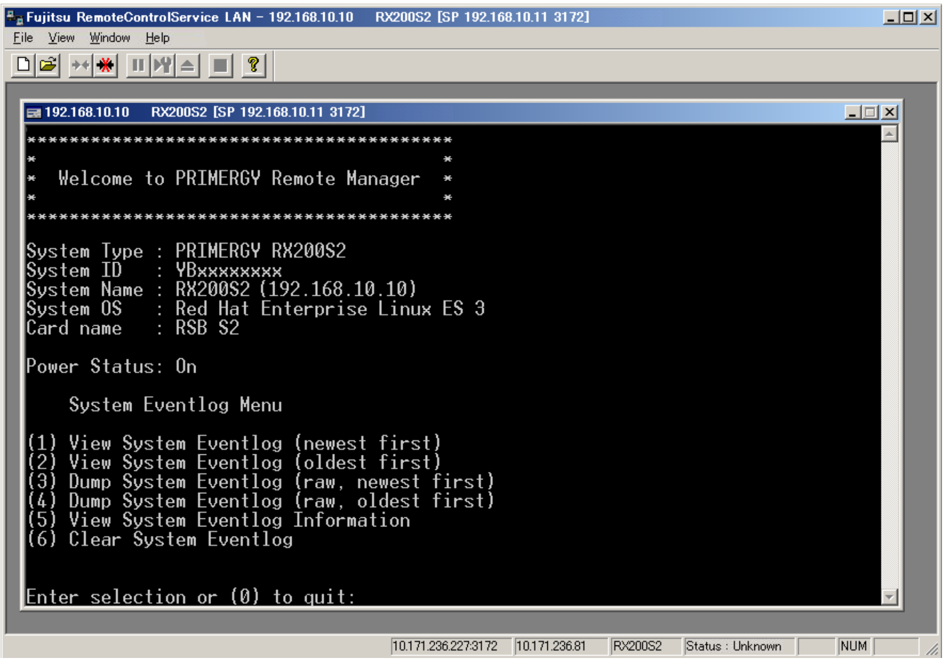
```
****************************************
*                                      *
*  Welcome to PRIMERGY Remote Manager  *
*                                      *
****************************************

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

    Enclosure Information Menu

(e) System Eventlog
(t) Temperature
(v) Voltages
(f) Fans
(p) Power Supplies
(d) Door Lock
(r) Reload Sensor Information

Enter selection or (0) to quit:
```

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.


Fujitsu RemoteControlService LAN - 192.168.10.10   RX200S2 [SP 192.168.10.11 3172]
File View Window Help
192.168.10.10   RX200S2 [SP 192.168.10.11 3172]
10.171.236.227:3172
10.171.236.81
RX200S2
Status : Unknown
NUM

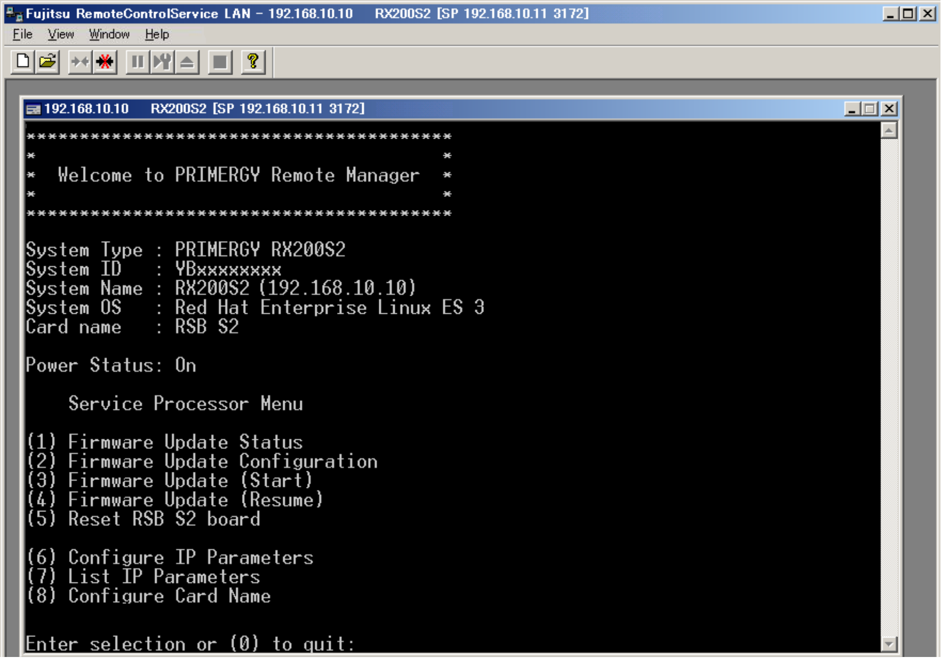
```
****************************************
*                                      *
*  Welcome to PRIMERGY Remote Manager  *
*                                      *
****************************************

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

    System Eventlog Menu

(1) View System Eventlog (newest first)
(2) View System Eventlog (oldest first)
(3) Dump System Eventlog (raw, newest first)
(4) Dump System Eventlog (raw, oldest first)
(5) View System Eventlog Information
(6) Clear System Eventlog


Enter selection or (0) to quit:
```

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
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.

5.4.4 ManagementBlade Telnet Connection

This section describes the support of ManagementBlade through RemoteControleService/Web.

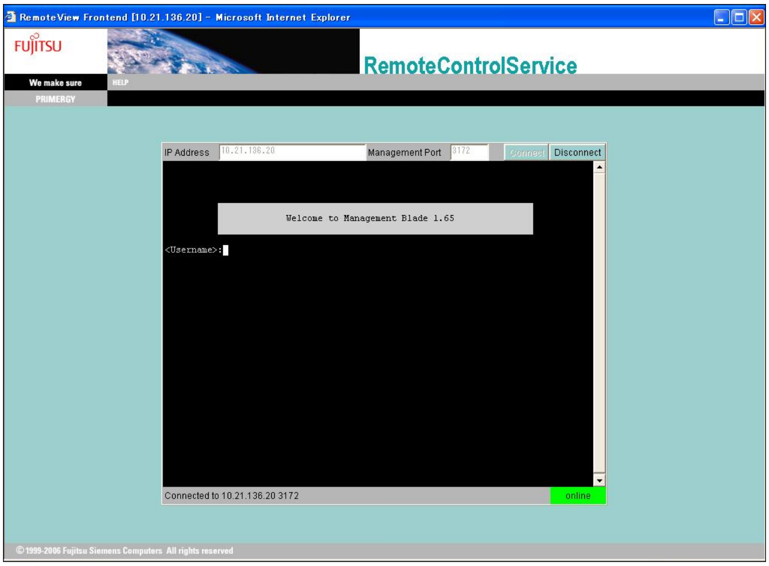
■ Connecting to ManagementBlade

The ManagementBlade includes the Telnet interface called remote manager, which can be connected from RemoteControleService/Web. The remote manager allows you to verify the information about the target server.
Follow the procedure below to connect to the ManagementBlade from RemoteControlService/Web.

IMPORTANT

- Before starting Telnet connection, use a Web interface in the ManagementBlade to enable a Telnet port.

1 Click [connect] from the RemoteConsoleService/Web window. Log in as an account that set for the ManagementBlade.


RemoteView Frontend [10.21.136.20] - Microsoft Internet Explorer
FUJITSU
RemoteControlService
We make sure
HELP
PRIMERGY
Connect
Disconnect
©1999-2006 Fujitsu Siemens Computers All rights reserved

IP Address 10.21.136.20 Management Port 3172

```
Welcome to Management Blade 1.65

<Username>:
```

Connected to 10.21.136.20 3172 online

2 The information can be referred and the following operations can be performed after connecting to ManagementBlade.

■ Main Menu

If the number or character on the left of each item is entered, the corresponding item is executed or its submenu items appear. For details about each item, refer to the manual supplied with the ManagementBlade.

Chapter 6

Using the Remote Service Board

This chapter explains how to use the Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104/PG-RSB105). This is available only for the server on which the Remote Service Board is installed.

6.1 Overview

This chapter explains the Remote Service Board .

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.

6.1.1 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 (Remote Storage functions)

● Communication interfaces supported by the Remote Service Board

- LAN interface
- USB interface

6.1.2 Notes

● Security

The Remote Management Controller handles personal information, such as the administrator’s name, and other important information. If you set up the server in a domain that is accessible from outside, take care of the security so that the specified information is inaccessible from outside and minimize the contents to be set.

● Other 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!

6.2 Preparation

This section explains preparation for using the Remote Service Board.

6.2.1 Setting the LAN Interface

■ For Windows

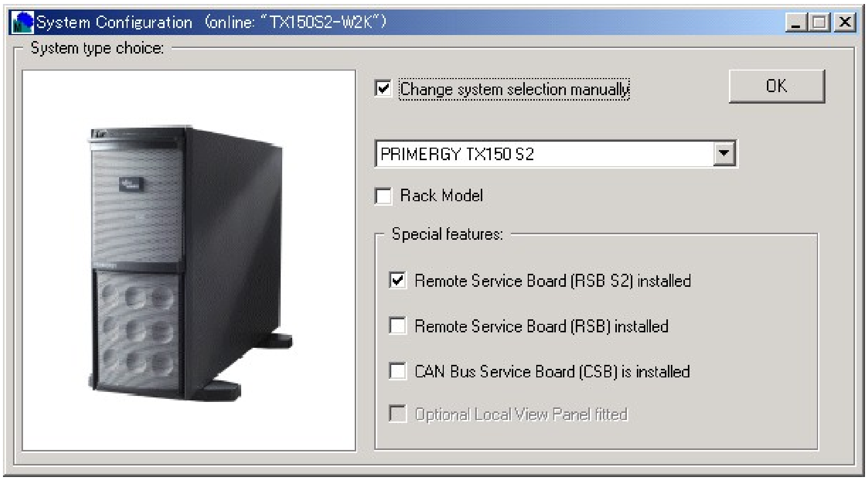
1 Log in to the server using the local user account belonging to the local Administrators group.

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.



System Configuration (online: "TX150S2-W2K")

System type choice:

☑ Change system selection manually

PRIMERGY TX150 S2

☐ Rack Model

Special features:

☑ Remote Service Board (RSB S2) installed

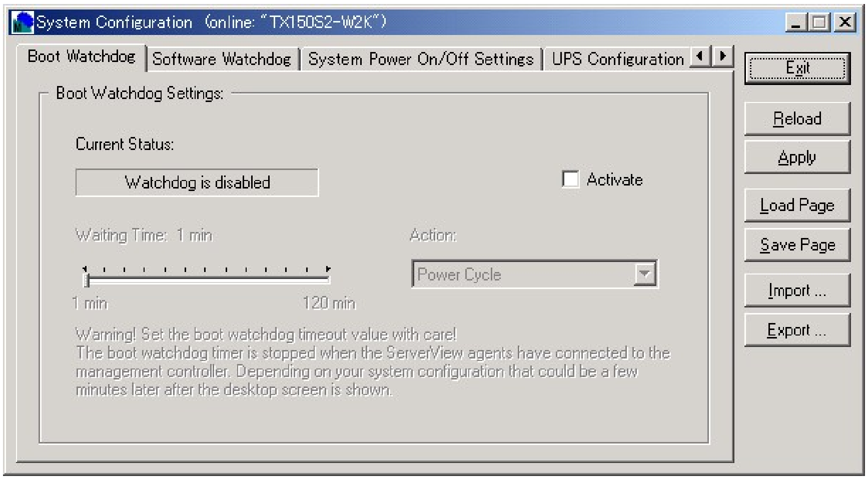
☐ Remote Service Board (RSB) installed

☐ CAN Bus Service Board (CSB) is installed

☐ Optional Local View Panel fitted

4 Check the [Change system selection manually] and [Remote Service Board (RSB S2) installed] checkboxes and click [OK].

The following window appears.



Boot Watchdog Settings:

Current Status:

Watchdog is disabled

□ Activate

Waiting Time: 1 min

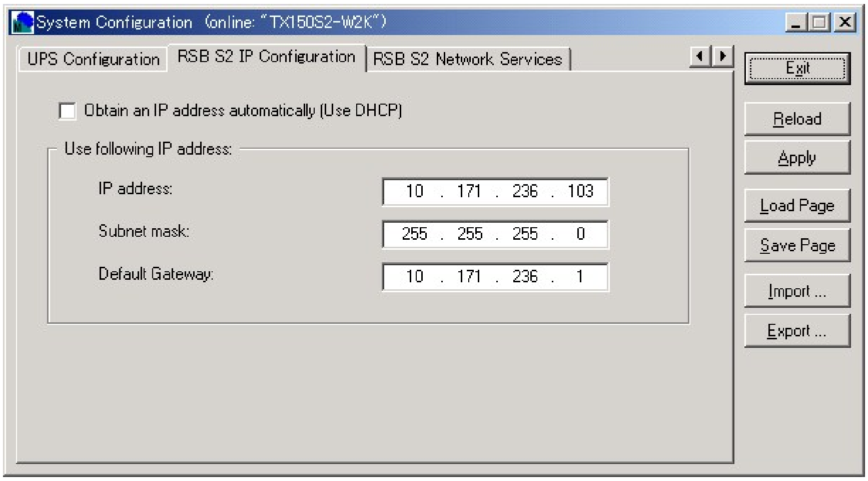
Action:

1 min 120 min

Power Cycle

Warning! Set the boot watchdog timeout value with care!
The boot watchdog timer is stopped when the ServerView agents have connected to the management controller. Depending on your system configuration that could be a few minutes later after the desktop screen is shown.

5 Click [▶] and select the [RSB S2 IP Configuration] tab.



□ Obtain an IP address automatically (Use DHCP)

Use following IP address:

IP address:	10 . 171 . 236 . 103
Subnet mask:	255 . 255 . 255 . 0
Default Gateway:	10 . 171 . 236 . 1

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.

- For Red Hat Linux

```
# /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/LinuxS-
VAgent/Tools/RSB_UTY/rsbs2_utyRedHat
```

- For SUSE Linux

```
# /media/cdrom/ or /media/dvd/Svmanage/LinuxSVAgent/Tools/RSB_UTY/
rsbs2_utySuSE
```

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/
```

6.2.2 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.316).

● 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 addtion to the disk image size.

■ 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 either of the following folder to the installation destination folder on the server:

[CD-ROM Drive]:\Svmanage\WinSVConsole\Tools\management_server
or
[CD-ROM Drive]:\Svmanage\LinuxSVConsole\Tools\management_server

■ 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".

IMPORTANT

- 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.

6.2.3 Configurating the Directory Service Function

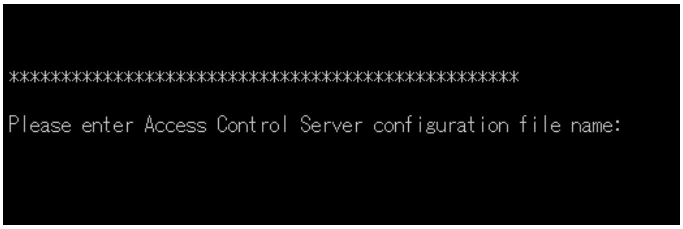
This section explains the settings necessary for using the directory service function.

■ 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:



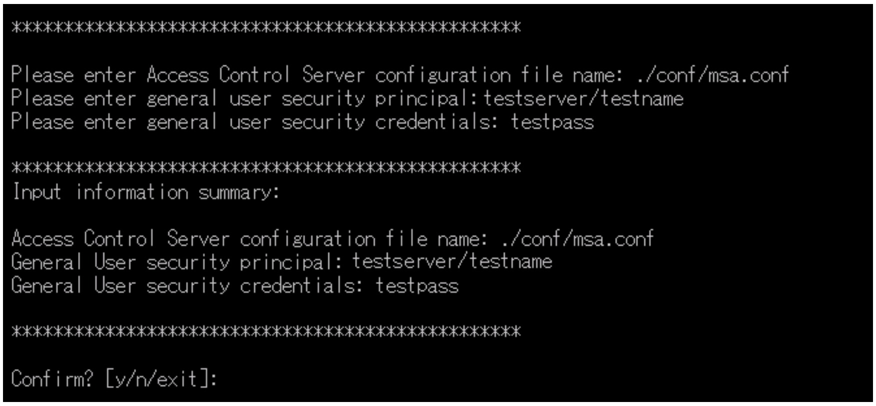
```
*************************************************

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:

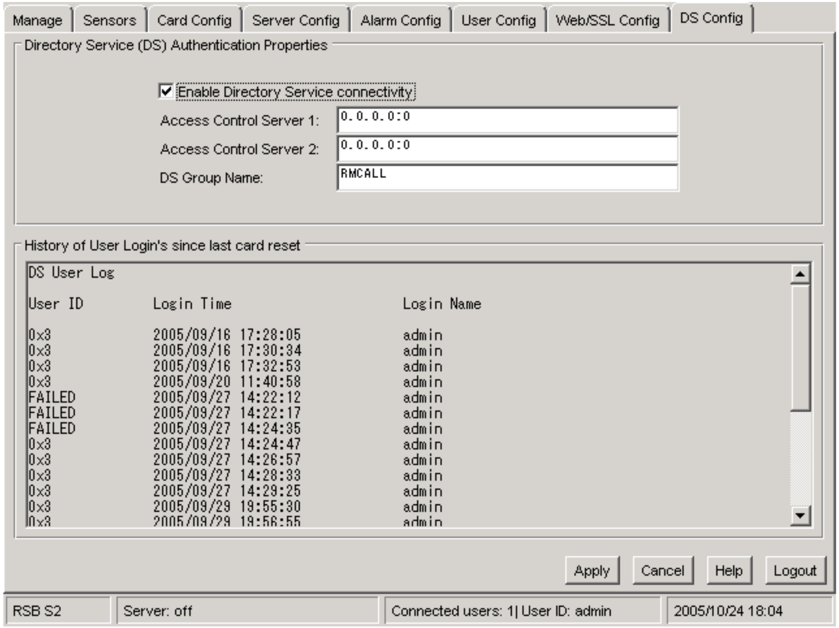


```
*************************************************

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: 0.0.0.0:0

Access Control Server 2: 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            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
```

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.

6.3 Displaying Each Monitoring Information

This section explains how to display server monitoring information using the Web interface.

6.3.1 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

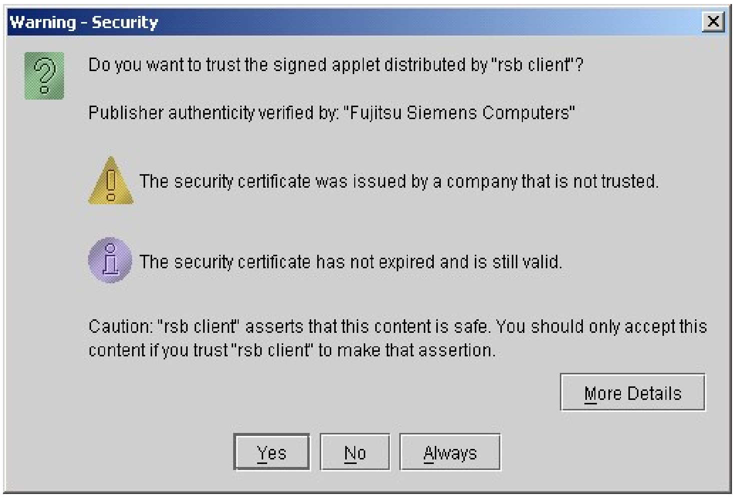
- To use a Web browser, it must be installed and set in advance. Refer to "2.4.1 Installing a Web Browser" (→pg.62) and "2.4.2 Installing Java™ 2 Runtime Environment Standard Edition" (→pg.63).
- Please download Java™ 2 Runtime Enviroment Standard Edition V1.4.2_08 (or later) from HP of Sun Microsystems.

6
Using the Remote Service Board

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:



Warning - Security

Do you want to trust the signed applet distributed by "rsb client"?

Publisher authenticity verified by: "Fujitsu Siemens Computers"

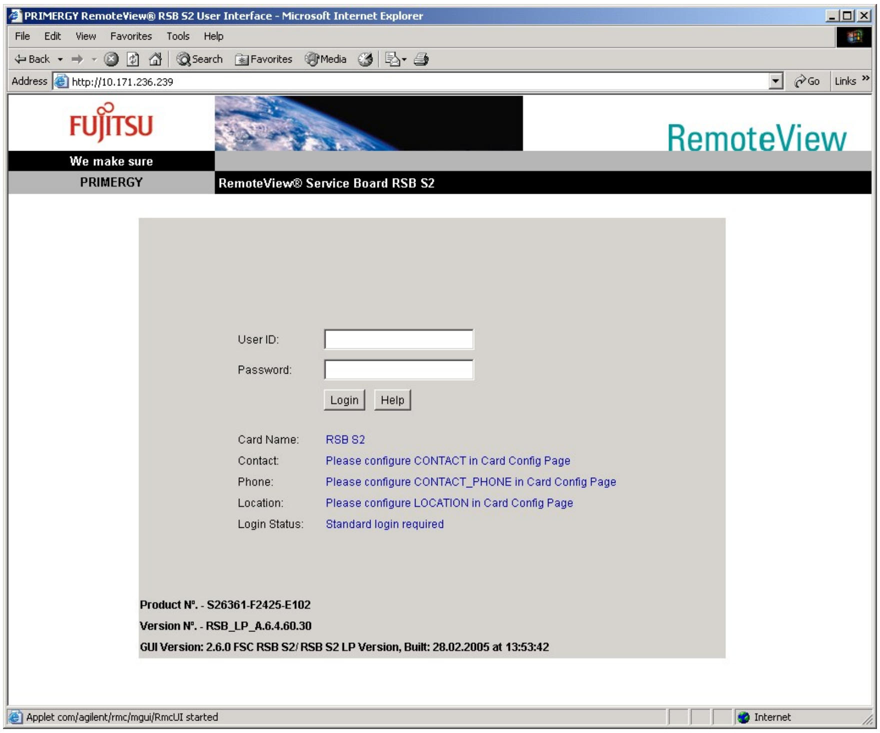
The security certificate was issued by a company that is not trusted.

The security certificate has not expired and is still valid.

Caution: "rsb client" asserts that this content is safe. You should only accept this content if you trust "rsb client" to make that assertion.

2 Click [Yes].

The login window appears.



PRIMERGY RemoteView® RSB S2 User Interface - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.171.236.239
Go Links
FUJITSU
We make sure
PRIMERGY
RemoteView
RemoteView® Service Board RSB S2

User ID:

Password:

Card Name: RSB S2

Contact: Please configure CONTACT in Card Config Page

Phone: Please configure CONTACT_PHONE in Card Config Page

Location: Please configure LOCATION in Card Config Page

Login Status: Standard login required

Product N°. - S26361-F2425-E102

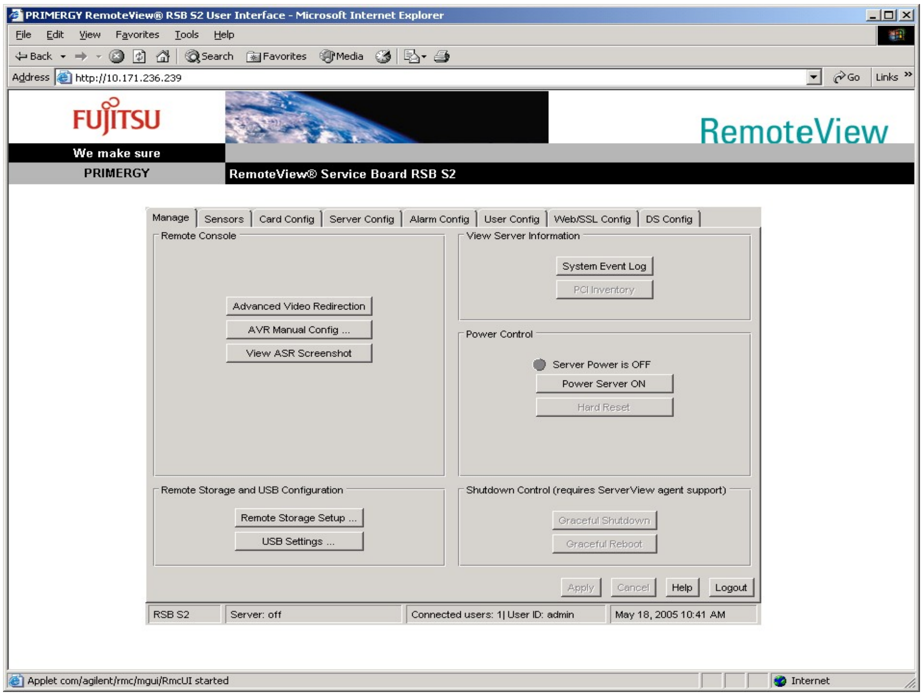
Version N°. - RSB_LP_A.6.4.60.30

GUI Version: 2.6.0 FSC RSB S2/ RSB S2 LP Version, Built: 28.02.2005 at 13:53:42

Applet com/agilent/rmc/mgui/RmcUI started

3 Enter the [User ID] and [Password].

After authentication succeeds, the following window appears:



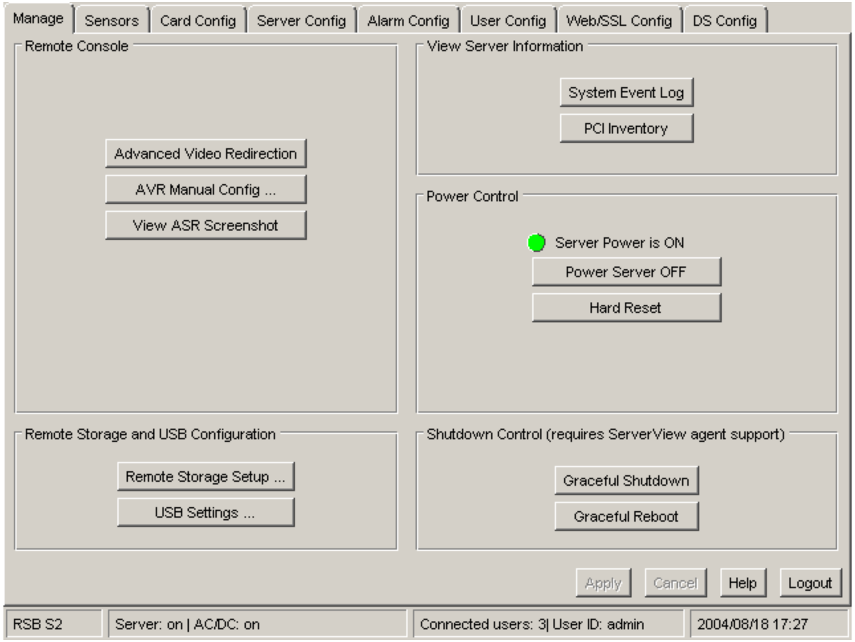
RSB S2 | Server: off | Connected users: 1| User ID: admin | May 18, 2005 10:41 AM

Applet com/agilent/rmc/mgui/RmcUI started

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.

6.3.2 [Manage] Page

The [Manage] page is available for setting how to display images and controlling power supply.



RSB S2 | Server: on | AC/DC: on | Connected users: 3| User ID: admin | 2004/08/18 17:27

table: Functions on the [Manage] Page

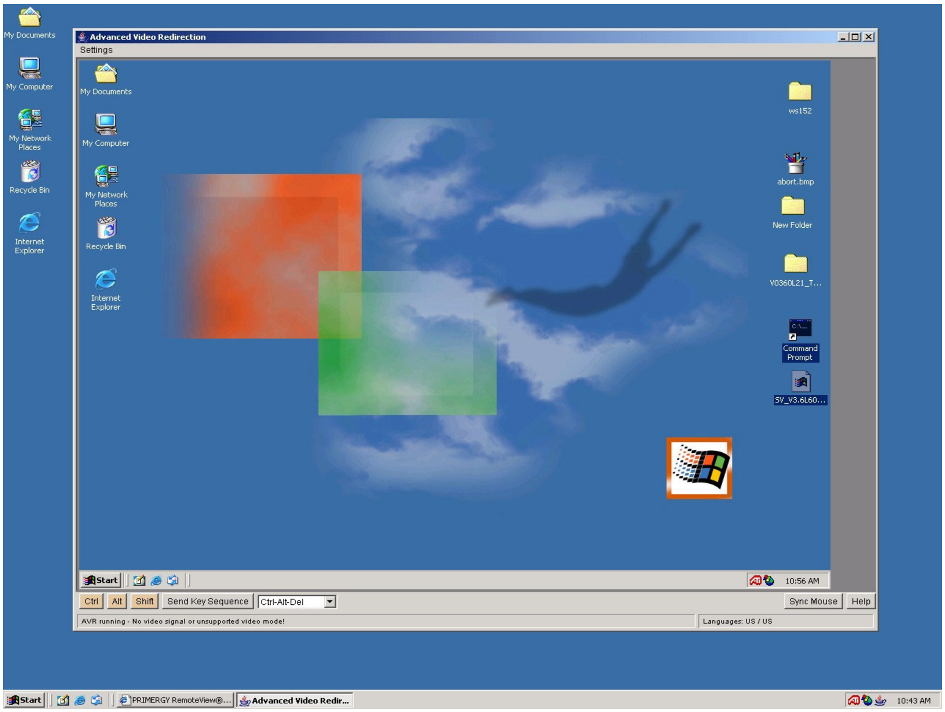
Item	Description
Remote Console	This function allows the server screen to be displayed in the AVR window of the console, and allow server operation from the console.
[Advanced Video Redirection]	Opens the AVR window and starts redirection of the server window. →"■ Advanced Video Redirection (AVR) Functions" (pg.307)
[AVR Manual Config ...]	Available for setting AVR functions. →"■ AVR Manual Configuration" (pg.310)
[View ASR Screenshot]	Displays the screenshot of the server window captured at watchdog detection. →"■ View ASR Screenshot" (pg.311)
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.312)
USB Setting	Available for setting USB functions. →"■ USB Settings" (pg.324)
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	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. POINT ▶ If the OS freezes, this may be the same as [Graceful Shutdown] for PG-RSB104/PG-RSB105. 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.



