SANUPS

IT Monitor Manager

User Guide

Doc #: M0006433D

SANYO DENKI

The following trademarks are used in this user guide:

- Windows NT, Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7 are trademarks of Microsoft Corporation.
- Internet Explorer is a trademark of Microsoft Corporation.
- Java and all Java-related trademarks and logos are trademarks of U.S. Sun Microsystems, Inc.

Disclaimer

(1) This software and this user guide cannot be copied or reprinted in whole or in part without prior consent.
(2) While all aspects of this product have been checked thoroughly, if you have any comments, please contact us using the contact information listed below.
(3) Contents of this product are subject to change without prior notice.
(4) Before using this product, read this user guide and make sure you understand the functions of this product. SANYO DENKI CO.,LTD shall not be liable for any damages arising from the use of this product.

Table of Contents

1. Introduction 1
1.1 What Is SANUPS IT Monitor Manager? 1
1.2 What Can SANUPS IT Monitor Manager Do? 1
1.3 Operating Environments 4
1.3.1 Operating environment for server 4
1.3.2 Operating environment for clients 4
2. System Configuration And Requirements 6
2.1 System Configuration 6
2.2 System Requirements 7
2.2.1 Network environment requirements 7
2.2.2 Operational requirements 7
2.2.3 Restrictions 9
3. Overall Procedure (From System Introduction To Operation) 11
4. Preparation On A Device 13
4.1 Setting The IP address Of The Device 13
4.2 Performing The SNMP Setting Of The Device 13
5. Installing SANUPS IT Monitor Manager 14
5.1 Before Installing 14
5.2 Install Procedure 14
5.3 Note On Using JavaVM (Java Virtual Machine) 17
5.4 Uninstall Procedure 18
5.4.1 If the server is already installed 18
5.4.2 If only the client is installed 18
6. Starting And Ending The Server 19
6.1 Starting 19
6.2 Ending 19
7. Starting And Ending The Client 21
7.1 Starting 21
7.2 Ending 22
8. Explanation Of Functions 23
8.1 About The Main Screen Of A Client 23
8.1.1 Menu bar 23
8.1.2 Consolidated monitoring tree view 25
8.1.3 Device operation status list 28
8.1.4 System log panel 29
8.1.5 List page setting 29
8.2 Adding A Device For Monitoring 30
8.2.1 Setting the default values for use when devices are added 30
8.2.2 Adding a device by specifying its host name or IP address 33
8.2.3 Adding a device by searching for it first 38
8.3 Modifying The Settings Of A Device Added 42
8.4 Deleting A Device Targeted For Monitoring 43
8.4.1 Using the procedure to delete a device 43

8.5 Notifying The Administrator Of A Device Fault 45
8.5.1 Fault notification sequence 45
8.5.2 Settings required for fault notification 46
8.6 Performing Fault Notification Setting 47
8.6.1 Fault notification setting procedure 47
8.6.2 Restrictions on fault notification 53
8.7 Setting Management Information (Device Management Information) 54
8.7.1 Changing the management information of a single device 54
8.7.2 Changing the management information of multiple devices at the same time 56
8.7.3 Notes on the management information settings 57
8.8 Starting The Web Applet Of A Device 58
8.8.1 What is applet startup? 58
8.8.2 Applet Startup procedure 58
8.8.3 Functions that can only be performed from the Web applet (environment monitoring device) 59
8.8.4 Functions that can only be performed from the Web applet (UPS) 59
8.8.5 Notes on changing the host name/IP address, and community names 59
8.9 Setting The Parameter Information Of A Device (Environment Monitoring Device) 60
8.9.1 What is the parameter information of environment monitoring device? 60
8.9.2 Parameter information setting procedure (common part) 60
8.9.3 Analog input parameter setting procedure 62
8.9.4 Digital input parameter setting procedure 63
8.9.5 Digital output parameter setting procedure 64
8.9.6 Environment monitoring device's trap recipient setting procedure 65
8.9.7 E-mail transmission address setting procedure 66
8.10 Setting The Parameter Information Of A Device (UPS) 67
8.10.1 What is the UPS parameter information? 67
8.10.2 Parameter information setting procedure 67
8.11 Performing Remote Control Of A Device (Environment Monitoring Device) 68
8.11.1 About remote control 68
8.11.2 Using the procedure to control the output of a single device 68
8.11.3 Batch control procedure 69
8.11.4 Schedule control setting procedure 72
8.12 Performing Remote Control Of A Device (UPS) 76
8.12.1 About remote control 76
8.12.2 Using the procedure to control the output of a single device 76
8.12.3 Batch control procedure 77
8.12.4 Schedule control setting procedure 80
8.13 Viewing The Device Operation Status 84
8.13.1 Customizing content of the device operation status list display (environment monitoring device) 84
8.13.2 Customizing content of the device operation status list display (UPS) 88
8.14 Viewing The System Log 91

8.14.1 Viewing details of the system log 91
18.4.2 Customizing the system log list 93
8.14.3 Data storage period of system log 95
8.15 Enabling The Real-time Display Of A Device 96
8.15.1 Enabling the real-time display of an environment monitoring device 96
8.15.2 Enabling the real-time display of UPS 98
8.16 Displaying The State/Analog Input Value History Of A Device 99
8.16.1 Displaying the state/analog input value history of a device (environment monitoring device) 99
8.16.2 Displaying the state/analog input value history of a device (UPS) 102
8.16.3 Notes on state/analog input value history display of a device 104
8.17 Outputting The System Log To A File 105
8.17.1 Using the procedure to output system log to a file 105
8.18 Outputting The State/Analog Input Value History To A File 106
8.18.1 Using the procedure to output state/analog input value history to a file 106
8.19 About The Security 108
8.19.1 Performing security setting 108
8.19.2 Functions that can have password confirmation 109
8.20 About The Password 110
8.20.1 Changing the password 110
8.21 About Database Backup 111
8.21.1 Backup target data 111
8.21.2 Performing a database backup immediately 111
8.21.3 Setting up a backup schedule 112
8.21.4 Note on backing up the database 112
8.22 About The Database Restore 113
8.23 About Database Cleanup 114
8.23.1 Cleanup target data 114
8.23.2 Performing a database cleanup immediately 114
8.23.3 Setting up a cleanup schedule 115
Appendix A: Ports Used 116
Appendix B: Explanation Of Events 117
Appendix C: Questions &Answers 120
Appendix D: Troubleshooting 121
Appendix E: Glossary 124
Appendix F: Explanation Of Items Displayed On The Operation Status List 125
Appendix G: UPS Alarm List 130
Appendix H: Windows Firewall Settings 132
Appendix I: Data Execution Prevention (DEP) Settings 147
Appendix J: User Account Control (UAC) Settings 149

1. Introduction

1.1 What Is SANUPS IT Monitor Manager?

SANUPS IT Monitor Manager is a software application that monitors, manages, and controls multiple target devices connected to a network in a consolidated way.
The current version supports the following target devices:

- Environment monitoring devices made by SANYO DENKI CO., LTD. (IT Monitor)
- UPS devices made by SANYO DENKI CO., LTD. (UPS with LAN interface card, Network Power Manager, SAN GUARD IV Lite, and SANUPS SOFTWARE)

[You must start the SNMP service first before using SAN GUARD IV Lite and SANUPS SOFTWARE].

Furthermore, the following abbreviations are used throughout this user guide, unless specified otherwise:

- A SANUPS IT Monitor Manager client is indicated as "client."
- The SANUPS IT Monitor Manager server is indicated as "server."
- Network Power Manager is indicated as "MT."
- SAN GUARD IV Lite and SANUPS SOFTWARE of subsequent products is indicated as "SG IV Lite." When using SANUPS SOFTWARE, read "SG IV Lite" in the following explanations as "SANUPS SOFTWARE."

1.2 What Can SANUPS IT Monitor Manager Do?

(1) Concentrated monitoring
Using this software application, you can monitor and manage target devices on a network, from a remote location.
Usually, the server obtains only the minimum information at a time interval specified by the administrator, and monitors the operation states of the devices.
However, when a device is added for monitoring, when changes in settings of target devices are detected, or when the ROM version of a target device is detected, the server then obtains all information of the target devices.

(2) Device's fault notification
Once the several settings of SANUPS IT Monitor Manager are configured, when a fault occurs at a device targeted for monitoring, this software application can notify the administrator of the fault by sending a pop-up message to a specified machine, running a specified batch file on the server, or sending an e-mail.

(3) Management and monitoring information setting
The administrator can add or delete a device targeted for monitoring from the server, or change the interval used to monitor the device.
The administrator can configure multiple devices at the same time to the same settings in monitoring interval and information (management information) necessary for accessing target devices managed by SANUPS IT Monitor Manager.

(4) Apply default information to devices added
You can set up default values for some settings (management information) that are used when a device is added as a target to be managed. Once the default values are set, they are used when devices are added subsequently.

(5) Saving and displaying system log
When an event about a device targeted for monitoring occurs, such as a change in the digital input state, or occurrence/recovery of a fault, the server stores this information in its system log.
The system log can be displayed on a client, or be saved to a file in the CSV format. This enables you to check any change in operation of a device.
Also, by applying a filter to this information, the administrator can customize the system log so that only a log for a specific device is displayed.

(6) Real-time display of a device
You can display the state of a device (digital input state, analog input state, digital output state, etc.) in real-time. Strictly speaking, however, the real-time display is not done in real-time, but at an interval of every five seconds, during which information is gathered and then displayed.

(7) Collecting and displaying the state/analog input value history of a device
By using the polling interval set up, the server collects information about a device and records the state/analog input value at that moment, as state/analog input value history information.
The state/analog input value is recorded when either of the following conditions is met: “when current time of the system exceeds the time that the state/analog input value save interval was added to the previous saved time” or “when occurrence/recovery of a fault is detected.”
Also, the administrator can specify the saving period of the state/analog input value history information. The recorded state/analog input value history information can be displayed on a client or saved to a file in the CSV format.

(8) Remote control of devices
The administrator can use the device real-time display screen to control the output of a device.
Also, by using batch control and schedule control, the administrator can control multiple devices as well.

(9) Device's applet startup
The administrator can start the Web applet of a device. The Web applet of the device can be used to perform detailed settings of the device.
Furthermore, if the Web applet is not running, the following operations cannot be performed:
① Setting the device's basic information “Network information of IP address, and SNMP operating environments”.
② Displaying the event log information kept by the device.

(10) Device parameter setting
For an environment monitoring device, you can set the analog input, digital input, and digital output parameters of the device, as well as the SNMP trap recipient and e-mail receipt settings.
Also, for a UPS device, you can set parameters to perform deviation monitoring of analog input value.
Furthermore, you can apply the same settings to multiple devices of the same type, all at the same time.

(11) Database backup
All information managed by SANUPS IT Monitor Manager can be backed up at any time, or the backup can be carried out according to a schedule set up by the administrator.

(12) Database cleanup
The state/analog input value history can be deleted (cleaned up) at any time, or the cleanup can be carried out according to a schedule set up by the administrator.

(13) Security setting
You can set a mode to force users to confirm their password when performing various functions on the clients, so that you can restrict operations by other users on each client.

(14) Password setting
You can modify the password used when a client logs on to the server, as well as when the various functions are executed.

(15) File output
You can output the system log and state/analog input value history to files in the CSV format.
These files can then be used for other applications for further data processing.

1.3 Operating Environments

1.3.1 Operating environment for server

At a minimum, the following environment is required for setting up SANUPS IT Monitor Manager as the server and then running it:

Computer hardware:	AT-compatible PC
CPU:	850 MHz (2 GHz or above recommended)
Memory:	192 MB or more (512 MB or more recommended)
Free disk amount:	200 MB or more (*1)
Operating systems:	Windows NT 4.0 with Service Pack 5 or later, Windows 2000 Professional and Server with Service Pack 4 or later, Windows XP Professional (x86/x64 supported) and Home Edition, Windows Server 2003 (including R2, x86/x64 supported), Windows Vista (x86/x64 supported), Windows Server 2008 (including R2, x86/x64 supported; excluding Server Core), Windows 7 (x86/x64 supported)

*1: If there is a large amount of data of state/analog input value information to store, then additional free disk space is required. To adjust the amount of data to store, use the database cleanup function.

1.3.2 Operating environment for clients

The following environment is required to set up SANUPS IT Monitor Manager as a client and then run it:

Computer hardware:	AT-compatible PC
CPU:	850 MHz (2 GHz or above recommended)
Memory:	64 Mbytes or more (256 MB or more recommended)
Free disk amount:	100 MB or more
Display:	Must be able to display 1024 x 768 dots or more
Operating systems:	Windows NT 4.0 with Service Pack 5 or later, Windows 2000 Professional and Server with Service Pack 4 or later, Windows XP Professional (x86/x64 supported) and Home Edition,

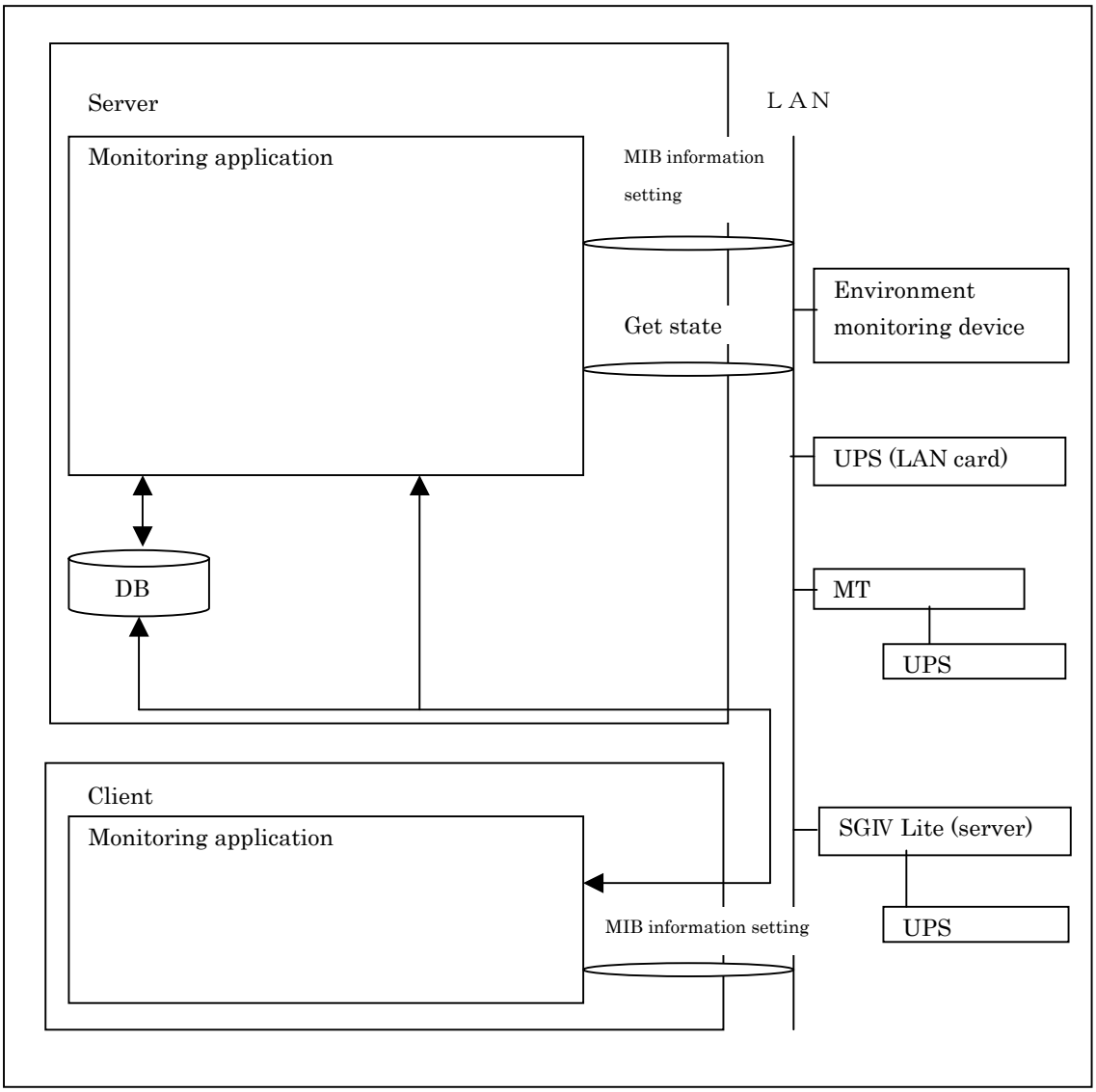
Windows Server 2003 (including R2, x86/x64 supported),
Windows Vista (x86/x64 supported),
Windows Server 2008 (including R2, x86/x64 supported; excluding Server Core),
Windows 7 (x86/x64 supported)

Furthermore, to use the function for running the Web applet, use a JavaVM compatible Web browser (only Internet Explorer is supported).

2. System Configuration And Requirements

2.1 System Configuration

This system consists of a server, clients, and devices targeted for monitoring. The server runs as a service program on the machine where SANUPS IT Monitor Manager is installed.
Also, each client runs as a GUI application.



* When SANUPS IT Monitor Manager is installed as the server, a client is also installed automatically. Also, you can choose to install only the client.

2.2 System Requirements

To use this system, the following requirements must be satisfied:

2.2.1 Network environment requirements

(1) Make sure a device targeted for monitoring has an IP address assigned to it and is already connected to the network.

(2) If the device targeted for monitoring uses the DHCP server, you need to register an IP address corresponding to the MAC address of the device to the DHCP server, and register a host name corresponding to the IP address to the DNS server or the Hosts file.

(3) Make sure the device targeted for monitoring and the machine with SANUPS IT Monitor Manager installed (server and client) are connected to a network and communication between them via TCP/IP if possible.

(4) When using operating systems that include Windows Firewall, you need to change the settings of Windows Firewall on the machines (server and clients) on which this software application is installed. For details on how to set Windows Firewall, see "Appendix H: Windows Firewall Settings" on page 132.

2.2.2 Operational requirements

(1) The server must be running 24 hours a day. (Monitoring is not possible when the server stops).

(2) Before a device is added as a device for monitoring, you need to set up the device as follows:

(a) Set its SNMP agent function to "Enable".

(b) The SNMP access permission must be given to the machine with SANUPS IT Monitor Manager installed. Also, the client machine must have SNMP access permission as well.

(3) When installing a server, you can use one of the following languages: Japanese, Chinese (simplified characters), and English (US). However, when selecting a language, you must select one that is the same as the language used in the ROM software of the environment monitoring device targeted for monitoring. If the language used by the device and the language used by the server are different, garbled text may appear on the screen of the client.

(4) When installing a client, you can use one of the following languages: Japanese, Chinese (simplified characters), and English (US). However, when selecting a language, you must select one that is the same as the language used by the server that is connected to the client. If the language used by the client and the language used by the server are different, garbled text may appear on the screen of the client.

