Areas Covered

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.

■ Consecutive Operations

Consecutive operations are described by connecting them with "–".

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

   ↓

   Click [Start] – [All Programs] – [Accessories].

■ CD/DVD Drive Descriptions

In this manual, both CD-ROM and DVD-ROM drives are described as a CD/DVD drive.

Select a proper drive depending on your environment.

■ 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/DVD drive letter is shown as [CD/DVD drive]. Enter your drive letter according to your environment.
  [CD/DVD drive]:\setup.exe

■ Operations for Linux

The mount commands for CD/DVD 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 RHEL5(x86)/RHEL5(Intel64)/RHEL-AS4(EM64T)/ES4(EM64T)
  /media/cdrom, /media/floppy

> **IMPORTANT**
>
> ▶ For RHEL5(x86)/RHEL5(Intel64), perform the following steps to mount drives.

```
# mkdir /media/cdrom
# mount /dev/cdrom /media/cdrom
or
# mkdir /media/floppy
# mount /dev/floppy /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.

■ Abbreviations

The following expressions and abbreviations are used throughout this manual.

table: Abbreviations of product names

Product name	Expressions and abbreviations	
Microsoft® Windows Server® 2008, Standard Microsoft® Windows Server® 2008, Enterprise Microsoft® Windows Server® 2008, Datacenter Microsoft® Windows Server® 2008, Standard without Hyper-V™ Microsoft® Windows Server® 2008, Enterprise without Hyper-V™ Microsoft® Windows Server® 2008, Datacenter without Hyper-V™	Windows Server 2008 or Windows Server 2008 (64-bit)	Windows
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 Microsoft® Windows® Small Business Server 2003	Windows Server 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 Microsoft® Windows® Small Business Server 2003 R2 Microsoft® Windows® Storage Server 2003 R2, Standard Edition	Windows Server 2003 R2	
Microsoft® Windows® 2000 Server Microsoft® Windows® 2000 Advanced Server	Windows 2000 Server	
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	
Microsoft® Windows NT® Workstation Operating System 4.0	Windows NT 4.0	
Red Hat Enterprise Linux 5 (for x86)	Red Hat Linux	Linux
	RHEL5(x86)	
Red Hat Enterprise Linux 5 (for Intel64)	RHEL5(Intel64)	
Red Hat Enterprise Linux AS (v.4 for x86)	RHEL-AS4(x86)	
Red Hat Enterprise Linux ES (v.4 for x86)	RHEL-ES4(x86)	
Red Hat Enterprise Linux AS (v.4 for EM64T)	RHEL-AS4(EM64T)	
Red Hat Enterprise Linux ES (v.4 for EM64T)	RHEL-ES4(EM64T)	
Red Hat Enterprise Linux AS (v.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)	
SUSE® LINUX ® Enterprise Server 9 for x86	SUSE Linux	
	SLES9(x86)	
Intel LANDesk® Server Manager	LDSM	

Product name	Expressions and abbreviations
Remote Service Board (PG-RSB102/PG-RSB103/PG-RSB104/PG-RSB105)	Remote Service Board

■ About the Server Core Installation Option

The environment in which the Windows Server 2008 operating system is installed by the Server Core installation option is written as Server Core in this manual.

Reference Information

■ Supported OS Associated with Machine Types

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

Microsoft, Windows, MS, MS-DOS, Windows Server, and Hyper-V are trademarks or registered trademarks of Microsoft Corporation in the USA and other countries.
Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the USA and other countries.
Linux is a trademark or registered trademark of Linus Torvalds in the USA and other countries.
Red Hat and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc. in the USA and other countries.
SUSE is a registered trademark of SUSE LINUX AG, a Novell business.
All other hardware and software names used are trademarks or registered trademarks of their respective manufacturers.