AVR running - No video signal or unsupported video mode!

Languages: US / US

POINT

- 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.

  IMPORTANT

  - Since the configuration utility [WebBIOS] window of the MegaRAID SCSI RAID card uses its original mouse driver, proper mouse operation is not available for Advaced 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

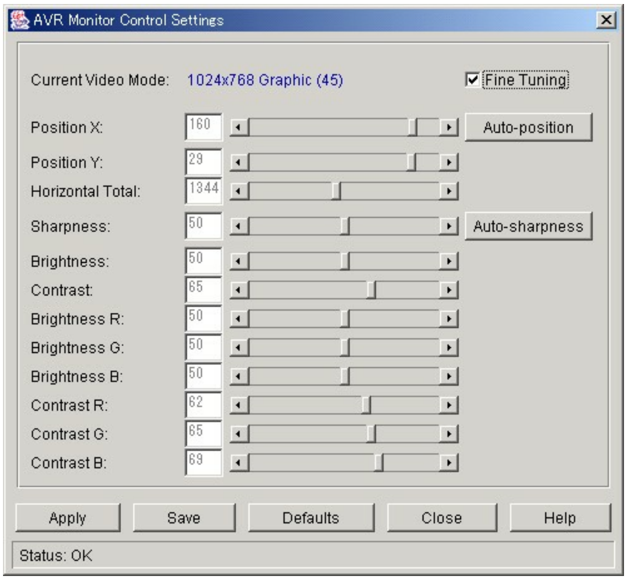
Item		Description
Display		Setting items related to window display.
	Monitor Controls	Opens the " [AVR Monitor Controls Settings] window" (→pg.309). Available for setting AVR window display.
	Video Capture Parameters	Opens the " [AVR Video Capture Settings] window" (→pg.310). Available for setting the 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.

IMPORTANT

- 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.



AVR Monitor Control Settings

Current Video Mode: 1024x768 Graphic (45)

☑ Fine Tuning

Position X: 160

Position Y: 29

Horizontal Total: 1344

Sharpness: 50

Brightness: 50

Contrast: 65

Brightness R: 50

Brightness G: 50

Brightness B: 50

Contrast R: 62

Contrast G: 65

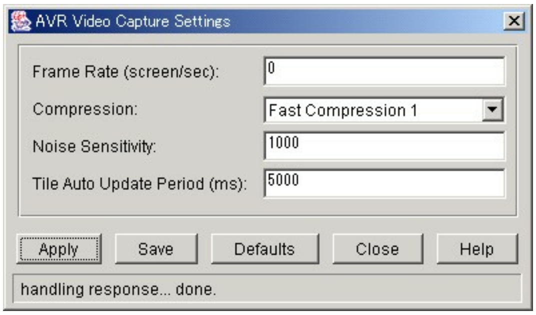
Contrast B: 69

Status: OK

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.


AVR Video Capture Settings

Frame Rate (screen/sec): 0

Compression: Fast Compression 1

Noise Sensitivity: 1000

Tile Auto Update Period (ms): 5000

handling response... done.

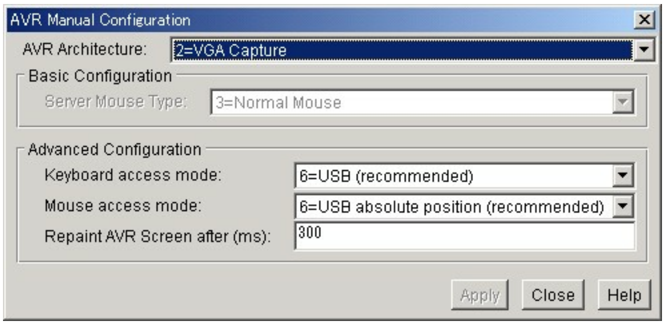
See the following table for settings in [Compression].

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


AVR Manual Configuration

AVR Architecture: 2=VGA Capture

Basic Configuration

Server Mouse Type: 3=Normal Mouse

Advanced Configuration

Keyboard access mode: 6=USB (recommended)

Mouse access mode: 6=USB absolute position (recommended)

Repaint AVR Screen after (ms): 300

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

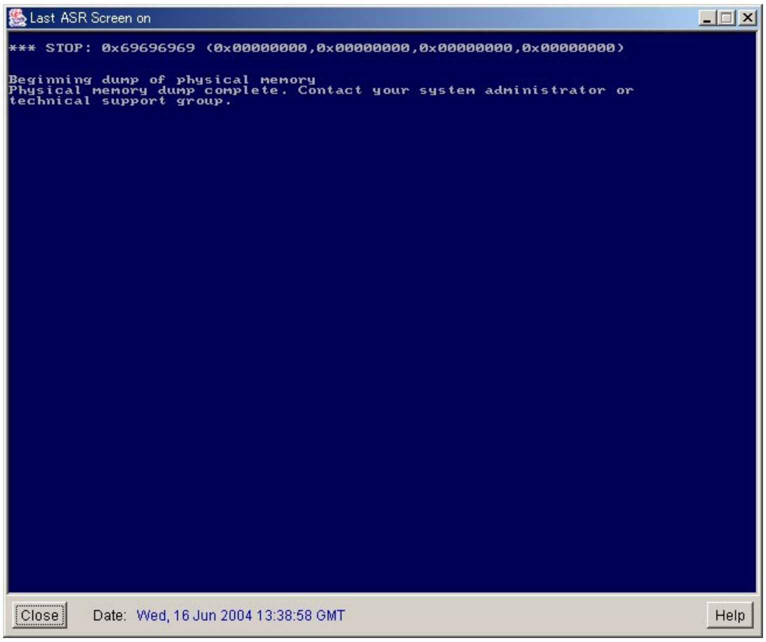
Item	Description
Repaint AVR Screen after (ms)	Set the update interval of the AVR window. Normally, it is not necessary to be changed from the default value (300).

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.



```
*** STOP: 0x69696969 (0x00000000,0x00000000,0x00000000,0x00000000)

Beginning dump of physical memory
Physical memory dump complete. Contact your system administrator or
technical support group.
```

Date: Wed, 16 Jun 2004 13:38:58 GMT

POINT

- [View ASR Screenshot] does not show the server window in real-time. Keyboard and mouse operations are not available.
- [View ASR Screenshot] is received at the timing of Watchdog detection. Enable the Watchdog of Software or Boot in the Watchdog settings of ServerView.
- The window received by the [View ASR Screenshot] function is deleted when the server is restarted normally next time.
- 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.
- 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.312)
- Connection to a drive or other devices on an "iSCSI server"
  →"● iSCSI connection" (pg.316)

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:

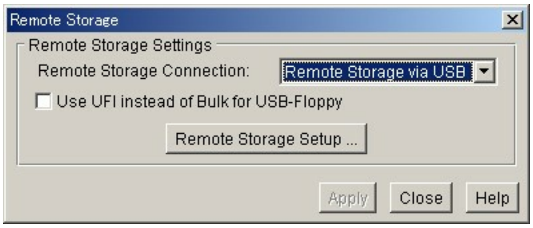
POINT

- [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/PG-RSB104/PG-RSB105, 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:].

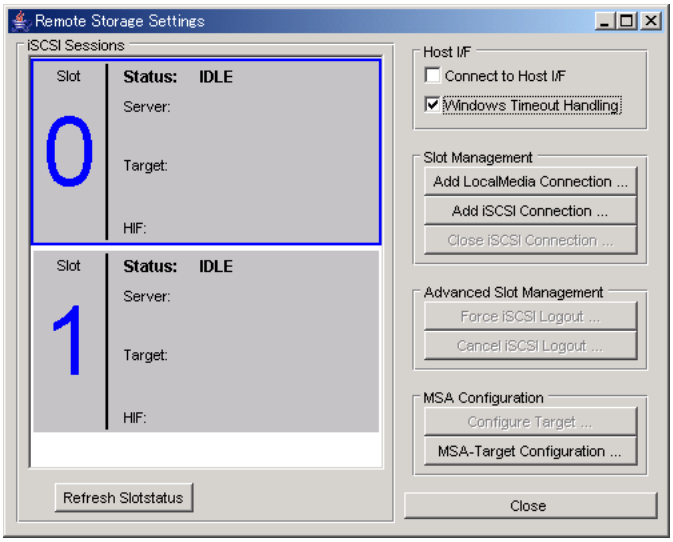
IMPORTANT

- 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.

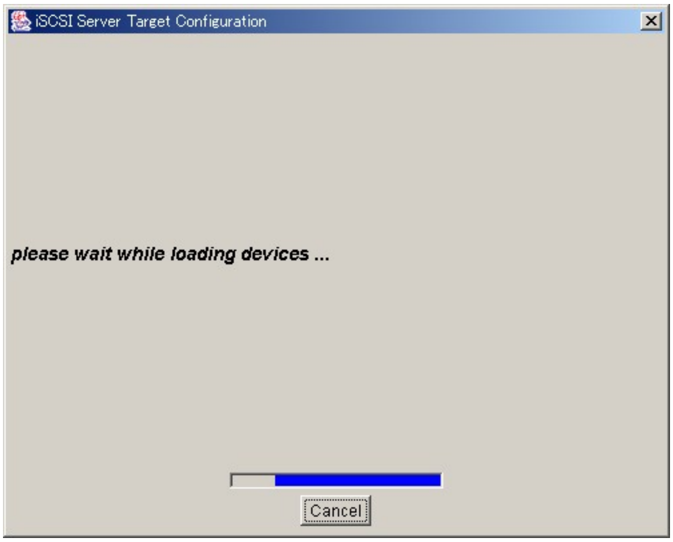
3 Click [Remote Storage Setup].

The following window appears.



4 Select a slot and click [Add Local Media Connection].

Search for drives on the console starts.

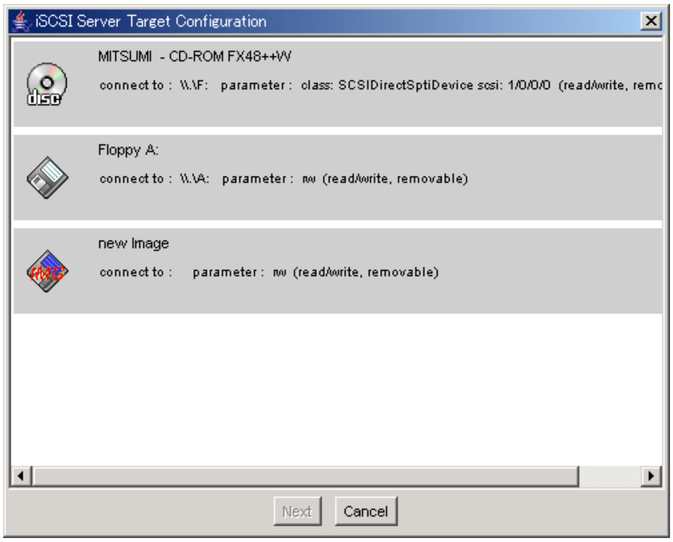


please wait while loading devices ...

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].



MITSUMI - CD-ROM FX48++W

connect to : \\.\F: parameter : class: SCSIDirectSptiDevice scsi: 1/0/0/0 (read/write, remc

Floppy A:

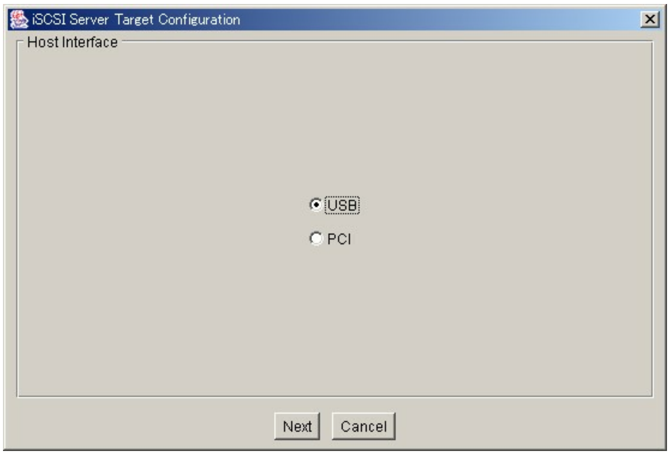
connect to : \\.\A: parameter : rw (read/write, removable)

new Image

connect to : parameter : rw (read/write, removable)

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



iSCSI Server Target Configuration

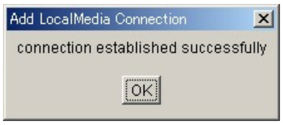
Host Interface

● USB

○ PCI

1. A window appears for selecting a connection interface. Select [USB] and click [Next].

   After connection succeeds, the following window appears:

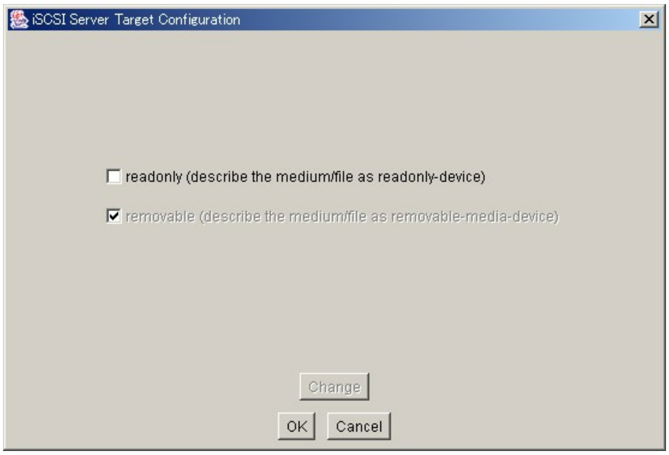


Add LocalMedia Connection

connection established successfully

2. Click [OK].

Example: Floppy disk



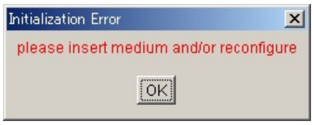
iSCSI Server Target Configuration

□ readonly (describe the medium/file as readonly-device)

☑ removable (describe the medium/file as removable-media-device)

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:

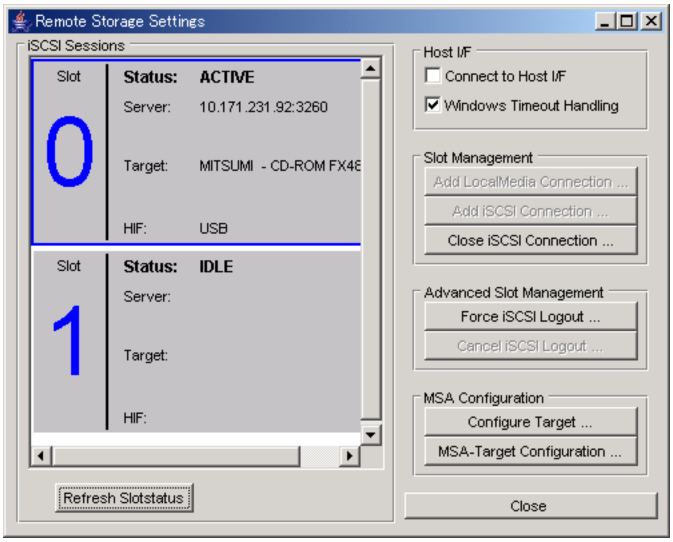


Initialization Error

please insert medium and/or reconfigure

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.



Slot 0
Status: ACTIVE
Server: 10.171.231.92:3260
Target: MITSUMI - CD-ROM FX48
HIF: USB

Slot 1
Status: IDLE
Server:
Target:
HIF:

☐ Connect to Host I/F
☑ Windows Timeout Handling

[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 "6.2.2 Installation and Configuration of the Management Server Application (MSA)" (→pg.299).

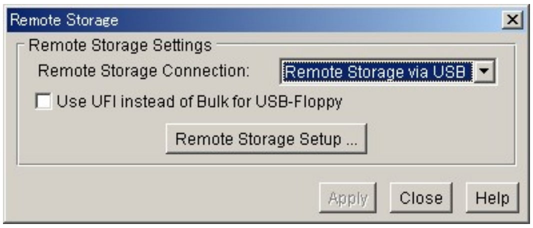
POINT

- 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/PG-RSB104/PG-RSB105, begin from Step 3.

1 Click [Remote Storage Setup].

The following window appears.



Remote Storage

Remote Storage Settings

Remote Storage Connection: Remote Storage via USB

☐ Use UFI instead of Bulk for USB-Floppy

2 Set the communication interface between the server and Remote Service Board.

Set [Remote Storage via USB] to [Remote Storage Connection:].

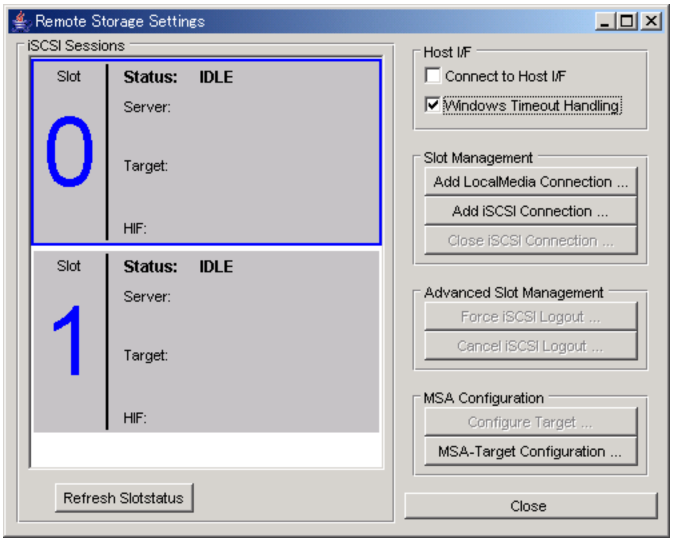
IMPORTANT

- 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 between the Remote Service Board and server.

3 Click [Remote Storage Setup].

The [Remote Storage Settings] window appears.



Remote Storage Settings

iSCSI Sessions

Slot 0 Status: IDLE
Server:
Target:
HIF:

Slot 1 Status: IDLE
Server:
Target:
HIF:

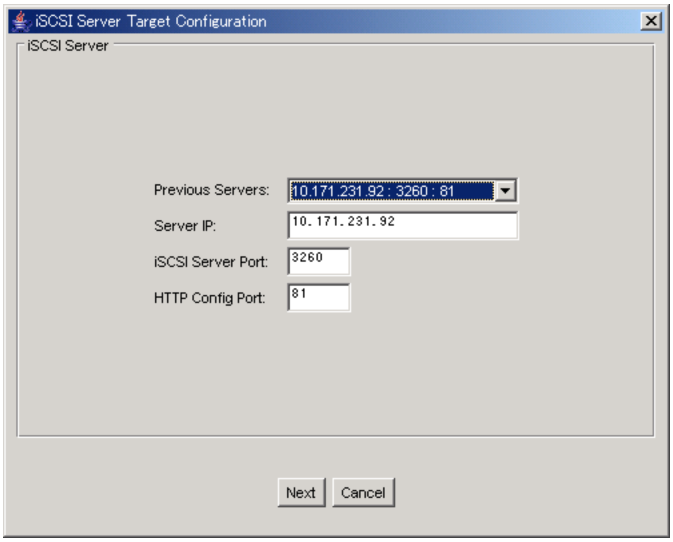
Host I/F

☐ Connect to Host I/F

☑ Windows Timeout Handling

4 Click [MSA- Target Configuration].

The following window appears.



iSCSI Server Target Configuration

iSCSI Server

Previous Servers: 10.171.231.92 : 3260 : 81

Server IP: 10.171.231.92

iSCSI Server Port: 3260

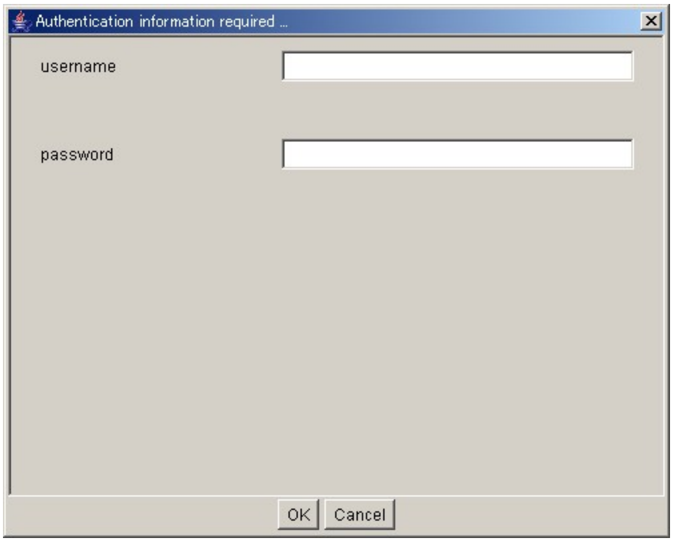
HTTP Config Port: 81

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.



Authentication information required ...

username

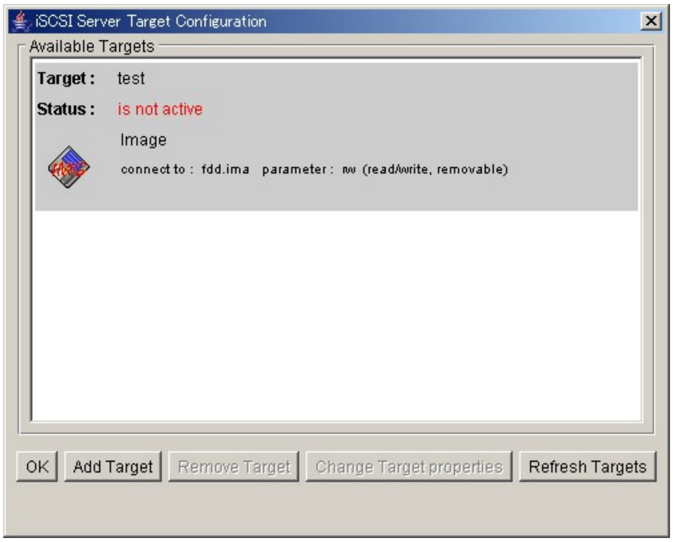
password

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.



iSCSI Server Target Configuration

Available Targets

Target : test

Status : is not active

Image

connect to : fdd.ima parameter : rw (read/write, removable)

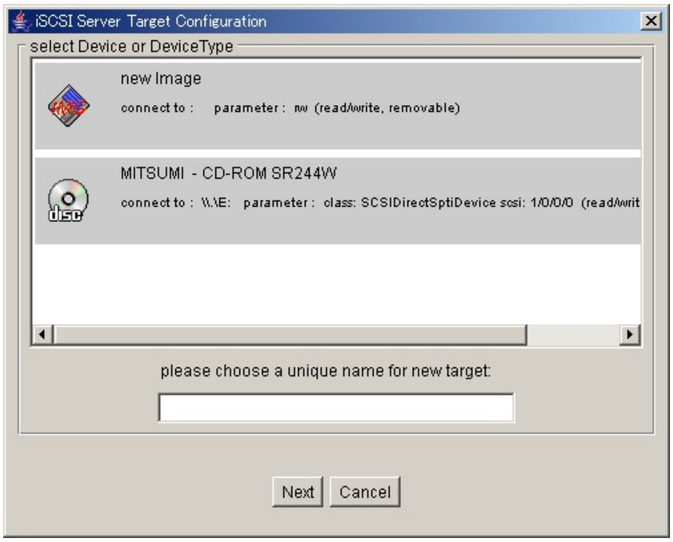
7 Create an iSCSI target object.

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.



iSCSI Server Target Configuration

select Device or DeviceType

new Image

connect to : parameter : rw (read/write, removable)

MITSUMI - CD-ROM SR244W

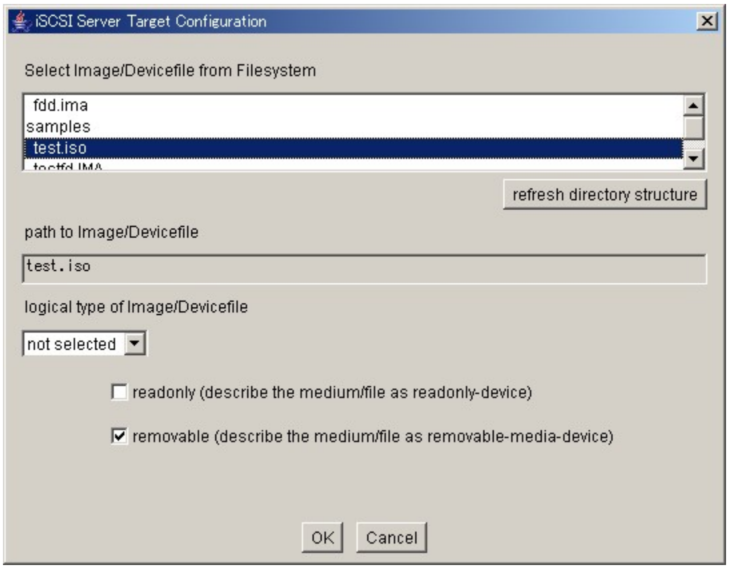
connect to : \\.\E: parameter : class: SCSIDirectSptiDevice scsi: 1/0/0/0 (read/writ

please choose a unique name for new target:

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.



iSCSI Server Target Configuration

Select Image/Devicefile from Filesystem

fdd.ima
samples
test.iso

path to Image/Devicefile: test.iso

logical type of Image/Devicefile: not selected

☐ readonly (describe the medium/file as readonly-device)

☑ removable (describe the medium/file as removable-media-device)

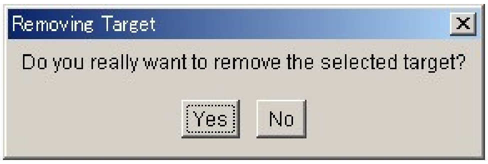
3. Select an image file, select a file type from the [Logical type of image/devicefile] list, and click [OK].

   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.



Removing Target

Do you really want to remove the selected target?

2. Click [Yes].

   The selected target object is removed.

Changing iSCSI target object settings

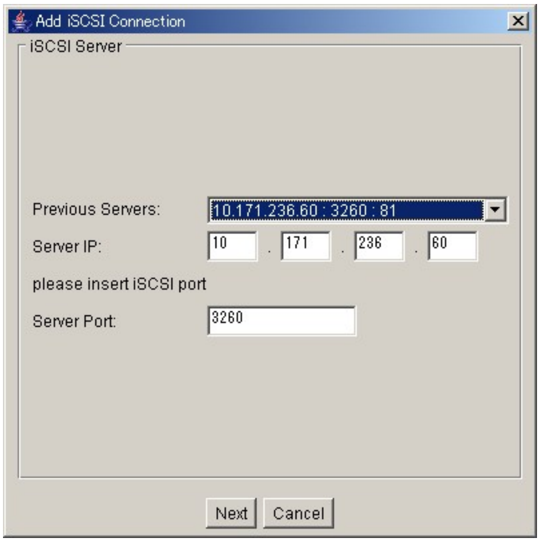
1. Select a target object to be changed and click [Change Target properties].

   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.