(5) When using operating systems that include Data Execution Prevention (DEP), you need to change the settings of DEP on the machines (server and clients) on which this software application is installed. For details on how to set DEP, see "Appendix I: Data Execution Prevention (DEP) Settings" on page 147.

(6) When this software application is used as a server on an operating system that includes User Account Control (UAC) and a database restore is performed, the settings of UAC need to be changed. For details, see "8.22 About The Database Restore" on page 113 and "Appendix J: User Account Control (UAC) Settings" on page 149

(7) After changing the server time zone information (time zone or automatic adjustment of daylight saving time), restart the server and clients.

(8) When using this software application in a region with daylight saving time, restart the clients when the daylight saving time starts and ends. Note that the time for the past event log and the status measurement history displayed before and after the daylight saving time is ahead or behind in accordance with the time difference of the day light saving time. This is a restriction at the moment.

(9) When the server and client are on different machines, communication cannot be performed in an environment that uses NAT and IP masquerading. Do not use NAT and IP masquerading.

(10) In an operating system that includes power management functions such as suspend, do not use a function that automatically stops the CPU.

2.2.3 Restrictions

(1) The maximum number of devices that can be monitored is 500. (The number of devices that can be monitored is 500 minus the number of the sub networks).

(2) Devices that can be monitored are SANYO DENKI products only.

(3) The following restrictions apply when monitoring and controlling UPS:

(a) Restriction on UPS connected to a LAN

- The start and stop control of UPS means the ON and OFF of the output of the UPS, but not the start and stop control of the UPS itself.

(b) Restriction on MT connected serially to UPS

- The start and stop control of MT means the ON and OFF batch control of the output of the UPS. There is no control of the output of the UPS. Also, output control of individual MT outlets is not performed.

(c) For SGIV Lite or MT connected to UPS

- Control on the start and stop control is not performed.
- The analog input value of UPS is not obtained and displayed.
- Only a small part of the information (power failure, low battery level) regarding the UPS alarm can be obtained.

(d) Restriction on SGIV Lite connected serially to UPS

- The start and stop control of UPS means the ON and OFF of the output of the UPS, but not the start and stop control of the UPS itself. Also, when the stop control of UPS is performed, the machine with SGIV Lite installed is shut down so that the start control can no longer be performed.

(4) When you change the IP address of a machine running an operating system other than Windows NT, the new IP address becomes valid without the need to restart the machine. However, while this software is running, the change to the new IP address is not known to this software application. **Therefore, after changing the IP address of a machine where SANUPS IT Monitor Manager is installed, be sure to close the server and the client running on this machine, and then restart.**
(For details on restarting the server, see "6. Starting And Ending The Server" on page 19)

(5) If there is a firewall set up between the server and the client, there are some notes you need to pay attention to. For details, see "Appendix A: Ports Used" on page 116.

3. Overall Procedure (From System Introduction To Operation)

This section describes the overall procedure, covering from system introduction to operation start.
For details on a particular step, go to the page listed beside the step.

Step 1 **Checking the system environment**

Checking the network environment ····· 7
Checking the system restrictions ····· 9

↓

Step 2 **Preparation on a device**

Set the SNMP agent of a device to "Enable".
In the SNMP access restrictions, give access permission to the server and client machines.

····· 13

↓

Step 3 **Installing and starting this software**

Installing ····· 14
Starting the server ····· 19
Starting the client ····· 21

↓

Step 4 **Adding a device as target for monitoring**

Adding a device as target for monitoring ····· 30

↓

Step 5 **Setting the management information and monitoring method of the device**

Performing setting required for fault occurrence notification ····· 46
Setting management information (device management information) ····· 54

↓

Step 6 **Starting system operation**

Managing and monitoring devices

Receiving fault notification ····· 45
Viewing the device operation status ····· 84
Viewing the system log ····· 91
Controlling a device from a remote location ····· 68
Enabling the real-time display of a device ····· 96
Displaying the state/analog input value history of a device ····· 99
Outputting the system log to a file ····· 105
Outputting the state/analog input value history to a file ····· 106
Deleting a device ····· 43

Setting up information kept by a device

Setting the parameter information of a device ····· 60, 67
Starting up the Web applet of a device ····· 58

Setting up information kept by the server

Setting management information ····· 54
Performing fault notification setting ····· 47
Performing a database backup ····· 111
Performing a database cleanup ····· 114
Setting up security ····· 108
Changing the password ····· 110

4. Preparation On A Device

Before adding a device as a target for monitoring by this software application, you must perform the following settings:

(1) Set up the IP address of the device, and connect it to the network.
(2) Set the SNMP agent function to "Enable".
(3) In the SNMP access restrictions, give access permission to the server and client machines.

4.1 Setting The IP address Of The Device

When you set a device as a target for monitoring by this software application, the following restrictions apply to the IP address of the device:

(1) If the target device uses the DHCP server, then you need to register the IP address corresponding to the MAC address of the device to the DHCP server, and register the host name corresponding to the IP address to the DNS server or the Hosts file.
(2) The target device and the machine where this software application is installed (server and client) must be connected to the network and be able to communicate with each other via TCP/IP.

You can use a Web administrative tool or terminal emulator software application, such as Hyper Terminal that comes standard with a PC, to set the IP address of the device. For details on how to set the IP address, refer to the user guide that comes with the device.

4.2 Performing The SNMP Setting Of The Device

You can use a Web administrative tool or terminal emulator software application, such as Hyper Terminal that comes standard with a PC, to set the SNMP of the device. For details on how to perform the SNMP setting, refer to the user guide that comes with the device.

5. Installing SANUPS IT Monitor Manager

5.1 Before Installing

Before installing SANUPS IT Monitor Manager, check the following items:

(1) During the install operation, some temporary files are created, which requires about 200 Mbytes of space. Therefore, make sure you have enough free disk space before starting the install operation.

(2) The install operation requires administrative rights of the machine administrators (Administrators). Make sure you have these rights.

5.2 Install Procedure

> Make sure you have the administrative rights of the administrators when performing the following steps.

(1) Start the install program.

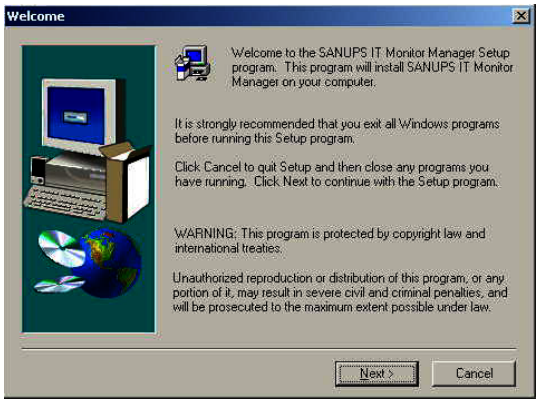
① Insert the SANUPS IT Monitor Manager CD-ROM in the CD-ROM drive.

② The install program runs automatically and displays the following screen:



> **If the install program does not run automatically**
>
> Start the Explorer and move to the CD-ROM drive.
> Double-click Setup.exe on the CD-ROM to run the install program.

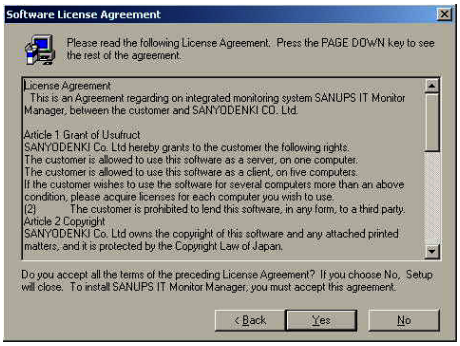
③ After selecting a language to use, click "OK". The following screen appears:



④ Click "Next".

(2) View the product license.

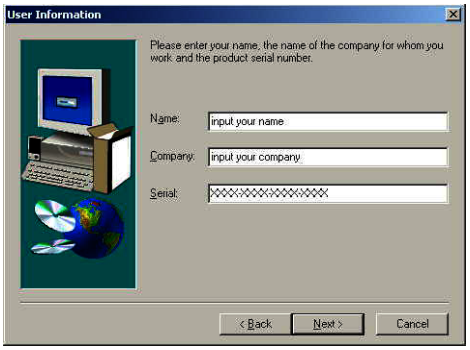
① The license agreement screen appears.



② To continue the install operation, click "Yes".

(3) Enter user information.

① The user information input screen appears.

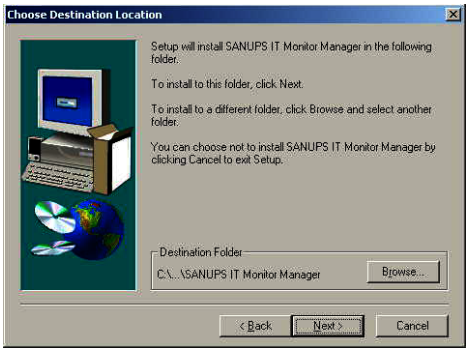


② Enter “Name”, ”Company”, and ”Serial”.
The serial number is written on the CD-ROM case of SANUPS IT Monitor Manager.

③ Click "Next".

(4) Check the install destination directory.

① The install destination selection screen appears.

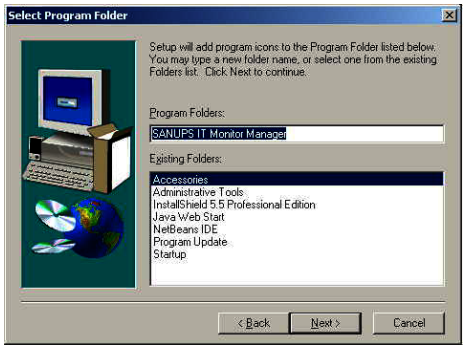


If necessary, change the install destination.

② Click "Next".

(5) Select a program folder.

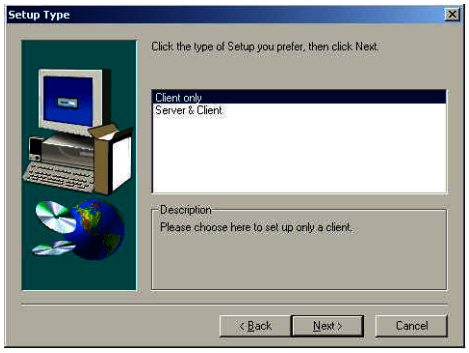
① The program folder selection screen appears.



② Click "Next".

(6) Select a setup type.

① The setup type selection screen appears.

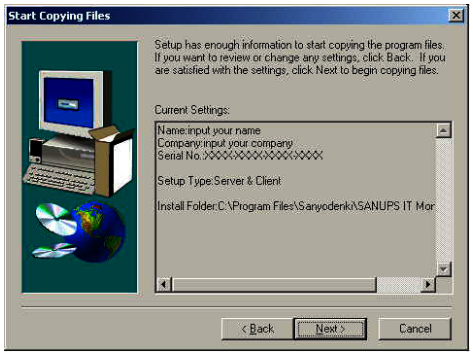


② To install the software application as a client on the machine, select "Client Only".

③ To install the software application as the server on the machine, select "Server & Client".

(7) Confirm that file copy can start.

① The file copy confirmation screen appears.



② Check the contents of the setup; then click "Next".

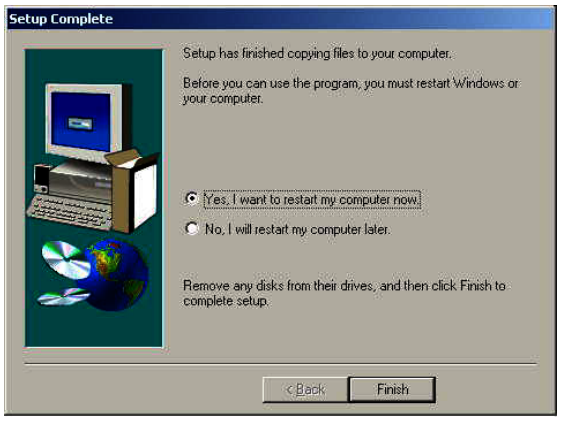
(8) Files are copied (install operation is in progress).

① The SANUPS IT Monitor Manager files are copied to the hard disk drive.
The install operation takes several minutes to finish, so please wait until it is finished.

> <Note>
> If the install destination does not have enough free space, the install operation may not be possible. If this happens, check to make sure that the operating environment has enough free space.

(9) The install operation is finished.

① The setup completion screen appears.



② Click "Finish" to end the install program.

* When the install program ends, restart the computer to complete the install operation. To start the SANUPS IT Monitor Manager service, be sure to restart the computer.

* After the install operation is complete, you can add devices and then monitor them.

5.3 Note On Using JavaVM (Java Virtual Machine)

SANUPS IT Monitor Manager runs as a Java application.
When you install this software application on a computer, JavaVM (*1) is set up automatically. Because this JavaVM is dedicated to running SANUPS IT Monitor Manager only, it does not affect any existing JavaVM installed already or JavaVM to be installed.

(*1) Java™ Runtime Environment Version 1.3 (JRE1.3) is set up.

If you have already installed JavaVM that is not part of the SANUPS IT Monitor Manager install operation, when you uninstall this JavaVM, this will not affect the JavaVM environment of SANUPS IT Monitor Manager.

5.4 Uninstall Procedure

5.4.1 If the server is already installed

Use the following procedure to uninstall SANUPS IT Monitor Manager:

① Stop the SANUPS IT Monitor Manager server.
If the SANUPS IT Monitor Manager server is running, see the "Starting And Ending The Server" section on page 19 and then stop the service.

<Note>
You cannot uninstall the SANUPS IT Monitor Manager service while it is running.

② Uninstall SANUPS IT Monitor Manager.
(a) Click the "Start" button and point to "Settings"; then select "Control Panel".
(b) From "Control Panel", select "Add/Remove Applications".
(c) From the application menu, select "SANUPS IT Monitor Manager"; then delete it.

5.4.2 If only the client is installed

Use the following procedure to uninstall SANUPS IT Monitor Manager:

① Uninstall SANUPS IT Monitor Manager.
(a) Click the "Start" button and point to "Settings"; then select "Control Panel".
(b) From "Control Panel", select "Add/Remove Applications".
(c) From the application menu, select "SANUPS IT Monitor Manager"; then delete it.

6. Starting And Ending The Server

6.1 Starting

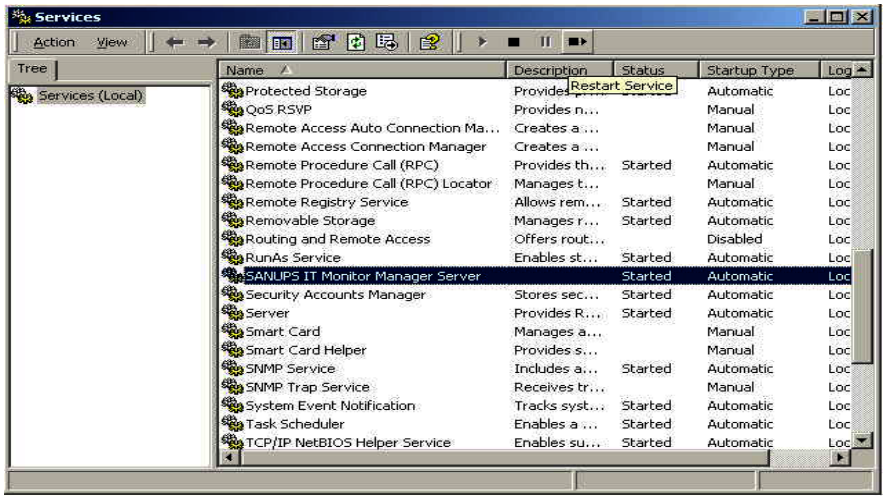
The SANUPS IT Monitor Manager server runs as a service using the name "SANUPS IT Monitor Manager Server".
After this software application is installed, when you start Windows again, the application runs automatically. (It runs in the background even if you do not log on to it).

6.2 Ending

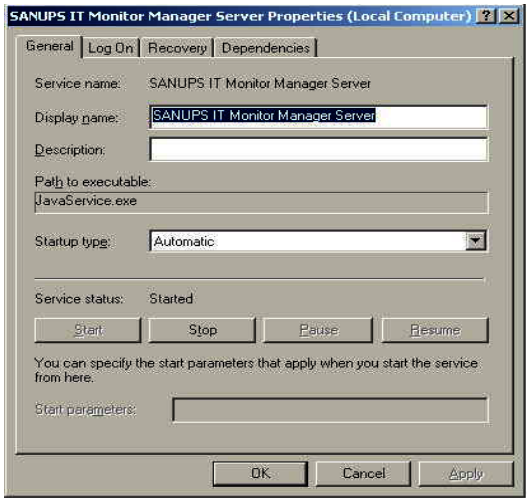
The following explanation uses Windows 2000 as an example. Perform the equivalent operation in another operating system.

① Click the "Start" button and point to "Settings"; then select "Control Panel".

② When "Control Panel" appears, select "Administrative Tools"; then click "Services".



③ Double-click "SANUPS IT Monitor Manager Server" to display the properties screen.



④ Use the "Stop" or "Start" button to stop or start the service.

[If Windows XP is used]

Click the "Start" button; then select "Control Panel". Select "Performance and Maintenance"; then select "Administrative Tools". Finally, select "Services". The subsequent operation is same as that for Windows 2000.

[If Windows NT is used]

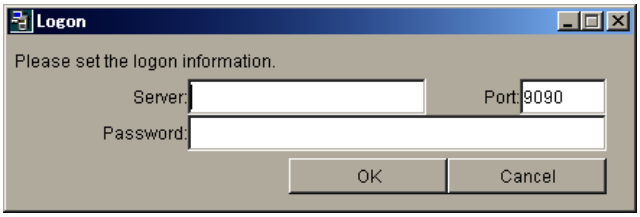
Click the "Start" button; then select "Control Panel". Select "Administrative Tools"; then select "Services". The subsequent operation is the same as that for Windows 2000.