Other product names are copyrights of their respective manufacturers.

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

Contents

Chapter 1

Overview of ServerView Windows Agent

This chapter explains overview of ServerView Windows Agent, and system requirements.

1.1 ServerView Windows Agent

ServerView Windows Agent is software that monitors hardware which is installed in the PRIMERGY monitored server and operates such functions as detection / notification of any abnormality (with event logs and sending SNMP traps).
It also provides ServerView Console the information about the monitored server using SNMP protocol.

This manual explains how to install and use ServerView Windows Agent.

For the functions of ServerView including ServerView Windows Agent, refer to the "ServerView User's Guide".

POINT

▶ ServerView Windows Agent does not have a function to notify the user errors with a pop-up message. Installing ServerView Console on the monitored server will allow the server to show pop-up error messages. The alarm service function provides these pop-up messages.

▶ ServerView Windows Agent stores logs in the OS event log.
The followings are the logs that ServerView Windows Agent stores.

　　Type of log: application

　　Source name: ServerView Agents

　　Event ID：[SNMP Trap Specific number] + 10000

▶ Example) In the case of the Detailed message "System status has changed at server xxx" log. The above [SNMP Trap Specific number] is shown as the number "1100" in the section of "SERVERVIEW-STATUS-MB (status.mib)" in ServerView Trap List. In this case, the event ID is displayed as "11100".

▶ For detailed information (such as meanings and measures) of logs stored in the OS event log of ServerView Windows Agent, refer to the section under [SNMP Trap specific number] in the "ServerView Trap List".

▶ ServerView Trap List also lists traps (logs) sent from applications other than ServerView Windows Agent. To see logs concerned ServerView Windows Agent in the Trap List (source name: ServerView Agents), refer to the following sections.

　　• SNI-TRAP-MIB (trap.mib)

　　• SNI-SERVER-CONTROL-MIB (sc.mib)

　　• SNI-HD-MIB (hd.mib)

　　• SERVERVIEW-STATUS-MIB (status.mib)

　　• FSC-SERVERCONTROL2-MIB (sc2.mib)

　　• FSC-THRESHOLD-REPORT-MIB (Threshold.mib)

1.2 System Requirements

The system requirements for server to use ServerView Windows Agent are as follows:

table: System requirements when installing ServerView Windows 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 Server 2008 • Windows Server 2003 R2 • Windows Server 2003 • Windows 2000 Server 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 Windows Agent is dedicated to PRIMERGY. Do not install it on the servers other than PRIMERGY.

Chapter 2
Installation

This chapter explains how to install ServerView
Windows Agent.

2

2.1 Installation Flow

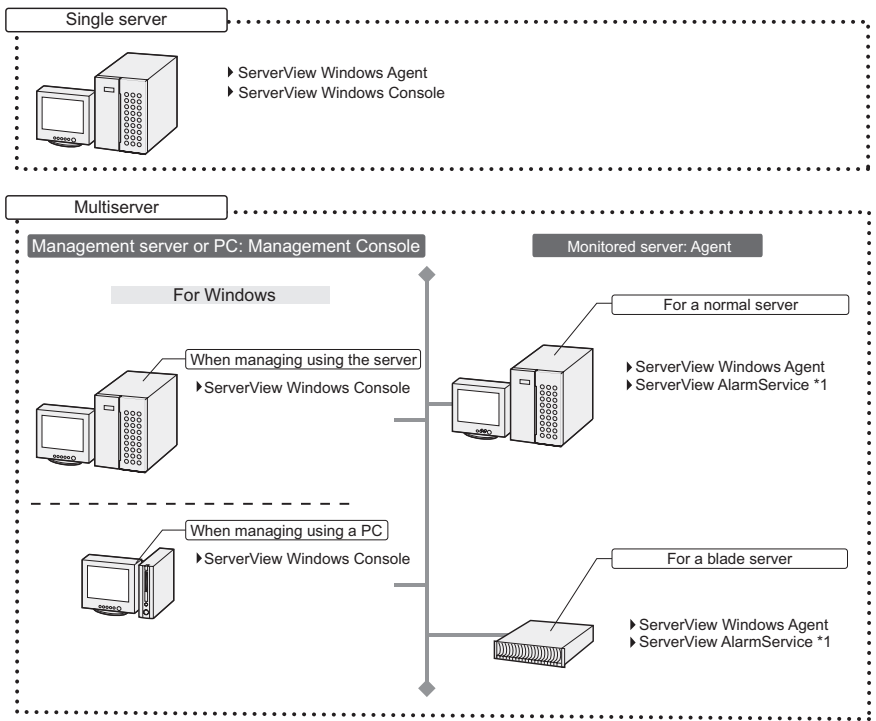The installation flow of ServerView Windows Agent is as follows:

POINT

▶ In order for ServerView Windows Agent to display monitoring information, the ServerView Console must be installed in the monitored server, the administration server, or the administration PC. For details on how to install the ServerView Console, refer to the "ServerView User's Guide".

Checking before installation

Before installing ServerView Windows Agent, check the following:

- Install TCP/IP and SNMP services
- Change the bind order
- Apply Service Pack

Installing

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

Single server

▶ ServerView Windows Agent
▶ ServerView Windows Console

Multiserver

Management server or PC: Management Console

Monitored server: Agent

For Windows

When managing using the server
▶ ServerView Windows Console

For a normal server

▶ ServerView Windows Agent