Previous Servers: 10.171.236.60 : 3260 : 81

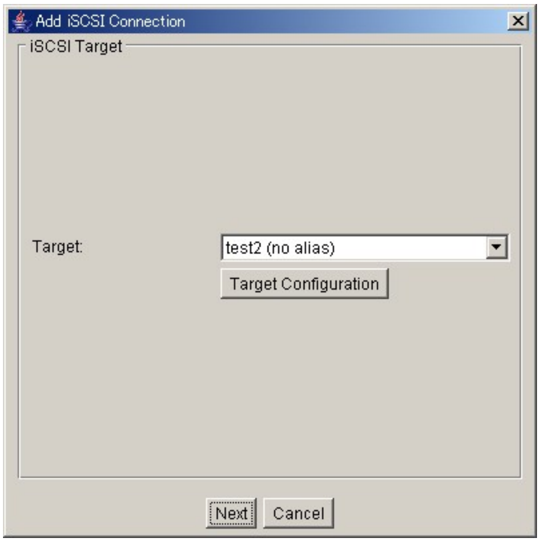
Server IP: 10 . 171 . 236 . 60

please insert iSCSI port

Server Port: 3260

9 Select the iSCSI server set in Step 4 to [Previous Servers] and click [Next].

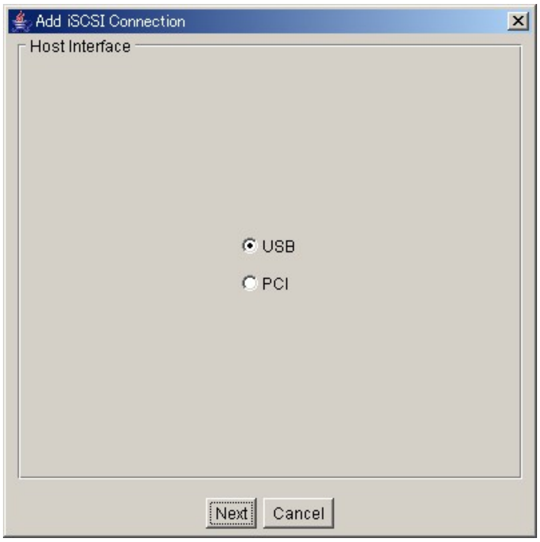
A window appears for selecting a target object.



Target: test2 (no alias)

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/PG-RSB105, this window does not appear. The window in step11 appears.

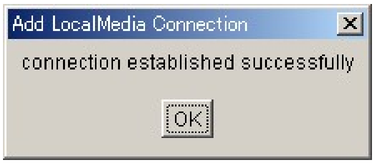


POINT

- 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].

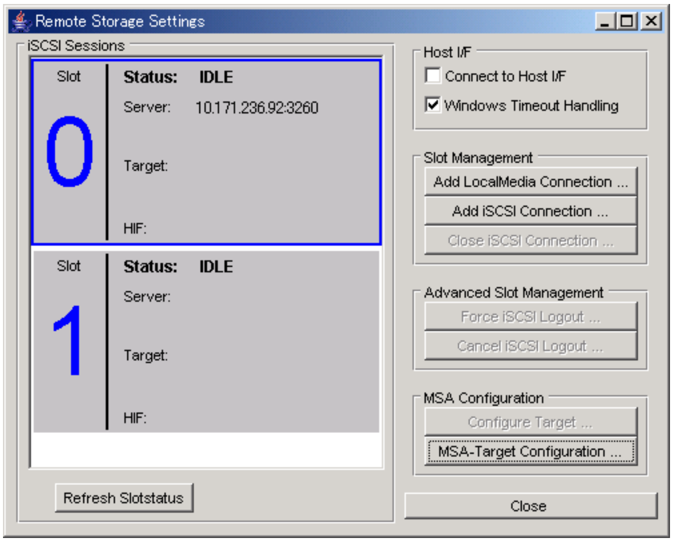
After connection succeeds, the following window appears:


Add LocalMedia Connection

connection established successfully

12 Click [OK] to return to the [Remote Storage Settings] window.

Make sure that the device information has been added.



Remote Storage Settings

iSCSI Sessions

Slot 0
Status: IDLE
Server: 10.171.236.92:3260
Target:
HIF:

Slot 1
Status: IDLE
Server:
Target:
HIF:

Host I/F
☐ Connect to Host I/F
☑ Windows Timeout Handling

[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.

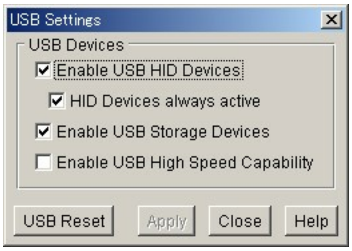
13 Select the slot marked [ACTIVE], check [Connect to Host I/F], and click [Configure Target].

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.



USB Settings

USB Devices

☑ Enable USB HID Devices

☑ HID Devices always active

☑ Enable USB Storage Devices

☐ Enable USB High Speed Capability

table: USB Function Settings

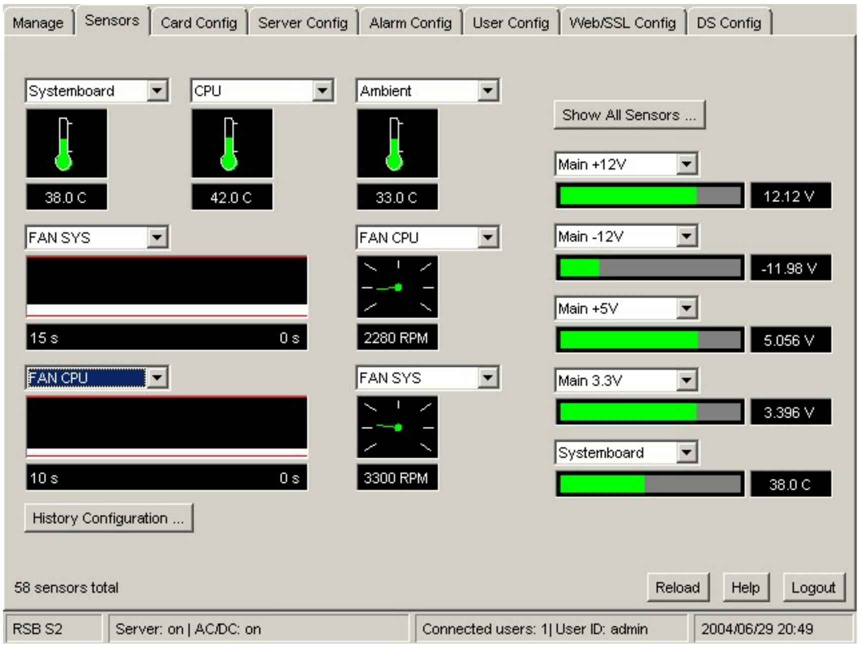
Item	Description
Enable USB HID Devices	Enables keyboard and mouse via USB. Make sure to check this checkbox to use AVR.
HID Devices always active	Check this checkbox if USB hot plug is not supported by the server BIOS.
Enable USB Storage Devices	Enables RemoteStorage via USB. Check this checkbox to use RemoteStorage.
Enable USB High Speed Capability	Enables high speed storage for RemoteStorage via USB.

POINT

- When “Enable USB Hige Speed Capabillity” is check, the keyboard and the mouse of USB might not be able to use it. In this case, this item check is removed.

6.3.3 [Sensors] Page

The [Sensors] page is available for viewing values of each sensor of the server.



Systemboard 38.0 C

CPU 42.0 C

Ambient 33.0 C

FAN SYS 15 s 0 s

FAN CPU 2280 RPM

FAN CPU 10 s 0 s

FAN SYS 3300 RPM

Main +12V 12.12 V

Main -12V -11.98 V

Main +5V 5.056 V

Main 3.3V 3.396 V

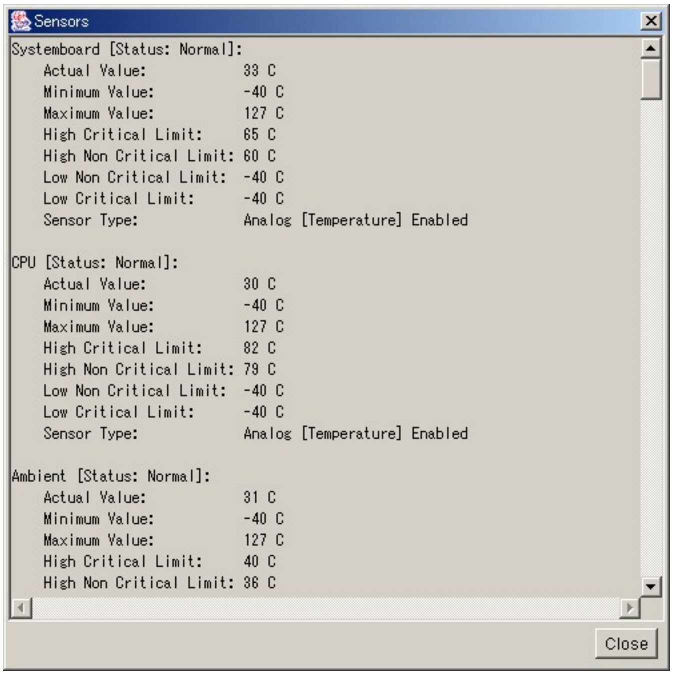
Systemboard 38.0 C

58 sensors total

RSB S2 | Server: on | AC/DC: on | Connected users: 1| User ID: admin | 2004/06/29 20:49

[Show All Sensors ...]

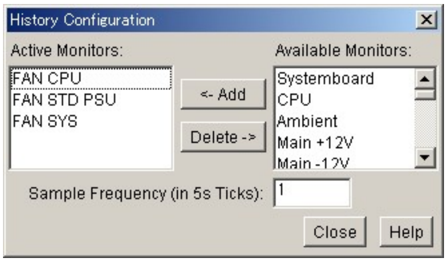
Shows values of all sensors.



```
Systemboard [Status: Normal]:
    Actual Value:             33 C
    Minimum Value:            -40 C
    Maximum Value:            127 C
    High Critical Limit:      65 C
    High Non Critical Limit:  60 C
    Low Non Critical Limit:   -40 C
    Low Critical Limit:       -40 C
    Sensor Type:              Analog [Temperature] Enabled

CPU [Status: Normal]:
    Actual Value:             30 C
    Minimum Value:            -40 C
    Maximum Value:            127 C
    High Critical Limit:      82 C
    High Non Critical Limit:  79 C
    Low Non Critical Limit:   -40 C
    Low Critical Limit:       -40 C
    Sensor Type:              Analog [Temperature] Enabled

Ambient [Status: Normal]:
    Actual Value:             31 C
    Minimum Value:            -40 C
    Maximum Value:            127 C
    High Critical Limit:      40 C
    High Non Critical Limit:  36 C
```

[History Configuration ...]

Shows values of a sensor at a certain frequency. The following window appears after [History Configuration ...] is clicked:



Active Monitors:
FAN CPU
FAN STD PSU
FAN SYS

Available Monitors:
Systemboard
CPU
Ambient
Main +12V
Main -12V

Sample Frequency (in 5s Ticks): 1

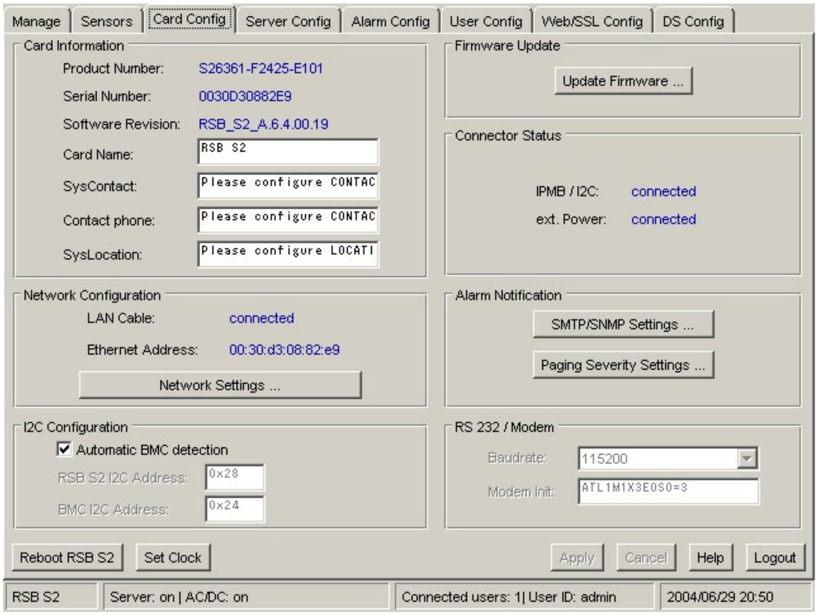
Select a target sensor from [Available Monitors] and click [<-Add] to add it to [Active Monitors]. The added sensor can be selected from the pull-down menu on the upper part of the window.

[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.

6.3.4 [Card Config] Page

The [Card Config] page is available for setting the Remote Service Board or checking its state.



Product Number: S26361-F2425-E101

Serial Number: 0030D30882E9

Software Revision: RSB_S2_A.6.4.00.19

Card Name: RSB S2

SysContact: Please configure CONTAC

Contact phone: Please configure CONTAC

SysLocation: Please configure LOCATI

IPMB / I2C: connected

ext. Power: connected

LAN Cable: connected

Ethernet Address: 00:30:d3:08:82:e9

☑ Automatic BMC detection

RSB S2 I2C Address: 0x28

BMC I2C Address: 0x24

Baudrate: 115200

Modem Init: ATL1M1X3E0S0=3

RSB S2 | Server: on | AC/DC: on | Connected users: 1 | User ID: admin | 2004/06/29 20:50

table: Functions on the [Card Config] Page

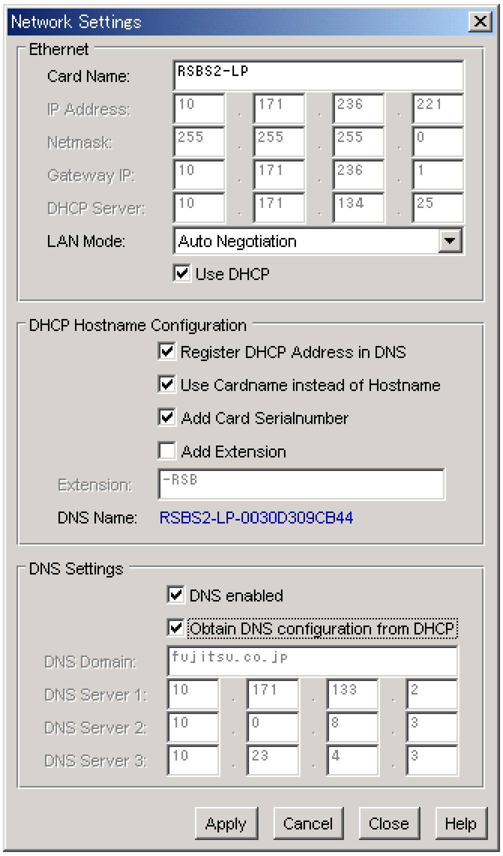
Item		Description
Card Information		Information related to the Remote Service Board.
	Product Number	Displays the product number of the Remote Service Board.
	Serial Number	Displays the serial number of the Remote Service Board.
	Software Revision	Version of the firmware applied to the Remote Service 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.327)
	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.328) Click [Paging Severity Settings ...] to set severities for each group. →"■ Paging Severity Setting" (pg.328)
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

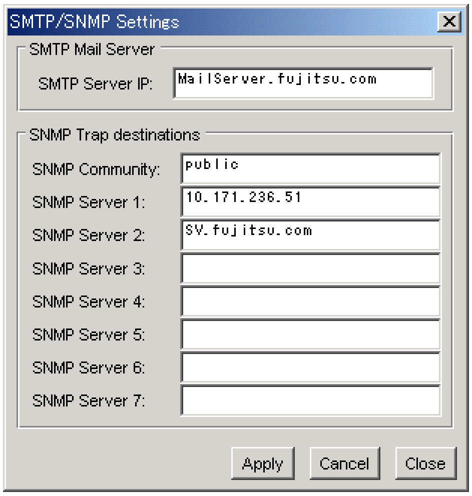
DNS Server 2: 10 . 0 . 8 . 3

DNS Server 3: 10 . 23 . 4 . 3

■ 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 Mail Server

SMTP Server IP: MailServer.fujitsu.com

SNMP Trap destinations

SNMP Community:	public
SNMP Server 1:	10.171.236.51
SNMP Server 2:	SV.fujitsu.com
SNMP Server 3:	
SNMP Server 4:	
SNMP Server 5:	
SNMP Server 6:	
SNMP Server 7:	

- SMTP Server IP

  The Remote Service Board sends mail to the SMTP server set here.

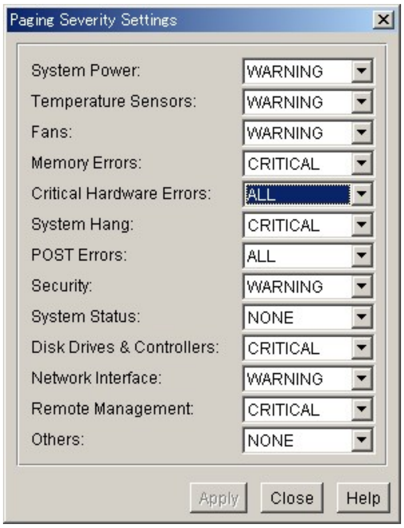
  Use the [Alarm Config] page for detailed settings such as mail destinations.

- SNMP Trap destinations

  Set destination IP addresses of SNMP traps sent by the Remote Service Board.

■ Paging Severity Setting

Set values (severities) to trigger E-mail of SEL writing for each group.



System Power:	WARNING
Temperature Sensors:	WARNING
Fans:	WARNING
Memory Errors:	CRITICAL
Critical Hardware Errors:	ALL
System Hang:	CRITICAL
POST Errors:	ALL
Security:	WARNING
System Status:	NONE
Disk Drives & Controllers:	CRITICAL
Network Interface:	WARNING
Remote Management:	CRITICAL
Others:	NONE

E-mail is triggered when each group reaches the set severity. Each severity means as follows:

table: Severity Settings

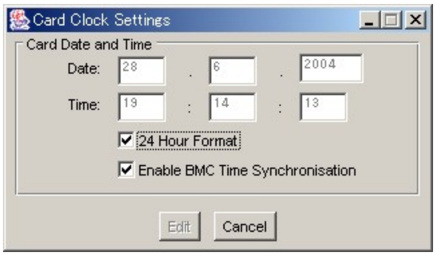
Item	Description
None	E-mail of SEL writing is not triggered.
Critical	E-mail of SEL writing is triggered by events at the critical and higher levels.
Warning	E-mail of SEL writing is triggered by events at the warning and higher levels.
All	E-mail of SELwriting is triggered by all severities.

■ [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:



Card Clock Settings

Card Date and Time

Date: 28 . 6 . 2004

Time: 19 : 14 : 13

☑ 24 Hour Format

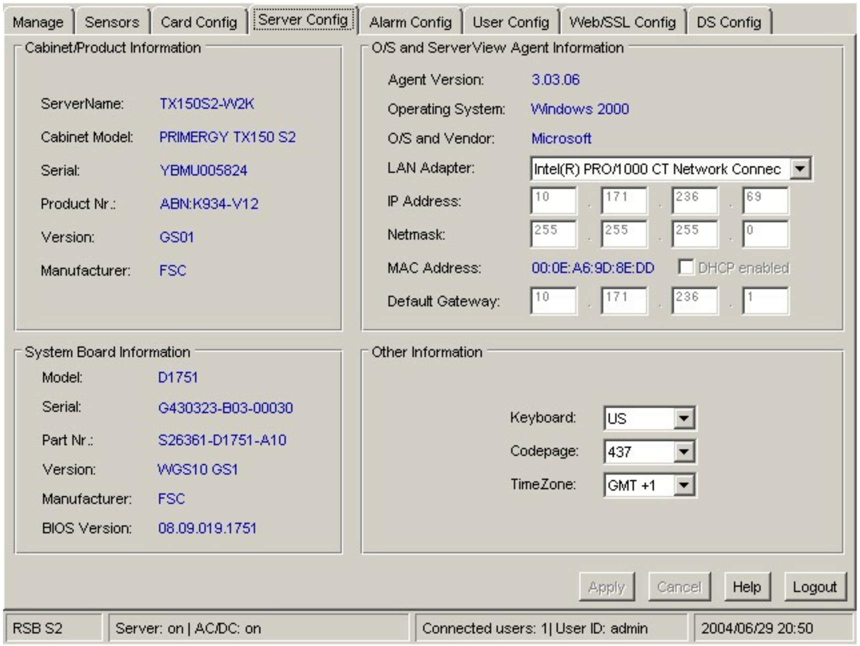
☑ Enable BMC Time Synchronisation

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.

6.3.5 [Server Config] Page

Obtains and displays various server information.



Cabinet/Product Information

ServerName: TX150S2-W2K
Cabinet Model: PRIMERGY TX150 S2
Serial: YBMU005824
Product Nr.: ABN:K934-V12
Version: GS01
Manufacturer: FSC

O/S and ServerView Agent Information

Agent Version: 3.03.06
Operating System: Windows 2000
O/S and Vendor: Microsoft
LAN Adapter: Intel(R) PRO/1000 CT Network Connec
IP Address: 10 . 171 . 236 . 69
Netmask: 255 . 255 . 255 . 0
MAC Address: 00:0E:A6:9D:8E:DD ☐ DHCP enabled
Default Gateway: 10 . 171 . 236 . 1

System Board Information

Model: D1751
Serial: G430323-B03-00030
Part Nr.: S26361-D1751-A10
Version: WGS10 GS1
Manufacturer: FSC
BIOS Version: 08.09.019.1751

Other Information

Keyboard: US
Codepage: 437
TimeZone: GMT +1

RSB S2 | Server: on | AC/DC: on | Connected users: 1| User ID: admin | 2004/06/29 20:50

table: Functions on the [Server Config] Page

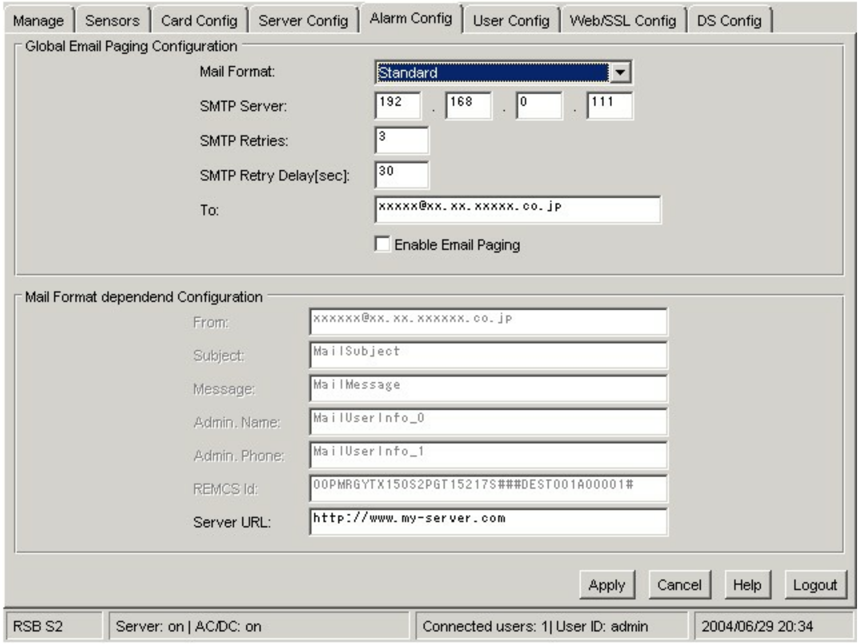
Item		Description
Cabinet/Product Information		Displays cabinet/product information.
	Server Name	Displays the server name.
	Model	Displays the model name.
	Serial	Displays the serial number.
	Product Nr	Displays the product number.
	Version	Displays version information.
	Manufacturer	Displays the manufacturer 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.

6.3.6 [Alarm Config] Page

Set alarm functions.



Global Email Paging Configuration

Mail Format: Standard

SMTP Server: 192 . 168 . 0 . 111

SMTP Retries: 3

SMTP Retry Delay[sec]: 30

To: xxxxx@xx.xx.xxxxx.co.jp

□ Enable Email Paging

Mail Format dependend Configuration

From: xxxxxx@xx.xx.xxxxxx.co.jp

Subject: MailSubject

Message: MailMessage

Admin. Name: MailUserInfo_0

Admin. Phone: MailUserInfo_1

REMCS Id: 00PMRGYTX150S2PGT15217S###DEST001A00001#

Server URL: http://www.my-server.com

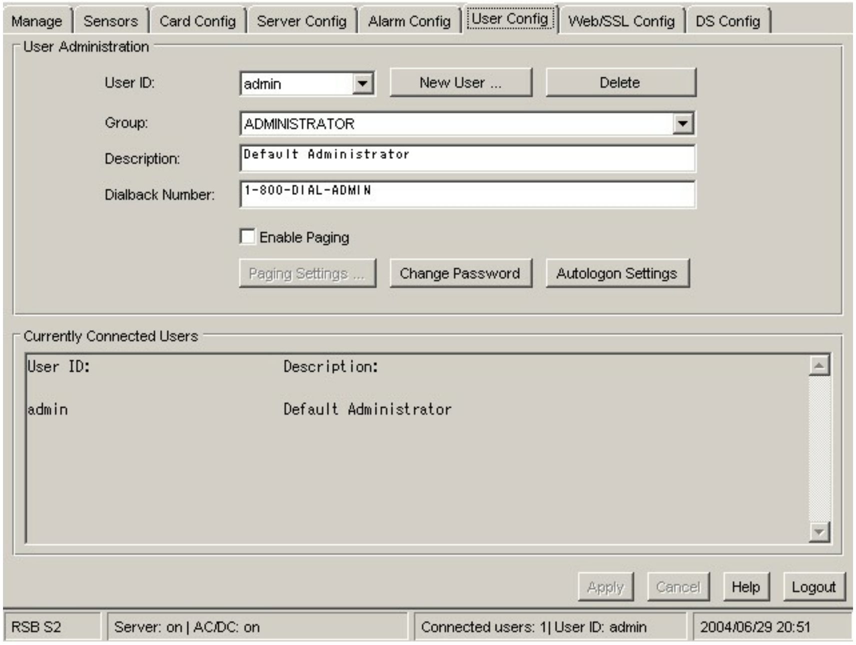
RSB S2 | Server: on | AC/DC: on | Connected users: 1| User ID: admin | 2004/06/29 20:34

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: • 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].

6.3.7 [User Config] Page

Set the user account-related items.



User ID: admin

Group: ADMINISTRATOR

Description: Default Administrator

Dialback Number: 1-800-DIAL-ADMIN

□ Enable Paging

```
User ID:                    Description:

admin                       Default Administrator
```

RSB S2 | Server: on | AC/DC: on | Connected users: 1| User ID: admin | 2004/06/29 20:51

table: Functions on the [User Config] Page

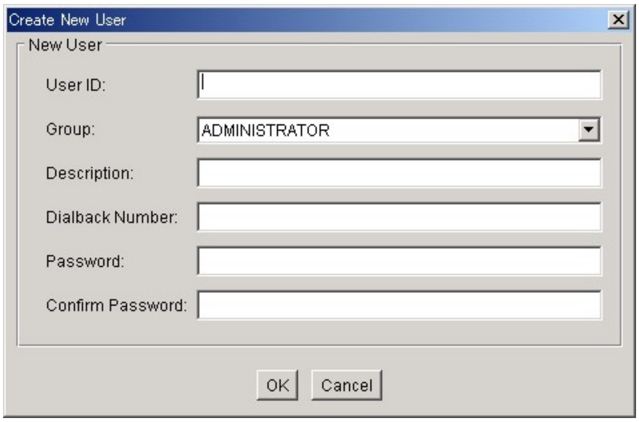
Item	Description
User ID	After a user account is selected in the combo box, information on the user account is displayed on the following items.
[New User ...]	Creates a new user. →"■ New User" (pg.334)
[Delete]	Deletes the user account displayed in [User ID]. When a confirmation message appears, click [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.334)
[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.335)

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. • 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.



Create New User

New User

User ID:

Group: ADMINISTRATOR

Description:

Dialback Number:

Password:

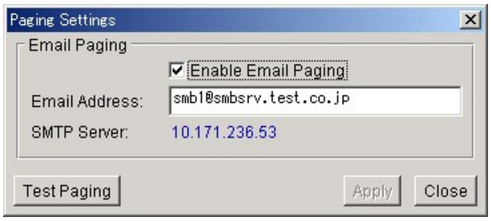
Confirm Password:

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.