7. Starting And Ending The Client

7.1 Starting

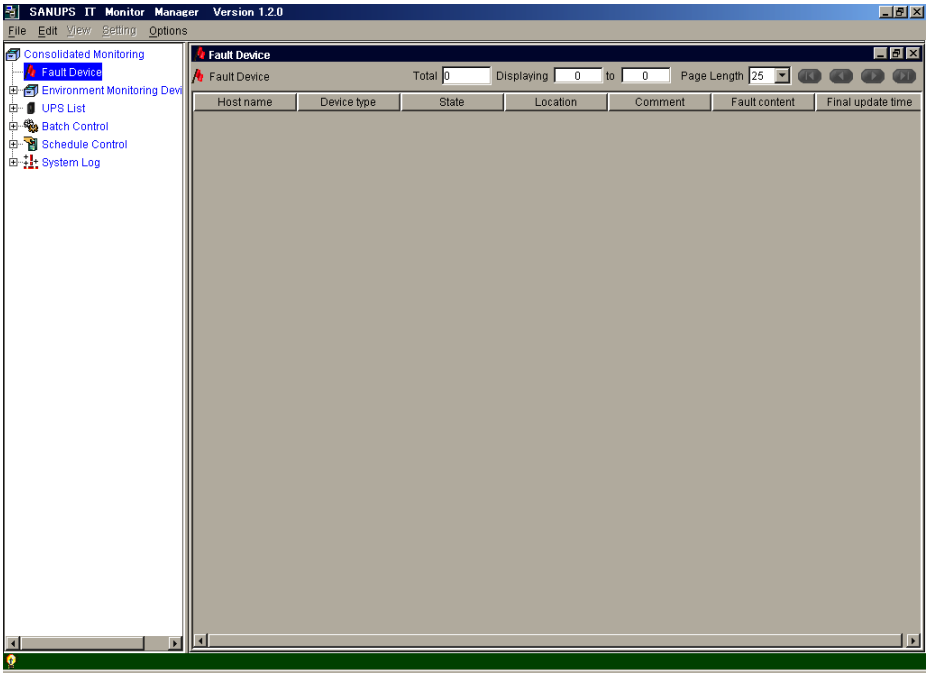
① Click the "Start" button on the task bar. Point to "Programs"; then select "SANUPS IT Monitor Manager". Click "Client".

② The following logon screen of the of SANUPS IT Monitor Manager server appears:



(a) In the "Server" text box, enter the host name or IP address of the SANUPS IT Monitor Manager server.
(b) In the "Port" text box, enter the port to connect to the SANUPS IT Monitor Manager server. Always use 9090 as the port number. If you enter a number other than 9090, you cannot log on to the SANUPS IT Monitor Manager server.
(c) Enter the password (the default is "public"); then click the "OK" button.

③ After you log on, the "SANUPS IT Monitor Manager" main screen appears.

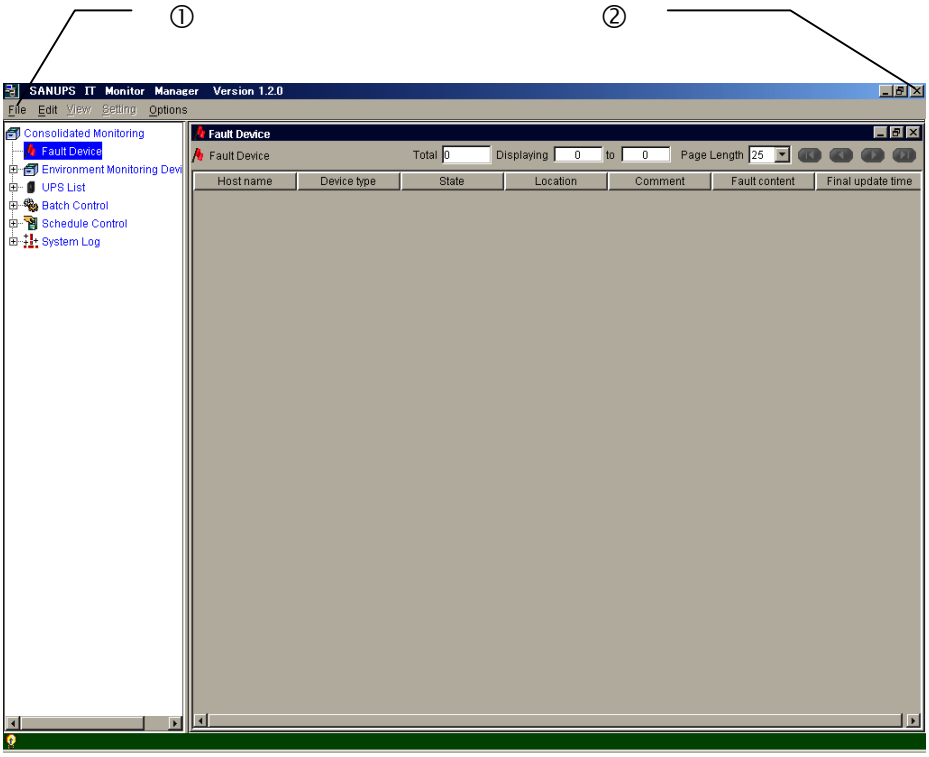


7.2 Ending

To exit a SANUPS IT Monitor Manager client, do one of the following:

① From the "File" menu, select "Exit".

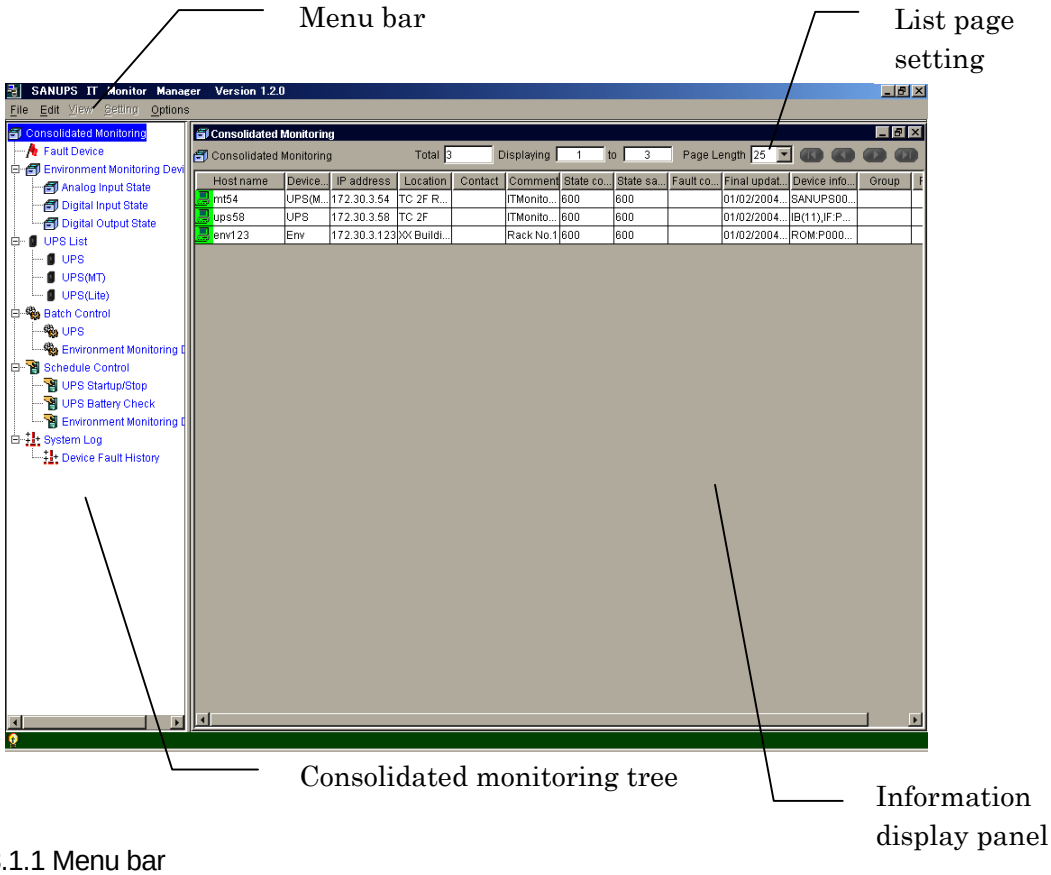
② Click the "x" on the title bar of the window.



8. Explanation Of Functions

8.1 About The Main Screen Of A Client

This section describes the various parts of the main screen of a client.



8.1.1 Menu bar

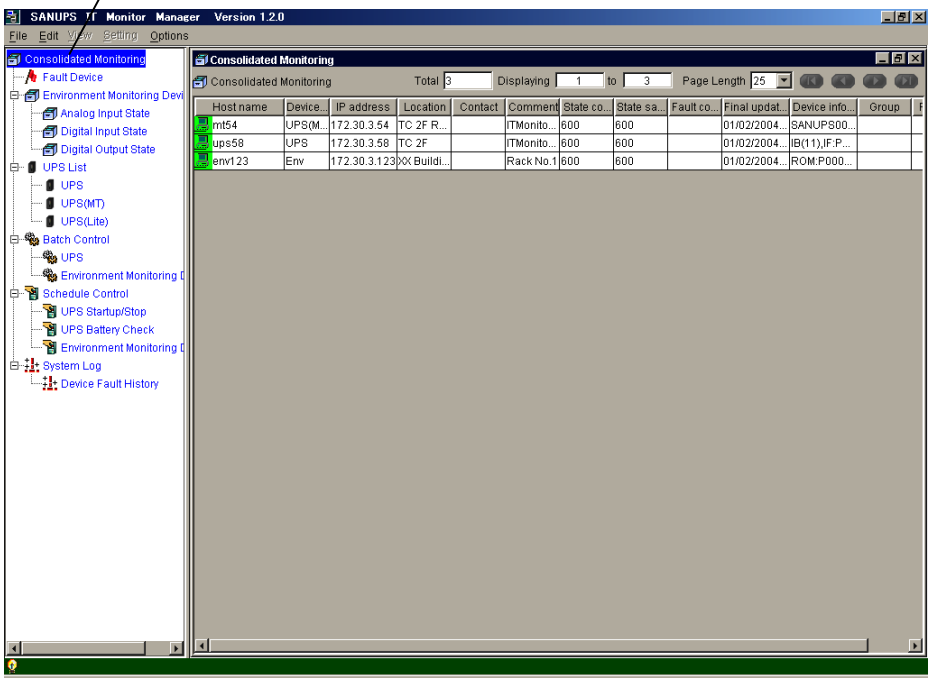
Menu name	Menu item	Description
File	System Log Output	Use this menu item to output the system log stored on the server to a file in the CSV format.
	State/Analog Input Value History File Output	Use this menu item to output the state/analog input value history stored on the server to a file in the CSV format.
	Exit	Use this menu item to exit a client.
Edit	Add Device Default Information Setting	Use this menu item to set the default values of access information used when a device is added.
	Add Device	Use this menu item to add a device as target for monitoring.
	Del Device (*)	Use this menu item to remove a device so that it is no longer targeted for monitoring.

Menu name	Menu item		Description
View	Real-time Display (*)		Use this menu item to enable real-time display of the state/analog input value of a device. You can select devices one by one, and then enable real-time display for the multiple devices.
	State/Analog Input Value History Display (*)		Use this menu item to enable display of state/analog input value history of a device. You can select devices one by one, and then display state/analog input value history for the multiple devices.
	Status update (*)		Use this menu item to get the state of a device again.
Setting	Management Information Setting (*)		Use this menu item to change the information required by the server or a client for accessing a device targeted for monitoring, or the information setting required for monitoring. You can also change the settings of multiple devices all at the same time.
	Parameter Setting (*)		For an environment monitoring device, you can use this menu item to change the analog input, digital input, and digital output parameters of the device. For a UPS device, you can set a parameter for deviation monitoring of the analog input value. You can also change the settings of multiple devices all at the same time.
	Applet Startup (*)		Use this menu item to start the Web applet of a device.
Options	Fault Notification Setting		Use this menu item to specify the fault notification method of a device.
	UPS Warning Setting		Use this menu item to set up alarm functioning as warnings, among the alarm information sent from UPS.
	Security Setting		You can use this menu item to enable or disable password authentication used in executing the various functions.
	Password Setting		You can use this menu item to change the password.
	Database Backup		
		Immediate Execution	You can use this menu item to immediately perform database backup.
		Schedule Setting	You can use this menu item to set up a database backup schedule.
	Database Cleanup		
		Immediate Execution	You can use this menu item to immediately perform database cleanup.
		Schedule Setting	You can use this menu item to set up a database cleanup schedule.

(*) When a device is selected from the device operation status list of the information display panel, menu selection becomes possible.

8.1.2 Consolidated monitoring tree view

Consolidated Monitoring tree view



(1) The consolidated monitoring tree view consists of four views: a view to display the device operation status, a view to display the batch control information, a view to display the schedule control information, and a view to display the system log information.

(2) Contents of the device operation status view and the system log view are as follows:

(a) Consolidated monitoring view
This view displays a list of device operation status of all devices targeted for monitoring.
The content of this view cannot be customized by users, as described later.

(b) Fault device view
This view displays a list of devices where a fault has occurred, among all devices targeted for monitoring.

(c) Environment monitoring device list view
This view displays a list of all information of all environment monitoring devices.

(d) Analog input state view
This view displays a list of analog input states of all environment monitoring devices.

(e) Digital input state view
This view displays a list of digital input states of all environment monitoring devices.

(f) Digital output state view
This view displays a list of digital output states of all environment monitoring devices.

(g) UPS list view
This view displays a list of states of all UPS devices.

(h) UPS view
This view displays a list of states of UPS devices directly connected to the LAN (UPS devices with LAN interface), among all UPS devices.

(i) UPS (MT) view
This view displays a list of states of UPS devices connected via the MT (Network Power Manager), among all UPS devices.

(j) UPS (Lite) view
This view displays a list of states of UPS connected via the SGIV Lite server, among all UPS devices.

(k) System log view
This view displays a log of events that occur in the SANUPS IT Monitor Manager system. For a description of the contents of the events, see "Appendix B: Explanation Of Events" on page 117.

(l) Device fault history view
This view displays only a log of event fault occurrence/recovery.

(3) You can add a custom view below the device operation status view or the system log view. Also, by applying a filter to a custom view, you can customize the contents to display. For details, see the "Customizing content of the device operation status list display" section on page 84 or the "Customizing the system log list" section on page 93.

(4) The batch control view and the schedule control view display the following contents:

(a) Batch control view
This view displays a list of all batch control saving information. The contents cannot be modified.

(b) UPS batch control view
This view displays all batch control saving information for UPS devices. You can add, modify, or delete batch controls from the information display panel.

(c) Environment monitoring device batch control view
This view displays all batch control saving information for environment monitoring devices. You can add, modify, or delete batch controls from the information display panel.

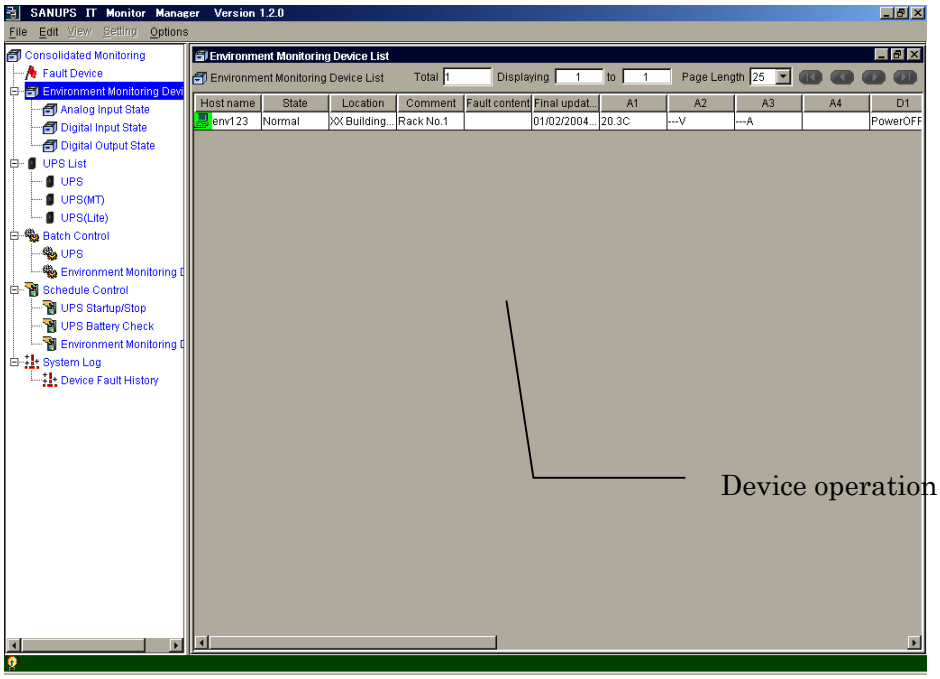
(d) Schedule control view
This view displays a list of all schedule control saving information. The contents cannot be modified.

(e) UPS start/stop schedule control view
This view displays all schedule control saving information of UPS start/stop. You can add, modify, or delete schedule controls from the information display panel.

(f) UPS battery check schedule control view
This view displays all schedule control saving information of UPS battery check. You can add, modify, or delete schedule controls from the information display panel.

(g) Environment monitoring device digital output schedule control view
This view displays all schedule control saving information of digital output of environment monitoring device. You can add, modify, or delete schedule controls from the information display panel.

8.1.3 Device operation status list



(1) When you select the device operation status view from the tree on the left side of the screen, the information display panel on the right side of the screen displays the device operation status list.

(2) The color of a device operation status list icon indicates the state of the device.

(a) Environment monitoring device icon colors

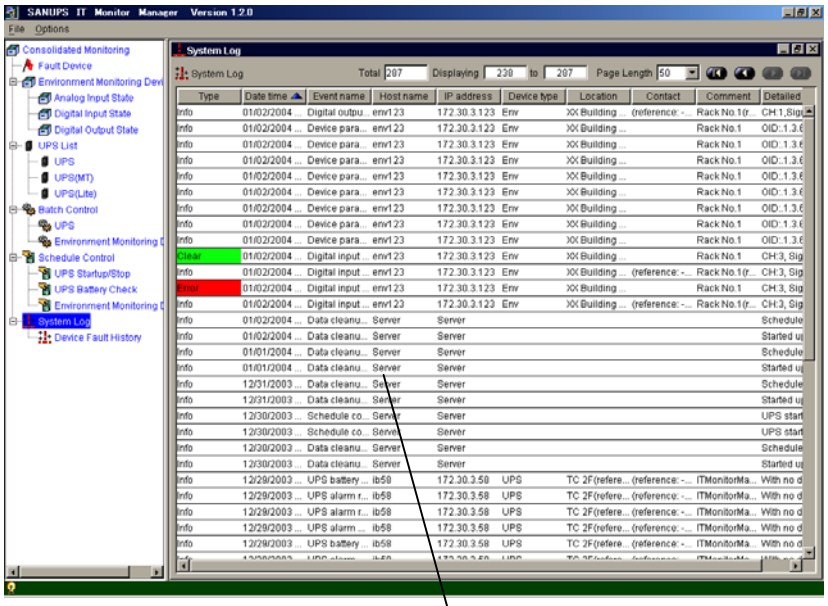
- Orange: Communication error
- Red: Fault (digital input state or analog input value deviation state that is defined as a fault in the parameter setting function and treated as a fault)
- Green: Normal

(b) UPS device icon colors

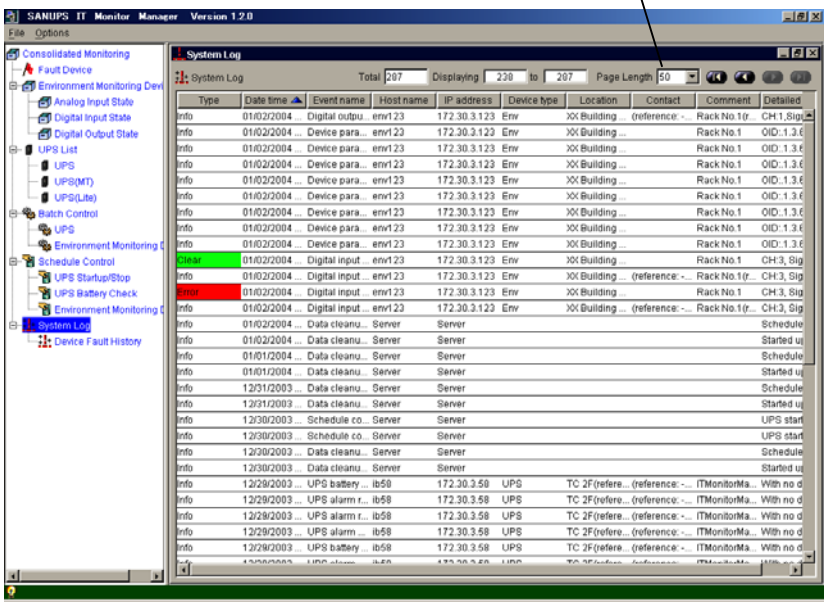
- Orange: Communication error
- Red: Fault (fault, or digital input value deviation state that is defined in the parameter setting function)
- Yellow: Warning (alarm occurrence state that is defined as a warning in the UPS warning setting function)
- Grey: Power failure
- White: Stop (output off)
- Green: Startup (output on)

8.1.4 System log panel

When you select the system log view, a list of system logs meeting the view filter criteria is displayed.