▶ ServerView AlarmService *1

When managing using a PC
▶ ServerView Windows Console

For a blade server

▶ ServerView Windows Agent
▶ ServerView AlarmService *1

*1 : In the monitored server, in order for RAID monitoring (linked with RAID Manager), you need to install ServerView Windows Console or ServerView AlarmService. For details about each installation, refer to "ServerView User's Guide".

Settings after installation

After the installation of ServerView Windows Agent, perform the various settings.

- Set an administrative user
- Change SNMP settings

2.2 Check before Installation

Before installing ServerView Windows Agent, 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, refer to "2.4.2 How to Change SNMP Settings" (→pg.29).

■ For Windows Server 2008

1 Open Control Panel and click [Programs].

2 Click [Turn Windows features on or off] in [Programs and Features].

3 Click [Features] in the tree on the left side of [Server Manager].

4 Click [Add Feature] on the right side of the [Features Summary] field.

5 Perform one of the following procedures.
The following operation depends on whether [SNMP Service] is checked or not.
If [SNMP Service] is already checked
If this check box is already checked, the SNMP service has been already installed. In this case, go to Step 6.
If [SNMP Service] is not checked
Follow the steps below to install the SNMP service.
1. Check both [SNMP Service] and [SNMP Service] under [SNMP Service].
2. Click [Next] and follow the messages on the window.

6 Open Control Panel and click [System and Maintenance] – [Administrative Tools].

7 Click [Computer Management].

8 In the left tree, click [Services and Applications] – [Services].

9 Click [SNMP Service] on the right side of the window.

10 Click the [Action] menu – [Properties].

11   In the [General] tab, make sure that [Startup Type] is set to "Automatic".

Set it to "Automatic" if it is not set.

12   Click the [Traps] tab.

13   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].

14   Click [Add] in the [Trap destinations] section.

15   Enter the host name and IP address of the server on which the ServerView Windows Console is installed and click [Add].

When installing the ServerView Windows Console in a single server environment, enter its own host name and IP address. When operating multiple ServerView Windows Consoles, enter each host name and IP address.

16   Click the [Security] tab.

17   Click "public" and [Edit].

18   Select [READ WRITE] or [READ CREATE] from [Community rights] and click [OK] ([READ WRITE] is recommended).

<u>If "public" does not exist in the [Accepted Community Names] list</u>

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].

19   Configure the hosts from which SNMP packets are accepted.

<u>When accepting SNMP packets from any host</u>

    1. Click [Accept SNMP packets from any host].

<u>When accepting SNMP packets from the specified hosts</u>

    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 Windows Agent is installed, make sure that the loopback address (127.0.0.1) is included.

20   Click [OK].

● **For Environment in which Server Core is Installed**

In the local console environment of Server Core, the GUI based management tool of Microsoft management console (MMC) is not available. You need to start the management tool from another terminal with Windows Server 2008, Windows Server 2003, or Windows XP and connect it remotely. The procedure is shown below.

IMPORTANT

▸ To configure the setting of SNMP Service, another Windows terminal (installed other than Server Core of Windows Server 2008) is required. Prepare it in advance.

1 On the terminal with Server Core, execute the following command. Check to see whether SNMP Service is installed and begins.