Paging Settings

Email Paging

☑ Enable Email Paging

Email Address: smb1@smbsrv.test.co.jp

SMTP Server: 10.171.236.53

The following settings are required to enable email paging:

table: Setting Items for Mail Paging

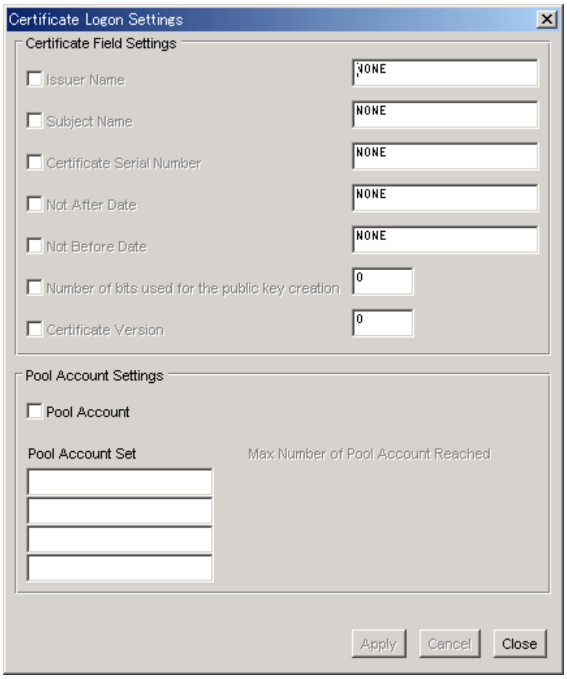
Item	Description
[Enable Email Paging]	Check this checkbox to enable it.
Email Address	Set the user's e-mail address.

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].



Certificate Logon Settings

Certificate Field Settings

☐ Issuer Name NONE

☐ Subject Name NONE

☐ Certificate Serial Number NONE

☐ Not After Date NONE

☐ Not Before Date NONE

☐ Number of bits used for the public key creation 0

☐ Certificate Version 0

Pool Account Settings

☐ Pool Account

Pool Account Set

Max Number of Pool Account Reached

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

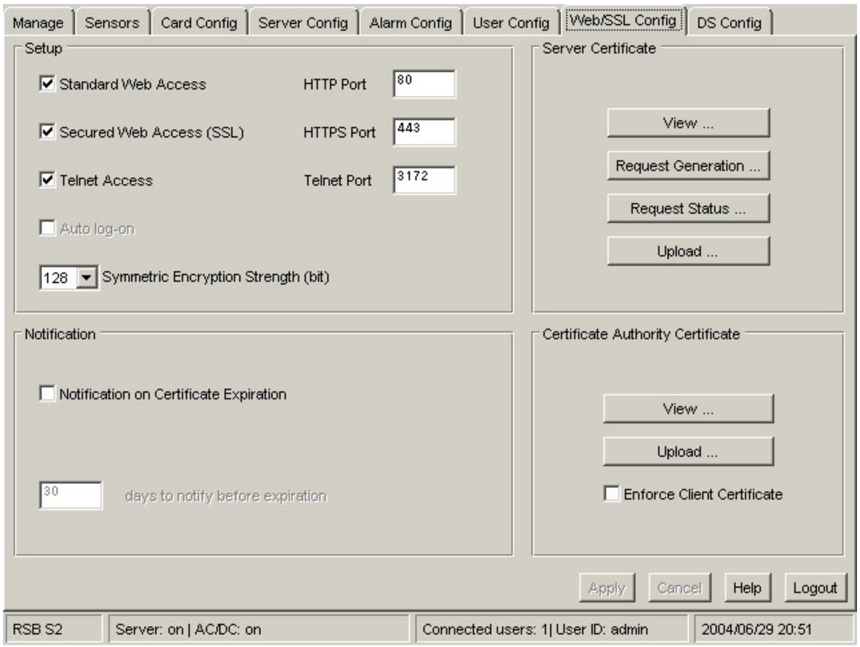
- Make sure to select two or more from the following items:
  - Issuer Name
  - Certificate Serial Number
  - Subject Name

POINT

[Pool Account] checkbox

- Check the [Pool Account] checkbox to allow multiple users to use the displayed account.

6.3.8 [Web/SSL Config] Page



Setup

☑ Standard Web Access HTTP Port 80

☑ Secured Web Access (SSL) HTTPS Port 443

☑ Telnet Access Telnet Port 3172

□ Auto log-on

128 Symmetric Encryption Strength (bit)

Notification

□ Notification on Certificate Expiration

30 days to notify before expiration

□ Enforce Client Certificate

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

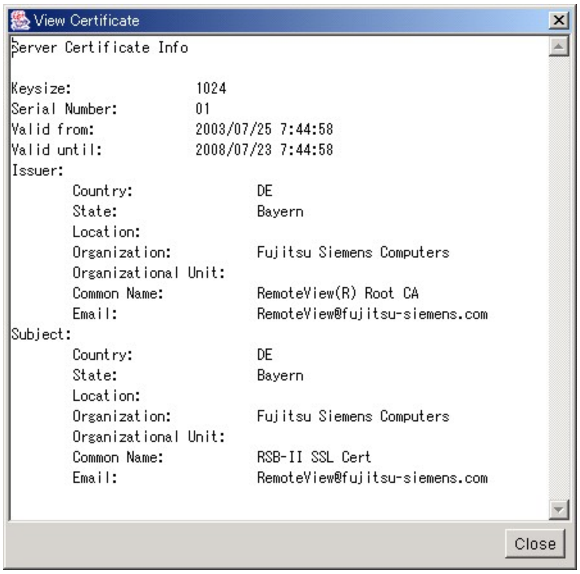
Item	Description
Setup	Set the port numbers of HTTP and Telnet to access the Remote Service Board.
Standard Web Access	Enables/disables HTTP access. If checked it is possible to perform HTTP access to the Remote Service Board.
HTTP Port	Set the port number for HTTP. The default value is "80".
Secured 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.338).
[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.339).
[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 ...

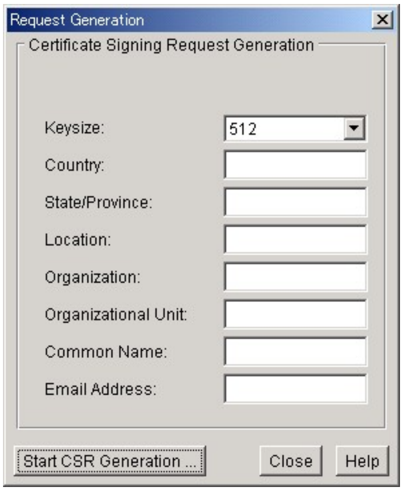
Displays information on the server certificate to be used next time the Remote Service Board is rebooted.



```
Server Certificate Info

Keysize:                1024
Serial Number:          01
Valid from:             2003/07/25 7:44:58
Valid until:            2008/07/23 7:44:58
Issuer:
        Country:                DE
        State:                  Bayern
        Location:
        Organization:           Fujitsu Siemens Computers
        Organizational Unit:
        Common Name:            RemoteView(R) Root CA
        Email:                  RemoteView@fujitsu-siemens.com
Subject:
        Country:                DE
        State:                  Bayern
        Location:
        Organization:           Fujitsu Siemens Computers
        Organizational Unit:
        Common Name:            RSB-II SSL Cert
        Email:                  RemoteView@fujitsu-siemens.com
```

● Request Generation

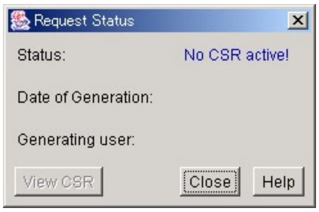
Generates a new server certificate.
Set each item in the [Request Generation] window and then click [Start CSR Generation ...].



Keysize: 512

● Request Status ...

Displays the current status for server certification requests.



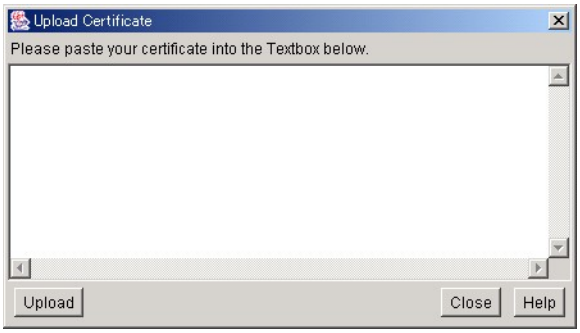
Status: No CSR active!

Date of Generation:

Generating user:

● Upload ...

Updates the server certificate.



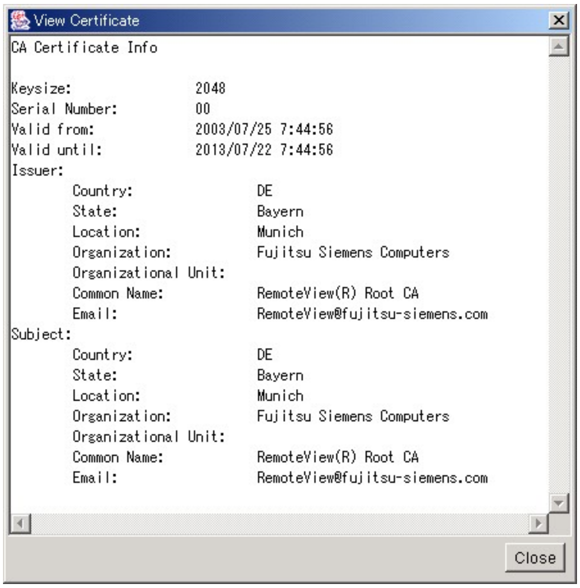
Please paste your certificate into the Textbox below.

■ 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.



```
CA Certificate Info

Keysize:                  2048
Serial Number:            00
Valid from:               2003/07/25 7:44:56
Valid until:              2013/07/22 7:44:56
Issuer:
        Country:                 DE
        State:                   Bayern
        Location:                Munich
        Organization:            Fujitsu Siemens Computers
        Organizational Unit:
        Common Name:             RemoteView(R) Root CA
        Email:                   RemoteView@fujitsu-siemens.com
Subject:
        Country:                 DE
        State:                   Bayern
        Location:                Munich
        Organization:            Fujitsu Siemens Computers
        Organizational Unit:
        Common Name:             RemoteView(R) Root CA
        Email:                   RemoteView@fujitsu-siemens.com
```

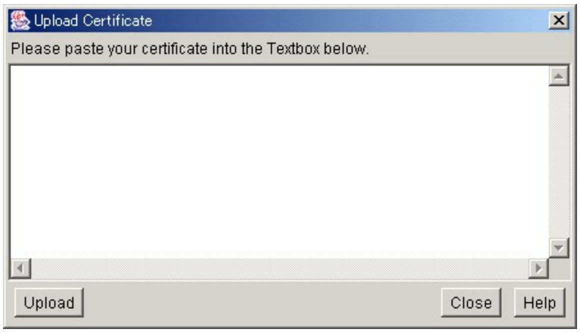
● Upload...

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.



Upload Certificate

Please paste your certificate into the Textbox below.

● 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.

IMPORTANT

- 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.

6.3.9 [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.

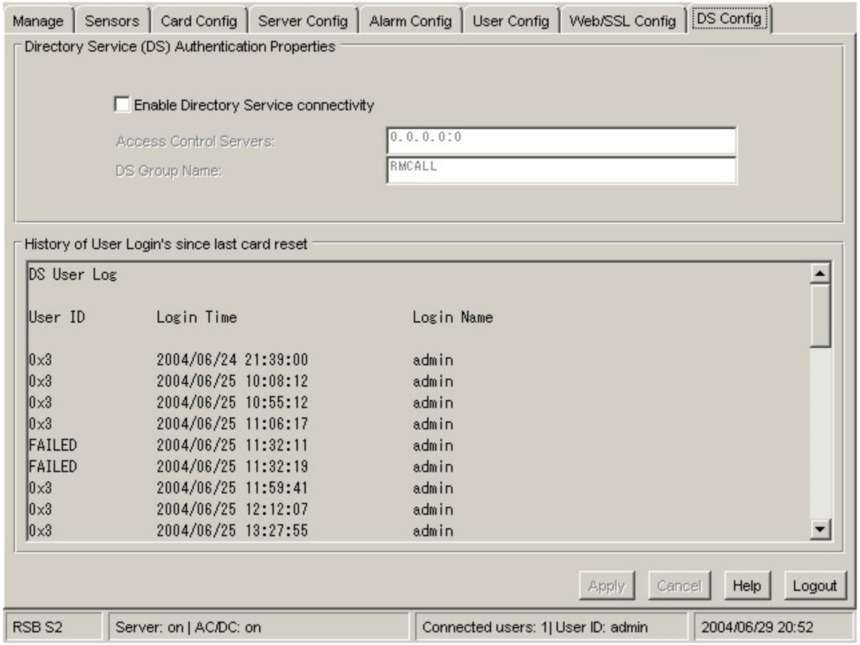
When a user tries to log in to the Remote Service Board, the Remote Service Board checks whether the user is included in its internal database.

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
```

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. • 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: • User ID • Login time • Login name

Chapter 7

Using the Remote Management Controller

This chapter describes the Web interface functions and the configuration of the Remote Management Controller.

7.1 Overview

This section describes the Web interface of the Remote Management Controller. The Remote Management Controller in this chapter refers to the Baseboard Management Controller (BMC) installed on the base board.

7.1.1 Supported Models and Functions

● Models Supported by the Remote Management Controller

The Remote Management Controller supports IPMI 2.0 and is used on the following servers:

- PRIMERGY RX300S3
- PRIMERGY RX200S3
- PRIMERGY TX200S3
- PRIMERGY TX150S5
- PRIMERGY RX100S4

● Web Interface Functions of the Remote Management Controller

The Web interface of the Remote Management Controller has the following functions:

- Display system information→"7.4.1 System Information" (pg.352)
- Control server (restart, power on/off)→"7.4.3 Power On/Off" (pg.355)
- Display sensor status (fan, temperature, voltage, power supply)→"7.4.4 Sensors" (pg.357)
- Display log→"7.4.5 System Event Log" (pg.365)
- Display and set server control information→"7.4.6 Server Management Information" (pg.366)
- Set up network→"7.4.7 Network Settings" (pg.368)
- Send alert→"7.4.8 Alerting" (pg.371)
- Display and set user information→"7.4.9 User Management" (pg.374)
- Video Redirection and Remote Storage Connection →"7.4.10 Console Redirection" (pg.378)

IMPORTANT

- ▸ The Remote Management Controller is a part of the Baseboard Management Controller (BMC) on the baseboard and is displayed as "iRMC".
- ▸ A separate license key (option) is necessary to use the Video Redirection function and Remote Storage Connection.

7.1.2 Notes

● Security

The Remote Management Controller handles personal information, such as the administrator’ s name, and other important information. If you set up the server in a domain that is accessible from outside, take care of the security so that the specified information is inaccessible from outside and minimize the contents to be set.

● Other Notes

- The Remote Management Controller is a part of the hardware (server). The Web interface is displayed in English.
- Java 2 Runtime Environment Standard Edition V1.4.2_10 or later JRE is required.
- An IP address is required to access the Remote Management Controller (or DHCP may be used).
- The LAN port for connecting to the Remote Management Controller is fixed for each model. Refer to "User's Guide" supplied with the server and connect to the correct LAN port.
- For controlling by the serial connection, refer to “User’s Guide“ supplied with the server.
- The following connection methods and configuration are not supported.
  - Serial/Modem Alerting function
  - Remote manager connection with the operating Shell set to "SMASH CLP/CLI" or operation when the Shell is set to "SMASH CLP/CLI" during remote manager connection
- Only following browsers are supported when using the Web interface of the Remote Management Controller.
  - Winsows
    Microsoft Internet Explorer 6.0 or later
  - Linux
    Mozilla FireFox

7.2 Preparations

The IP address, user name, and password must be set to access the Web interface and remote manager of the Remote Management Controller.

7.2.1 Setting the IP Address

Setting IP address is required because DHCP is "Disabled" by default.
To set the IP address manually, use the Server Management Tools (IPMIview), Web interface, or the BIOS setup utility.

POINT

- You can use the Server Management Tools (IPMIview) to check the current IP address.

7.2.2 Setting the User Name and Password

By default, the following user name and password are provided to access the Remote Management Controller.

table: Default user name and password

User name	Password	Access level/Operating shell type
admin	admin	OEM / RemoteManager

Use the Server Management Tools (IPMIview) or the Web interface to set the user name and password manually.

POINT

- You can use the Server Management Tools (IPMIview) to check the current user name and password.

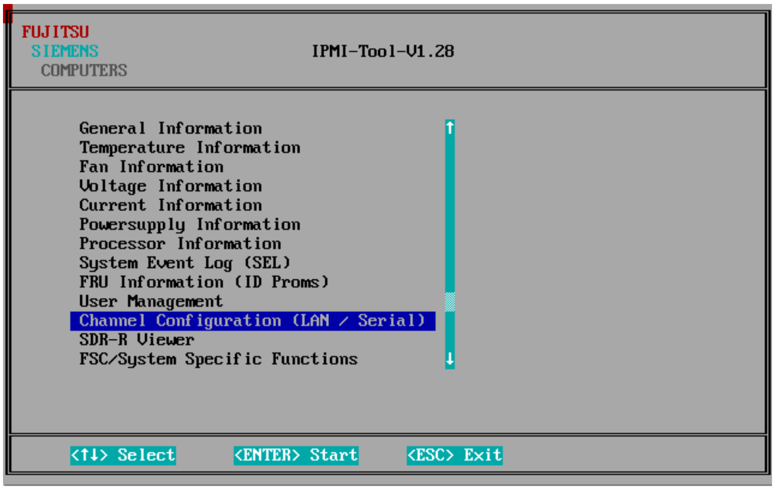
■ Configuration using the Server Management Tools (IPMIview)

This section describes how to configure the IP address, user name, and password using the Server Management Tools (IPMIview).

1 Startup the IPMIVIEW from the DOS boot floppy disk in which IPMIVIEW.exe is include.

```
>ipmiview.exe
```

2 Select the desired menu from the IPMIVIEW menu.



IP address settings for iRMC

1. Select [Channel Configuration (LAN / Serial)] from the menu.
2. Select [2 802.3_LAN] from the menu.
3. Press the [F1] key (General Settings).
4. Configure each item.

   Set IPAddressSource to 3.
5. Press the [F1] key (SetValues) to save the settings and close the window.

User name and the password settings for iRMC

1. Select [User Management] from the menu.
2. Select a user name to modify from the user list, or an unused number to add a user.
3. Set the user name, password, and authorization.
4. Press the [F1] key (SetValues) to save the settings and close the window.

3 Press the [Esc] key to exit the IPMIVIEW.

7.3 Starting and Exiting

This section describes how to start and exit the Web interface of the Remote Management Controller.

POINT

- The Web interface of the Remote Management Controller uses Java or JavaScript. You must enable your Web browser to use Java or JavaScript.
- When accessing the server's Remote Management Controller Web interface from the OS of the server itself, if the LAN port for iRMC is shared with the LAN port for the OS, disable the LAN port for the OS.

7.3.1 Starting the Web Interface of the Remote Management Controller

A Web browser is used to start the Web interface of the Remote Management Controller.

1 Start the Web browser.

2 Enter the following in the address field of the Web browser.

When using http:

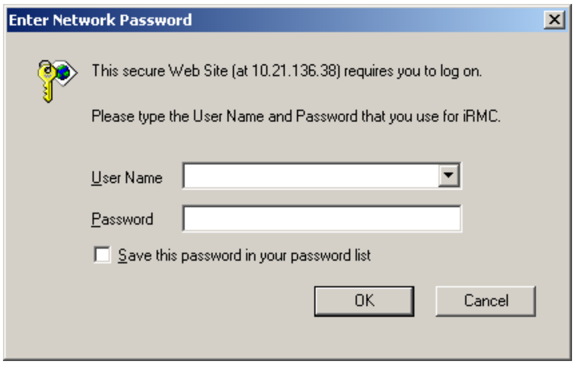
http://<IP address of the Remote Management Controller>:<Port number (default is 80)>

When using https:

https://<IP address of the Remote Management Controller>:<Port number (default is 443)>

3 Press the [Enter] key.

The network password window appears.



Enter Network Password

This secure Web Site (at 10.21.136.38) requires you to log on.

Please type the User Name and Password that you use for iRMC.

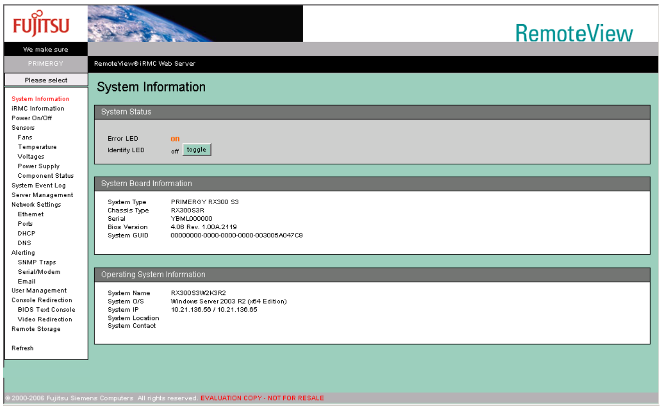
User Name

Password

□ Save this password in your password list

4 Enter the user name and password set for the Remote Management Controller and click [OK].

The Web interface main window appears.



System Information

System Status

Error LED on
Identify LED off

System Board Information

System Type PRIMERGY RX300 S3
Chassis Type RX300S3R
Serial YBML000000
Bios Version 4.06 Rev. 1.00A.2119
System GUID 00000000-0000-0000-0000-003005A047C9

Operating System Information

System Name RX300S3W2K3R2
System O/S Windows Server 2003 R2 (x64 Edition)
System IP 10.21.136.56 / 10.21.136.65
System Location
System Contact

© 2000-2006 Fujitsu Siemens Computers All rights reserved. EVALUATION COPY - NOT FOR RESALE

POINT

- You can also start the Remote Management Controller Web Interface from the RemoteControlService window. For details, see "5.3.2 Start and Exit for RemoteControleService/Web (For iRMC / BMC IPMI connection)" (→pg.275).

■ Web Interface Menu List

table: Web interface menu

Menu		Description
System Information		Displays information of the system on which the Remote Management Controller is running. →"7.4.1 System Information" (pg.352)
iRMC Information		Displays Remote Management Controller information and configures the controller
Power On/Off		Displays the server power status. This is also used to turn the server power ON/ OFF or restart. →"7.4.3 Power On/Off" (pg.355)
Sensors		Displays the status of each server sensor. See each item for details.
	Fans	Displays the fan status and is used set the action in case of failure. →"■ Fans" (pg.357)
	Temperature	Displays the temperature sensor status and is used set the action in case of an error. →"■ Temperature" (pg.359)
	Voltages	Displays the server internal voltage and current status. →"■ Voltages and Current" (pg.361)
	Power Supply	Displays the power supply unit status. →"■ Power Supply" (pg.363)
	Component Status	Displays the status of each sensor. →"■ Component Status (Lightpath)" (pg.364)
System Event Log		Displays the system event log stored on the baseboard. →"7.4.5 System Event Log" (pg.365)

table: Web interface menu

Menu		Description
Server Management		Displays the server management information. This is also used to set the server start and restart settings. →"7.4.6 Server Management Information" (pg.366)
Network Settings		Configures the network settings of the Remote Management Controller. See each item for details.
	Ethernet	Sets the IP address and subnet mask of the Remote Management Controller. →"■ Ethernet" (pg.368)
	Ports	Sets the port number. →"■ Ports" (pg.369)
	DHCP	Configures the DHCP settings. →"■ DHCP Settings" (pg.369)
	DNS	Configures the DNS settings. →"■ DNS Settings" (pg.370)
Alerting		Configures the SNMP trap and alert email settings. See each item for details.
	SNMP Traps	Configures the SNMP trap alerting settings. →"■ SNMP Trap Alerting" (pg.371)
	Serial/Modem	Configures the serial port/modem settings. This is not supported.
	Email	Configures the outgoing email settings. →"■ Email Alerting" (pg.372)
User Management		Sets the information of users logging on to the Remote Management Controller. →"7.4.9 User Management" (pg.374)
Console Redirection		Configures the console redirection and starts it up.
	BIOS Text Console	Configures the console redirection settings when using it in the RemoteControlService.
	Video Redirection	Starts Video Redirection. Configures the remote console redirection settings. Also, sets the remote storage. →"7.4.10 Console Redirection" (pg.378)
Remote Storage		Displays the remote storage unit status.
Refresh		Refreshes the Web interface window of the Remote Management Controller. →"■ Refreshing the Web Interface Window" (pg.350)

■ Refreshing the Web Interface Window

Select [Refresh] from the Web interface menu of the Remote Management Controller to refresh the Web interface window.

POINT

- The Web interface window is automatically refreshed every 120 to 360 seconds. The refresh interval varies depending on the server in use (the iRMC version). The interval cannot be changed.

7.3.2 Exiting the Web Interface of the Remote Management Controller

Exit the Web browser to exit the Web interface of the Remote Management Controller. The Remote Management Controller is automatically logged off when you exit the Web browser.

7.4 Setting and Referencing User Information

This section describes the meaning and settings of each Web interface window of the Remote Management Controller.

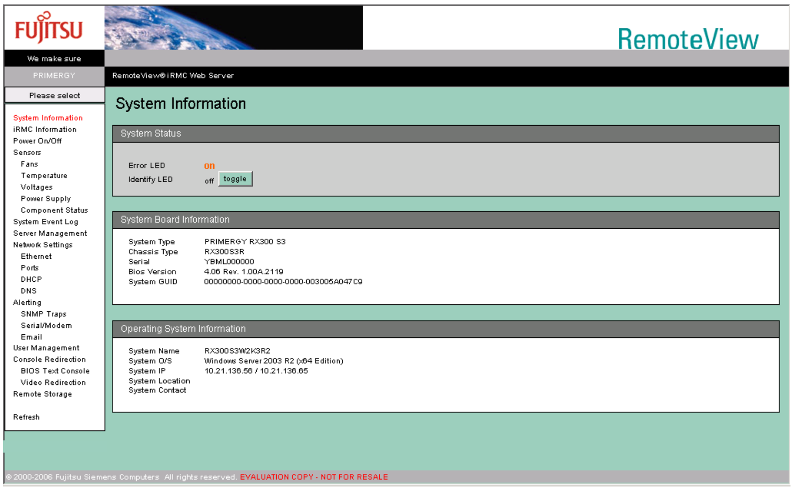
Each window is displayed by selecting it from the menu on the left side of the Web interface.

POINT

- The menu item [Alerting-Serial / Modem] is not yet supported.

7.4.1 System Information

Select [System Information] from the Remote Management Controller Web interface menu to display information about the system on which the Remote Management Controller is running.



System Information

System Status

Error LED on
Identify LED off

System Board Information

System Type PRIMERGY RX300 S3
Chassis Type RX300S3R
Serial YBML000000
Bios Version 4.06 Rev. 1.00A.2119
System GUID 00000000-0000-0000-0000-003005A047C9

Operating System Information

System Name RX300S3W2K3R2
System O/S Windows Server 2003 R2 (x64 Edition)
System IP 10.21.136.56 / 10.21.136.65
System Location
System Contact

© 2000-2006 Fujitsu Siemens Computers All rights reserved. EVALUATION COPY - NOT FOR RESALE

Each item is described below.

table: Description of Items Displayed in the System Information

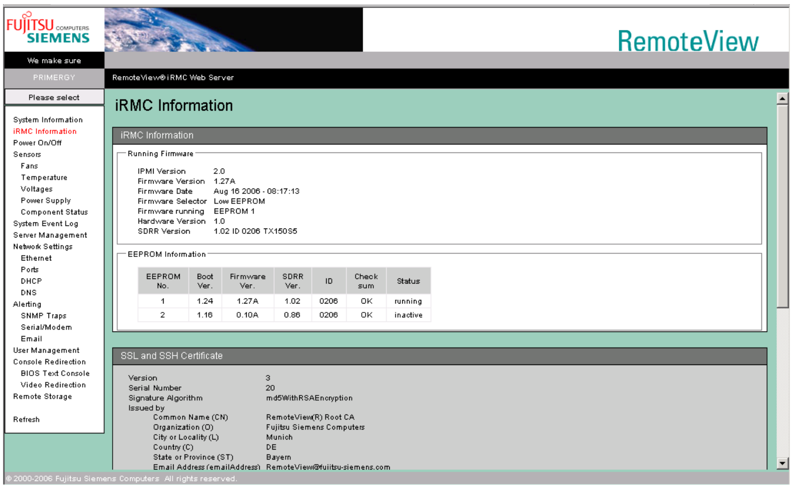
Item		Description
System Status		Displays the states of the system LEDs.
	Error LED	Displays whether the Error LED on the front of the server is On or Off.
	Identify LED	Displays whether the server system identification lamp is On or Off. Click [Toggle] displayed on the right side of the information name to turn the lamp On or Off.
System Board Information		Displays the baseboard information.
	System Type	Displays the server system type.
	Chassis Type	Displays the server chassis type.
	Serial	Displays the serial number of the baseboard.

table: Description of Items Displayed in the System Information

Item		Description
	Bios Version	Displays the BIOS version.
	System GUID	Displays the baseboard ID.
Operating System Information		Displays the OS information.
	System Name	Displays the server name set by the OS.
	System O/S	Displays the OS type.
	System IP	Displays the IP address of the OS.
	System Location	Displays the system location set in the SNMP Service of the OS.
	System Contact	Displays the administrator name set in the SNMP Service of the OS.

7.4.2 iRMC Information

Select [iRMC Information] from the Remote Management Controller Web interface menu to display information about the Remote Management Controller and to configure it.



iRMC Information

iRMC Information

Running Firmware

IPMI Version	2.0
Firmware Version	1.27A
Firmware Date	Aug 16 2006 - 08:17:13
Firmware Selector	Low EEPROM
Firmware running	EEPROM 1
Hardware Version	1.0
SDRR Version	1.02 ID 0206 TX150S5

EEPROM Information

EEPROM No.	Boot Ver.	Firmware Ver.	SDRR Ver.	ID	Check sum	Status
1	1.24	1.27A	1.02	0206	OK	running
2	1.16	0.10A	0.86	0206	OK	inactive

SSL and SSH Certificate

```
Version                        3
Serial Number                  20
Signature Algorithm            md5WithRSAEncryption
Issued by
    Common Name (CN)           RemoteView(R) Root CA
    Organization (O)           Fujitsu Siemens Computers
    City or Locality (L)       Munich
    Country (C)                DE
    State or Province (ST)     Bayern
    Email Address (emailAddress) RemoteView@fujitsu-siemens.com
```

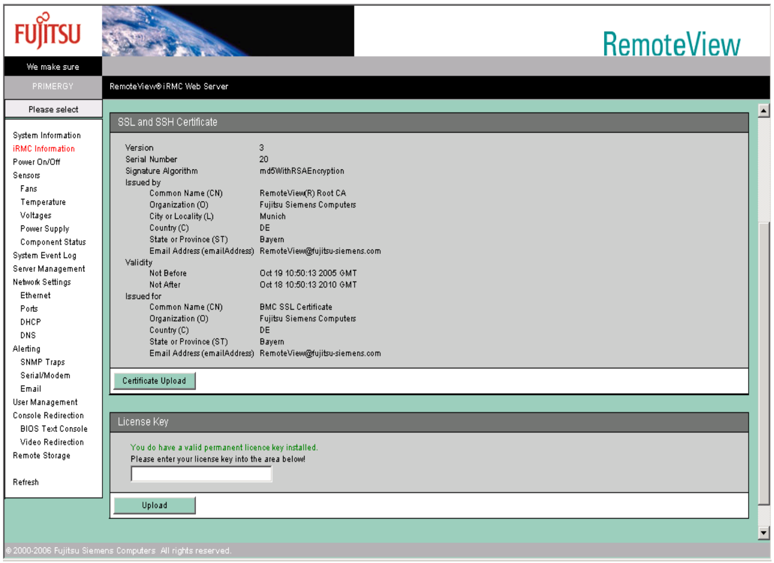
© 2000-2006 Fujitsu Siemens Computers All rights reserved.

table: Description of Items Displayed in iRMC Information

Item		Description
iRMC Information		Displays the iRMC information.
	IPMI Version	Displays the IPMI version supported by iRMC.
	Firmware Version	Displays the iRMC version.
	Firmware Date	Dislays the creation date of iRMC firmware.
	Firmware Selector	Displays the location of firmware (in ROM).
	Firmware running	Displays the active firmware number (in ROM).
	Hardware Version	Displays the server hardware version.
	SDRR Version	Displays the version of information defining the sensor and threshold.
	EEPROM Information	Information from the ROM storing the firmware.
SSL & SSH Certificate		Displays the certificates used for SSL/SSH.

■ Configuring the Remote Management Controller

This section describes the configuration and the operation of the Remote Management Controller.