8.1.5 List page setting



(a) Page length
You can set the amount of data to display in a list.

(b) Total
It displays the total amount of the appropriate data. The content cannot be modified.

(c) Display
It displays the position of the data being displayed currently in the list. The content cannot be modified.

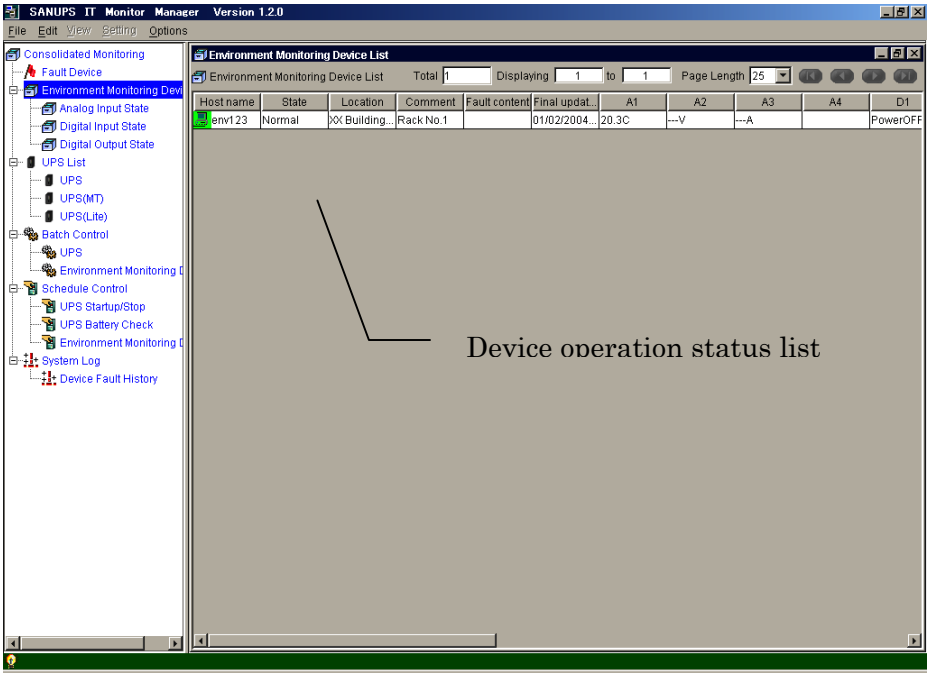
8.2 Adding A Device For Monitoring

Before SANUPS IT Monitor Manager can start managing and monitoring a device, you must add this device as a target for monitoring.
When you add a device, if you know its hosts name or IP address, see the “Adding a device by specifying its host name or IP address” section on page 33.
If you do not know its host name and IP address, see the "Adding a device by searching for it first" section on page 38 and then add the device.

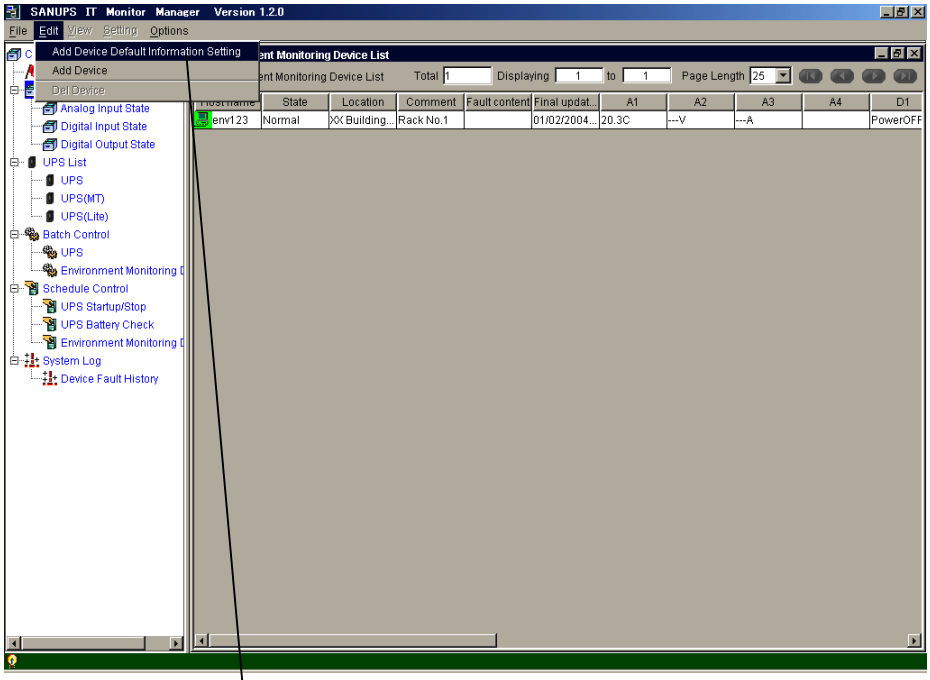
8.2.1 Setting the default values for use when devices are added

To save time required in inputting some information every time you add a device, you can set up default values for the READ community name, WRITE community name, polling interval, and state/analog input value save interval. This is very useful when you are adding a large number of devices.

① From the main screen, display the device operation status list.

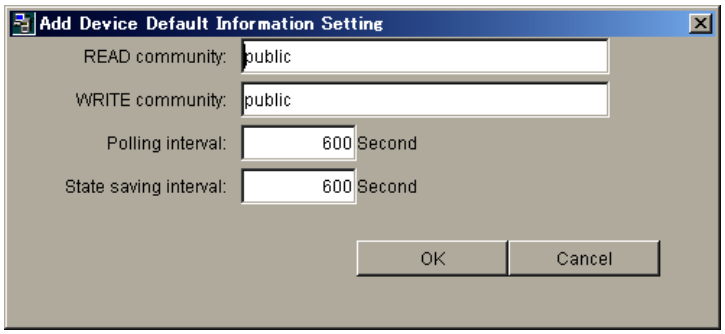


② From the "Edit" menu, select "Add Device Default Information Setting".



Add Device Default Information setting

③ The "Add Device Default Information Setting" screen appears.



(a) In the "READ community" and "WRITE community" text boxes, enter their default names.

(b) In the "Polling interval" text box, enter a default interval to use to check the state of the device.
If the interval you set here is too short, when more and more advices are added, this will increase the load on the network as well as the server machine, causing problems in the monitoring operation.
If a device fault happens or the state is changed, the SNMP trap is received and the state is obtained automatically. Therefore, the polling interval does not need to be that short. By default, the polling interval is set to 600 seconds (10 minutes).
As a general rule, if the number of devices is 200 or more, set the polling interval to 1200 seconds. If the number of devices is 400 or more, set the interval to 1800 seconds.

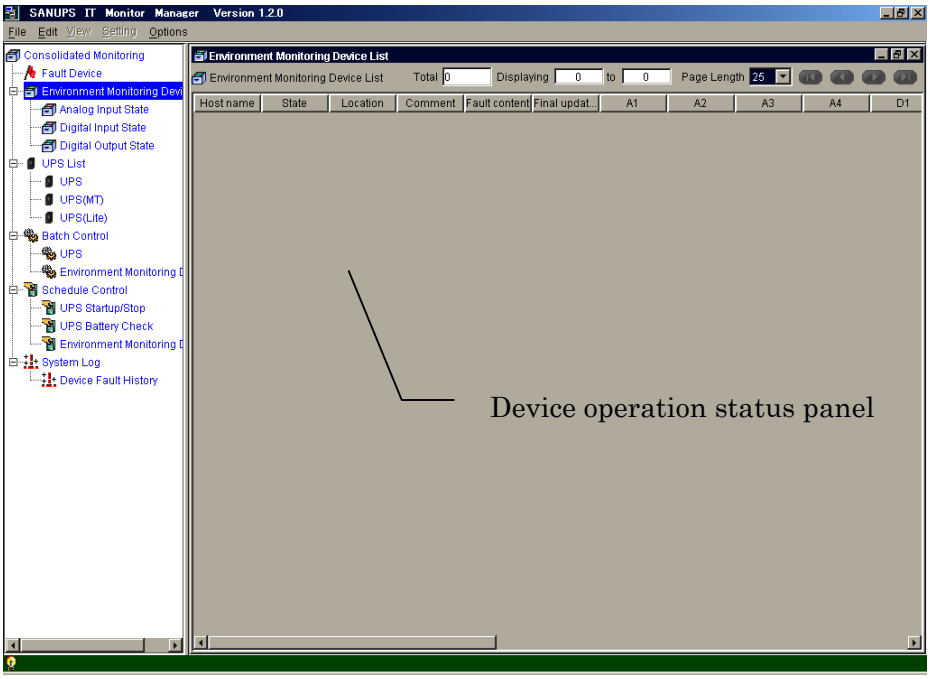
(c) In the "State saving interval" text box, enter the default interval to use to save the state/analog input value history of the device.
If you set the interval to 0, the information is saved only when the state of the device changes. For an environment monitoring device, the information is saved only when a change in the state of the digital input or in the state of the analog input value deviation is detected. For a UPS device, the information is saved only when a change in the state of the SNMP alarm or in the state of the analog input value deviation is detected.
Furthermore, data saving is performed during the polling interval; when the device state is checked, the data obtained is saved. For this reason, when setting this value, use a multiple of the value set for polling interval.

<Note>
The polling and saving operations are not performed at exactly the intervals specified in "Polling interval" and "State saving interval." Depending on the network state and server load, the operations may be delayed.
Also, if a communication error occurs, the state and analog input value cannot be obtained and therefore cannot be saved.

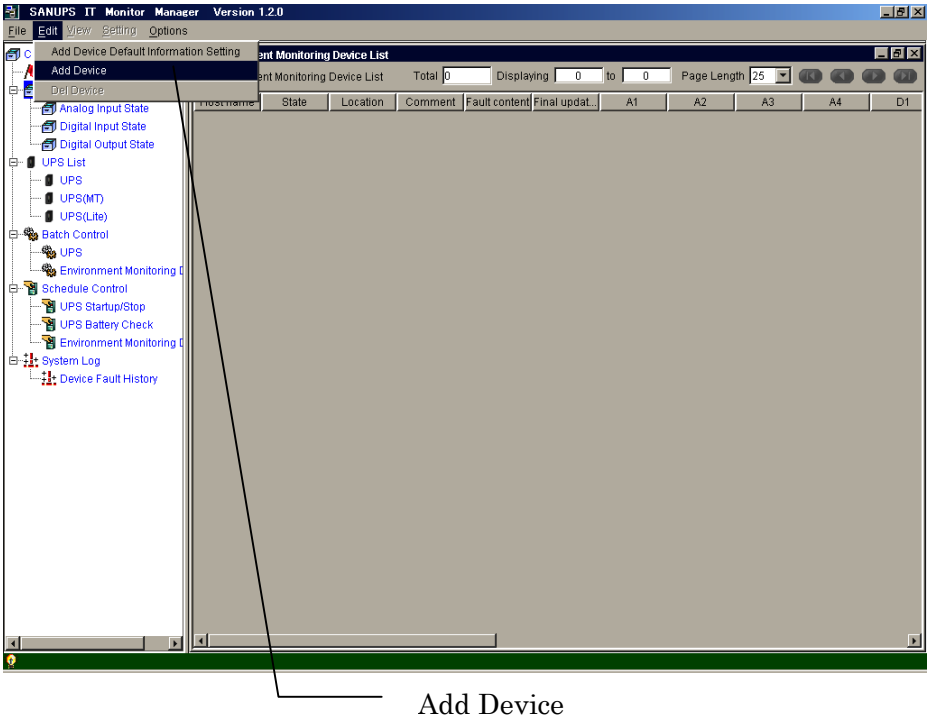
8.2.2 Adding a device by specifying its host name or IP address

Use the following procedure to add a device if you know its host name or its IP address:

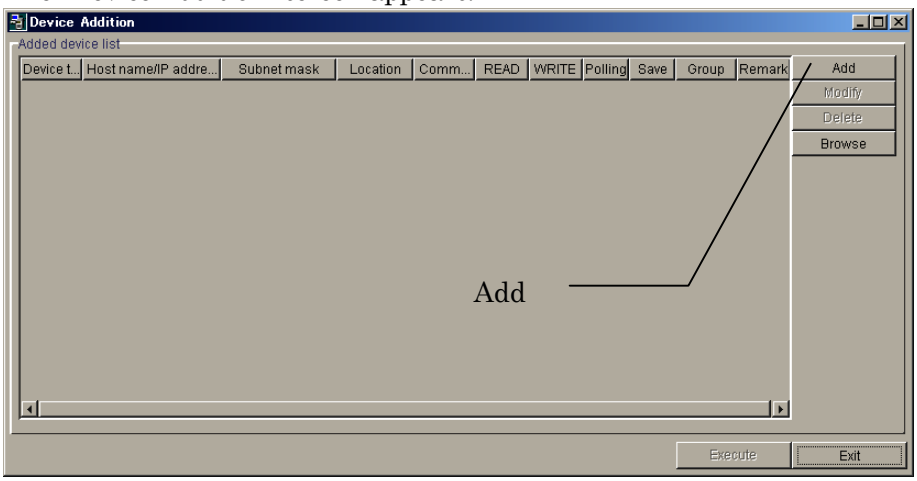
① From the main screen, display the device operation status list.



Using the main screen, select "Add Device" from the "Edit" menu.

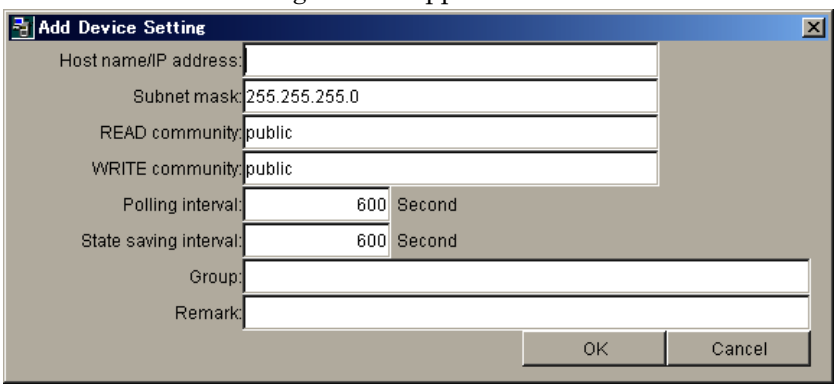


② The "Device Addition" screen appears.



③ From the "Device Addition" screen, click the "Add" button.

④ The "Add Device Setting" screen appears.



⑤ Enter information required for accessing the device, as well as information used when the device is managed.

(a) In the "Host name/IP address" text box, enter the host name or the IP address of the target device you want to add.

(b) You must enter information into all text boxes except "Group" and "Remark".

(c) For the "READ community" and "WRITE community" text boxes, enter the names according to the settings on the device.

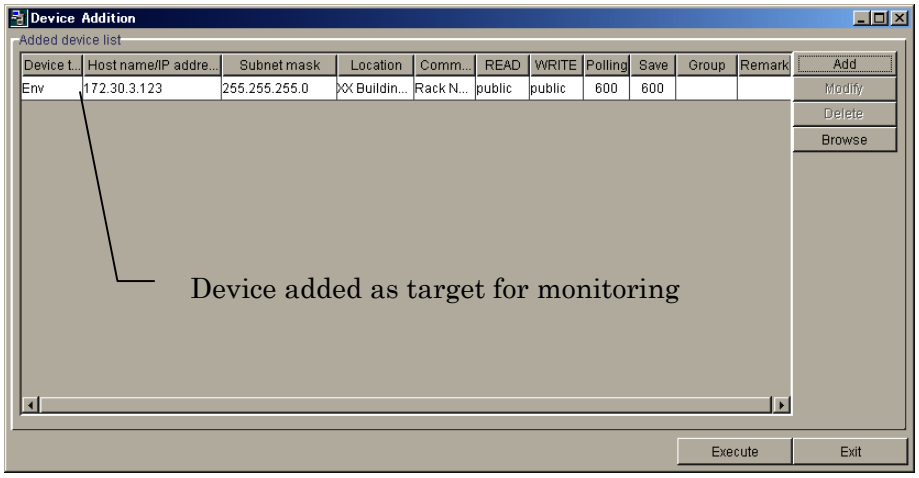
(d) In the "Polling interval" text box, enter a default interval to use to check the state of the device.
If the interval you set here is too short, when more and more advices are added, this will increase the load on the network as well as the server machine, causing problems in the monitoring operation.
If a device fault happens or the state is changed, the SNMP trap is received and the state is obtained automatically. Therefore, the polling interval does not need to be that short. By default, the polling interval is set to 600 seconds (10 minutes).
As a general rule, if the number of devices is 200 or more, set the polling interval to 1200 seconds. If the number of devices is 400 or more, set the interval to 1800 seconds

(e) In the "State saving interval" text box, enter the default interval to use to save the state/analog input value history of the device.
If you set the interval to 0, the information is saved only when the state of the device changes. For an environment monitoring device, the information is saved only when a change in the state of the digital input or in the state of analog input value deviation is detected. For a UPS device, the information is saved only when a change in the state of the SNMP alarm or in the state of the analog input value deviation is detected.
Furthermore, data saving is performed during the polling interval; when the device state is checked, the data obtained is saved. For this reason, when setting this value, use a multiple of the value set for the polling interval.

<Note>
The polling and saving operations are not performed at exactly the intervals specified in "Polling interval" and "State saving interval." Depending on the network state and server load, the operations may be delayed.
Also, if a communication error occurs, the state and analog input value cannot be obtained and therefore cannot be saved.