```
> sc query SNMP
```

When SNMP service is not installed

Execute the following command to install the SNMP service.

```
> start /w ocsetup SNMP-SC
```

2 Log in as an administrator or a user with administrator privileges.

3 Execute the following commands at the command prompt.

For Windows Server 2008, the firewall is enabled by default. It is necessary to permit the access to manage it remotely.

```
> netsh firewall set service remoteadmin enable
> netsh advfirewall set currentprofile settings remotemanagement enable
```

On another Windows terminal, follow the steps below to connect Server Core.

4 On another Windows terminal, start a command prompt and execute the following command.

During the operation, you are prompt to enter Administrator password.
Enter IP address of monitoring server (Server Core) in "xxx.xxx.xxx.xxx" of the following command.

```
net use ¥¥xxx.xxx.xxx.xxx¥c$ /u:Administrator
```

5 Execute the following commands.

```
>services.msc
```

The service window appears.

6 Click [Action] menu – [Connect to another computer...].
[Select Computer] window appears.

7 Enter IP address or the machine name of the above-mentioned Server Core
server to [Another computer], and click [OK].

Service list of Server Core server is displayed.

Make sure that [SNMP Service] exists in the service and proceed to Step 9 of "■ For Windows Server
2008" (→pg.15).

IMPORTANT

‣ Neither the setting nor the changes of SNMP in the local console environment are supported.

■ For Windows Server 2003

1 Open Control Panel.

2 Double-click [Network Connections].

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

4 Perform one of the following procedures.

The following operation depends on whether [Management and Monitoring Tools] in [Optional
Networking Components Wizard] is checked or not.

If [Management and Monitoring Tools] is already checked

1. Click [Management and Monitoring Tools], click [Details], and then make sure that
[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 [Management and Monitoring Tools] is not checked

Follow the steps below to install the SNMP service.

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

Follow the messages on the window.

5 Open 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 side of the window.

9 Click the [Action] menu – [Properties].

10 In the [General] tab, make sure that [Startup Type] is set to "Automatic".

Set it to "Automatic" if it is not set.

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 Windows Console is installed and click [Add].

When installing the ServerView Windows Console in a single server environment, enter its own host name and IP address. When operating multiple ServerView Windows 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 Windows Agent is installed, make sure that the loopback address (127.0.0.1) is included.

19 Click [OK].

■ For Windows 2000 Server

1 Open 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 procedures.

The following operation depends on whether [Management and Monitoring Tools] on [Optional Networking Components Wizard] is checked or not.

If [Management and Monitoring Tools] is already checked
  1. Click [Management and Monitoring Tools], click [Details], and then make sure that [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 [Management and Monitoring Tools] is not checked
  1. Check [Management and Monitoring Tools] in [Optional Networking Components Wizard].
  2. Click [Details] and make sure that [Simple Network Management Protocol (SNMP)] is checked, and then click [OK].
  3. In [Optional Networking Components Wizard], click [Next].
  4. Follow the messages on the window.

5 Double-click the [Administrative Tools] icon in 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 side of the window.

9 Click the [Action] menu – [Properties].

10 In the [General] tab, make sure that [Startup Type] is set to "Automatic".
Set it to "Automatic" if it is not set.

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 Windows Console is installed and click [Add].

When installing the ServerView Windows Console in a single server environment, enter its own host name and IP address.

When operating multiple ServerView Windows 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 Windows 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 administration server or the administration PC, which ServerView Console are installed, searches first.

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

POINT

▸ The IP address searched here is used as the source IP address of the SNMP Trap that is sent by ServerView Windows Agent.