```
Version                              3
Serial Number                        20
Signature Algorithm                  md5WithRSAEncryption
Issued by
      Common Name (CN)               RemoteView(R) Root CA
      Organization (O)               Fujitsu Siemens Computers
      City or Locality (L)           Munich
      Country (C)                    DE
      State or Province (ST)         Bayern
      Email Address (emailAddress)   RemoteView@fujitsu-siemens.com
Validity
      Not Before                     Oct 19 10:50:13 2005 GMT
      Not After                      Oct 18 10:50:13 2010 GMT
Issued for
      Common Name (CN)               BMC SSL Certificate
      Organization (O)               Fujitsu Siemens Computers
      Country (C)                    DE
      State or Province (ST)         Bayern
      Email Address (emailAddress)   RemoteView@fujitsu-siemens.com
```

You do have a valid permanent licence key installed.
Please enter your license key into the area below!

table: Configuration and Operation of the Remote Management Controller

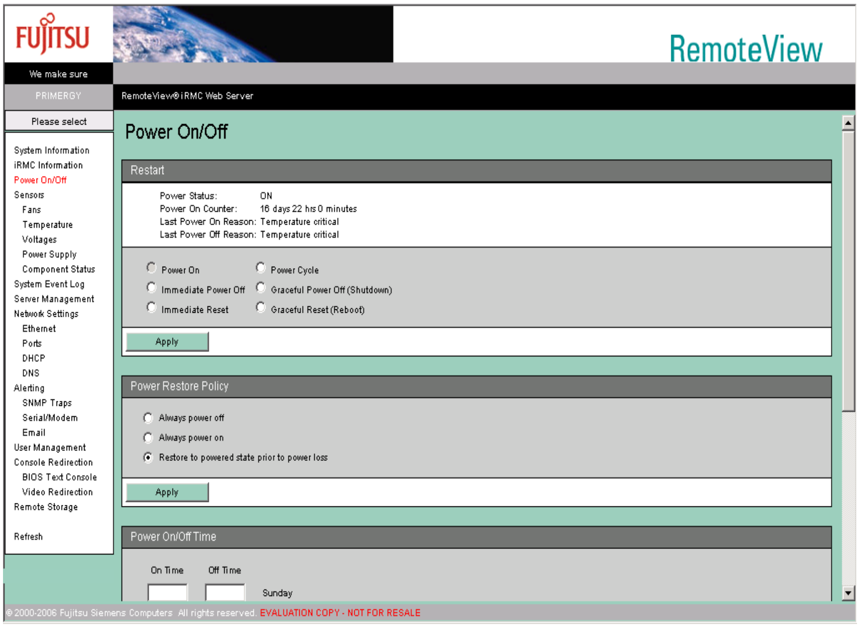
Item		Description
SSL & SSH Certificate		Displays information about the certificates used for SSL/SSH.
	Certificate Upload	Uploads the certificates.
License Key		Handles the license key for the management controller.
	Upload	Authorizes the license for the Remote Management Controller. When the license is authorized, the Video Redirection and Remote Storage functions become available.

POINT

- For details on the license key and how to authorize the license, see the “Remote Management Controller Upgrade User’s Guide“. Before the license is authorized, the Video Redirection and Remote Storage functions are not available.

7.4.3 Power On/Off

Select [Power On/Off] from the Remote Management Controller Web interface menu to turn on, turn off, or restart the server.



Power On/Off

Restart

Power Status: ON
Power On Counter: 16 days 22 hrs 0 minutes
Last Power On Reason: Temperature critical
Last Power Off Reason: Temperature critical

○ Power On ○ Power Cycle
○ Immediate Power Off ○ Graceful Power Off (Shutdown)
○ Immediate Reset ○ Graceful Reset (Reboot)

Apply

Power Restore Policy

○ Always power off
○ Always power on
● Restore to powered state prior to power loss

Apply

Power On/Off Time

On Time Off Time
Sunday

© 2000-2006 Fujitsu Siemens Computers All rights reserved. EVALUATION COPY - NOT FOR RESALE

Each item is described below.

table: Description of Items Displayed on the Power On/Off Screen

Item		Description
Restart		Displays the current power status.
	Power Status	The current power status is displayed as On or Off.
	Power On Counter	Displays the total operating hours since the server power was turned On.
	Last Power On Reason	Displays the reason for the previous server power on.
	Last Power Off Reason	Displays the reason for the previous server power off.
	Power On	Select and click [Apply] to turn on the server power.
	Immediate Power Off	Select and click [Apply] to turn off the server power immediately without saving system information.
	Immediate Reset	Select and click [Apply] to reset the server power immediately without saving system information.
	Power Cycle	Select and click [Apply] to turn off the server power after saving system information and then turn it back on.(Unused)
	Graceful Power Off (Shutdown)	Select and click [Apply] to turn off the server power after saving system information.
	Graceful Reset (Reboot)	Select and click [Apply] to reset the server power after saving system information.
Power Restore Policy		Configures the power restore action if the server power is interrupted by a power failure. Select the desired operation and click [Apply].
	Always Power off	The server does not perform any power restore action if there is a power failure.

table: Description of Items Displayed on the Power On/Off Screen

Item		Description
	Always Power on	The server automatically performs a power restore action if there is a power failure.
	Restore to powered state prior to power loss	The server restores the status just before the power failure occurred. If the server power was "On", the power is restored automatically. If the server power was "Off", the power is not restored and remains off.
Power On/Off Time		Set the time to automatically power on and off the server for one week. For details, see "■ Power On/Off Time" (→pg.356).

POINT

- The power control related settings of [Restart] may not be selectable depending on the server status.

■ Power On/Off Time

The time to automatically power on and off the server can be set for one week.

1 Select [Power On/Off] from the Remote Management Controller Web interface menu.

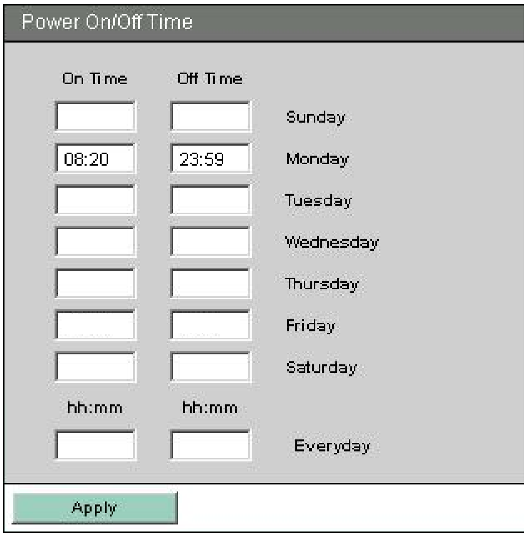
The [Power On/Off] window appears.

2 Enter the time to turn on the power in the [On Time] field and the time to turn off the power in the [Off Time] field for each day in the [Power On/Off Time] window.

POINT

- Enter the time in hh:mm format (where hh is a two-digit hour from 00 to 23, and mm is a two-digit minute from 00 to 59).

For example, enter the following to turn on the server power every Monday at 8:20 AM and turn it off at 11:59 PM.



Power On/Off Time

On Time	Off Time	
		Sunday
08:20	23:59	Monday
		Tuesday
		Wednesday
		Thursday
		Friday
		Saturday
hh:mm	hh:mm	
		Everyday

3 Click [Apply].

POINT

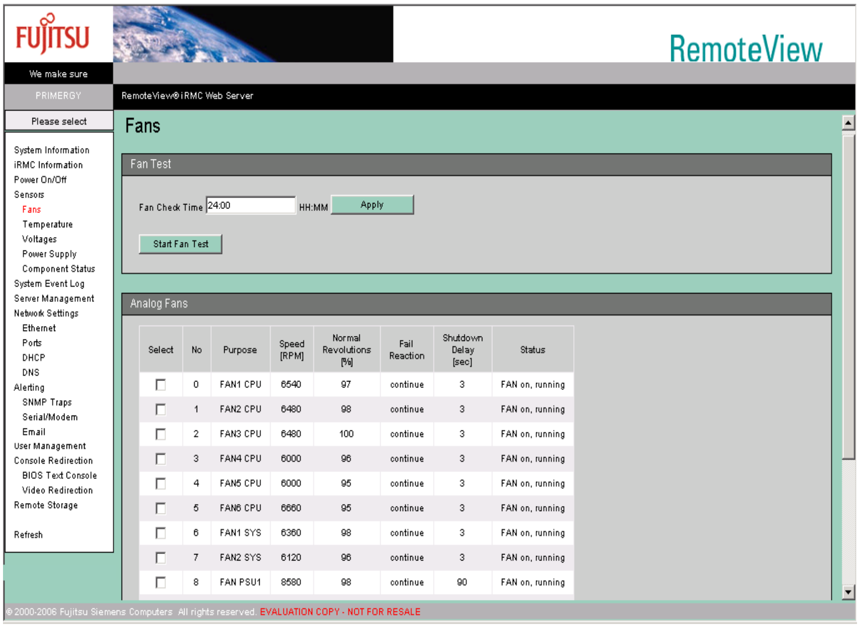
- To turn on and off the server at the same time every day of the week, enter the time in the [On Time] and [Off time] fields for [Everyday] and click [Apply].
- To cancel the setting, erase the entered time and click [Apply].

7.4.4 Sensors

The status of the fans, the temperature sensor, the voltage and the power unit inside the server can be viewed.

■ Fans

Select [Fans] from the Remote Management Controller Web interface menu to display the status of the fans inside the server, such as the CPU fan or the system fan, and to set the action in case of failure.



Fans

Fan Test

Fan Check Time 24:00 HH:MM

Analog Fans

Select	No	Purpose	Speed [RPM]	Normal Revolutions [%]	Fail Reaction	Shutdown Delay [sec]	Status
□	0	FAN1 CPU	6540	97	continue	3	FAN on, running
□	1	FAN2 CPU	6480	98	continue	3	FAN on, running
□	2	FAN3 CPU	6480	100	continue	3	FAN on, running
□	3	FAN4 CPU	6000	96	continue	3	FAN on, running
□	4	FAN5 CPU	6000	95	continue	3	FAN on, running
□	5	FAN6 CPU	6660	95	continue	3	FAN on, running
□	6	FAN1 SYS	6360	98	continue	3	FAN on, running
□	7	FAN2 SYS	6120	96	continue	3	FAN on, running
□	8	FAN PSU1	8580	98	continue	90	FAN on, running

Each item is described below.

table: Description of Items Displayed on the [Fans] Screen

Item	Description
Fan Test	Sets the time to check the status of the fans. Enter the time to check the fan status in [Fan Check Time] and click [Apply]. Enter the time in hh:mm format (where hh is a two-digit hour from 00 to 23, and mm is a two-digit minute from 00 to 59). Click [Start Fan Test] to check the current fan status immediately.

table: Description of Items Displayed on the [Fans] Screen

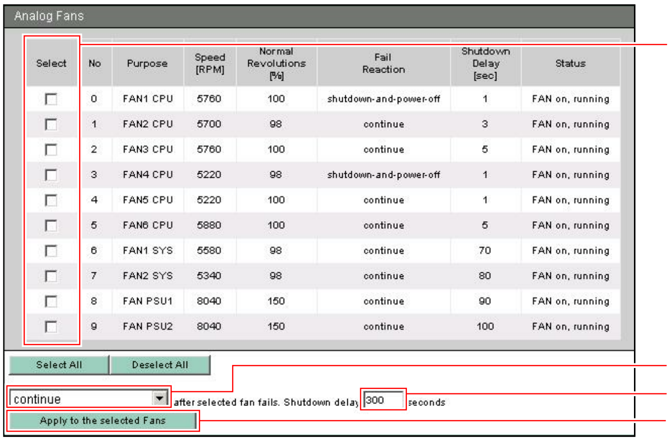
Item		Description
Analog Fans		Displays the current fan status. Also, configures the system action in case a fan failure occurs.
	Select	Check the checkbox to select the fan for which to set the action in case of a failure. For how to set the action, see "● Action in Case of a Fan Failure" (→pg.358).
	No	Displays the sequence number of the fan.
	Purpose	Displays the sensor name of the fan.
	Speed	Displays the current rotating speed of the fan in RPM.
	Normal Revolutions	Displays the current fan rotation speed as a percentage of the rotation speed during the previous fan status check.
	Fail Reaction	Displays the action to be taken by the system is there is a fan failure. For how to set the action, see "● Action in Case of a Fan Failure" (→pg.358).
	Shutdown Delay	Displays the delay in seconds from the time a fan failure is detected until the system starts the set action. For how to set the action, see "● Action in Case of a Fan Failure" (→pg.358).
	Status	Displays the current fan status (installed/not installed, operating/stopped).

POINT

- Some items may be blank if the fan information cannot be obtained because the fan power is off.

● Action in Case of a Fan Failure

Set the action to be taken by the system in case of a fan failure.



Analog Fans

Select	No	Purpose	Speed [RPM]	Normal Revolutions [%]	Fail Reaction	Shutdown Delay [sec]	Status
□	0	FAN1 CPU	5760	100	shutdown-and-power-off	1	FAN on, running
□	1	FAN2 CPU	5700	98	continue	3	FAN on, running
□	2	FAN3 CPU	5760	100	continue	5	FAN on, running
□	3	FAN4 CPU	5220	98	shutdown-and-power-off	1	FAN on, running
□	4	FAN5 CPU	5220	100	continue	1	FAN on, running
□	5	FAN6 CPU	5880	100	continue	5	FAN on, running
□	6	FAN1 SYS	5580	98	continue	70	FAN on, running
□	7	FAN2 SYS	5340	98	continue	80	FAN on, running
□	8	FAN PSU1	8040	150	continue	90	FAN on, running
□	9	FAN PSU2	8040	150	continue	100	FAN on, running

continue after selected fan fails. Shutdown delay 300 seconds

1. Select the desired fan
2. Select the action
3. Enter the delay time
4. Click here to apply the setting

1 Select the desired fan by checking the checkbox in the [Select] column.

POINT

- Click [Select All] if you want to select all of the displayed fans. Click [Deselect All] to deselect all selected fans.

2 Select "Continue" or "shutdown-and-power-off" from the action list displayed at the bottom.

table: Fan Action Items

Action	Description
Continue	The system continues operation in the event of a fan failure.
shutdown-and-power-off	If a fan failure is detected, the system continues operation for the specified delay time (set by the next procedure). If the failure is not recovered within that time, the system shuts down automatically.

3 Enter the delay time until the system takes action for the fan failure.

The unit is seconds. Enter a number between 0 and 300.

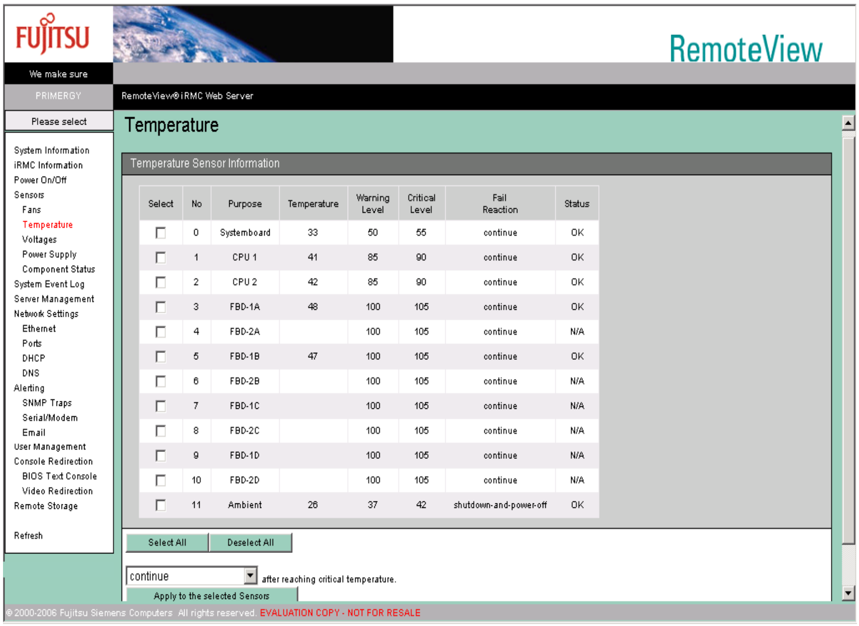
4 Click [Apply to the selected Fans] to apply the setting.

View each item in the window to confirm that the setting is applied.

- Action setting → [Fail Reaction] column
- Delay time setting → [Shutdown Delay] column

■ Temperature

Select [Temperature] from the Remote Management Controller Web interface menu to display the status of each temperature sensor in the server and to set the action in case of failure.



Temperature

Temperature Sensor Information

Select	No	Purpose	Temperature	Warning Level	Critical Level	Fail Reaction	Status
□	0	Systemboard	33	50	55	continue	OK
□	1	CPU 1	41	85	90	continue	OK
□	2	CPU 2	42	85	90	continue	OK
□	3	FBD-1A	48	100	105	continue	OK
□	4	FBD-2A		100	105	continue	N/A
□	5	FBD-1B	47	100	105	continue	OK
□	6	FBD-2B		100	105	continue	N/A
□	7	FBD-1C		100	105	continue	N/A
□	8	FBD-2C		100	105	continue	N/A
□	9	FBD-1D		100	105	continue	N/A
□	10	FBD-2D		100	105	continue	N/A
□	11	Ambient	26	37	42	shutdown-and-power-off	OK

Select All | Deselect All

continue ▼ after reaching critical temperature.

Apply to the selected Sensors

© 2000-2006 Fujitsu Siemens Computers All rights reserved. EVALUATION COPY - NOT FOR RESALE

Each item is described below.

table: Description of Items Displayed on the [Temperature] Screen

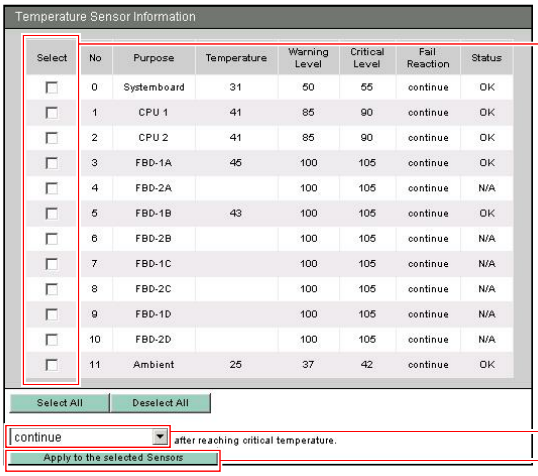
Item	Description
Temperature Sensor Information	Displays the current temperature sensor status. Also configures the system action when a temperature error occurs.
Select	Check the checkbox to select the temperature sensor to set the action in case of a temperature error. For how to set the action, see "● Action in Case of a Temperature Error" (→pg.360).
No	Displays the sequence number of the temperature sensor.
Purpose	Displays the sensor name of the temperature sensor.
Temperature	Displays the current temperature.
Warning Level	Displays the warning level temperature.
Critical Level	Displays the critical level temperature.
Fail Reaction	Displays the action to be taken by the system in case of a temperature error. For how to set the action, see "● Action in Case of a Temperature Error" (→pg.360).
Status	Displays whether the current temperature is abnormal or not. • OK: There is no problem. • N/A: Not connected. • Warning: Warning level. • Critical: Critical level.

POINT

- Some items may be blank if temperature information cannot be obtained.

● Action in Case of a Temperature Error

Set the action to be taken by the system in case of a temperature error.



Temperature Sensor Information

Select	No	Purpose	Temperature	Warning Level	Critical Level	Fail Reaction	Status
□	0	Systemboard	31	50	55	continue	OK
□	1	CPU 1	41	85	90	continue	OK
□	2	CPU 2	41	85	90	continue	OK
□	3	FBD-1A	45	100	105	continue	OK
□	4	FBD-2A		100	105	continue	N/A
□	5	FBD-1B	43	100	105	continue	OK
□	6	FBD-2B		100	105	continue	N/A
□	7	FBD-1C		100	105	continue	N/A
□	8	FBD-2C		100	105	continue	N/A
□	9	FBD-1D		100	105	continue	N/A
□	10	FBD-2D		100	105	continue	N/A
□	11	Ambient	25	37	42	continue	OK

continue after reaching critical temperature.

1. Select the desired temperature sensor
2. Select the action
3. Click here to apply the setting

1 Select the desired temperature sensor by checking the checkbox in the [Select] column.

POINT

- Click [Select All] if you want to select all of the displayed temperature sensors. Click [Deselect All] to deselect all selected temperature sensors.

2 Select [Continue] or [shutdown-and-power-off] from the action list displayed at the bottom.

table: Temperature Sensor Action Items

Action	Description
Continue	The system continues operation in the event of a temperature error.
shutdown-and-power-off	The system shuts down automatically in the event of a temperature error.

3 Click [Apply to the selected Sensors] to apply the setting.

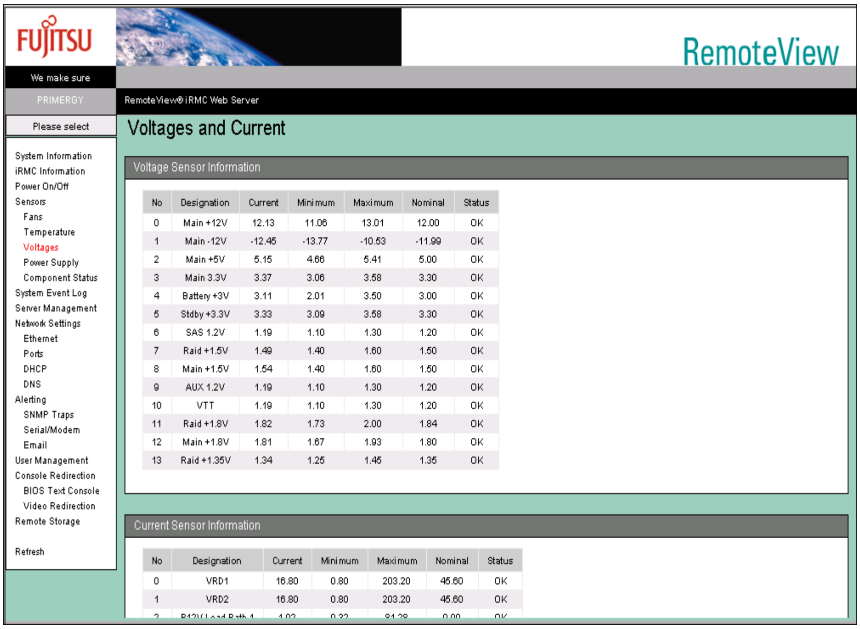
View the [Fail Reaction] column to check that the setting is applied.

POINT

- There is no delay time for actions against temperature errors. The action is taken immediately when an error is detected.

■ Voltages and Current

Select [Voltages] from the Remote Management Controller Web interface menu to display the server internal voltages.



Voltages and Current

Voltage Sensor Information

No	Designation	Current	Minimum	Maximum	Nominal	Status
0	Main +12V	12.13	11.06	13.01	12.00	OK
1	Main -12V	-12.45	-13.77	-10.53	-11.99	OK
2	Main +5V	5.15	4.66	5.41	5.00	OK
3	Main 3.3V	3.37	3.06	3.58	3.30	OK
4	Battery +3V	3.11	2.01	3.50	3.00	OK
5	Stdby +3.3V	3.33	3.09	3.58	3.30	OK
6	SAS 1.2V	1.19	1.10	1.30	1.20	OK
7	Raid +1.5V	1.49	1.40	1.60	1.50	OK
8	Main +1.5V	1.54	1.40	1.60	1.50	OK
9	AUX 1.2V	1.19	1.10	1.30	1.20	OK
10	VTT	1.19	1.10	1.30	1.20	OK
11	Raid +1.8V	1.82	1.73	2.00	1.84	OK
12	Main +1.8V	1.81	1.67	1.93	1.80	OK
13	Raid +1.35V	1.34	1.25	1.45	1.35	OK

Current Sensor Information

No	Designation	Current	Minimum	Maximum	Nominal	Status
0	VRD1	16.80	0.80	203.20	45.60	OK
1	VRD2	16.80	0.80	203.20	45.60	OK

Each item is described below.

table: Description of Items Displayed on the [Voltages] Screen

Item		Description
Voltage Sensor Information		Displays the information about the voltage sensor.
	No	Displays the sequence number of the voltage sensor.
	Designation	Displays the voltage sensor name.
	Current	Displays the current voltage.
	Minimum	Displays the allowed minimum voltage.
	Maximum	Displays the allowed maximum voltage.

table: Description of Items Displayed on the [Voltages] Screen

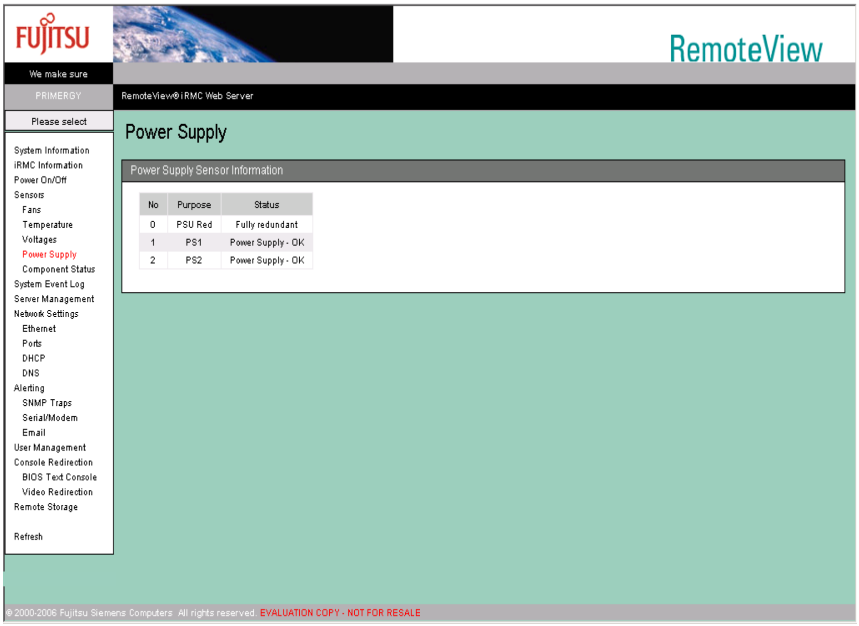
Item		Description
	Nominal	Displays the nominal voltage.
	Status	Displays whether the current voltage is abnormal or not. • OK: There is no problem. • N/A: Not connected or digital sensor (On/Off only). • Upper-Warning: Upper warning level. • Lower-Warning: Lower warning level.
Current Sensor Information		Displays the information about the current sensor.
	No	Displays the sequence number of the current sensor.
	Designation	Displays the current sensor name.
	Current	Displays the current current.
	Minimum	Displays the allowed minimum current.
	Maximum	Displays the allowed maximum current.
	Nominal	Displays the nominal current.
	Status	Displays whether the current current is abnormal or not. • OK: There is no problem. • N/A: Not connected or digital sensor (On/Off only). • Upper-Warning: Upper warning level. • Lower-Warning: Lower warning level.