⑥ After you enter the information, click the "OK" button on the "Add Device Setting" screen.

⑦ The device is added to the added device list on the "Device Addition" screen.



⑧ If you want to add more devices, repeat steps ④ to ⑦ The devices are added to the added device list.

⑨ To delete a device, select the device from the list; then click the "Delete" button.

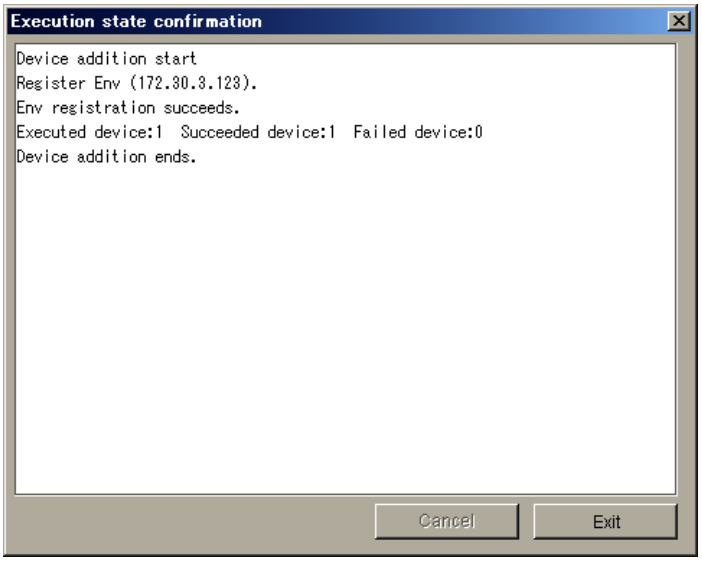
⑩ If you want to change the settings of any device in the added device list, see the "Modifying The Settings Of A Device Added" section on page 42 and then change the settings.

⑪ After you have added all devices you want to monitor to the added device list, click the "Execute" button.

⑫ When a message box appears to prompt you whether to add the devices, click the "Yes" button.

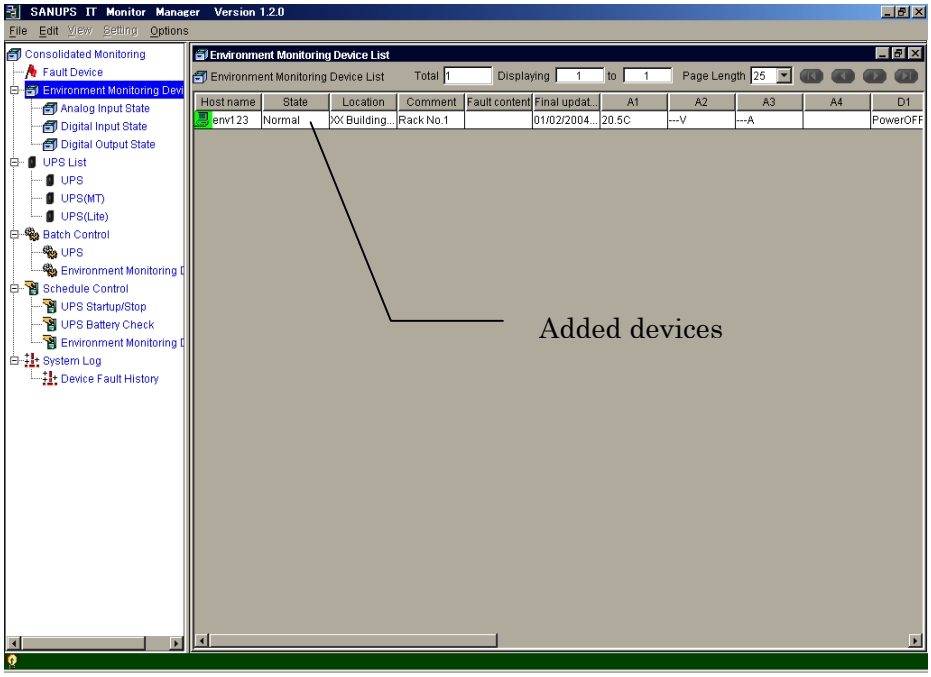


⑬ The "Execution state confirmation" screen appears.



⑭ After the devices are added, the following information appears: number of executed devices, number of succeeded devices, and number of failed devices.
Devices that have been added successfully are automatically removed from the added device list in step ⑫, and only devices that failed to be added remain in the added device list. If there are devices that failed to be added, see “Appendix D: Troubleshooting” on page 121 and try to add them again.

⑮ Devices that have been added now appear in the device operation status list of the main screen.

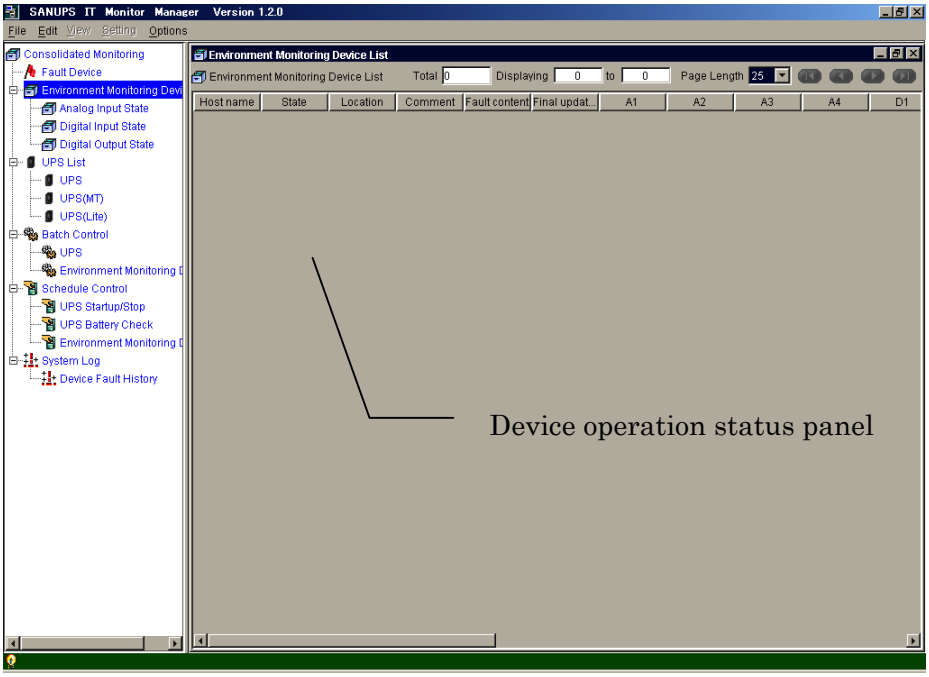


⑯ This completes the addition of devices.

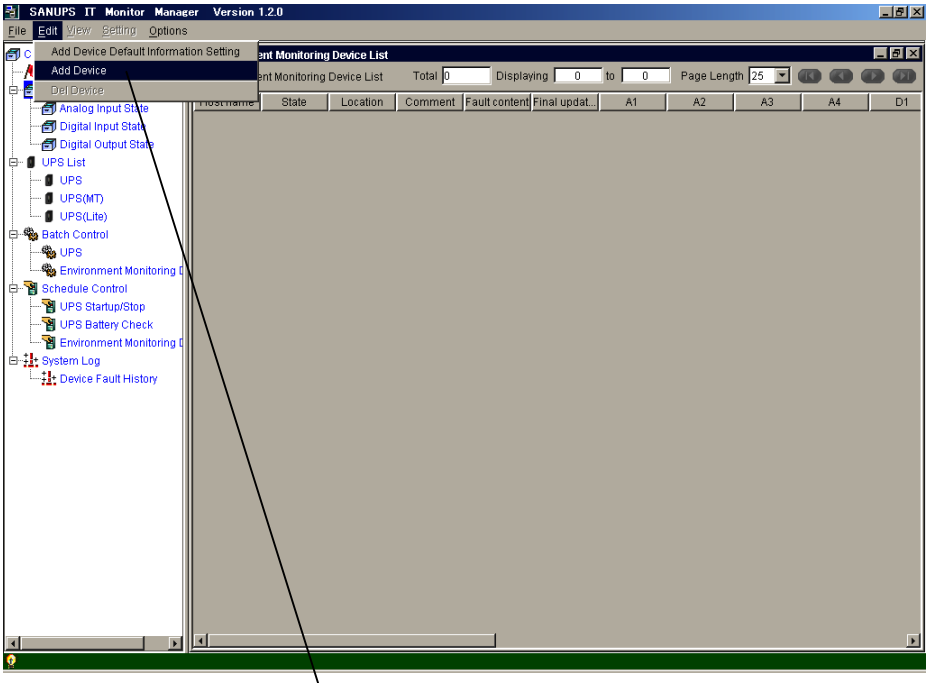
8.2.3 Adding a device by searching for it first

If there is a device you want to add but you do not know its host name or IP address, you can use the following procedure to find out the information and then add the device:

① From the main screen, display the device operation status list.

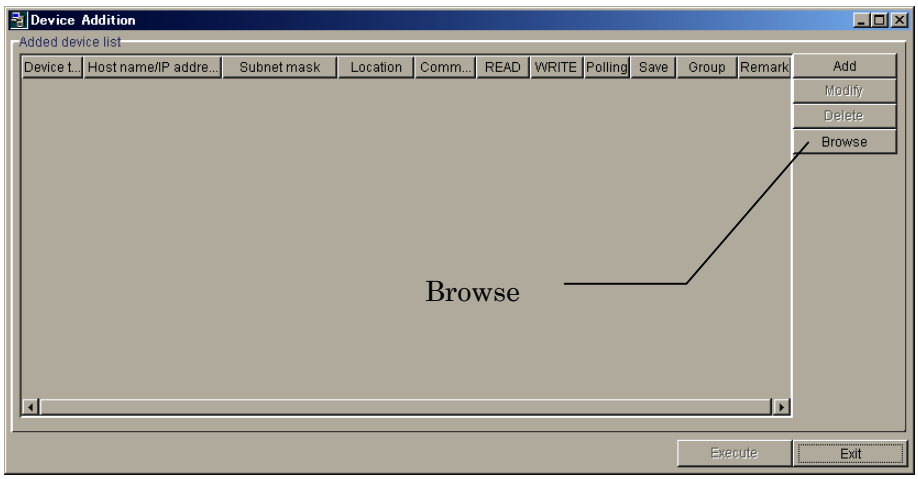


② Using the main screen, select "Add Device" from the "Edit" menu.

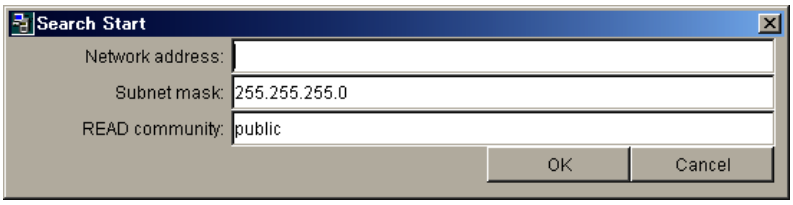


③ The "Device Addition" screen appears.

④ From the "Device Addition" screen, click the "Browse" button.



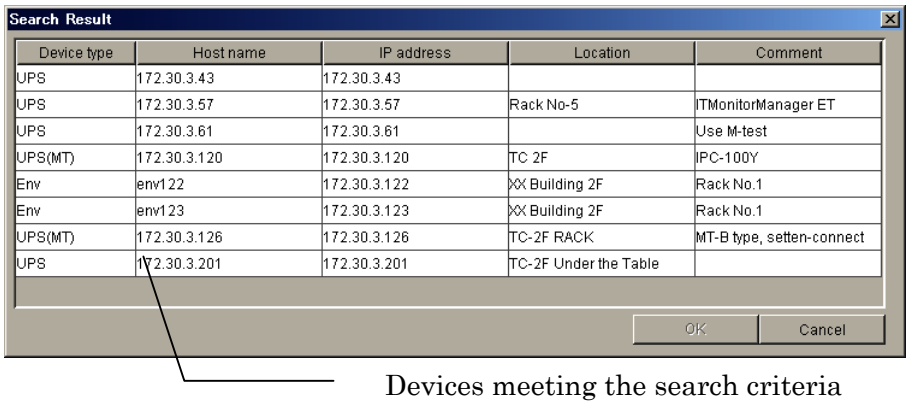
⑤ On the "Search Start" screen, enter the search criteria.



Example: Network address: `172.30.1.0`
Subnet mask: `255.255.255.0`
READ community: `public`

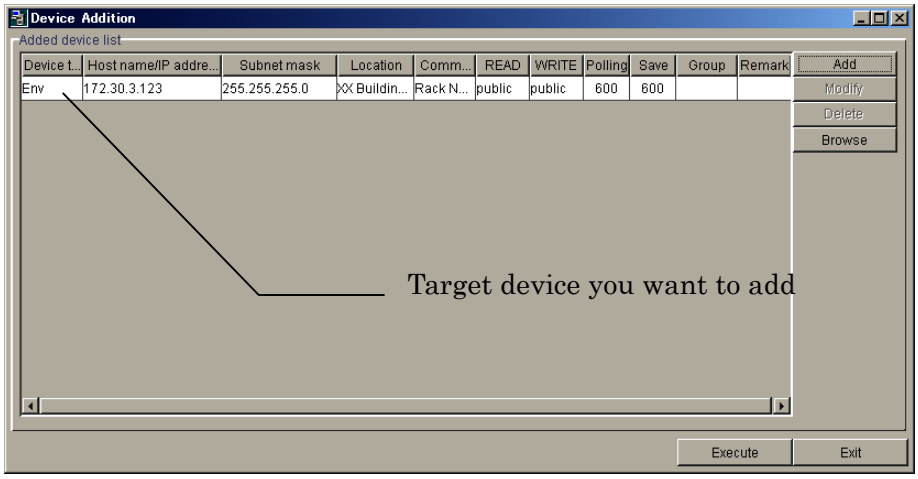
In the current version, the first 3 bytes of the subnet mask must be 255.

⑥ Click the "OK" button. Devices that are located on the sub network but not targeted for monitoring are searched, and the search result appears on "Search Result" screen.



⑦ From the list of devices in the search result list, select one or more devices that you want to monitor; then click the "OK" button.

⑧ The selected devices are added to the list on the "Device Addition" screen.



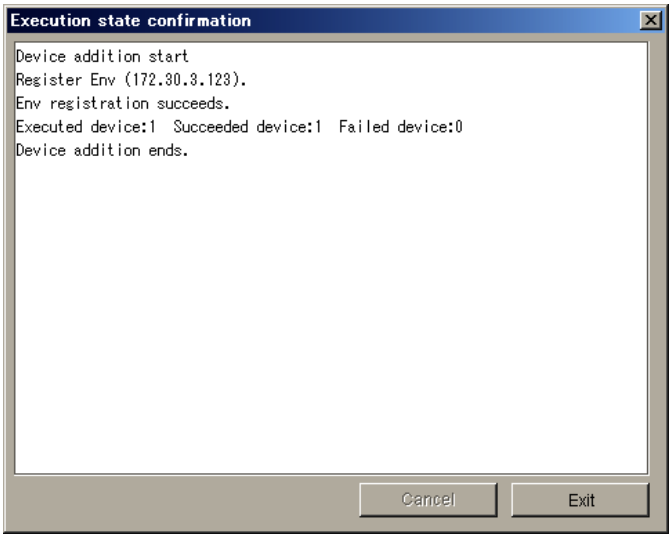
⑨ Here, the default values are set to "READ community" and "WRITE community" of each device in the added device list. If the default values of a device are different from the community names of the device, this device cannot be added to the list. Therefore, be sure to check the default values. If such difference does happen, see the "Modifying The Settings Of A Device Added" section on page 42 and then change its settings.

⑩ After you have added the devices you want to monitor to the added device list, click the "Execute" button.

⑪ When a message box appears to prompt you whether to add the devices, click the "Yes" button.

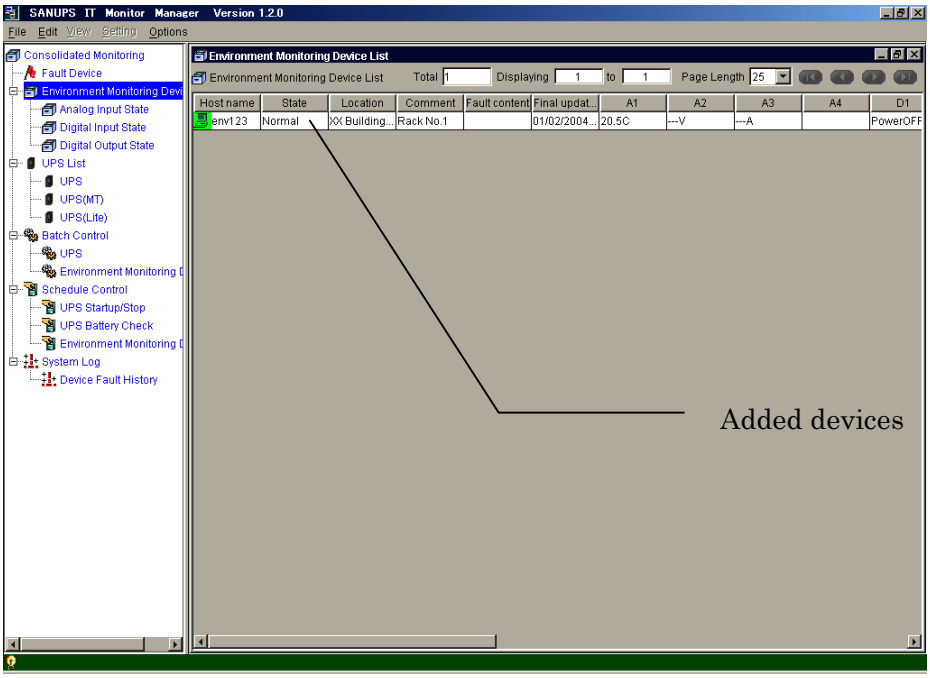


⑫ The "Execution state confirmation" screen appears.



⑬ After the devices are added, the following information appears: the number of executed devices, number of succeeded devices, and number of failed devices.
Devices that have been added successfully are automatically removed from the added device list in step ⑧, and only devices that failed to be added remain in the added device list. If there are devices that failed to be added, see “Appendix D: Troubleshooting” on page 121 and try to add them again.

⑭ Devices that have been added now appear in the device operation status list of the main screen.