▸ The operation of ServerView is not supported when IP address, which is used for monitoring server, uses the adapter, which multiple addresses (such as VLAN, VPN, etc.) are assigned.
It is required that IP address, which is used for monitoring server, uses the adapter which only the real IP address is assigned.

■ For Windows Server 2008

1 Open Control Panel.

2 Click [Network and Internet] – [Network and Sharing Center].

3 Click [Manage network connections] in the left side of the window.
The [Network Connections] window appears.

4 In the [Network Connection] window, click [Advanced Settings...] in the [Advanced] menu.
The [Advanced Settings...] window appears.

5 Click the [Adapters and Bindings] tab.

6 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.

■ For Windows Server 2003 / Windows 2000 Server

1 Open 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 Server 2008 / Windows Server 2003. For Windows 2000 Server, apply Service Pack 4 or later.

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, you do not need to reapply.
▶ Before applying the Service Pack, make sure that the SNMP service is installed.

2.3 Installation

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

IMPORTANT

▸ You cannot do overwrite installation the ServerView Windows Agent. If you want to update the ServerView Windows Agent, uninstall the ServerView Windows Agent and install it again.
  For details on how to uninstall the ServerView Windows Agent, refer to "2.5 Uninstallation" (→pg.31).
▸ For a system on which a terminal server has been installed, the installation method is different from the usual methods. To install the ServerView Windows 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 Server 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.
▸ When the following software has been installed and a service is running, you need to stop the service temporarily before installing ServerView Windows Agent.

table: Service need to be stopped temporarily before installation

Software	Service
HRM/server (Windows)	F5EP70_HRM_ctrl Service

You need to restart the service after installing ServerView Windows Agent.

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 Windows Console or the ServerView AlarmService. For installation steps, refer to "ServerView User's Guide".
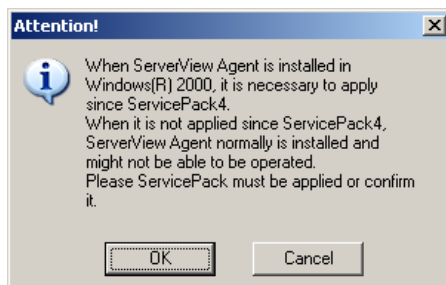▸ You do not need to restart Windows after the ServerView Windows Agent installation.

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

2 Exit all running applications.

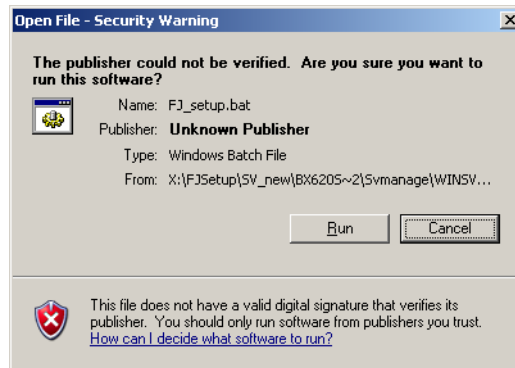*3* Insert the PRIMERGY Startup Disc and start the following installer.
  [CD/DVD drive]:\PROGRAMS\Japanese2\Svmanage\WinSVAgent\Agents_setup.EXE
  The [Attention!] window appears.

4 Click [OK].

The [ServerView Hints] window appears.

5 Click [OK].

The following security warning may be displayed.

6 Click [Run].

After finishing the installation, refer to "2.4 Setting after Installation" (→pg.26) and make the settings required to operate ServerView.

2.4 Setting after Installation

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

2.4.1 Setting an Administrative User

Only users belonging to the group (FUJITSU SVUSER) that have Administrator privileges for ServerView can perform operations such as configuring Automatic Server Reconfiguration & Restart (ASR) settings (e.g. fans, temperature, restart settings) for the monitored server and shutting down the server from ServerView Console. At this time, the administrative user's name and password are required to be input. Follow the steps below to set an administrative user.

The FUJITSU SVUSER group and users belonging to the group are not created automatically. Create a group each monitored server and add the ServerView administrative user to the FUJITSU SVUSER group.

POINT

▶ An administrative user in ServerView means a user who belongs to the "FUJITSU SVUSER" group.

▶ In Windows Server 2008 / Windows Server 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 [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.

1 Open 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...].

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...].

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].

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 Environment in which Server Core is Installed

In the local console environment of Server Core, the GUI based management tool of Microsoft management console (MMC) is not available. Execute the following command to set the group and administrative user.

1 Execute the following commands to create the "FUJITSU SVUSER" group.