POINT

- There is no system action in case of an error for [Voltages].

■ Power Supply

Select [Power Supply] from the Remote Management Controller Web interface menu to display the status of the server's power supply unit (PSU).



Power Supply

Power Supply Sensor Information

No	Purpose	Status
0	PSU Red	Fully redundant
1	PS1	Power Supply - OK
2	PS2	Power Supply - OK

Each item is described below.

table: Description of Items Displayed on the [Power Supply] Screen

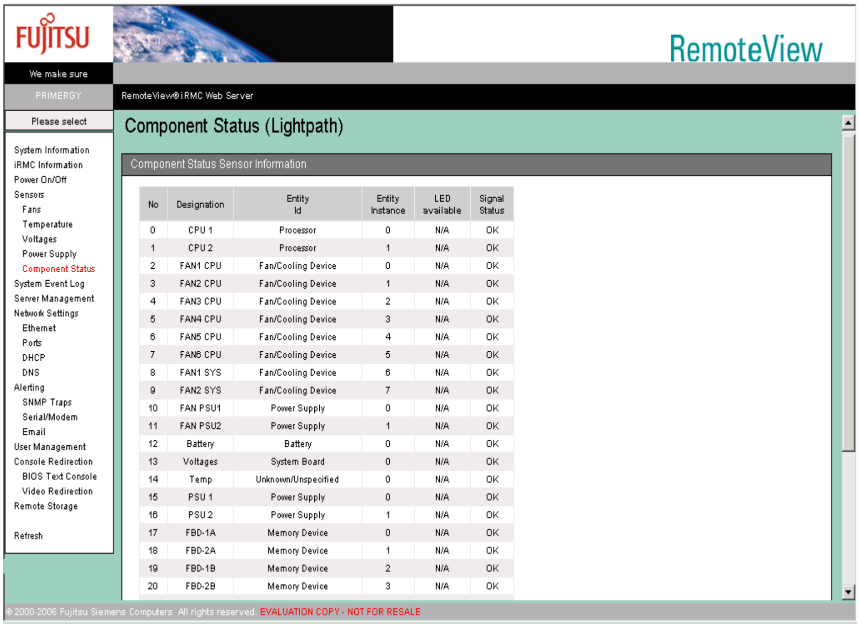
Item	Description
No	Displays the sequence number of the power supply unit.
Purpose	Displays the power supply unit name.
Status	Displays the status of the power supply unit.

POINT

- If the power supply unit has a redundant configuration, a sensor indicating the redundancy status is also displayed. In the above screen example, No. 0 [PSU Red] is the redundancy status sensor.

■ Component Status (Lightpath)

Select [Component Status] from the Remote Management Controller Web interface menu to display the status of each sensor in the server.



Component Status (Lightpath)

Component Status Sensor Information

No	Designation	Entity Id	Entity Instance	LED available	Signal Status
0	CPU 1	Processor	0	N/A	OK
1	CPU 2	Processor	1	N/A	OK
2	FAN1 CPU	Fan/Cooling Device	0	N/A	OK
3	FAN2 CPU	Fan/Cooling Device	1	N/A	OK
4	FAN3 CPU	Fan/Cooling Device	2	N/A	OK
5	FAN4 CPU	Fan/Cooling Device	3	N/A	OK
6	FAN5 CPU	Fan/Cooling Device	4	N/A	OK
7	FAN6 CPU	Fan/Cooling Device	5	N/A	OK
8	FAN1 SYS	Fan/Cooling Device	6	N/A	OK
9	FAN2 SYS	Fan/Cooling Device	7	N/A	OK
10	FAN PSU1	Power Supply	0	N/A	OK
11	FAN PSU2	Power Supply	1	N/A	OK
12	Battery	Battery	0	N/A	OK
13	Voltages	System Board	0	N/A	OK
14	Temp	Unknown/Unspecified	0	N/A	OK
15	PSU 1	Power Supply	0	N/A	OK
16	PSU 2	Power Supply	1	N/A	OK
17	FBD-1A	Memory Device	0	N/A	OK
18	FBD-2A	Memory Device	1	N/A	OK
19	FBD-1B	Memory Device	2	N/A	OK
20	FBD-2B	Memory Device	3	N/A	OK

© 2000-2006 Fujitsu Siemens Computers All rights reserved. EVALUATION COPY - NOT FOR RESALE

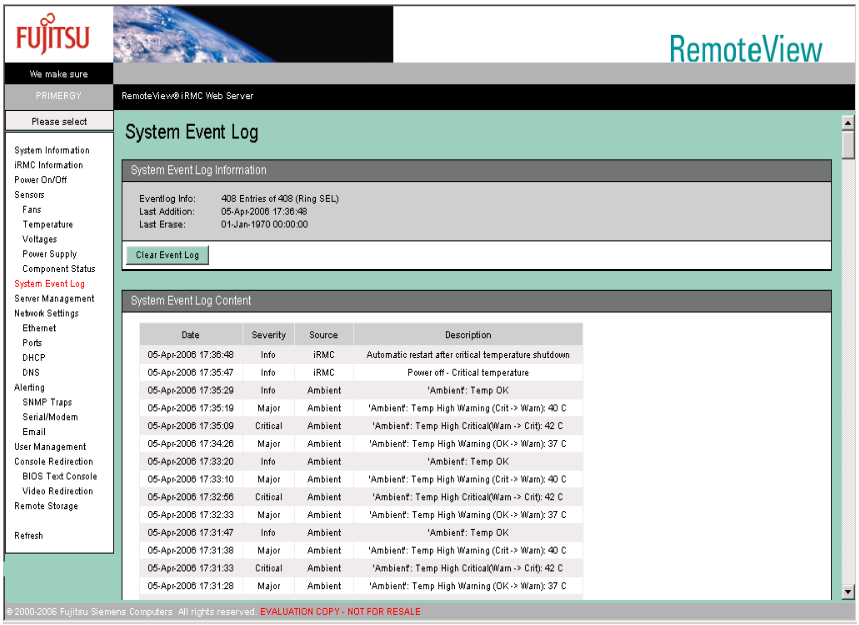
Each item is described below.

table: Description of Items Displayed on the [Component Status Sensor Information] Screen

Item	Description
Component Status Sensor Information	
No	Displays the sequence number of the sensor.
Designation	Displays the sensor name.
Entity Id	Displays the sensor type.
Entity Instance	Displays the sequence number by sensor type.
LED available	Displays the On/Off status of the sensor LED.
Signal Status	Displays the sensor status.

7.4.5 System Event Log

Select [System Event Log] from the Remote Management Controller Web interface menu to display the system event log (SEL) stored in the baseboard.



System Event Log

System Event Log Information

Eventlog Info: 408 Entries of 408 (Ring SEL)
Last Addition: 05-Apr-2006 17:36:48
Last Erase: 01-Jan-1970 00:00:00

Clear Event Log

System Event Log Content

Date	Severity	Source	Description
05-Apr-2006 17:36:48	Info	iRMC	Automatic restart after critical temperature shutdown
05-Apr-2006 17:35:47	Info	iRMC	Power off - Critical temperature
05-Apr-2006 17:35:29	Info	Ambient	'Ambient': Temp OK
05-Apr-2006 17:35:19	Major	Ambient	'Ambient': Temp High Warning (Crit -> Warn): 40 C
05-Apr-2006 17:35:09	Critical	Ambient	'Ambient': Temp High Critical(Warn -> Crit): 42 C
05-Apr-2006 17:34:26	Major	Ambient	'Ambient': Temp High Warning (OK -> Warn): 37 C
05-Apr-2006 17:33:20	Info	Ambient	'Ambient': Temp OK
05-Apr-2006 17:33:10	Major	Ambient	'Ambient': Temp High Warning (Crit -> Warn): 40 C
05-Apr-2006 17:32:56	Critical	Ambient	'Ambient': Temp High Critical(Warn -> Crit): 42 C
05-Apr-2006 17:32:33	Major	Ambient	'Ambient': Temp High Warning (OK -> Warn): 37 C
05-Apr-2006 17:31:47	Info	Ambient	'Ambient': Temp OK
05-Apr-2006 17:31:38	Major	Ambient	'Ambient': Temp High Warning (Crit -> Warn): 40 C
05-Apr-2006 17:31:33	Critical	Ambient	'Ambient': Temp High Critical(Warn -> Crit): 42 C
05-Apr-2006 17:31:28	Major	Ambient	'Ambient': Temp High Warning (OK -> Warn): 37 C

All system event logs currently stored in the baseboard are displayed.

Each item is described below.

table: Description of Items Displayed on the [System Event Log] Screen

Item		Description
System Event Log Information		Displays information about the event logs. Click [Clear Event Log] to clear all event logs.
	Eventlog Info	Displays the current number of event logs.
	Last Addition	Displays the date and time of the last log entry.
	Last Erase	Displays the date and time when the event log was last cleared.
	［Clear Event Log］	Clears the ststem event log.
System Event Log Content		The List of Event Logs
	Date	Displays the date and time the event occurred.
	Severity	Displays the severity of the event. The four severity levels are in ascending order: Info, Minor, Major, and Critical.
	Source	Displays the source of the event.
	Description	Displays a description of the event.

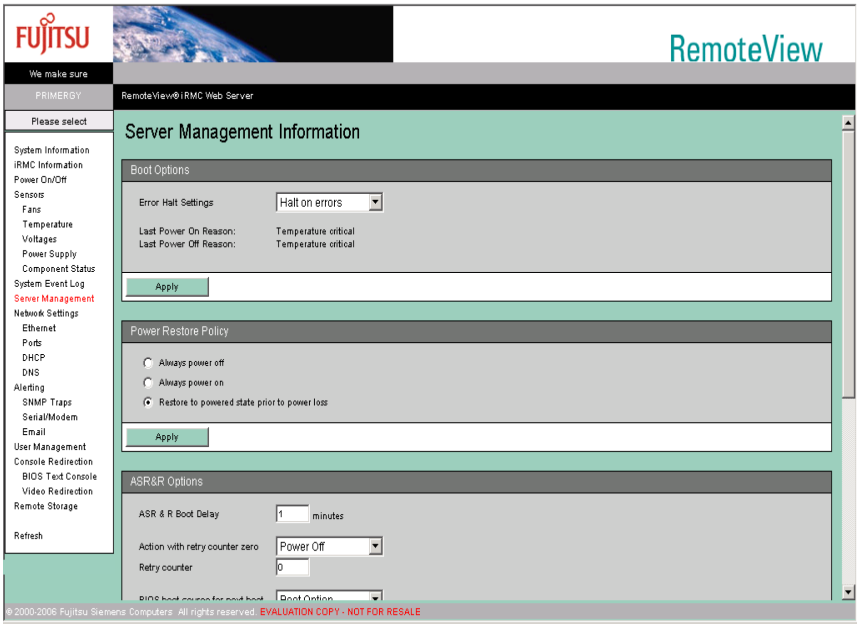
POINT

- The maximum number of events stored in the system event log is 256 to 512 depending on the server (BIOS).
- For the system event log storage method (overwrite, etc.), refer to "User's Guide" supplied with the server.

7.4.6 Server Management Information

Select [Server Management] from the Remote Management Controller Web interface menu to display and set the server management information.

Some items have restrictions depending the servers. For details, refer to "User's Guide" supplied with the server.



Server Management Information

Boot Options

Error Halt Settings: Halt on errors

Last Power On Reason: Temperature critical
Last Power Off Reason: Temperature critical

Power Restore Policy

○ Always power off
○ Always power on
● Restore to powered state prior to power loss

ASR&R Options

ASR & R Boot Delay: 1 minutes

Action with retry counter zero: Power Off

Retry counter: 0

BIOS boot source for next boot: Boot Option

© 2000-2006 Fujitsu Siemens Computers. All rights reserved. EVALUATION COPY - NOT FOR RESALE

Each item is described below.

table: Description of Items Displayed on the [Server Management Information] Screen

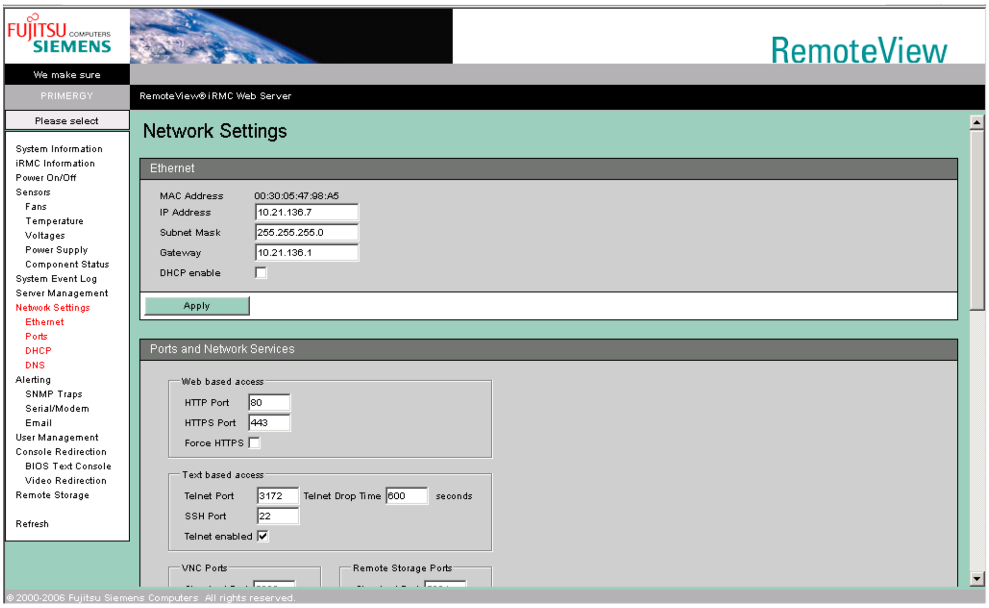
Item	Description
Boot Options	Configures the server startup settings. Enter or select each setting and click [Apply] to apply the setting. The information set here is also applied to the server BIOS setup utility.
Error Halt Settings	Sets the server action to take in case an error occurs during startup. The following two settings are available. Select one from the list and click [Apply].
Continue	Continues startup processing when an error occurs during startup.
Halt on errors	Stops startup until the operator intervenes when an error occurs during startup.
Last Power On Reason	Displays the reason for the previous server power on.
Last Power Off Reason	Displays the reason for the previous server power off.
Power Restore Policy	Configures the power restore action when the server power is interrupted by an unexpected event such as a power failure. Select the desired action and click [Apply]. The same setup can be performed by "7.4.3 Power On/Off" (→pg.355).
Always Power off	The server does not perform any power restore action if there is a power failure.
Always Power on	The server automatically performs a power restore action if there is a power failure.
Restore to powered state prior to power loss	The server restores the status just before the power failure occurred. If the server power was "On", the power is restored automatically. If the server power was "Off", the power is not restored and remains off.

table: Description of Items Displayed on the [Server Management Information] Screen

Item	Description
ASR&R Options	Configures the server restart settings. The information set here is also applied to the server BIOS setup utility.
ASR & R Boot Delay	If the server shuts down due to a fan failure or temperature error, the server automatically powers on again after the time set here (in minutes). However, if the [Retry Counter] is set to 0, the action for [Action with retry counter zero] is taken.
Action with retry counter zero	Sets the action when the [Retry Counter] is "0".
Power Off	The server does not power on. It remains off.
Start Diagnostic IDE Disk	Starts the diagnostic system HDD.(Unused)
Boot PXE	Boots from PXE device.
Boot iRMC Remote Imag	Boots from remote storage (USB).
Retry Counter	Sets the auto restart count (between 0 and 7) after the server shuts down in the event of an error. This counter is decremented by 1 each time restart is performed due to a fan failure, temperature error, OS watchdog timeout, or boot watchdog timeout. When the counter reaches 0, the action set for "Action with retry counter zero" is taken.
BIOS boot source for next boot	Sets the boot option for the next server startup.
Boot Option	Performs normal startup.
Diagnostic System	Starts the diagnostic system menu.(Unused)
BIOS recovery flash bit	Configures the auto rewrite settings of BIOS.
Enabled	Enables auto rewrite. BIOS is rewritten automatically if the BIOS image to be written is set in the BIOS auto rewrite area.(Unused)
Disabled	Disables auto rewrite.
Power Cycle Delay	Sets the time (0 to 15 seconds) between power off and power on when using power cycles.
Watchdog Settings	Configures the action to take when there is no response from the OS within the specified time or when the boot does not finish. The information set here is also applied to the server BIOS setup utility.
Enabled	Enables Software Watchdog/Boot Watchdog.
Software Watchdog	Monitors response from OS.
Power Cycle	Performs power off/on when timeout occurs.
Reset	Restarts the server when timeout occurs.
Continue	Does nothing when timeout occurs.
Boot Watchdog	Monitors the boot time (time after BIOS ends until OS starts).
Power Cycle	Performs power off/on when timeout occurs.
Reset	Restarts the server when timeout occurs.
Continue	Does nothing when timeout occurs.
Timeout time specification	Specify a value between 1 and 120 (in minutes). The maximum value and the values that can be set depend on the server (BIOS).

7.4.7 Network Settings

Select [Network Settings] from the Remote Management Controller Web interface menu to configure the network settings for the Remote Management Controller.



Network Settings

Ethernet

MAC Address 00:30:05:47:98:A5
IP Address 10.21.136.7
Subnet Mask 255.255.255.0
Gateway 10.21.136.1
DHCP enable □

Ports and Network Services

Web based access
HTTP Port 80
HTTPS Port 443
Force HTTPS □

Text based access
Telnet Port 3172 Telnet Drop Time 600 seconds
SSH Port 22
Telnet enabled ☑

VNC Ports
Remote Storage Ports

POINT

- Select [Ethernet], [Ports], [DHCP], [DNS] under the [Network Settings] menu to move to the top of each item.

■ Ethernet

Specifies the IP address and subnet mask of the Remote Management Controller. Enter each setting and click [Apply] to apply the setting.
The information set here is also applied to the server BIOS setup utility.
Each item is described below.

table: Description of Items Displayed on the [Ethernet] Screen

Item	Description
MAC Address	Displays the MAC address of the LAN installed on the Remote Management Controller.
IP Address	Specifies the IP address of the Remote Management Controller. Enter the IP address and click [Apply] to set.
Subnet Mask	Specifies the subnet mask of the Remote Management Controller. Enter the subnet mask and click [Apply] to set.
Gateway	Specifies the gateway address of the Remote Management Controller. Enter the gateway address and click [Apply] to set.
DHCP	Check this to use DHCP for the Ethernet settings for the Remote Management Controller. When this setting is enabled, DHCP is given preference over the above setting.

■ Ports

Specifies the port number for each access. Enter each setting and click [Apply] to apply the setting. The item is disabled if it is left blank.
Each item is described below.

table: Description of Items Displayed on the [Ports] Screen

Item		Description
Web based access		
	HTTP Port	Specifies the port number for accessing HTTP. The default is "80".
	HTTPS Port	Specifies the port number for accessing HTTPS. The default is "443".
	Force HTTPS	Check this to only enable the HTTPS connection. The default is [Disabled].
Text based access		
	Telnet Port	Specifies the port number for accessing Telnet. The default is "3172".
	Telnet Drop Time	Specifies the auto disconnect time (in seconds) during Telnet connection. The default is [600].
	SSH Port	Specifies the port number for accessing through SSH. The default is "22".
	Telnet enabled	Check to enable Telnet connection. The default is [Enabled].
VNC Ports		
	Standard Port	Displays the port number for performing Video Redirection. The default is "5900" (fixed).
	Secure Port	Displays the port number for using SSH/SSL with Video Redirection. The default is "5910" (fixed).
Remote Storage Ports		
	Standard Port	Displays the port number when connecting remote storage with Video Redirection. The default is "5901" (fixed).
	Secure Port	Displays the port number when connecting remote storage using SSH/SSL with Video Redirection. The default is "5911" (fixed).
Keyboard/Mouse Ports		
	Standard Port	Displays the port number when connecting a keyboard/mouse with Video Redirection. The default is "5902" (fixed).
	Secure Port	Displays the port number when connecting a keyboard/mouse using SSH/SSL with Video Redirection. The default is "5904" (fixed).
Video Ports		
	Standard Port	Displays the port number for the console screen transmission. The default is "5903" (fixed).
	Secure Port	Displays the port number for the console screen transmission when using SSH/SSL. The default is "5913" (fixed).

■ DHCP Settings

Configures the DHCP settings. Enter each setting and click [Apply] to apply the setting.
Each item is described below.

table: Description of Items Displayed on the [DHCP Settings] Screen

Item	Description
Register DHCP Address in DNS	Enable this to the register address obtained by DHCP in DNS.

table: Description of Items Displayed on the [DHCP Settings] Screen

Item	Description
Use iRMC Name instead of Hostname	Enable this to use the characters entered in [iRMC Name] box as DNS registration name.
Add Serial Number	Enable this to add the serial number to the DNS registration name.
Add Extension	Enable this to add the characters entered in the [Extension] box to the end of the DNS registration name.
DNS Name	Displays the name registered in DNS.

■ DNS Settings

Configures the DNS settings. Enter each setting and click [Apply] to apply the setting.
Each item is described below.

table: Description of Items Displayed on the [Network Settings] Screen

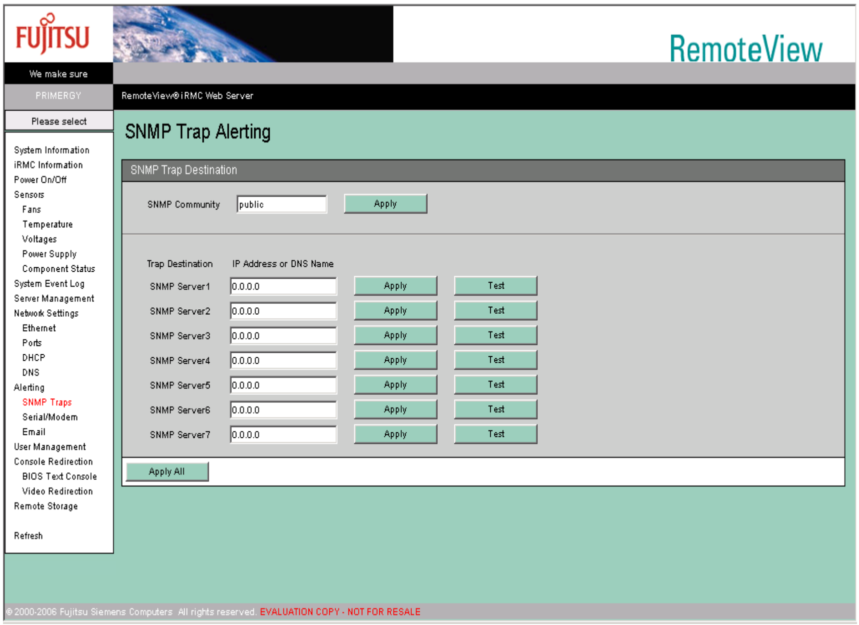
Item	Description
DNS enabled	Enable this to use DNS for name resolution.
Obtain DNS configuration from DHCP	Enable this to obtain DNS settings from DHCP.
DNS Domain	Sets the DNS domain.
DNS Server 1 to 5	Sets the IP of the DNS servers 1 to 5.

7.4.8 Alerting

Sets the SNMP trap and alert email settings. Also shows the SNMP trap alert history.

■ SNMP Trap Alerting

Select [SNMP Traps] from the Remote Management Controller Web interface menu to configure SNMP trap alerting.



SNMP Trap Alerting

SNMP Trap Destination

SNMP Community: public

Trap Destination	IP Address or DNS Name
SNMP Server1	0.0.0.0
SNMP Server2	0.0.0.0
SNMP Server3	0.0.0.0
SNMP Server4	0.0.0.0
SNMP Server5	0.0.0.0
SNMP Server6	0.0.0.0
SNMP Server7	0.0.0.0

Each item is described below.

table: Description of Items Displayed on the [SNMP Trap Alerting] Screen

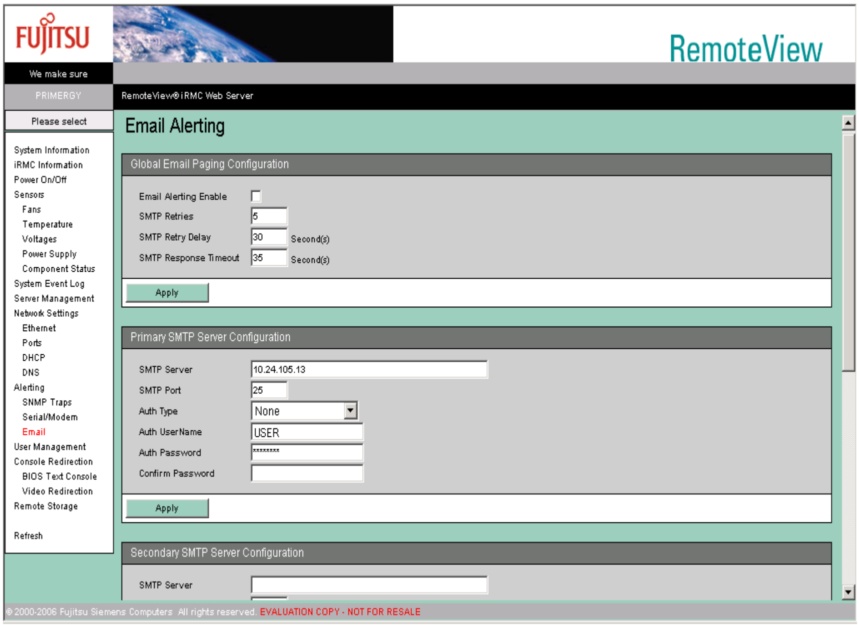
Item	Description
SNMP Trap Destination	Enter each setting and click [Apply All] to apply all settings.
SNMP Community	Set the community name during SNMP trap alert. The default is [Public]. Enter the community name and click [Apply] to set. The SNMP receive community name must be the same in order for the receiving server to receive traps.
Trap Destination SNMP Server 1 to 7	Specify the IP address of the SNMP trap destination server (Trap receive server). Up to seven destination servers may be specified. Enter the IP address of the destination server and click [Apply] to apply. If DNS is enabled, the server name may be set instead of the IP. Click [Test] to send a test trap to the specified server.

POINT