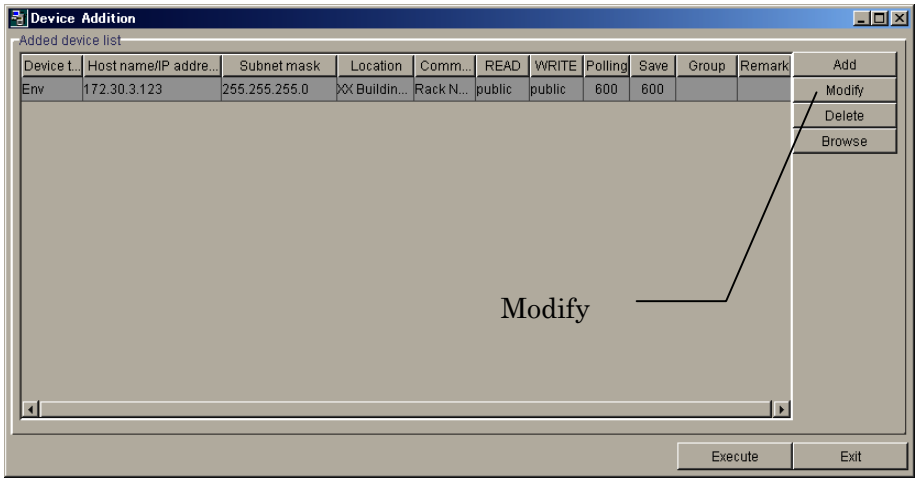


⑮ This completes the addition of devices.

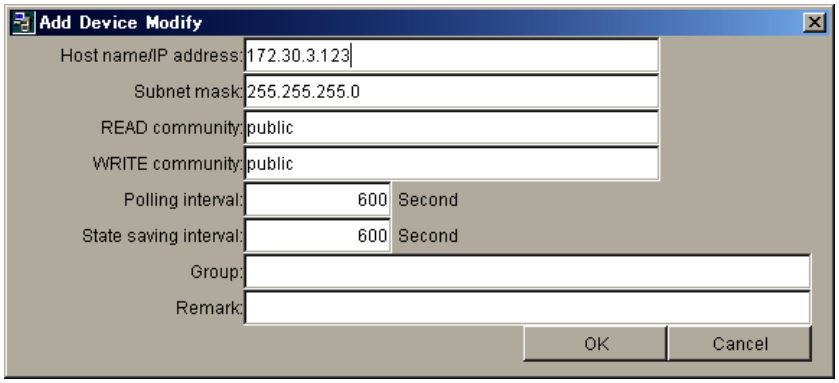
8.3 Modifying The Settings Of A Device Added

Use the following procedure to modify the settings of a device in the added device list:

① From the added device list on the "Device Addition" screen, select a device; then click the "Modify" button.

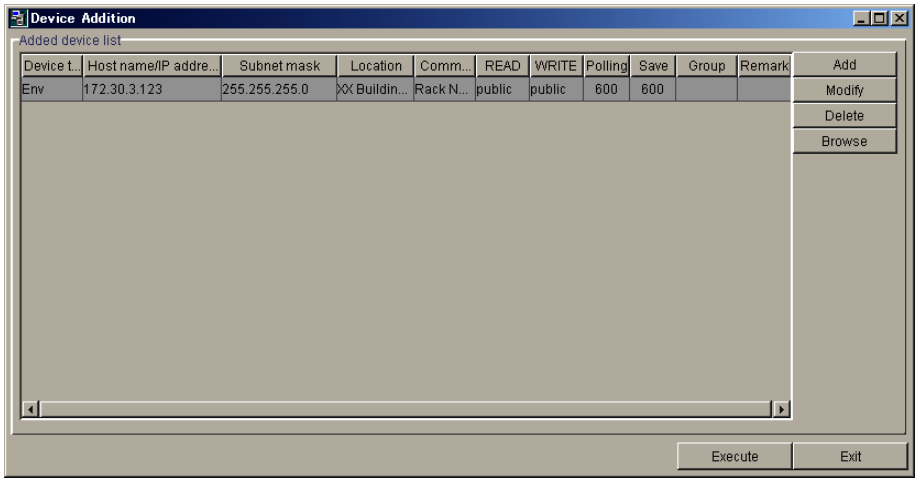


② The "Add Device Modify" screen appears.



③ Use the "Add Device Modify" screen to modify settings (they are used in accessing the device) that you want to change; then click the "OK" button.

④ After you perform the task in step ③, the "Device Addition" screen returns.

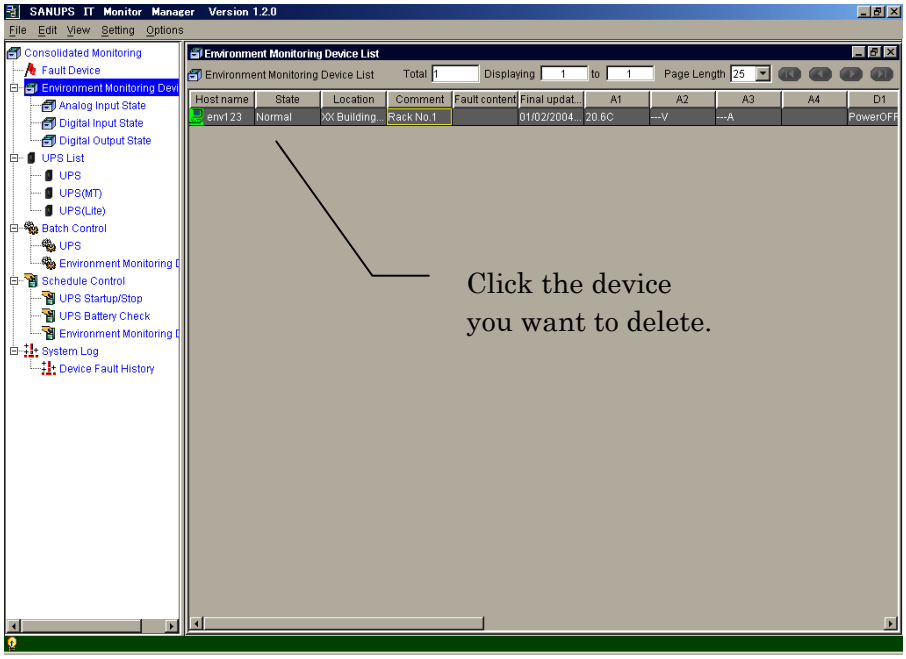


8.4 Deleting A Device Targeted For Monitoring

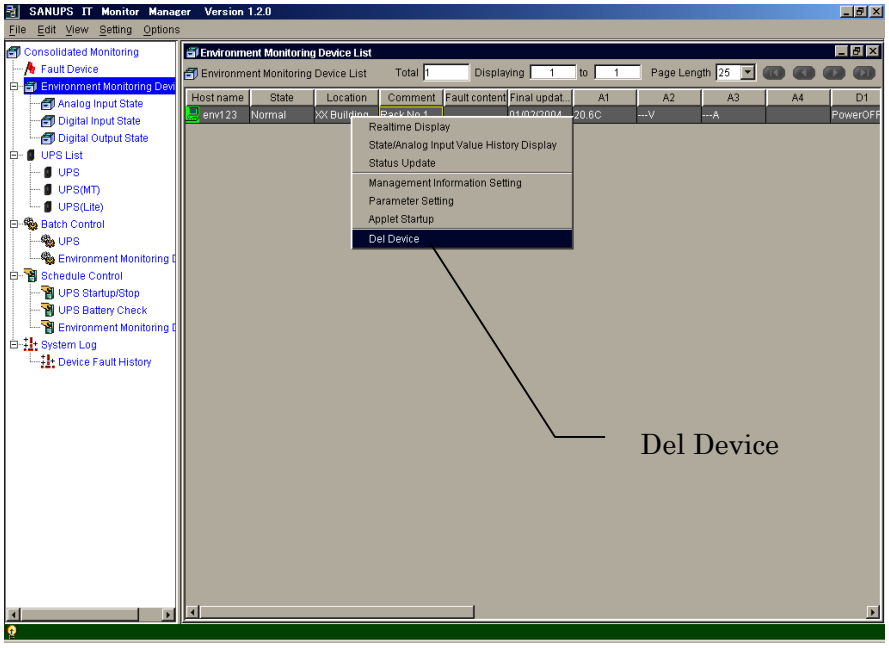
This section describes how to remove a device targeted for monitoring by SANUPS IT Monitor Manager.

8.4.1 Using the procedure to delete a device

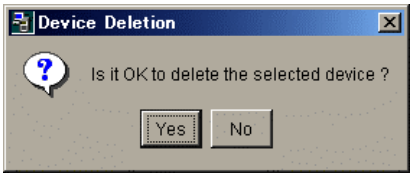
① Using the main screen, select a device from the device operation status list that you want to delete. (You can select multiple devices for deletion).



② From the "Edit" menu, select "Del Device". You can also right-click to display a shortcut menu and then select "Del Device".



③ The "Device Deletion" screen appears.

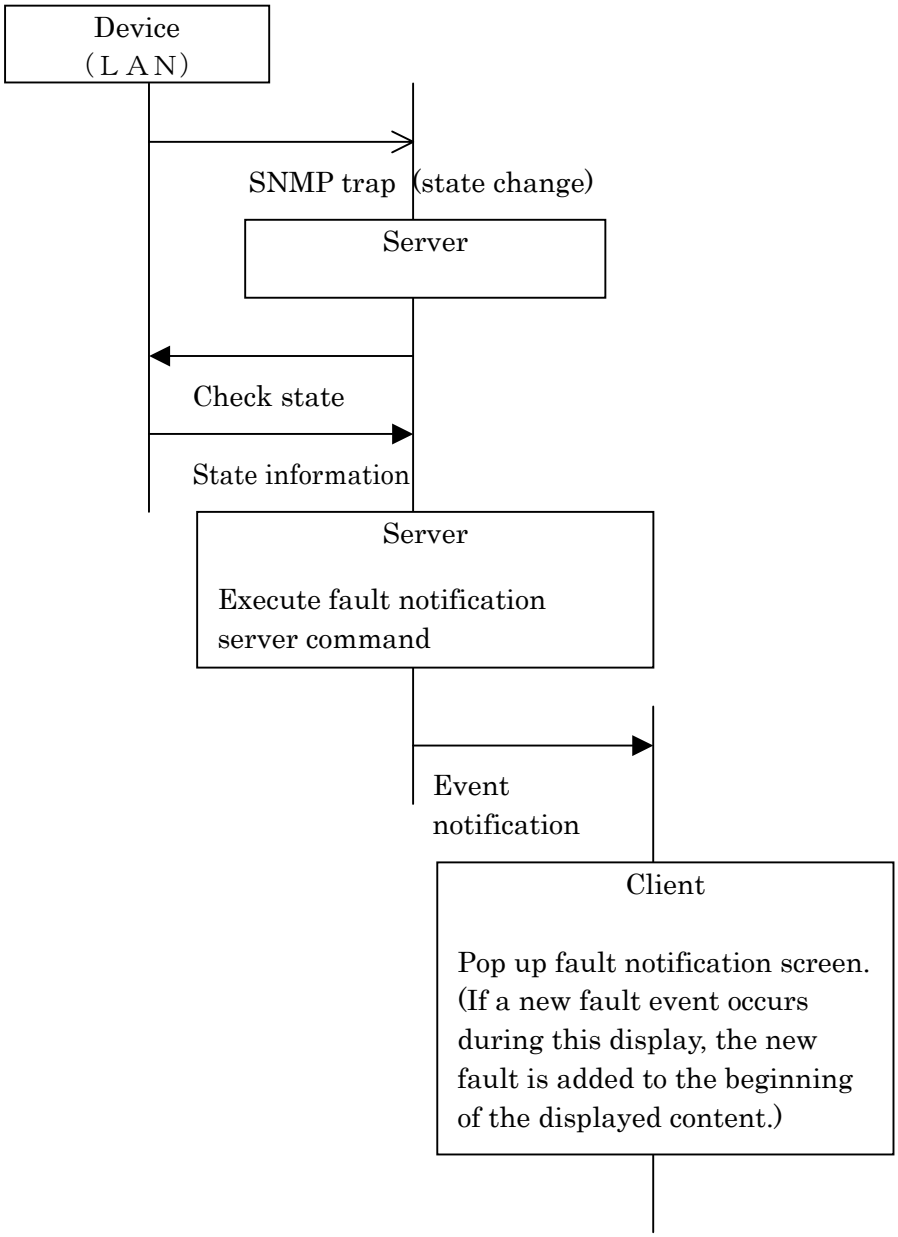


④ Clicking the "Yes" button removes the device so that it is no longer monitored by SANUPS IT Monitor Manager.

8.5 Notifying The Administrator Of A Device Fault

When a device fault occurs, the SANUPS IT Monitor Manager system can notify the administrator of the fault.
This section describes the sequence in fault notification, as well as settings required for fault notification.

8.5.1 Fault notification sequence



8.5.2 Settings required for fault notification

The following settings are required to perform fault notification:

(1) SNMP trap recipient setting
Specify the server machine as the SNMP trap recipient of the device.
   (a) For environment monitoring device
   To set up the SNMP trap recipient, you can use either of the methods described in the following sections: "Environment monitoring device's trap recipient setting procedure" on page 65 or “Starting The Web Applet Of A Device” on page 58
   (b) For UPS (LAN connection) and MT (LAN connection)
   To perform the SNMP trap recipient setting, you can use the procedure described in the "Starting The Web Applet Of A Device" section on page 58.
   (c) For SGIV Lite server
   The method to perform the SNMP trap recipient setting differs depending on the OS used by SGIV Lite. For details on this information, refer to the SGIV Lite manual.

(2) Parameter setting of device
   (a) For environment monitoring device
   For the digital input signal where fault notification is to apply, set “Send SNMP trap” and “Failure Status” and then set the signal state as warning (to decide whether to use the “ON side” or “OFF side” to indicate fault occurrence).
   For analog input signal, set up the normal range, and then set “Deviation monitoring” and “Send SNMP trap”.
   For details on the setting methods, see the "Setting The Parameter Information Of A Device (Environment Monitoring Device)" section on page 60.
   (b) For UPS
   To perform deviation monitoring of analog input value, set “Deviation monitoring” for the analog input; then set up a normal range.
   For details on the setting method, see the "Setting The Parameter Information Of A Device (Environment Monitoring Device)" section on page 60.

(3) UPS warning setting
Use the UPS warning setting to set up whether to treat a specific alarm sent from the UPS. For details on the setting method, see the "Performing Fault Notification" section on page 47.

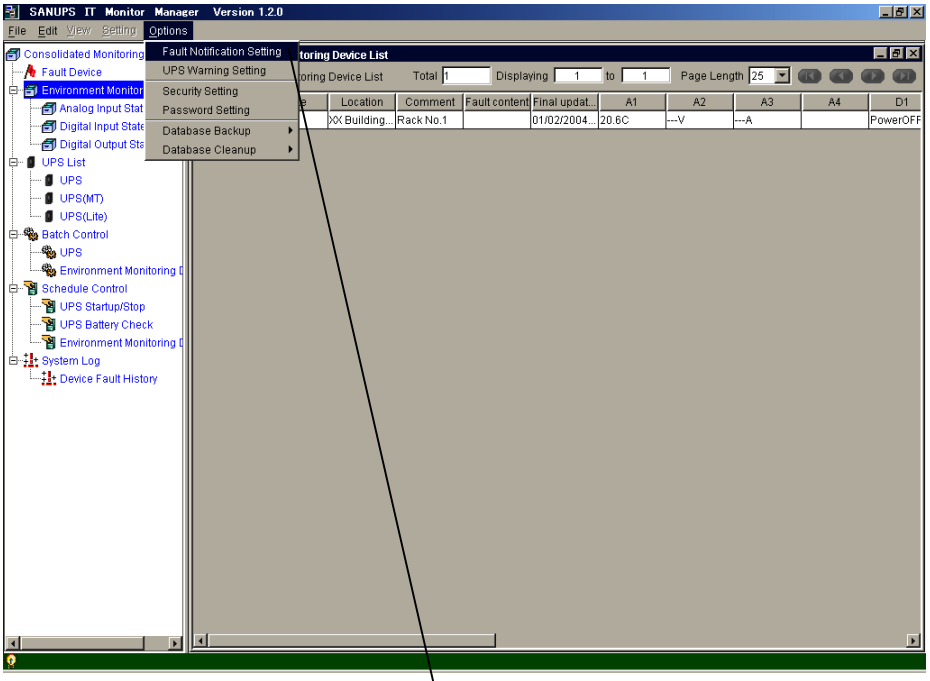
(4) Fault notification setting
Use this setting to specify a method to use to notify the administrator of a fault occurrence or recovery.
For details on the setting method, see the "Performing Fault Notification" section on page 47.

8.6 Performing Fault Notification Setting

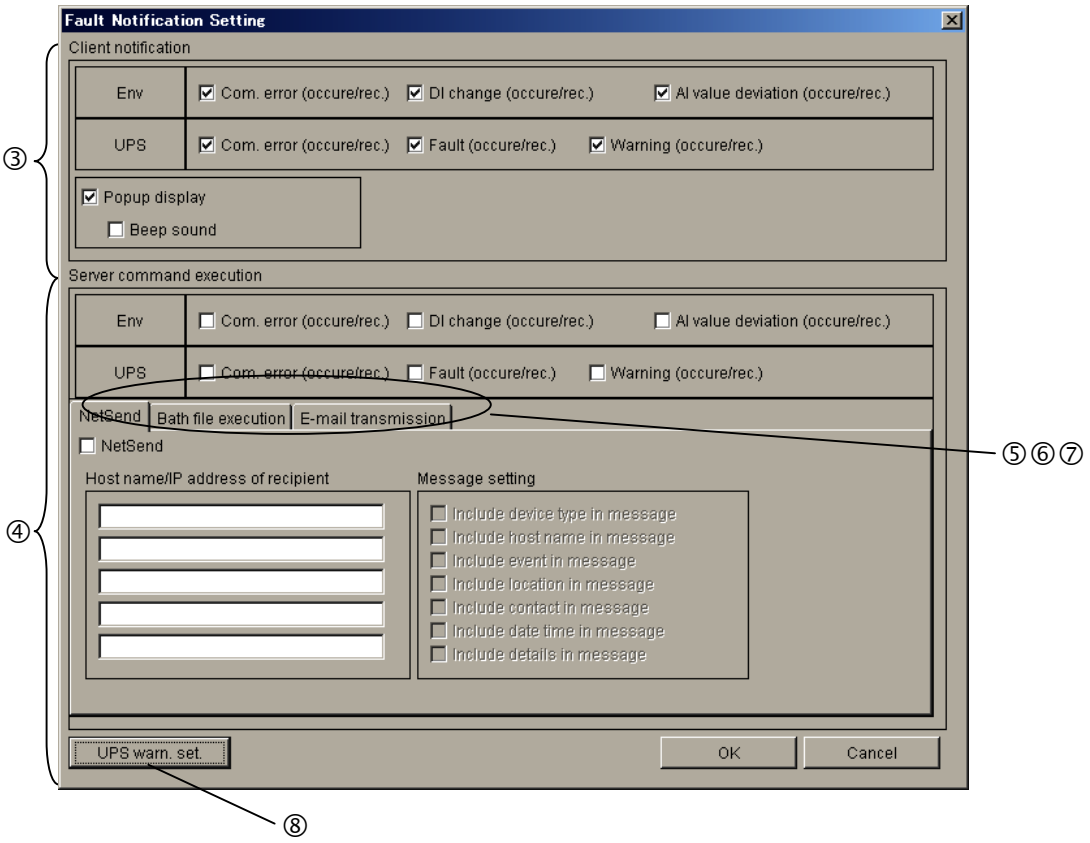
This section describes how to set up fault notification to notify the administrator when a device fault occurs.