```
>net localgroup "FUJITSU SVUSER" /add
```

2 Create an administrative user and set a password.

```
>net user <user name> /add *
```

After executing the command, you are prompted to enter a password.

3 Add the newly created user to the "FUJITSU SVUSER" and "Administrators" group.

```
>net localgroup "FUJITSU SVUSER" /add <user name>
>net localgroup "Administrators" /add <user name>
```

₽POINT

▸ To refer to or delete the created group and administrative user, execute the following commands.
  • To refer to the group

```
>net localgroup "FUJITSU SVUSER"
```

  • To refer to the administrative user

```
>net user <user name> /
```

  • To delete the group

```
>net localgroup "FUJITSU SVUSER" /delete
```

  • To delete the administrative user

```
>net user <user name> /delete
```

2.4.2 How to Change SNMP Settings

This section explains how to change SNMP settings.

If there is an error in SNMP settings, monitoring function does not work properly.

For the details on how to display "SNMP Service Properties", refer to "2.2.1 Installation of TCP/IP Protocol and SNMP Service" (→pg.15).

■ Changing the SNMP Community Name

The same community name needs to be set as the one the monitored server receives and the one ServerView Console uses for the SNMP communication with the monitored server.

To change community name, follow the procedure below.

● How to Change at the Monitored Server's Side

Change the property ([Security] tab) of SNMP Service.

How to Change the Community Name

1 Select the entry that you wish to change from "Accepted community names", and click [Edit].

2 Change "community name" to any community names, and click [OK].

Adding New Community Names

1 Click [Add] on "Accepted community names".

2 Perform one of the following procedures according to OS used.

For Windows Server 2008 / Windows Server 2003

Select "READ WRITE" or "READ CREATE" from [Community rights]. ("READ WRITE" is recommended).

For Windows 2000 Server

Click "READ_WRITE" or "READ_CREATE" from [Community rights] ("READ_WTITE" is recommended).

3 Enter any community names on [community names], and click [Add].

● How to Change at the ServerView Console

To change the monitored server that has already been registered, right-click the monitored server in the server list, select [Server Properties] – [Network/SNMP] tab from the menu displayed, and change the community name.

For the details or for how to add a new server, refer to "ServerView User's Guide".

■ Changing the Setting of SNMP Packet Reception

On the monitored server, you need to arrange how to receive the SNMP packet from the ServerView Console.

Change the SNMP Service property ([Security] tab).

● When Accepting the SNMP Packet from any Servers and ServerView Consoles

Select the "Accept SNMP packet from any hosts".

● When Accepting SNMP Packets only from the Specified Hosts or the ServerView Console

Select the "Accept SNMP Packets from These Host".

In this case, make sure that you enter the following three assigned values.

- The host name or the IP address of the ServerView Console
- The host name or the IP address of the monitored server
- The loop back address (127.0.0.1 or localhost) of the monitored server

■ Changing the Destination of the SNMP Trap

Change the SNMP Service property ([Trap] tab).

On the monitored server, make sure to enter the ServerView Console host name or the IP address on the destination of the SNMP Trap.

2.5 Uninstallation

This section explains how to uninstall the ServerView Windows Agent.

IMPORTANT

▶ Uninstall ServerView Windows Agent after all ServerView programs are closed. After ServerView Windows Agent is uninstalled, the directories, subdirectories and files may not be deleted. In addition, ServerView may not be removed 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 Windows Agent 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 Windows Agent is uninstalled. Restore the settings to the original state, and then uninstall ServerView Windows Agent.

▶ Some characters may get garbled on the uninstallation window. It, however, does not affect the operation.

▶ Make sure to do the followings before uninstalling ServerView Windows Agent.

• Disable Software Watchdog, BOOT Watchdog and Power ON/OFF settings.

• If threshold monitoring and report creation are applied by Performance Manager, cancel these performances to the server.

• When uninstalling ServerView Windows Agent, the settings that are configured using ServerView Console 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 Windows Agent, perform the following steps.

■ For Windows Server 2008

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

2 Exit all running applications.

3 Open Control Panel and click [Programs] – [Programs and Features].

4 Select [ServerView Agents] and click [Uninstall].
ServerView Windows Agent will be uninstalled.

● For Environment in which Server Core is Installed

1 Insert the PRIMERGY Startup Disc.

2 Execute the following file.
[CD/DVD drive]:\PROGRAMS\Japanese2\Svmanage\WinSVAgent\Unagents.bat

■ For Windows Server 2003 / Windows 2000 Server

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

2 Exit all running applications.

3 Open [Control Panel] and double-click [Add/Remove Programs].

4 Select [ServerView Agents] and click [Delete].
ServerView Windows Agent will be uninstalled.

POINT

‣ You do not need to restart Windows after uninstalling ServerView Windows Agent.

Chapter 3

How to Use ServerView Windows Agent

This chapter explains how to use the ServerView Windows Agent.

3.1 How to Use ServerView Windows Agent

This section explains how to use ServerView Windows Agent.
ServerView Windows Agent is installed in "ServerView Server Control Service" and "Extension Agent of the SNMP Service".

3.1.1 How to Start ServerView Windows Agent

By starting "ServerView Server Control Service" and "SNMP Service", you can start ServerView Windows Agent.

🔍**POINT**

▸ In the Default settings of "ServerView Server Control Service" and "SNMP Service", "Startup Types" is arranged as "Automatic". So, ServerView Windows Agent is automatically started on starting the server without operating any other functions. If you do not want it to start automatically, set "Manual" on "Startup Types".

1 Open Control Panel and double-click [Administrative Tools].

2 Double-click the [Service] icon.

3 Select "ServerView Server Control Service" on the Service list.

4 Click the [Operation] menu – [Start].
"ServerView Server Control Service" is started.

5 Select "SNMP Service" on the Service list.

6 Click [Operation] menu – [Start].
"SNMP Service" is started, and ServerView Windows Agent is started working.

■ For Environment in which Server Core is Installed

To start ServerView Windows Agent in the Server Core installation environment, execute the following command.