- Serial/Modem Alarting is not supported.

■ Email Alerting

Select [Email] from the Remote Management Controller Web interface menu to configure email settings.



Email Alerting

Global Email Paging Configuration

Email Alerting Enable □
SMTP Retries 5
SMTP Retry Delay 30 Second(s)
SMTP Response Timeout 35 Second(s)

Primary SMTP Server Configuration

SMTP Server 10.24.105.13
SMTP Port 25
Auth Type None
Auth UserName USER
Auth Password ********
Confirm Password

Secondary SMTP Server Configuration

SMTP Server

Each item is described below.

table: Description of Items Displayed on the [Email Alerting] Screen

Item	Description
Global Email Paging Configuration	Sets the SMTP server settings. Enter each setting and click [Apply] to apply the setting.
Email Alerting Enable	Enables/disables the SMTP server settings.
SMTP Retries	Sets the retry count when there is an email transmission error.
SMTP Retry Delay	Sets the retry interval (in seconds).
SMTP Response Timeout	Sets the timeout for the SMTP server response (in seconds).
Primary SMTP Server Configuration	Configures the primary SMTP server.
SMTP Server	Sets the primary SMTP server IP (or the server name if DNS is enabled).
SMTP Port	Sets the port number used by the primary SMTP.
Auth Type	Sets the authorization type for the SMTP server.
NONE	The SMTP server does not require user authorization.
SMTP AUTH (RFC2554)	The SMTP server performs user authorization defined in RFC2554. This is not supported.
Auth UserName	Sets the user name for user authorization. If NONE is set as the [Auth Type], do not set this field.
Auth Password	Sets the password for the [Auth UserName].
Confirm Password	Reenter the password for confirmation.
Secondary SMTP Server Configuration	Configures the secondary SMTP server.

table: Description of Items Displayed on the [Email Alerting] Screen

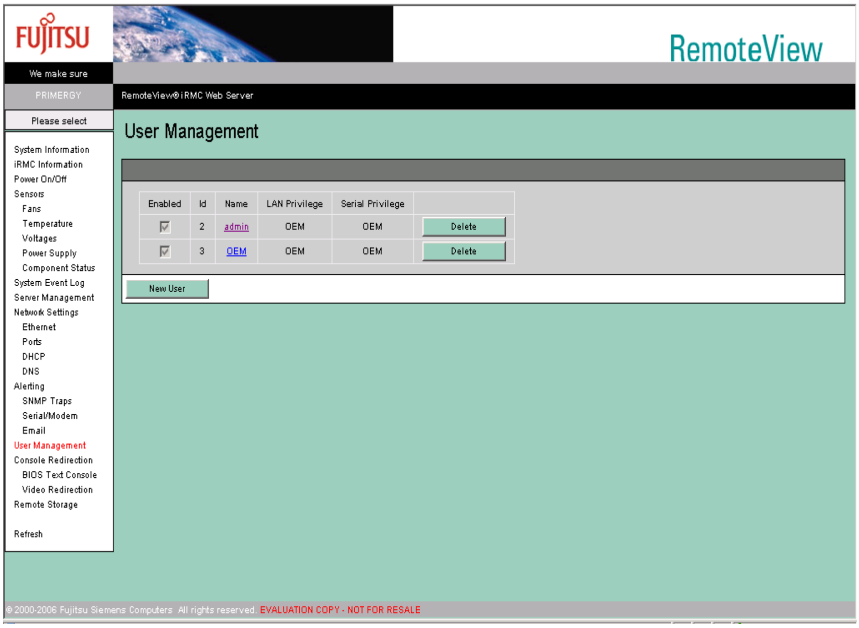
Item	Description
SMTP Server	Sets the secondary SMTP server IP (or the server name if DNS is enabled).
SMTP Port	Sets the port number used by the secondary SMTP.
Auth Type	Sets the authorization type for the SMTP server.
NONE	The SMTP server does not require user authorization.
SMTP AUTH (RFC2554)	The SMTP server performs user authorization defined in RFC2554. This is not supported.
Auth UserName	Sets the user name for user authorization. If NONE is set as the [Auth Type], do not set this field.
Auth Password	Sets the password for the [Auth UserName].
Confirm Password	Reenter the password for confirmation.
Mail Format dependent Configuration	Sets the outgoing email format. Enter each setting and click [Apply] to apply the setting.
From	Sets the sender name.
Subject	Sets the subject of the email. Note that this setting is only valid if it is in ITS format.
Message	Sets the body of the email. Note that this setting is only valid if it is in ITS format.
Admin.Name	Sets the source administrator name. Note that this setting is only valid if it is in ITS format.
Admin.Phone	Sets the source administrator phone number. Note that this setting is only valid if it is in ITS format.
REMCS Id	Sets the REMCS ID. Note that this setting is only valid if it is in REMCS format.
Server URL	Sets the source URL.

POINT

- Only the transmission format can be set in [Mail Format dependent Configuration]. The destination is specified and the transmission level is set in "7.4.9 User Management" (→pg.374).
- E-mail may not be delivered depending on the e-mail software of the specified mail server or LAN line speed. In this case, change the value of "SMTP Response Timeout" of "Global Email Paging Configuration" to about 50 seconds.

7.4.9 User Management

Select [User Management] from the Remote Management Controller Web interface menu to set the user name and password to log in to the Remote Management Controller, the operation level for the user name, and the details for sending email.



Enabled	Id	Name	LAN Privilege	Serial Privilege	
☑	2	admin	OEM	OEM	Delete
☑	3	OEM	OEM	OEM	Delete

Each item is described below.

table: Description of Items Displayed on the [User Management] Screen

Item	Description
Enabled	Enables/disables the user.
Id	Displays the sequence number of the user.
Name	Displays the user name.
LAN Privilege	Displays the access privilege via the LAN port.
Serial Privilege	Displays the access privilege via the serial port. (Unused)

Click [Delete] to delete the registered user. For the default user name, password, and privileges, see "7.2 Preparations" (→pg.346).

IMPORTANT

- In the following cases, the Web interface of the Remote Management Controller cannot be accessed, or not all of its functions are available, so that "Users" cannot be created or modified.
  - When all users are removed
  - When all users with Administrator/OEM privileges are removed or when their privileges are modified to be restricted

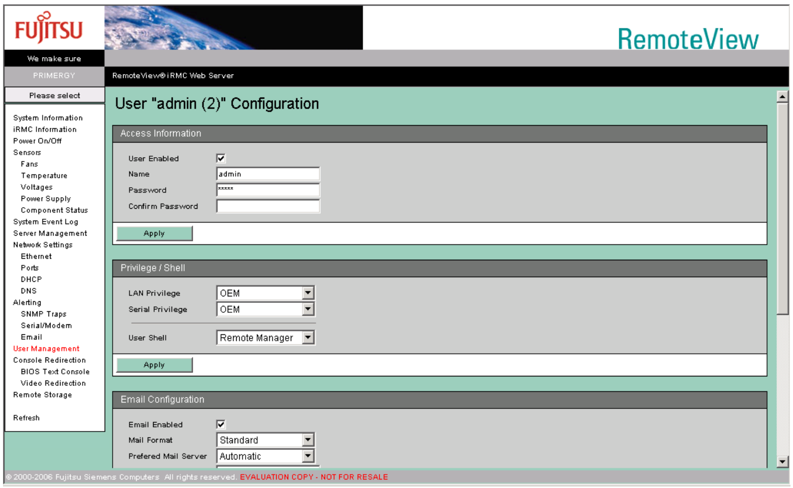
  In these cases, restore the original settings using the "Server Management Tools" supplied with the server as follows:

  1. Insert the "Server Management Tools" disk into the floppy disk drive and turn on the server.

2. Start the Server Management Tools (IPMI-Tool).
   For how to start the Server Management Tools, see the “User's Guide” on the "Documents & Tools CD" supplied with the server.
3. When the IPMI-Tool window is displayed, select [User Management].
4. Select one of "1" through "16".
   To change the privileges for an existing User ID, proceed to Step 7.
5. Enter [User Name], [Password], and [Confirm Password].
6. Press the [F1] key (Set Value) to save the settings, and then press the [Esc] key to return to the [User Settings] window.
7. Press the [F2] key (Configure Access) to select "2 802_3_LAN", and then select "5" (OEM) from [Privilege Limit].
8. Press the [F1] key (Set Value) to save the settings.
   Press the [Esc] key several times to exit the IPMIview.

■ Changing User Information

Click a registered user name to change the registered settings.



User "admin (2)" Configuration

Access Information

User Enabled ☑
Name: admin
Password: *****
Confirm Password:

Privilege / Shell

LAN Privilege: OEM
Serial Privilege: OEM
User Shell: Remote Manager

Email Configuration

Email Enabled ☑
Mail Format: Standard
Prefered Mail Server: Automatic

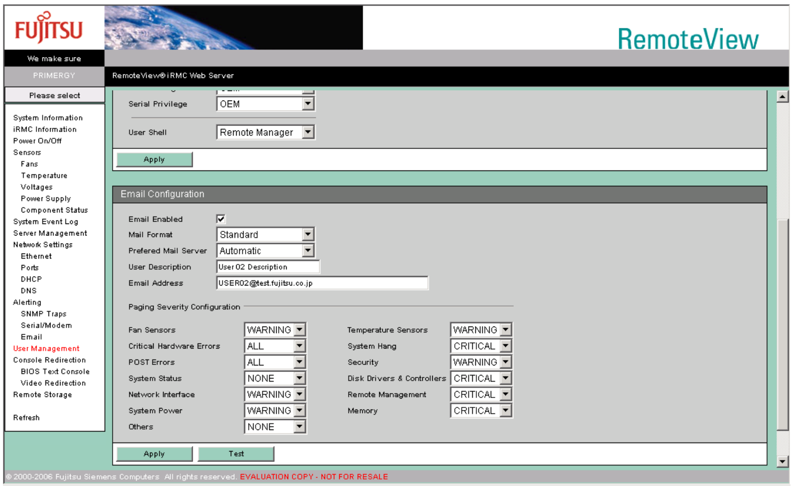
© 2000-2006 Fujitsu Siemens Computers All rights reserved. EVALUATION COPY - NOT FOR RESALE

table: Description of Items Displayed on the [User Configuration] Screen

Item	Description
Access Information	Sets the user information. Set or change each item and click [Apply].
User Enabled	Enables/disables the user. This setting must be enabled.
Name	Sets the user ID.
Password	Sets the password.
Confirm Password	Reenter the password.
Privilege / Shell	Sets the operation level. Set or change each item and click [Apply].
LAN Privilege	Sets the LAN connection operation level.
USER	Permission to only view most items.
Operator	Permission to make changes in addition to USER privileges.
Administrator	Permission to create users in addition to Operator privileges.
OEM	Permission to use special Telnet commands in addition to Administrator privileges.
Serial Privilege	Sets the serial port connection operation level. This is not supported.
User Shell	Sets the Telnet connection operation level. Only Remote Manager is supported.

■ Settings for Sending Email

Configures the email sending settings for each user.



Serial Privilege: OEM

User Shell: Remote Manager

Email Configuration

Email Enabled ☑

Mail Format: Standard

Prefered Mail Server: Automatic

User Description: User 02 Description

Email Address: USER02@test.fujitsu.co.jp

Paging Severity Configuration

Fan Sensors	WARNING	Temperature Sensors	WARNING
Critical Hardware Errors	ALL	System Hang	CRITICAL
POST Errors	ALL	Security	WARNING
System Status	NONE	Disk Drivers & Controllers	CRITICAL
Network Interface	WARNING	Remote Management	CRITICAL
System Power	WARNING	Memory	CRITICAL
Others	NONE		

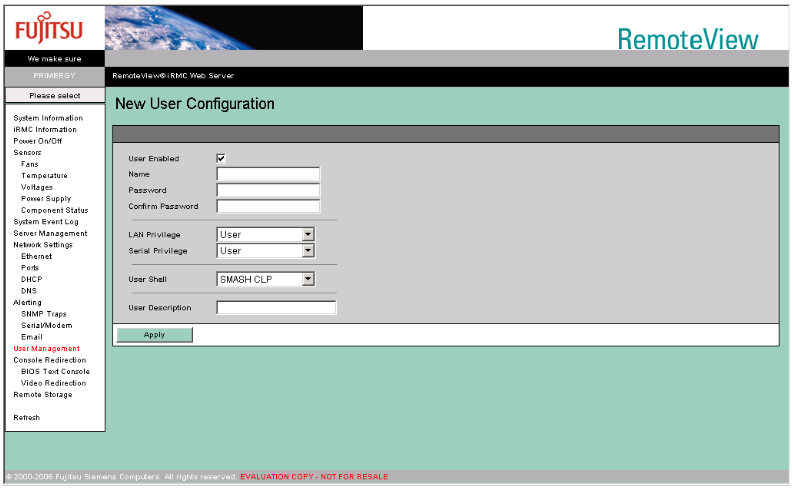
© 2000-2006 Fujitsu Siemens Computers All rights reserved. EVALUATION COPY - NOT FOR RESALE

table: Description of Items Displayed on the [Email Configuration] Screen

Item	Description
Email Configuration	Sets the outgoing email settings. Set or change each item and click [Apply].
Email Enabled	Enable/disable the setting.
Mail Format	Select the outgoing email format.
Standard	Normal email format.
ITS-Format	ITS type email format. This is not supported.
Fujitsu REMCS-Format	REMCS type email format.
Prefered Mail Server	Selects the SMTP server to be used from the SMTP servers set in "■ Email Alerting" (→pg.372).
Automatic	Selects the available SMTP server from the primary and secondary servers in this order.
Primary	Selects the SMTP server specified in the Primary SMTP Server Configuration.
Secondary	Selects the SMTP server specified in the Secondary SMTP Server Configuration.
User Description	Enters the description of the email sending user.
Email Address	Sets the email destination address.
Paging Severity Configuration	Selects the event to send the email. Set this for each event.
NONE	No email is sent.
CRITICAL	Send an email when a critical level event occurs.
WARNING	Send an email when a warning or higher-level event occurs.
ALL	Send an email for all event levels.
Test button	Sends a test email.

■ Creating New User Information

Click [New User] to create a new user.



New User Configuration

User Enabled ☑

Name

Password

Confirm Password

LAN Privilege: User

Serial Privilege: User

User Shell: SMASH CLP

User Description

© 2000-2006 Fujitsu Siemens Computers All rights reserved. EVALUATION COPY - NOT FOR RESALE

table: Description of Items Displayed on the [New User Configuration] Screen

Item		Description
User Enabled		Enables/disables the user. This setting must be enabled.
Name		Sets the user ID.
Password		Sets the password.
Confirm Password		Reenter the password.
LAN Privilege		Sets the LAN connection operation level.
	USER	Permission to only view most items.
	Operator	Permission to make changes in addition to USER privileges.
	Administrator	Permission to create users in addition to Operator privileges.
	OEM	Permission to use special Telnet commands in addition to Administrator privileges.
Serial Privilege		Sets the serial port connection operation level. This is not supported.
User Shell		Sets the Telnet connection operation level. Only Remote Manager is supported.
User Description		Enters the description of the user.

IMPORTANT

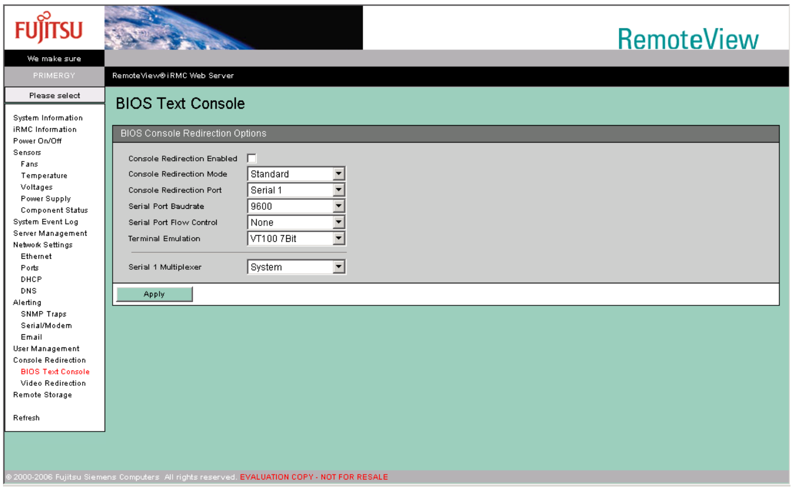
- When using the iRMC Telnet function from the RemoteControlService, the login user needs the following privileges:
  - LAN Privilege: Administrator
  - USER Shell : Remote Manager

7.4.10 Console Redirection

This function is used to configure and display the redirection settings for the console screen.

■ BIOS Text Console

Select [BIOS Text Console] from the Remote Management Controller Web interface menu to configure the text screen redirection of the RemoteControlService.



BIOS Text Console

BIOS Console Redirection Options

Console Redirection Enabled	□
Console Redirection Mode	Standard
Console Redirection Port	Serial 1
Serial Port Baudrate	9600
Serial Port Flow Control	None
Terminal Emulation	VT100 7Bit
Serial 1 Multiplexer	System

IMPORTANT

- The BIOS Text Console settings vary depending on the server type. For each setting, see "5.2.3 Configuration for IPMI" (→pg.270).

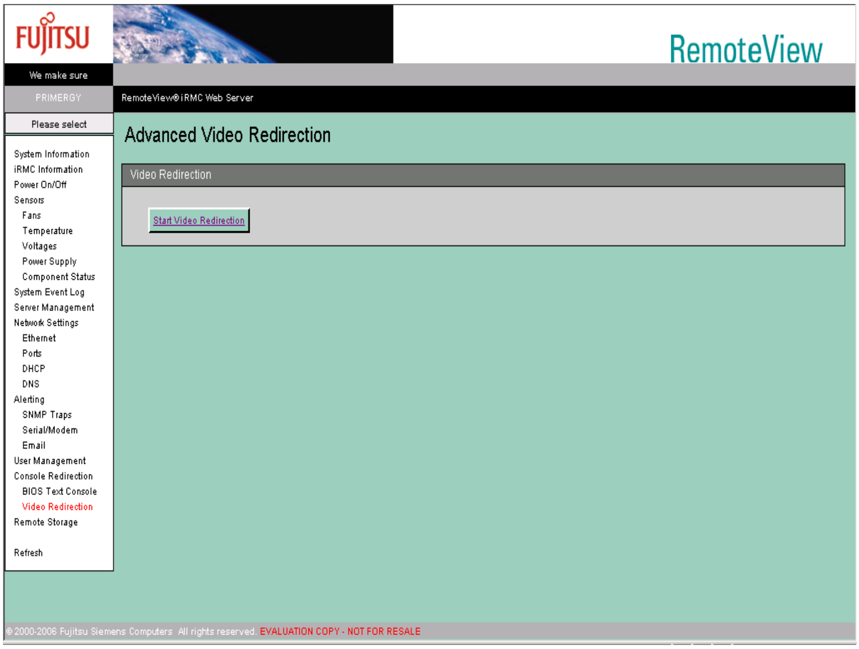
■ Advanced Video Redirection

Select [Video Redirection] from the Remote Management Controller Web interface menu to remotely perform console redirection.

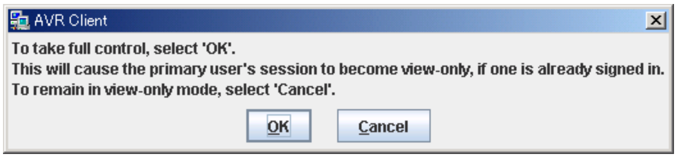
IMPORTANT

- A separate license key is necessary to use the Video Redirection function.
  For details on the license key and how to authorize the license, see the “Remote Management Controller Upgrade User’s Guide“.

When the license is authorized, the following window appears.



When clicking [Start Video Redirection], the Video Redirection window opens. Initially, the following screen is displayed.

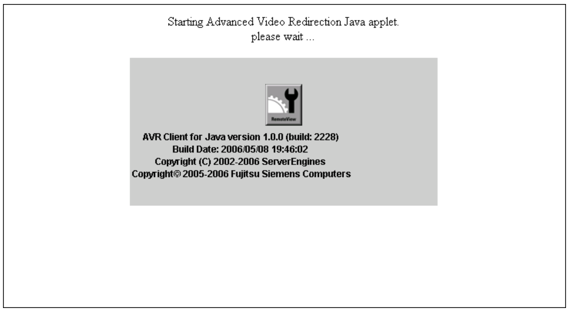


To take full control, select 'OK'.
This will cause the primary user's session to become view-only, if one is already signed in.
To remain in view-only mode, select 'Cancel'.

When using a mouse or a keyboard, click [OK] to enter the Full Control mode. If you click [Cancel], the View mode is applied and you cannot use a mouse or a keyboard. The console is only displayed.

POINT

- Because the Video Redirection function uses Java, the following window opens. However, it does not close automatically when you exit the Video Redirection. Close it manually.



Starting Advanced Video Redirection Java applet.
please wait ...

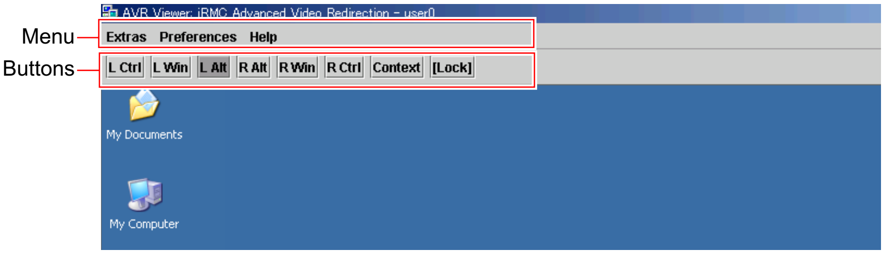
AVR Client for Java version 1.0.0 (build: 2228)
Build Date: 2006/05/08 19:46:02
Copyright (C) 2002-2006 ServerEngines
Copyright© 2005-2006 Fujitsu Siemens Computers

IMPORTANT

- The Video Redirection does not support the following display mode:
  - 1024 x 768 24-bit/32-bit color mode
  - Using the VGA driver other than standard one
- When Video Redirection is started repeatedly without closing the Web interface of the Remote Management Controller, Java error may occur or Video Redirection may not make a response. In this case, close all browsers and start the Web interface of the Remote Management Controller again.

■ Video Redirection Window Layout

When the Video Redirection is started, the following window appears.
At the top of the window, there is a menu with buttons below.



● Menu

table: Video Redirection Menu

Item		Description
Extras		
	Remote...	Sets the remote storage connection settings. →"■ Remote Storage Connection" (pg.383)
	Virtual Keyboard...	Displays the graphical keyboard. →"■ Graphical Keyboard" (pg.384)
	Refresh Screen	Refreshes the Redirection window.
	Take Full Control...	Changes the mode to the Full Control mode. (Only effective in the View mode)
	Disconnect Session...	Disconnects the Video Redirection. (Not supported)
	Relinquish Full Control...	Changes the mode to the View mode. (Only effective in the Full Control mode)
	Exit	Exits the Video Redirection.
Preferences		Sets the mouse, keyboard, and log settings. →"■ Mouse and Keyboard Settings" (pg.384)
Help		Displays the Video Redirection version.

● Buttons

table: Video Redirection Buttons

Button	Description
[L Ctrl]/[R Ctrl]	Correspond to the left and right [Ctrl] keys.
[L Win]/[R Win]	Correspond to the left and right Windows keys.
[L Alt]/[R Alt]	Correspond to the left and right [Alt] keys.
[Context]	Displays the right mouse click menu.
[Lock]	Holds the status of pressing the [Ctrl], [Alt], or [Windows] key. These keys are not automatically released. To release them, press the [Lock] button again.

POINT

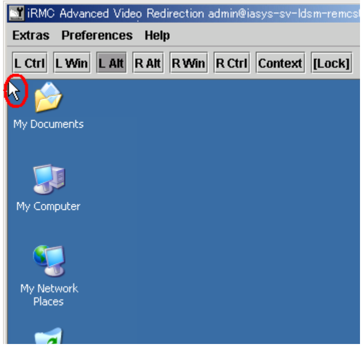
- To log on to Windows, click the [R Ctrl] (or [L Ctrl]) button and the [R Alt] (or [L Alt]) button in this order, and then press the [Delete] key on the keyboard.

IMPORTANT

- When changing the URL to connect other Remote Management Controller without closing the Web interface of the Remote Management Controller, [Storage...] of the [Extras] menu of Video Redirection is not displayed. To connect other Remote Management Controller, close the browser once.

■ Enabling Mouse Cursor Synchronization

When moving the mouse cursor to the upper-left corner of the Video Redirection window, the mouse cursor moves in synchronization.



If the mouse cursor does not move in synchronization, configure the following settings on the server for Video Redirection:

After configuring the settings, synchronize the mouse in the upper left of the Video Redirection screen.

● For Windows

- Mouse Settings
  1. Open the Control Panel and double-click the [Mouse] icon.
  2. In the [Motion] tab, set the [Acceleration] item to "None" and uncheck [Enhance Pointer Precision] if checked.
- Display Settings
  1. Open the Control Panel and double-click the [Display] icon.
  2. Click [Advanced] in the [Settings] tab.
  3. Slide the [Hardware Accelerator] in the [Troubleshooting] tab one-notch left from "Maximum" and click [OK].

● For Linux

- For Red Hat (Enterprise Linux 3)
  1. Use the editor such as vi to open the X Window configuration file.