8.6.1 Fault notification setting procedure

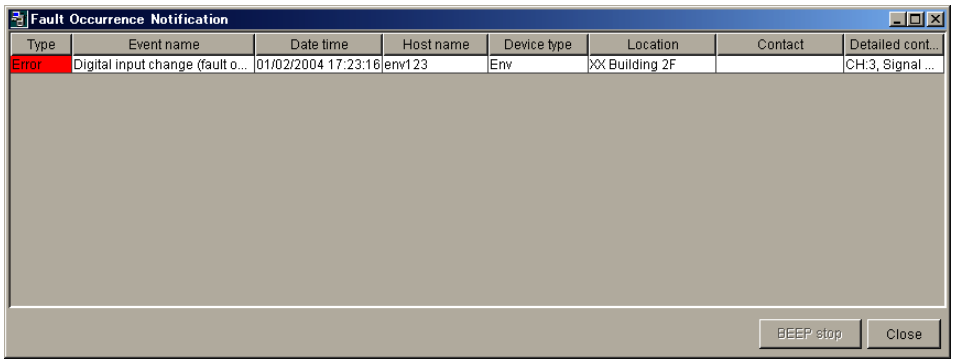
① Using the main screen, select "Fault Notification Setting" from the "Options" menu.



② The "Fault Notification Setting" screen appears.



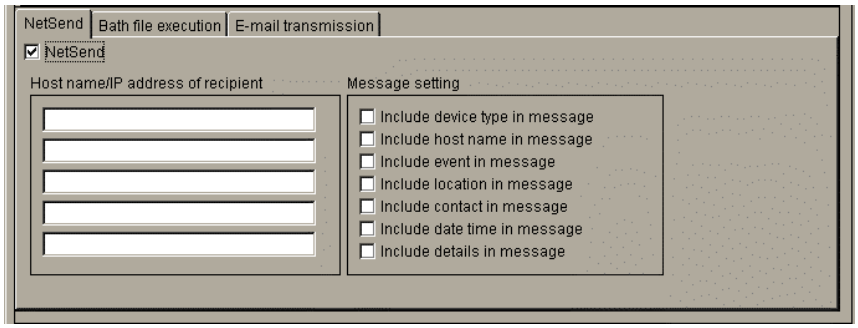
③ To display a popup on the client, select the check boxes for the events for popup; then select the "Popup display" check box. Also, if you want to have a beep sound accompany the popup, select the "Beep sound" check box.
Once the popup display is enabled, the following "Fault Occurrence Notification" screen (such as the example shown below) pops up when an event occurs. You can double-click any row on the "Fault Occurrence Notification" screen to start the real-time display.



"Fault Occurrence Notification" screen image

④ If you want the server command to execute when a fault occurrence/recovery event occurs, select the check boxes for the events, and then use the "NetSend", "Batch file execution", and "E-mail transmission" tabs to perform the detailed settings.

⑤ "NetSend" tab settings



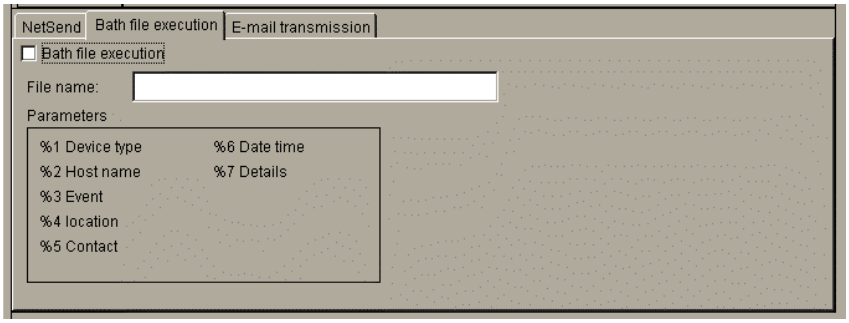
(a) "NetSend" check box
Use this check box to specify whether to send a NetSend message to a specified machine when a device fault occurs. If this check box is selected, a NetSend message is sent when a fault occurs.

(b) "Host name/IP address of recipient"
Use the text boxes to enter the host names or IP addresses of the machine to send NetSend messages to.
* If the server is Windows NT, then you must specify the host name of the recipient of NetSend messages.

(c) "Message setting"
Use the check boxes to specify what kind of information to include in the message.
Select the check box for the information you want to include in the message.

<Note>
NetSend executes the NetSend command of the OS. Depending on the environment, NetSend may not work correctly. If this is the case, issue the NetSend command from the DOS prompt, and then check that the transmission is normal.
Also, when the server stops, all NetSend commands on the queue are abandoned.
This function (NetSend) cannot be used in Windows Vista and later operating systems. This is because NetSend commands are not supported from Windows Vista and later operating systems.

⑥ "Batch file execution" tab settings

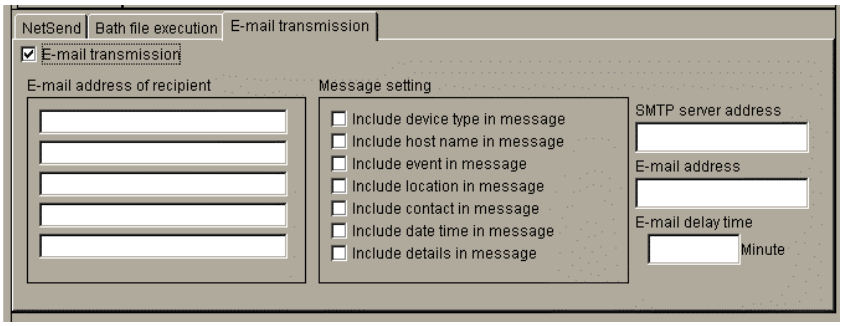


(a) "Batch file execution" check box
Use this check box to specify whether to perform batch file execution when a device fault occurs. If you select this check box, the specified batch file will be executed when a device fault occurs.

(b) "File name"
Use this text box and enter a batch file located on the server machine to execute when a device fault occurs.
The following parameters can be used with the batch file:
%1 Device type, %2 Host name, %3 Event,
%4 Location, %5 Contact , %6 Date time, %7 Details

<Note>
The batch file must be stored in the "batch" directory of the install directory on the server. **The content of the batch file must end with the "Exit" command.**
Also, be sure that the content of the batch file can be executed to finish within **60 seconds.**
The batch file execution will be forced to end if it takes more than 60 seconds.
A batch file sample (sample.bat) is installed in the "batch" directory. Use it as a reference when writing your batch file.
Also, when the server stops, all batch files on the queue are abandoned.

⑦ "E-mail transmission" tab settings



(a) "E-mail transmission" check box
Use this check box to specify whether to send an email to the specified e-mail addresses when a device fault occurs.
If the check box is selected, an email is sent to the specified e-mail addresses when a device fault occurs.

(b) "E-mail address of recipient"
Use the text boxes and enter the e-mail addresses of recipients to send the e-mail.

(c) "Message setting"
Use the check boxes to specify what kind of information to include in the message.

(d) "SMTP server address" text box
Enter the host name or IP address of the SMTP server in the text box.

(e) "E-mail address" text box
Enter the e-mail address of the sender in the text box. If a transmission error occurs at the mail server, an e-mail containing the error message will be sent to this e-mail address.

(f) "E-mail delay time" text box.
Use this text box to specify how long to wait when an event occurs, before sending an e-mail. If multiple events occur during this delay period, they are all grouped and sent in just one e-mail.
If you enter 0, the delay time will be 15 seconds.

<Note>
E-mail transmission is done using the SMTP port number fixed at 25.
Also, the character encoding of e-mail is ASCII.
Depending on the content of e-mail, gabled text may occur.
During e-mail transmission delay, if the server stops, e-mail transmission does not occur but becomes abandoned.
Also, POP before SMTP is not supported for e-mail transmission.

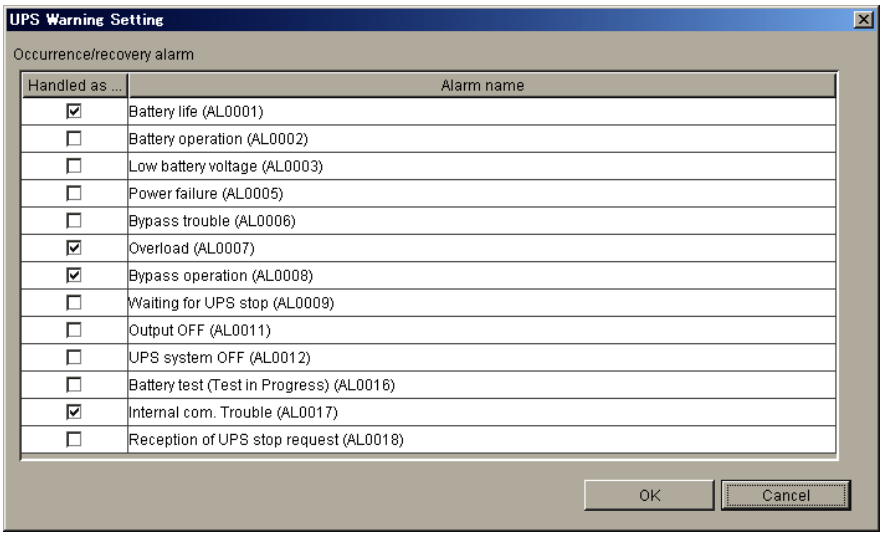
⑧ UPS Warning Setting

When you click the "UPS warn. set" button, the "UPS Warning Setting" screen appears.

You can also display this screen by using the menu. From the "Options" menu, select "UPS Warning Setting".

From this screen, you can select alarms sent from UPS that you want to use as warnings.

By default, the following four alarms are handled as warnings: "Battery life", "Bypass operation", "Overload", and "Internal com. Trouble".



8.6.2 Restrictions on fault notification

The following restrictions apply to the fault notification function:

① Depending on the operation state of other applications, the client pop up display may not work in some cases. This problem is indicated by blinking of the task bar.

② The detection of fault occurrence and recovery is performed by the device's state checking operation (polling operation).
This operation is performed in the following cases:

- Checking is performed regularly as specified by the polling interval.
- Checking is performed to the target device when the SNMP trap is received.

For this reason, detection may not be possible if the fault (communication error occurrence, UPS analog input deviation) does not come with any SNMP trap. Also, detection may not be possible if the fault occurrence and recovery happens within a short time (5 seconds), even if it comes with a SNMP trap. In the latter case, only a record of receiving the SNMP trap is stored in the system log.

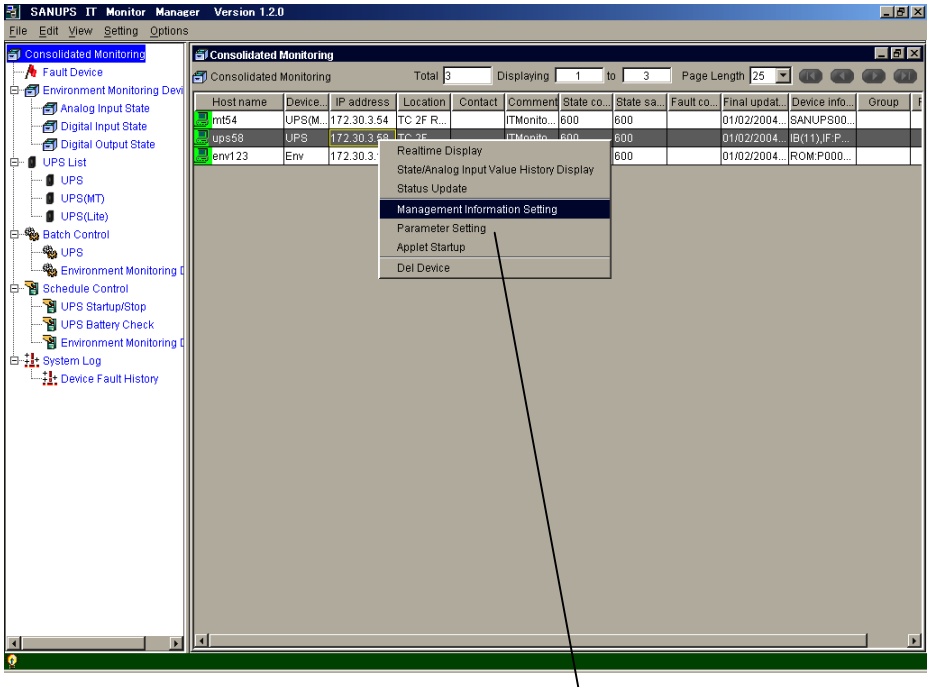
8.7 Setting Management Information (Device Management Information)

There are two types of management information: information required for accessing a device, and information required for monitoring the device.
The information required for accessing a device includes the READ community name, WRITE community name, etc. of the device.
The information required for monitoring a device includes the polling interval used to check the device's state, and state/analog input value history save interval.
You can use the "Management Information Setting" menu command to change the management information set up when a device was added.
You can change the information for a single device, or you can change the information for multiple devices at the same time.

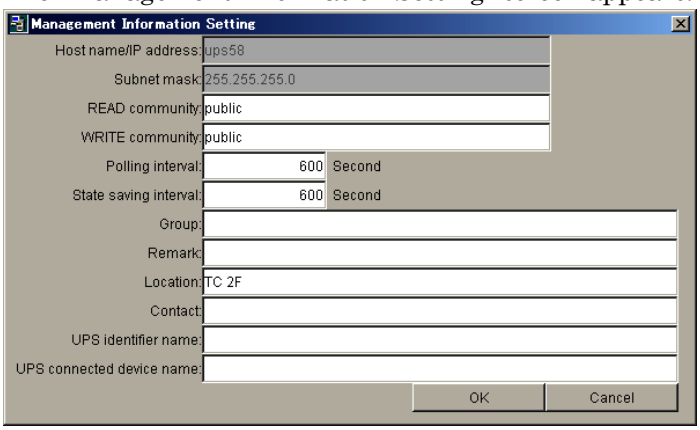
8.7.1 Changing the management information of a single device

Use the following procedure to change the management information of a single device:

① Using the main screen, select a desired device from the device operation status list.
② From the "Setting" menu or the short-cut menu, select "Management Information Setting".



③ The "Management Information Setting" screen appears.



The example here indicates that a UPS device has been selected. For an environment monitoring device, the UPS identifier name and UPS connected device name do not appear.

(a) If "READ community" and "WRITE community" have been changed, you need to change the device so that it has the same community names.

(b) In the "Polling interval" text box, specify an interval to use to check the state of the device.
If the interval you set here is too short, when more and more devices are added, this will increase the load on the network as well as the server machine, causing problems in the monitoring operation.
If a device fault happens or the state is changed, the SNMP trap is received and the state is obtained automatically. Therefore, the polling interval does not need to be that short. By default, the polling interval is set to 600 seconds (10 minutes).
As a general rule, if the number of devices is 200 or more, set the polling interval to 1200 seconds. If the number of devices is 400 or more, set the interval to 1800 seconds.

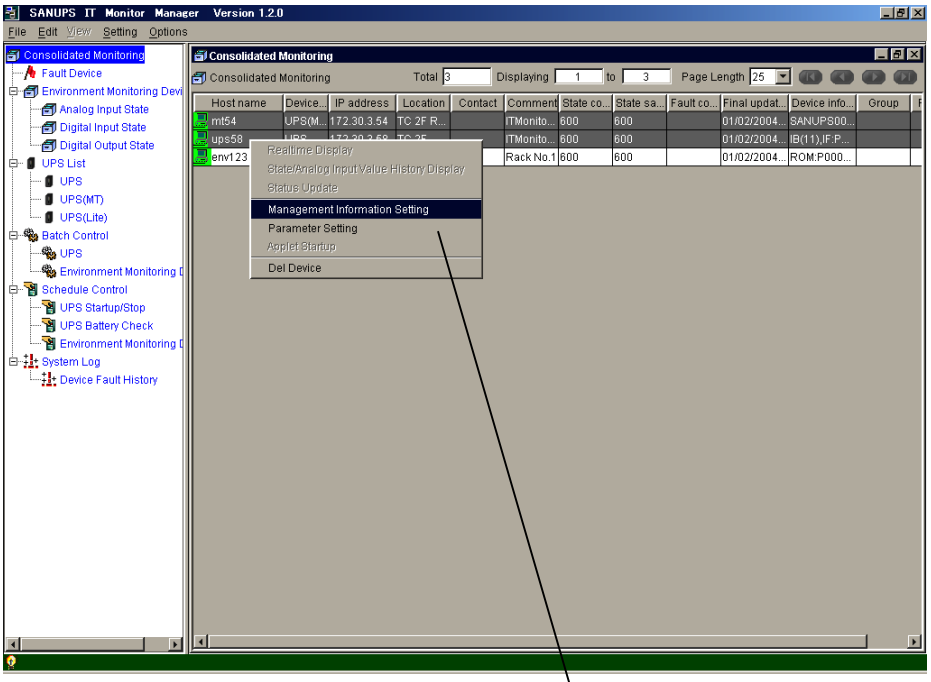
(c) In the "State saving interval" text box, enter the interval to use to save the state/analog input value history of the device.
If you set the interval to 0, the information is saved only when the state of the device changes. For an environment monitoring device, the information is saved only when a change in the state of the digital input or in the state of the analog input value deviation is detected. For a UPS device, the information is saved only when a change in the state of the SNMP alarm or in the state of the analog input value deviation is detected. Furthermore, data saving is performed during the polling interval; when the device state is checked, the data obtained is saved. For this reason, when setting this value, use a multiple of the value set for polling interval.

<Note>
The polling and saving operations are not performed at exactly the intervals specified in "Polling interval" and "State saving interval." Depending on the network state and server load, the operations may be delayed.
Also, if a communication error occurs, the state and analog input value cannot be obtained and therefore cannot be saved.