```
>sc start srvctrl
```

or

```
>net start srvctrl
```

3.1.2 How to Exit ServerView Windows Agent

Exiting "SNMP Service" and "ServerView Server Control Service" can exit ServerView Windows Agent.

IMPORTANT

▶ When you stop "SNMP Service", you also stop other agents than ServerView Windows Agent installed as an expansion agent.

1 Open Control Panel and double-click [Administrative Tools].

2 Double-click the [Service] icon.

3 Select "SNMP Service" on the Service list.

4 Click the [Operation] menu – [Exit].
"SNMP Service" is exited.

5 Select "ServerView Server Control Service" on the Service list.

6 Click the [Operation] menu – [Exit].
"ServerView Server Control Service" is exited, and ServerView Windows Agent is exited working.

■ For Environment in which Server Core is Installed

To stop ServerView Windows Agent in the Server Core installation environment, execute the following commands.

1 Execute the following commands to stop the "SNMP Service".

```
>sc stop SNMP
```

or

```
>net stop SNMP
```

2 Execute the following commands to stop ServerView Windows Agent.

```
>sc stop srvctrl
```

or

```
>net stop srvctrl
```

3.1.3 How to Restart ServerView Windows Agent

Restart ServerView Windows Agent with "Restart ServerView Base Services", its restarting tool. This tool helps execute the shutdown and the restart in a serial manner.

1 Click [Start] – [All Programs] – [Fujitsu ServerView Agents] – [Diagnostic Tools] – [Restart ServerView Base Service].

For environment in which Server Core is installed

Perform the following steps.

1. Move a directory.

```
>cd [system drive]:\Program Files\Fujitsu\F5FBAG01\ServerView Agents
\Diagnostics Tools
```

2. Execute the following command.

```
>SCDoctor.exe /restart
```

The [Restart ServerView Agents] window appears.

2 Enable "Search for management hardware", and click [Restart].

3 After restart, "Restart Services completed successfully!" is displayed. Then, click [Exit].

3.2 Settings for ServerView Windows Agent

Configuration Tools enables you to save and restore the settings of ServerView Windows 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 Windows 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.

▶ Do not use the Configuration Tools to change the settings. If a management console or another web interface tool is running on another PC, this may lead to inconsistencies and server errors. However, the initial IP settings for PG-RSB102 through 105 and the initial IP settings for Remote Management Controller can be modified.

▶ For environment in which Server Core is installed, you cannot save and restore the settings by Configuration Tools because of restriction.

■ Configuring the Remote Service Board IP

When ServerView Windows Agents are installed in the Windows server, the remote service board can be configured. To change the configuration, perform the following steps.

1 Click [Start] – [All Programs] – [Fujitsu ServerView Agents] – [Configuration Tools] – [System Configuration].

<u>For environment in which Server Core is installed</u>
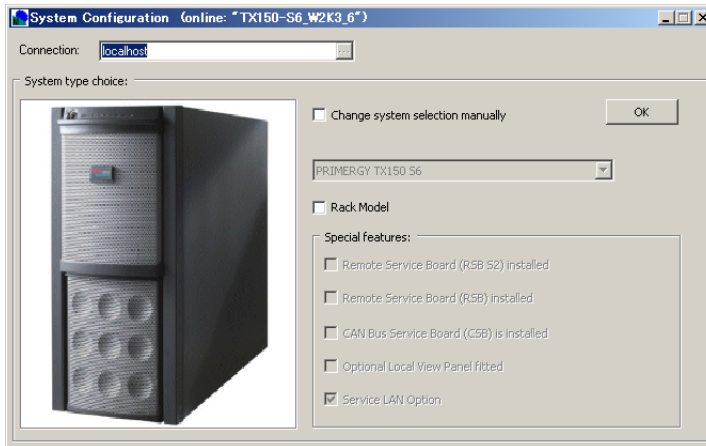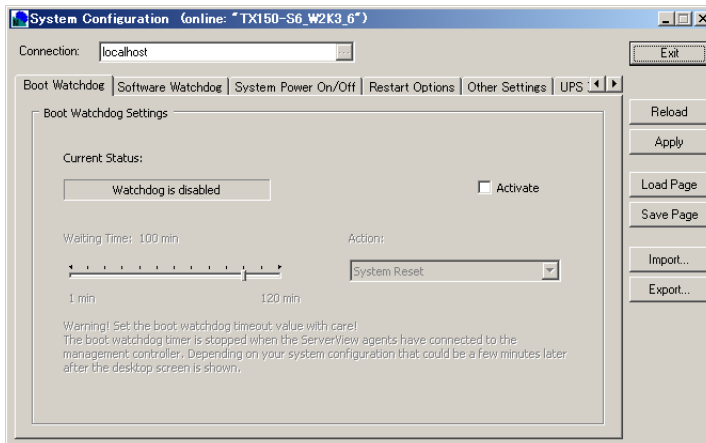
Perform the following steps.

1. Move a directory.