```
>vi /etc/X11/XF86Config
```

  2. Change the following two lines.

```
Identifier  "Mouse0"          →  Identifier  Change to "DevInputMice"
Driver      "mouse"
Option      "Protocol" "PS/2"

Identifier  "DevInputMice"    →  Identifier  Change to "Mouse0"
Driver      "mouse"
Option       "Protocol" "IMPS/2"
```

  3. Close the file and restart the X Window.
  4. Start [Main Menu] - [Preferences] - [Mouse] and click the [Motion] tab to adjust [Acceleration].
     The amount in which the slider is moved depends the machinetype where the Web interface starts and the server type.
     - When the cursor of the server does not catch up with the cursor of Video Redirection
       Move the slider to [Slow].
     - When the cursor of the server moves faster than the cursor of Video Redirection
       Move the slider to [Fast].
- For Red Hat (Enterprise Linux 4)
  1. Execute the following command.

```
>xset m 0 0
```

- For SUSE Linux
  1. When there are two or more mice installed, remove all mice except the first one.
     1. Execute "sax32" from the menu.
     2. Select [Input device] → [mouse] and remove all mice except the first one.
  2. Select [Control Center] → [Input device] → [mouse] from the Main menu.
  3. Set the [Advance Pointer Accelerator] value to "1x".

IMPORTANT

- Restrictions on synchronizing the mouse cursor on Red Hat (Enterprise Linux 3) are as follows.
  - Abnormality may occur when the gpm service is used.
  - If the settings for the mouse of X-Window (including the redhat-config-mouse command) is performed, the mouse of the server cannot be used.

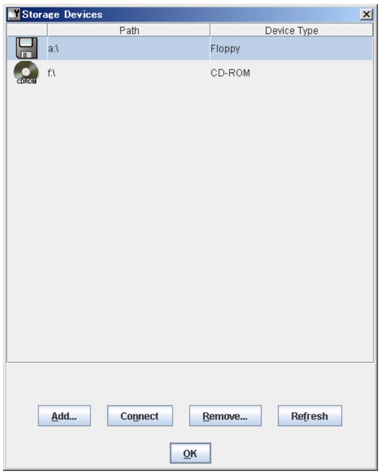
  Even if Video Redirection is closed, the settings are taken over. Restore the settings when Video Redirection is closed, and restart X-Window.

■ Remote Storage Connection

Select [Extra] and then [Storage...] from the menu to execute the Remote Storage Connection.

The remote storage connection is a function to connect the external memory of the machine that has the Web interface as a remote connected device of the object server of Video Redirection.

Select the desired device and click [Connect] to connect to the server used for the Video Redirection.



Path	Device Type
a:\	Floppy
f:\	CD-ROM

IMPORTANT

- To use a function of the remote storage connection, the license key is required.
  For details on the license key and how to authorize the license, see the “Remote Management Controller Upgrade User’s Guide“.
- The remote storage connection is available to the following devices. However, the writing function in DVD drive is not supported.
  - Internal floppy drive
  - ATAPI CD-ROM drive
  - ATAPI DVD drive
  - USB floppy drive
  - USB CD-ROMdrive
- The remote storage connection is automatically released when exiting VideoRedirection.

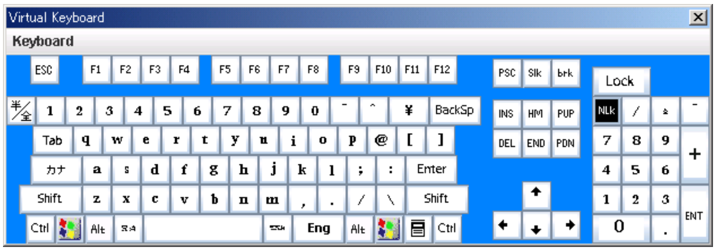
POINT

- To disconnect a device, select the desired device and click [Disconnect].
- If there are devices not displayed in the remote storage list, click [Refresh]. The devices are searched once more.
- To add a device not displayed in the window (such as ImageFile), click [Browse] and specify.
- Floppy disk drives and CD-ROM drives are not displayed in the list unless a medium is inserted.
- Remote devices cannot be connected additionally or disconnected individually.
- To connect to multiple remote devices at a time on Linux, you need to enable the Multi LUN setting on the OS. For details, see the OS command reference.
- If the BIOS supports USB Legacy, you can boot from the media connected by Remote Storage. Use the BIOS Setup Utility to set [Multiboot] and [USB Legacy Support] to [Enabled] and set the media connected by Remote Storage to the top of the BOOT order.

■ Graphical Keyboard

Select [Extras] and then [Virtual Keyboard...] from the menu to display a graphical keyboard in the Video Redirection window.

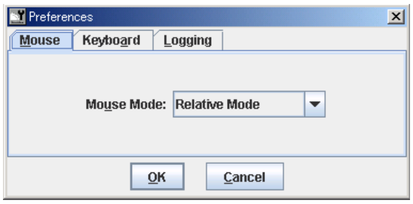
Click the displayed keyboard with the mouse to send the corresponding key to the server.


Virtual Keyboard
Keyboard
ESC F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 PSC Slk brk Lock
半/全 1 2 3 4 5 6 7 8 9 0 - ^ ¥ BackSp INS HM PUP NLk / * -
Tab q w e r t y u i o p @ [ ] DEL END PDN 7 8 9 +
カナ a s d f g h j k l ; : Enter 4 5 6
Shift z x c v b n m , . / \ Shift 1 2 3
Ctrl Alt Eng Alt Ctrl 0 . ENT

■ Mouse and Keyboard Settings

Select [Preferences] and then [Preferences...] from the menu to set the mouse mode, keyboard key arrangement, log collection, and window settings.

After changing the settings and clicking [OK], you are prompted to enter the user name and the password. Enter your user name and password and click [Yes] to apply the setting.



Mouse Mode: Relative Mode

IMPORTANT

- A user name and password for a user with Remote Management Controller Administrator privileges are required to configure these settings.

● Mouse Tab

This tab is used to set the mouse mode.

table: Mouse Settings

Item		Description
Mouse Mode:		
	Hide Mode (Relative)	Disables the display of the mouse cursor at the operator side (in Relative Mode).
	Absolute Mode	X axis, Y axis address movement mode.
	Relative Mode	Relative address movement mode.

● Keyboard Tab

This tab is used to set the keyboard key arrangement and connection type.

table: Keyboard Settings

Item	Description
Language:	Sets the keyboard layout.

● Logging Tab

This is used to create the Video Redirection log.

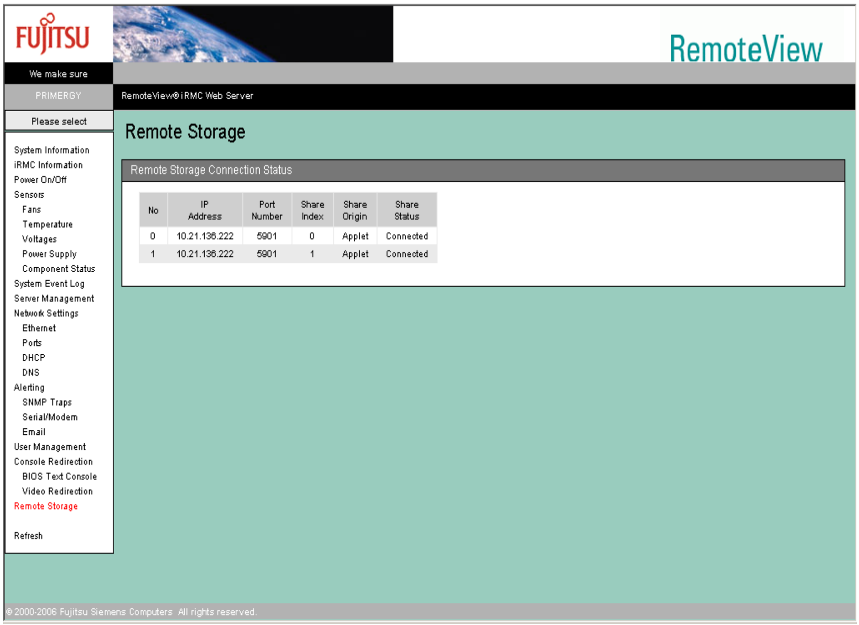
table: Log Creation Method

Item		Description
Global Logging		Specifies the output path for the logs.
	None	Does not output a log file.
	Console	Outputs the logs to the Java Console.
	Log File	Outputs the logs into the specified file.
	Console and Log File	Outputs the logs to the Java Console and to the specified file.
Console Log File		Specifies the log to be output.
Overwrite Native Library		Allows overwriting of DLLs. (Not supported)

7.4.11 Remote Storage

Select [Remote Storage] from the Remote Management Controller Web interface menu to display the remote storage status.

This function displays the status of the remote devices specified in the Video Redirection.



Remote Storage

Remote Storage Connection Status

No	IP Address	Port Number	Share Index	Share Origin	Share Status
0	10.21.136.222	5901	0	Applet	Connected
1	10.21.136.222	5901	1	Applet	Connected

Each item is described below.

table: Description of Items Displayed on the [Remote Storage] Screen

Item		Description
No		Sequential number of remote devices
IP Address		IP address of the server or PC where the device is installed
Port Number		Port number that the remote device uses for connection/communication.
Share Index		Number assigned to the connection
Share Origin		Status of the device at the server or PC where the device is installed
	None	Not connectable (Unfound)
	Applet	Connectable (Found)
Share Status		Current status of connection
	Idol	Not connected
	Connected	Connected

POINT

- This item is displayed only. Connection and disconnection can only be performed in the Video Redirection.

Appendix

This chapter explains supplementary information such as troubleshooting and how to uninstall ServerView.

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 Console Manually" (→pg.57) 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 Console Manually" (→pg.57).
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. • (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 Console Manually" (→pg.57) 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. # cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/LinuxSVAgent/Agent/ snmpd.conf /etc/snmp/snmpd.conf
4103–4401	failure in "***" command.
	Error occurred in the Linux system command. Refer to "■ Installing ServerView Linux Console Manually" (→pg.57) and then perform the installation.
4402	failure in "/etc/init.d/snmpd start" command.
	Failed to start up the snmp service. Check whether the /etc/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 Console Manually" (→pg.57).
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/LinuxSVAgent/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/init.d/srvmagt stop # /etc/init.d/eecd stop # /etc/init.d/eecd start # /etc/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/LinuxSVAgent/Agent/ srvmagt-eecd-X.XX- XX.redhat.rpm (X.XX-XX means version number.) # cd / # /etc/init.d/srvmagt stop # /etc/init.d/eecd stop # /etc/init.d/eecd start # /etc/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/LinuxSVAgent/Agent/ srvmagt-agents-X.XX- XX.redhat.rpm (X.XX-XX means version number.) # groupadd svuser # cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/LinuxSVAgent/Agent/config /etc/ srvmagt/config # chmod 644 /etc/srvmagt/config # cd / # /etc/init.d/srvmagt stop # /etc/init.d/eecd stop # /etc/init.d/eecd start # /etc/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/LinuxSVConsole/Console/ # ./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/LinuxSVConsole/Console/ # ./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. # cd /mnt/cdrom/, /media/cdrom/ or /media/cdrecorder/Svmanage/LinuxSVAgent/Agent/config/etc/ srvmagt/ config # chmod 644 /etc/srvmagt/config # cd / # /etc/init.d/srvmagt stop # /etc/init.d/eecd stop # /etc/init.d/eecd start # /etc/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	failure in "cd /" command.
	Failed to change the current directory. Execute the command below. # cd / # /etc/init.d/srvmagt stop # /etc/init.d/eecd stop # /etc/init.d/eecd start # /etc/init.d/srvmagt start
7008	failure in "/etc/init.d/srvmagt start" command.
	Failed to start up ServerView Agent (srvmagt-agents). Execute the command below. # cd / # /etc/init.d/srvmagt stop # /etc/init.d/eecd stop # /etc/init.d/eecd start # /etc/init.d/srvmagt start
7009	failure in "/etc/init.d/eecd start" command.
	Failed to start up ServerView Agent (srvmagt-eecd). Execute the command below. # cd / # /etc/init.d/srvmagt stop # /etc/init.d/eecd stop # /etc/init.d/eecd start # /etc/init.d/srvmagt start
9900	failure in make Inventory data. ServerView's RPMs are installed failed.
	Inventory data (VersionView.sav) creation has failed. Rerun the installation script or confirm that the SNMP service has been started.

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.219)).

● 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.136).

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/init.d/eecd stop.
3. Execute # /etc/init.d/eecd rescan.
4. Execute # /etc/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 [Uncoltrollable] 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.401)).

- 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, AlarmSerice will not run correctly.
From the [Start] button, execute [Change Computer Details] (refer to "2.4.8 Changing Computer Information after Installation" (→pg.80)).

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 (Recov-
ery)
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 ServierView 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].

IMPORTANT

- Generally, do not start [Restart ServerView Base Services].

B Uninstallation

This appendix describes how to uninstall the ServerView.

B.1 Uninstalling ServerView

IMPORTANT

- 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

IMPORTANT

- When uninstalling ServerView Console, configurations such as the server list and alarm settings are deleted. The function to take over the settings automatically is not provided, so keep a copy of settings before uninstalling it. Configure the settings again after the update installation.

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

IMPORTANT

- 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.136) and "■ [Watchdog] Tab (ServerView S2) / [Watchdog Settings] Tab (Management Console)" (→pg.136).
  - Stop monitoring by Treshold Manager of Management Console.
    Refer to "■ Stopping Threshold Monitoring" (→pg.227).
  - 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.188).
  - When uninstalling ServerView Agent, the settings that are configured using Management Console or ServerView S2 such as the power schedule and ASR settings are deleted. The function to take over the settings automatically is not provided, so keep a copy of settings before uninstalling it. Configure the settings again after the update installation.

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

IMPORTANT

- 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.136) and "■ [Watchdog] Tab (ServerView S2) / [Watchdog Settings] Tab (Management Console)" (→pg.136).
  - Stop monitoring by Treshold Manager of Management Console.
    Refer to "■ Stopping Threshold Monitoring" (→pg.227).
  - When uninstalling ServerView Linux Agent, the settings that are configured using Management Console or ServerView S2 such as the power schedule and ASR settings are deleted. The function to take over the settings automatically is not provided, so keep a copy of settings before uninstalling it. Configure the settings again after the update installation.

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-eecd
# rpm -e srvmagt-mods_src
```

ServerView Linux will be uninstalled.

If necessary, change the value to "/etc/snmp/snmpd.conf" to an initial value.

■ [Linux]Uninstalling ServerView S2/AlarmService

IMPORTANT

- Since there is a dependency between ServerView S2 and RemoteControlService/Web, ServerView S2 cannot be uninstalled when RemoteControlService/Web is installed. RemoteControlService/Web must be uninstalled before uninstalling ServerView S2.
  For information about how to uninstall RemoteControlService/Web, refer to "5.2.1 Installing/Uninstalling RemoteControleService/Web" (→pg.269).

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

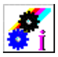
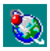
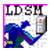
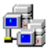
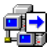
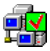
Icon	Meaning
	OK. All components are OK.
	Error. Any errors occurring in one or more components.
	The status deteriorates. The status for one or more components deteriorates.
	Uncontrollable. Status of components is not determined.
	Investigation status. Undetermined status during investigation status.
	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:

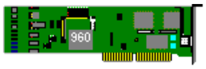
table: List of icons shown on the [Server List] menu

Icon	Meaning
	Maintenance Buttery support
+	ASR: Automatic System Reconfiguration/Restart Automatic server search
↷	Restart Restarting the server
✕ GO	Terminating server shutdown/power-off
OFF	Shut down and OFF Server shut down and power off
RAM RAM RAM	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

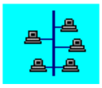
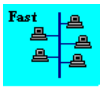
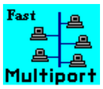
Icon	Meaning
	Ethernet network card
	Fast Ethernet network card
	Ethernet network card (multiple network connections mulitiport)
	Fast Ethernet network card (multiple network connections mulitiport)

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 1	Slot location on the systemboard: Slot 1 is bottom
Slot 1	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.
DOS	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:

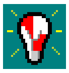
table: Blade server status icons

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

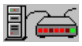
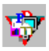
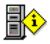
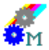
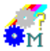
C.10 Other icons

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)
SCAN	Scanner (red: error, green: online, yellow: stand-by, blue: unknown)
▭	Tape drive device (red: error, green: online, yellow: stand-by, blue: unknown)
1	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	Graph view
431 1707 470 24	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.HardError Count	Hardware error count (configured DAC disk only)
physDev960.MiscErrorCount	Various error counts (configured DAC disk only)
physDev960.ParityError Count	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.InternalMacTransmit Errors	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: • 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

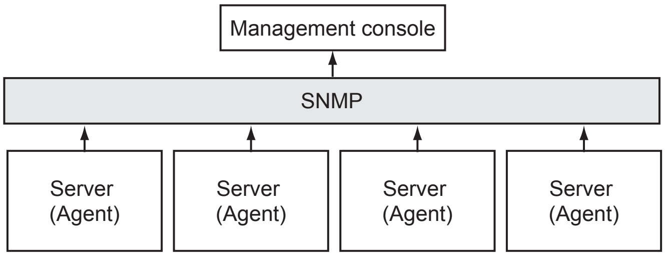
Value	Meaning
ups.TimeOnBattery	The elapsed time since the UPS switched to battery power.

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.424).

■ Fujitsu server management

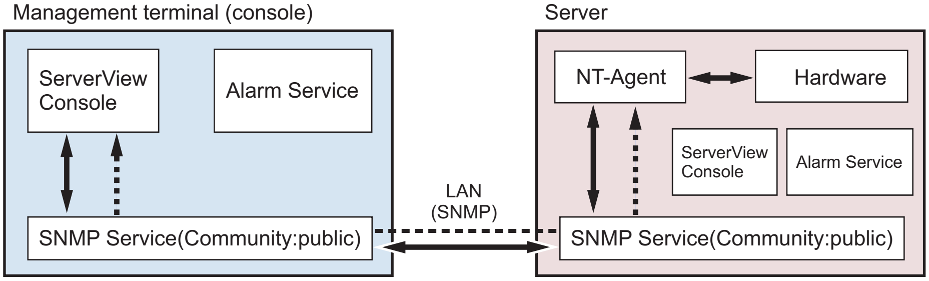
Behind the server management, there is a basic idea that there must be the Management Console accesses to the server management information on the network.
To accomplish this function, the server hardware and firmware are designed to follow this concept.
The Agent accesses the existing information and 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.

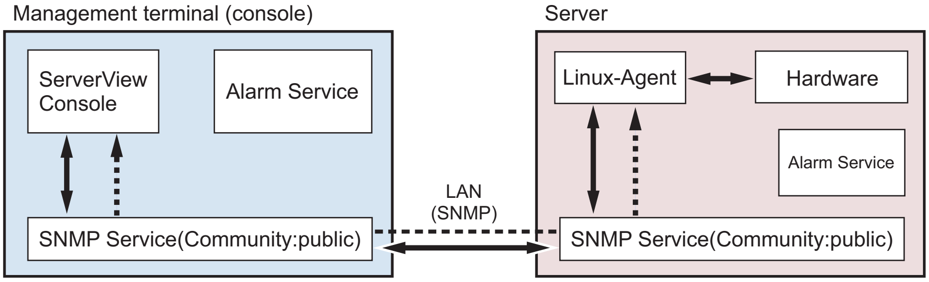
● For Windows:

Install ServerView Agent on the server.



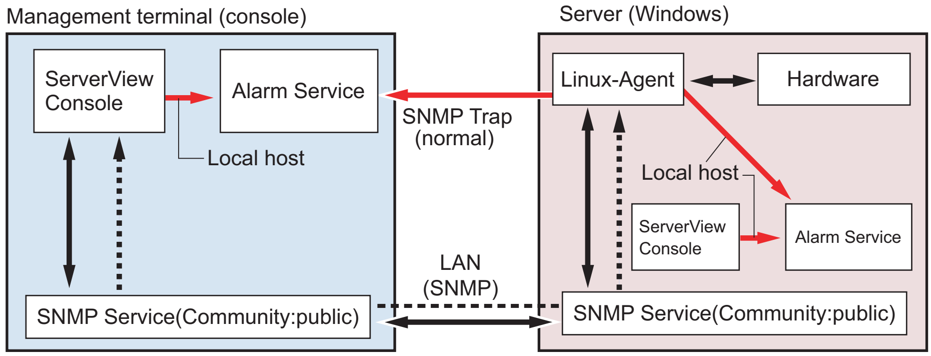
● For Linux:

Install Linux Agent and Linux AlarmService on the server.


Management terminal (console)
ServerView Console
Alarm Service
SNMP Service(Community:public)
LAN (SNMP)
Server
Linux-Agent
Hardware
Alarm Service
SNMP Service(Community:public)

● 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 a 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 snmpd.conf to any community name.

For the location of the snmpd.conf, see "2.3.4 [Linux] Installing ServerView Linux Agent" (→pg.46).

```
com2sec svSec localhost public
com2sec svSec default public
(snip)
trapsink 127.0.0.1 public
```

IMPORTANT

- ▶ Do not change the line “com2sec svSec localhost public”, since the ServerView Linux Agent uses “public” in internal communication. If the line is missing, add the line.

2 If the version of your ServerView Linux Agent is V4.30-16 or prior, add the following lines to the [Configuration] sections of /etc/srvmagt/VersionView.ini and /etc/srvmagt/Status_MIB.ini.

For information on how to check the version of ServerView Linux Agent, see "2.3.4 [Linux] Installing ServerView Linux Agent" (→pg.46).

```
SnmpCommunity = new community name
```

3 After editing, execute the following commands.

```
# /etc/init.d/srvmagt stop
# /etc/init.d/snmpd stop
# /etc/init.d/eecd stop
# /etc/init.d/eecd start
# /etc/init.d/snmpd start
# /etc/init.d/srvmagt start
```

IMPORTANT

- ▶ If a software that configures the SNMP community name is installed, such as Systemwalker CentricMGR, set the same community name as the revised name. For information about the settings, refer to the manual supplied with the software.

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

This section describes how to check the firmware version of remote service board (RSB).

■ 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.

F.8 Configuring Access Privileges

This section explains how to configure the access privileges to ServerView S2 (WebExtension) / AlarmService.
ServerView S2 (WebExtension) / AlarmService is a web-browser-based SNMP management console utilizing Apache or IIS. The access privileges to the management console depend on the configuration of the web server in use.

IMPORTANT

- The explanation here is for the minimum configuration for using the ServerView console. If further settings are required, see the documentations of the respective web server.

■ Configuring Apache (Linux)

For Linux, the ServerRoot and/or DocumentRoot vary depending on the distribution.
In the configuration examples below, Red Hat Enterprise Linux AS/ES v.4 is assumed.

● Access Restriction by the Connecting Host

In the configuration example below, the accessible host is limited to "192.168.0.2" only.
Add the following lines to the file "/etc/httpd/conf/httpd.conf":

```
<Directory "/var/www/cgi-bin/ServerView">
    Order deny,allow
    deny from all
    Allow from  192.168.0.2
</Directory>
<Directory "/var/www/html/ServerView">
    Order deny,allow
    deny from all
    Allow from  192.168.0.2
</Directory>
<Directory "/var/www/html/AlarmService">
    Order deny,allow
    deny from all
    Allow from  192.168.0.2
</Directory>
<Files "sv_www.html">
    Order deny,allow
    Deny from all
    Allow from  192.168.0.2
</Files>
<Files "AlarmService.html">
    Order deny,allow
    Deny from all
    Allow from  192.168.0.2
</Files>
<Files "svagent.html">
    Order deny,allow
    Deny from all
    Allow from  192.168.0.2
</Files>
```

● Access Restriction by User Authentication

User authentication is required when connecting to the management console. Execute the following command to create a user and set a password:

```
# htpasswd -c /etc/httpd/conf/svpasswd websvuser
New password: ******
Re-type new password: ******
Adding password for user websvuser
```

Then, add the following lines to the file "/etc/httpd/conf/httpd.conf":

```
<Directory "/var/www/cgi-bin/ServerView">
    AuthType Basic
    AuthName "SV Console"
    AuthUserFile /etc/httpd/conf/svpasswd
    Require user websvuser
</Directory>
<Directory "/var/www/html/ServerView">
    AuthType Basic
    AuthName "SV Console"
    AuthUserFile /etc/httpd/conf/svpasswd
    Require user websvuser
</Directory>
<Directory "/var/www/html/AlarmService">
    AuthType Basic
    AuthName "SV Console"
    AuthUserFile /etc/httpd/conf/svpasswd
    Require user websvuser
</Directory>
```

■ Configuring Apache (Windows)

● When Installed with SSL Enabled

If SSL is selected to be enabled during ServerView installation, "ssl.conf" is effective as a configuration file. In this case, limitation using a password is enabled for the whole web server with the default settings. The following setting disables the default password security setting:

Access Restriction by the Connecting Host

In the configuration example below, the accessible host is limited to "192.168.0.2" only.
Comment out the following section in the configuration file "C:\Program Files\Fujitsu\F5FBFE01\ServerView Services\WebServer\conf\ssl.conf".

```
# settings for user/password authentication:
# wwwroot
... omitted ...
#</IfDefine>
```

Then add the following section to "C:\Program Files\Fujitsu\F5FBFE01\ServerView Services\WebServer\conf\ssl.conf".

```
<Directory "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/scripts/SERVER~1">
    Order deny,allow
    deny from all
    Allow from  192.168.0.2
</Directory>
<Directory "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/wwwroot/SERVER~1">
    Order deny,allow
    deny from all
    Allow from  192.168.0.2
</Directory>
<Directory "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/wwwroot/ALARMS~">
    Order deny,allow
    deny from all
    Allow from  192.168.0.2
</Directory>
<Files "sv_www.html">
    Order deny,allow
    Deny from all
    Allow from  192.168.0.2
</Files>
<Files "AlarmService.htm">
    Order deny,allow
    Deny from all
    Allow from  192.168.0.2
</Files>
<Files "svagent.html">
    Order deny,allow
    Deny from all
    Allow from  192.168.0.2
</Files>
```

Access Restriction by User Authentication

User authentication is required when connecting to the management console. Execute the following command at the command prompt to create a user and set a password:

```
C:\>cd C:\Program Files\Fujitsu\F5FBFE01\ServerView Services\WebServer\bin
C:\Program Files\Fujitsu\F5FBFE01\ServerView Services\WebServer\bin
>htpasswd -c svpasswd websvuser
New password: ******
Re-type new password: ******
Adding password for user websvuser
```

Comment out the following section in the configuration file "C:\Program Files\Fujitsu\F5FBFE01\ServerView Services\WebServer\conf\ssl.conf".

```
# settings for user/password authentication:
# wwwroot
... omitted ...
#</IfDefine>
```

Then add the following section to "C:\Program Files\Fujitsu\F5FBFE01\ServerView Services\WebServer\conf\ssl.conf".

```
<Directory "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/scripts/SERVER~1">
    AuthType Basic
    AuthName "SV Console"
    AuthUserFile "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/WebServer/bin/passwd"
    Require user websvuser
</Directory>
<Directory "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/wwwroot/SERVER~1">
    AuthType Basic
    AuthName "SV Console"
    AuthUserFile "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/WebServer/bin/passwd"
    Require user websvuser
</Directory>
<Directory "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/wwwroot/ALARMS~">
    AuthType Basic
    AuthName "SV Console"
    AuthUserFile "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/WebServer/bin/passwd"
    Require user websvuser
</Directory>
```

● When Installed with SSL Disabled

If SSL is selected to be disabled during ServerView installation, "ssl.conf" is ineffective.
In this case, limitation using a password is disabled for the web server with the default settings.

Access Restriction by the Connecting Host

In the configuration example below, the accessible host is limited to "192.168.0.2" only.

Add the following section to the configuration file "C:\Program Files\Fujitsu\F5FBFE01\ServerView Services\WebServer\conf\httpd.conf".

```
<Directory "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/scripts/SERVER~1">
    Order deny,allow
    deny from all
    Allow from  192.168.0.2
</Directory>
<Directory "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/wwwroot/SERVER~1">
    Order deny,allow
    deny from all
    Allow from  192.168.0.2
</Directory>
<Directory "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/wwwroot/ALARMS~">
    Order deny,allow
    deny from all
    Allow from  192.168.0.2
</Directory>
<Files "sv_www.html">
    Order deny,allow
    Deny from all
    Allow from  192.168.0.2
</Files>
<Files "AlarmService.htm">
    Order deny,allow
    Deny from all
    Allow from  192.168.0.2
</Files>
<Files "svagent.html">
    Order deny,allow
    Deny from all
    Allow from  192.168.0.2
</Files>
```

Access Restriction by User Authentication

User authentication is required when connecting to the management console. Execute the following command to create a user and set a password:

```
C:\>cd C:\Program Files\Fujitsu\F5FBFE01\ServerView Services\WebServer\bin
C:\Program Files\Fujitsu\F5FBFE01\ServerView Services\WebServer\bin
>htpasswd -c svpasswd websvuser
New password: ******
Re-type new password: ******
Adding password for user websvuser
```

Add the following section to the configuration file "C:\Program Files\Fujitsu\F5FBFE01\ServerView Services\WebServer\conf\httpd.conf".

```
<Directory "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/scripts/SERVER~1">
    AuthType Basic
    AuthName "SV Console"
    AuthUserFile "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/WebServer/bin/passwd"
    Require user websvuser
</Directory>
<Directory "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/wwwroot/SERVER~1">
    AuthType Basic
    AuthName "SV Console"
    AuthUserFile "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/WebServer/bin/passwd"
    Require user websvuser
</Directory>
<Directory "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/wwwroot/ALARMS~">
    AuthType Basic
    AuthName "SV Console"
    AuthUserFile "C:/PROGRA~1/Fujitsu/F5FBFE01/SERVER~1/WebServer/bin/passwd"
    Require user websvuser
</Directory>
```

■ Configuring IIS (Windows)

The following describes operations for IIS on Windows Server 2003 when the IIS configuration has been never changed. If you have changed the IIS DocumentRoot setting etc. before installing ServerView, read these descriptions with your settings in mind.
Click [Start] → [Programs] → [Management Tools] → [Internet Information Service Manager] in this order to start IIS manager.

● Access Restriction by the Connecting Host

Change the settings for the following three folders:

- Default Web Site\scripts\ServerView
- Default Web Site\ServerView
- Default Web Site\AlarmService

1 For each folder's properties, open the [Directory Security] tab and click [Edit] under [IP Address and Domain Name Restrictions].

2 Select [Denied access] and add IP addresses or domain names to be granted access.

3 Configure the same access restriction for the following files under "Default Web Site".

AlarmService.htm, AlarmService.html, svagent.htm, and sv_www.html

POINT

- If there are no other contents than ServerView in "Default Web Site", you can simply configure access restriction for the "Default Web Site".

● Access Restriction by User Authentication

Change the settings for the following three folders:

- Default Web Site\scripts\ServerView
- Default Web Site\ServerView
- Default Web Site\AlarmService

1. For each folder's properties, open the [Directory Security] tab and click [Edit] under [Authentication and Access Control].

2. Uncheck the [Enable anonymous access] checkbox and add the desired authentication to [Authenticated access].

3. Configure the same access restriction for the following files under "Default Web Site".
   AlarmService.htm, AlarmService.html, svagent.htm, and sv_www.html

Index

ServerView

User's Guide
B7FH-4661-01ENZ0-00

Issued on December, 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.