```
>cd  [system drive]:\Program Files\Fujitsu\F5FBAG01\ServerView Agents
\Configuration Tools
```

2. Execute the following command.

```
>SCConfig.exe
```

The [System Configuration] window appears.

2 Select the [Change system selection manually] checkbox and click [OK].

A window appears for specifying items.

3 Click each Tab and set items if necessary.

The displayable and configurable tabs vary depending on the server components.

If not equipped with a Remote Management Controller/Remote Service Board/Controller

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	The settings are associated with the power schedule.
Other Settings	The time when to perform a fan test.

If equipped with a Remote Management Controller (iRMC)

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.
System Power On/Off	The settings are associated with the power schedule.
Restart Options	The settings are associated with the restart of the server.
Other Settings	The time when to perform a fan test.
iRMC Power Consumption Control	The settings are associated with power consumption of the server.
iRMC Remote Storage	The remote storage server configuration for the Remote Management Controller.
iRMC LAN Settings	The IP configuration for the Remote Management Controller.
iRMC Networking Port	The port configuration for the Remote Management Controller.
iRMC DNS Registration	The DNS configuration for the Remote Management Controller.
iRMC DNS Server	The DNS server configuration for the Remote Management Controller.
iRMC EMail Alerting	The SMTP server configuration for the Remote Management Controller.
iRMC EMail Format Settings	The email format configuration for the Remote Management Controller.
iRMC SNMP Alerting	The SNMP configuration for the Remote Management Controller.
iRMC User Management [Note 1]	The user configuration for the Remote Management Controller.
iRMC Directory Service	The directory service configuration for the Remote Management Controller.

[Note 1]: Settings in the [iRMC User Management] tab cannot be backed up or restored.

IMPORTANT

- ▸ Change the configurations only on the [iRMC LAN Settings] tab. Use the Web interface of the Remote Management Controller to set the items on the other tabs.
  The setting items on the tabs other than the [iRMC LAN Settings] tab are not supported.
- ▸ When you set a license key for Remote Management Controller, recovering the backed up data by WinSCU through Remote Management Controller Web interface results in an error item "License Key" of iRMC Remote Storage. When you recover the data, delete data that display item "License Key" of iRMC Remote Storage. This does not affect the set license key.

If equipped with a Remote Service Board (PG-RSB102 through 105)

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.
RSB S2 IP Configuration	The IP configuration for the Remote Service Board.
RSB S2 Network Services [Note 1]	Various network settings for the Remote Service Board.
RSB S2 User administration [Note 1]	The user configuration for the Remote Service Board.
RSB S2 SNMP Configuration [Note 1]	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 Tools.

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] oth-
erwise.
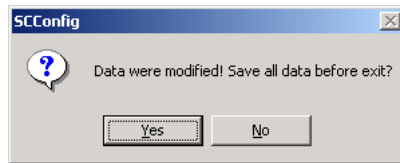
Configuration Tools exit.

■ Save Settings

Save the settings as a file.

1 Start Configuration Tools.

The [System Configuration] window is displayed.

2 Click [Export].

The [Select export mode] window is displayed.

3 Select the export mode and click [OK].

The [Save As] window is displayed.

4 Specify a file name and a location to which the file is saved, and click [Save].

The file is saved.

5 Click [Exit].

Configuration Tools exit.

■ 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 [Apply].

The message appears to confirm whether to save the settings.

5 Click [Yes].

Click [No] when you suspend restoration of the setting.

Configuration Tools exit.

Index