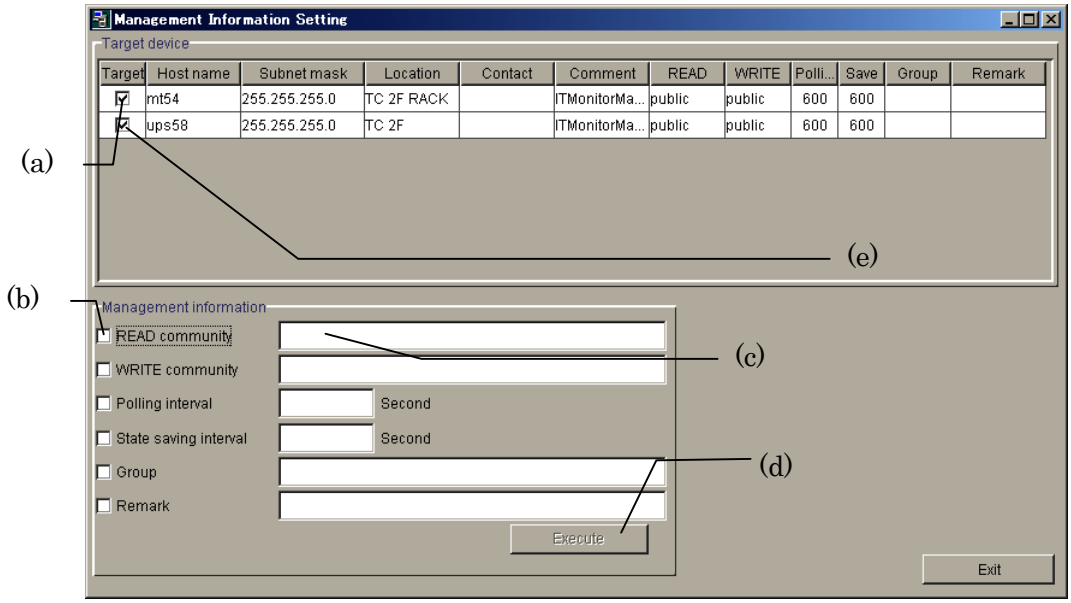
8.7.2 Changing the management information of multiple devices at the same time

Use the following procedure to change the management information of multiple devices at the same time:

① Using the main screen, select multiple devices from the device operation status list.
② From the "Setting" menu or the short-cut menu, select "Management Information Setting".



③ The "Management Information Setting" screen appears.



(a) If there are devices in the target device list that you do not want to apply the settings to, clear their "Target" check boxes.

(b) Select the check box of settings you want to apply to all selected devices.

(c) Enter details of each setting you want to apply to all selected devices.

(d) Click the "Execute" button.

(e) The "Management Information Setting" screen is updated with the results. In addition, the check boxes of devices with their settings changed successfully are cleared.

8.7.3 Notes on the management information settings

(1) Among the management information settings, "Location", "Contact", "UPS identifier name", and "UPS connected device name" are kept by the devices themselves. Therefore, they are applied to the devices. The other settings are saved on the server, and are used by SANUPS IT Monitor Manager to monitor and manage the devices.
If you use the management information settings to change the READ community name or WRITE community name, their settings on the devices are not changed.
Furthermore, if you want to change settings on the devices, use "Applet Startup" from the "Setting" menu.

(2) For environment monitoring devices and UPS devices (other than SGIV Lite), the READ community name and the WRITE community name are identical.
When performing the management information settings for environment monitoring devices and UPS devices (other than SGIV Lite), always make sure the READ community name and the WRITE community name are identical.

8.8 Starting The Web Applet Of A Device

8.8.1 What is applet startup?

This is a function that you can use to start from a client the Web applet (Web administrative tool) of a device.

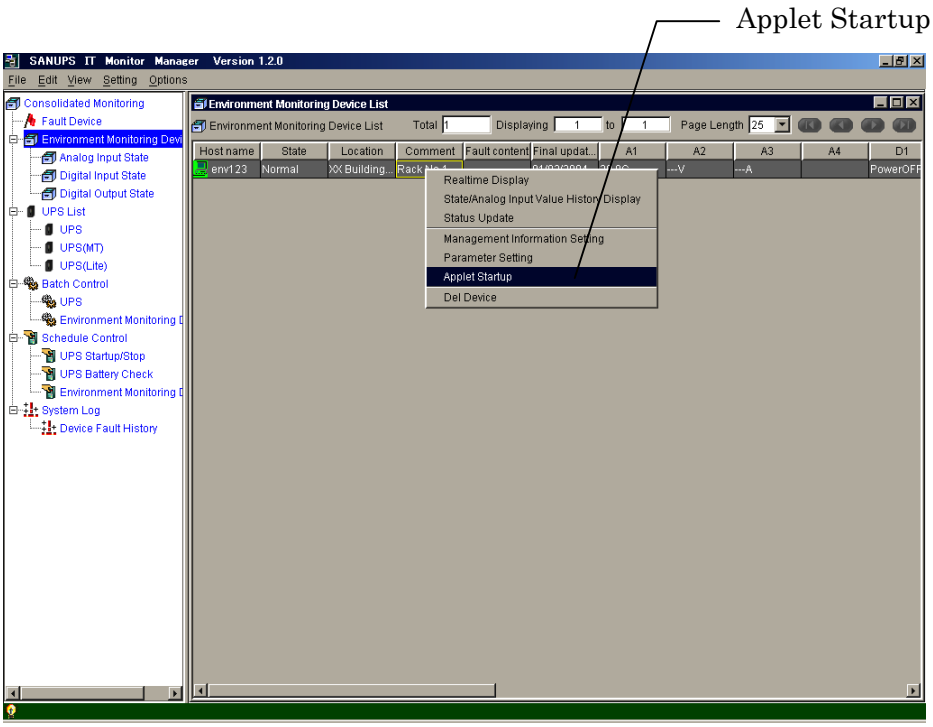
By using the Web applet, you can perform detailed settings of the device. However, since SGIV Lite does not support Web applet, you cannot start the applet from SGIV Lite.

8.8.2 Applet Startup procedure

Use the following procedure to start the applet:

① From the main screen, display the device operation status list.

② Select a desired device from the device operation status list. From the "Setting" menu or the short-cut menu, select "Applet Startup".



③ A Web browser starts and displays the Web applet of the device.

④ For details on how to use the Web applet, refer to the user guide that comes with each device.

8.8.3 Functions that can only be performed from the Web applet (environment monitoring device)

The following functions cannot be performed unless the Web applet is running:

(1) Basic settings of a device
The basic settings include: network environment such as IP address, SNMP operating environment (however, trap recipient can be set from the "Parameter Setting" screen), as well as the saving interval of the state/analog input value history kept by the device.

(2) Clock setting of a device
The clock setting must be performed from the Web applet. Furthermore, when SANUPS IT Monitor Manager adds a device as a target for monitoring or every 24 hours after the server starts, it automatically adjusts the time of the device to match the system time of the server.

(3) Display of event log of a device
This is a function to display the event log kept by the device, which is different from the system log kept by the server.

(4) Display of the state/analog input value history of a device
This is a function to display the state/analog input value history kept by a device, which is different from the state/analog input value history kept by the SANUPS IT Monitor Manager server machine.

8.8.4 Functions that can only be performed from the Web applet (UPS)

On a LAN interface card and MT, network environment such as IP address, SNMP operating environment, and other information settings cannot be performed unless the Web applet is running.
Note: SG IV Lite does not have any Web applet function. For information on how to start an SNMP agent and perform settings, refer to the SG IV Lite manual.

8.8.5 Notes on changing the host name/IP address, and community names

When the host name, IP address, and community names of a device are modified, the changes are not reflected automatically in the management information of SANUPS IT Monitor Manager.
Therefore, when the host name is changed or its IP address is changed, be sure to delete the device, and then add it back again.
An exception applies if the IP address of an added device is changed when the host name has its name already resolved (in other words, the host name of device in the operation status state list is not displayed in the IP address format). In this case, the IP address is updated when the state of the device is checked.
If settings kept by the device are different from the management information, a communication error exists between the device and

SANUPS IT Monitor Manager. In this case, because SANUPS IT Monitor Manager can no longer manage and monitor the device, you need to adjust it to the settings kept by the device.

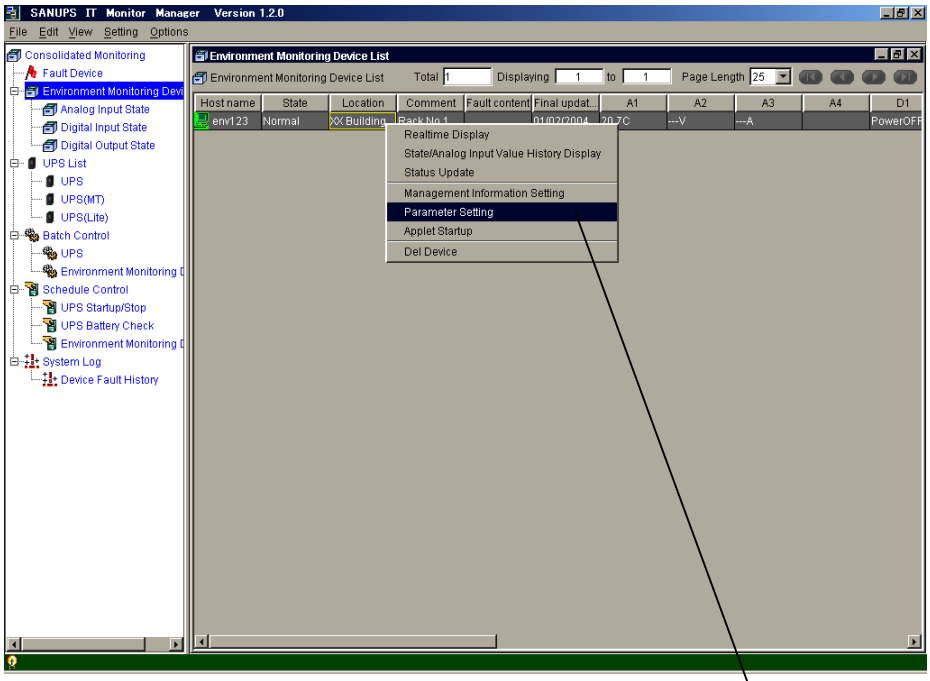
8.9 Setting The Parameter Information Of A Device (Environment Monitoring Device)

8.9.1 What is the parameter information of environment monitoring device?

The parameter information includes definitions of the analog input, digital input, digital output, SNMP trap recipient, and e-mail recipient kept by a device itself. To set up this information, you can start the Web applet of the device, or select "Parameter Setting" from the "Setting" menu.

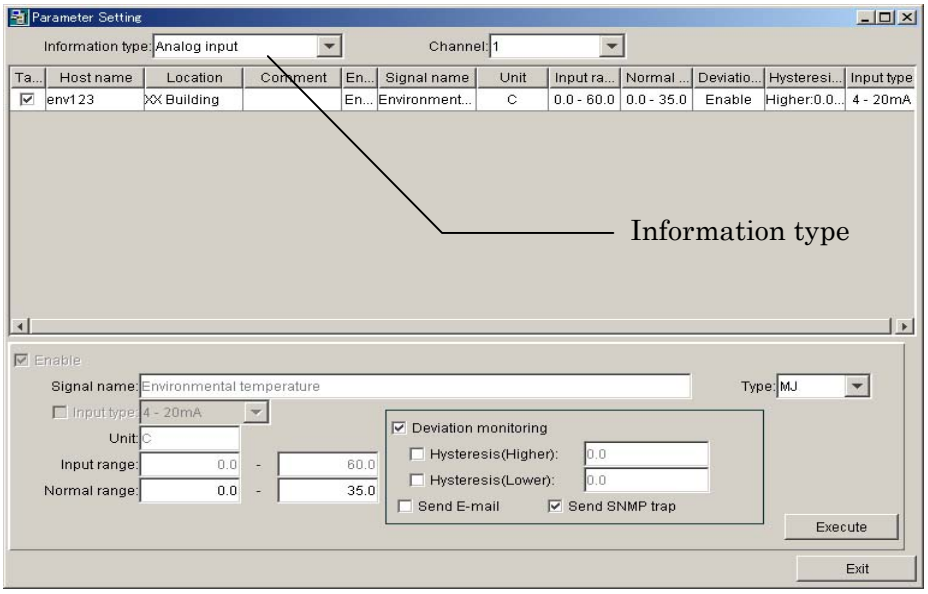
8.9.2 Parameter information setting procedure (common part)

① Using the main screen, select a device from the device operation status list that you want to set the parameter information. (You can select multiple devices). From the "Setting" menu or the short-cut menu, select "Parameter Setting".

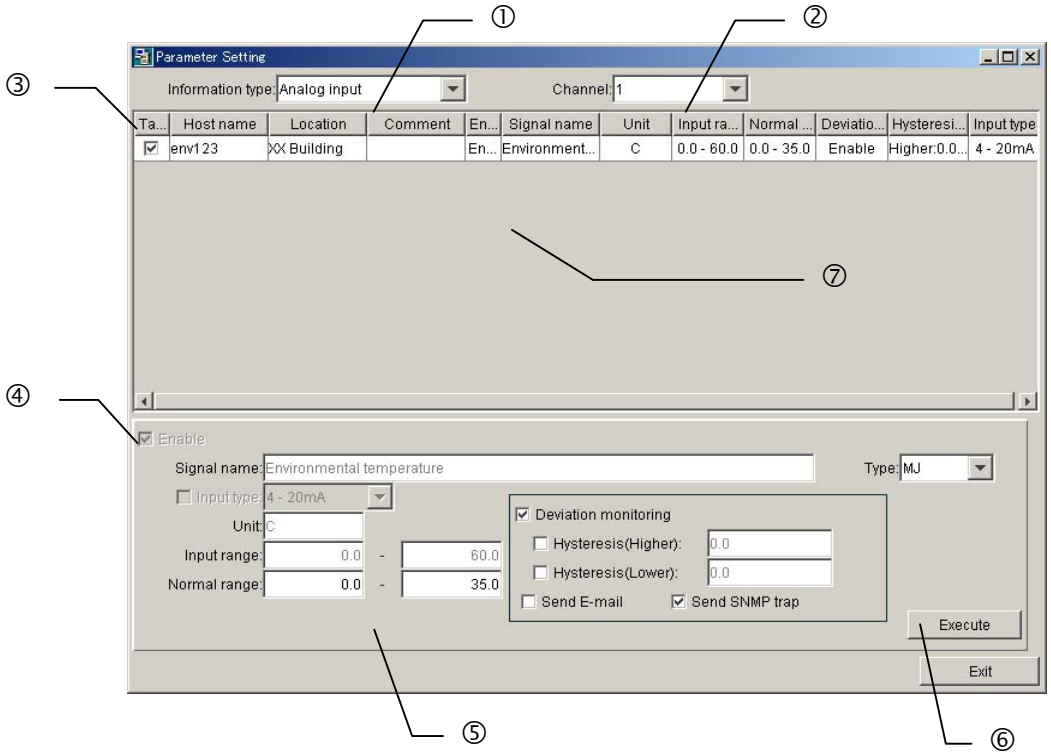


② The "Parameter Setting" screen appears.

③ From the "Information type" drop-down list, select one of the following items to set: "Analog input", "Digital input", "Digital output", "Trap recipient", and "E-mail recipient".



8.9.3 Analog input parameter setting procedure



① Using the "Parameter Setting" screen, select "Analog input" from the "Information type" drop-down list.

② From the "Channel" drop-down list, select a channel to change.

③ If there are devices in the target device list that you do not want to apply the settings to, clear their "Target" check boxes.

④ Select the "Enable" check box.

⑤ Specify the signal name, unit, analog input range, normal range, type, whether deviation monitoring is used, whether to send an e-mail when deviation occurs, and whether to send the SNMP trap when deviation occurs. For detailed information on how to set each of these items, refer to the environment monitoring device's user guide.

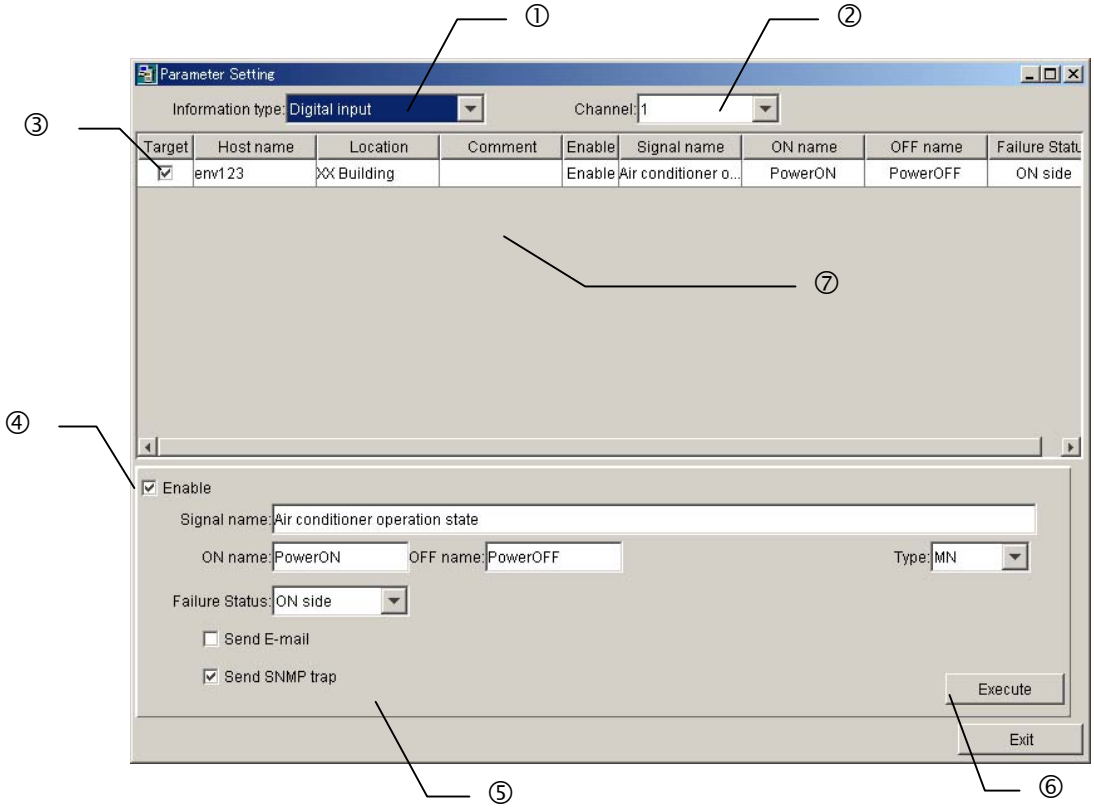
⑥ Make sure that you have entered the information correctly and the target devices are correct; then click the "Execute" button.

⑦ The target devices are updated with the changes.

<Note>

The types (MJ, MN, and ST) are used for function expansion in the future. It has no meaning in the current version in particular.

8.9.4 Digital input parameter setting procedure



① Using the "Parameter Setting" screen, select "Digital input" from the "Information type" drop-down list.

② From the "Channel" drop-down list, select a channel to change.

③ If there are devices in the target device list that you do not want to apply the settings to, clear their "Target" check boxes.

④ Select the "Enable" check box.

⑤ Specify the signal name, ON name, OFF name, type, whether to send an e-mail, whether to send the SNMP trap, whether to treat an alarm as a warning, and whether to use the “ON side” or “OFF side” or ”None” signal as an indication of a warning. For detailed information on how to set each of these items, refer to the environment monitoring device's user guide.

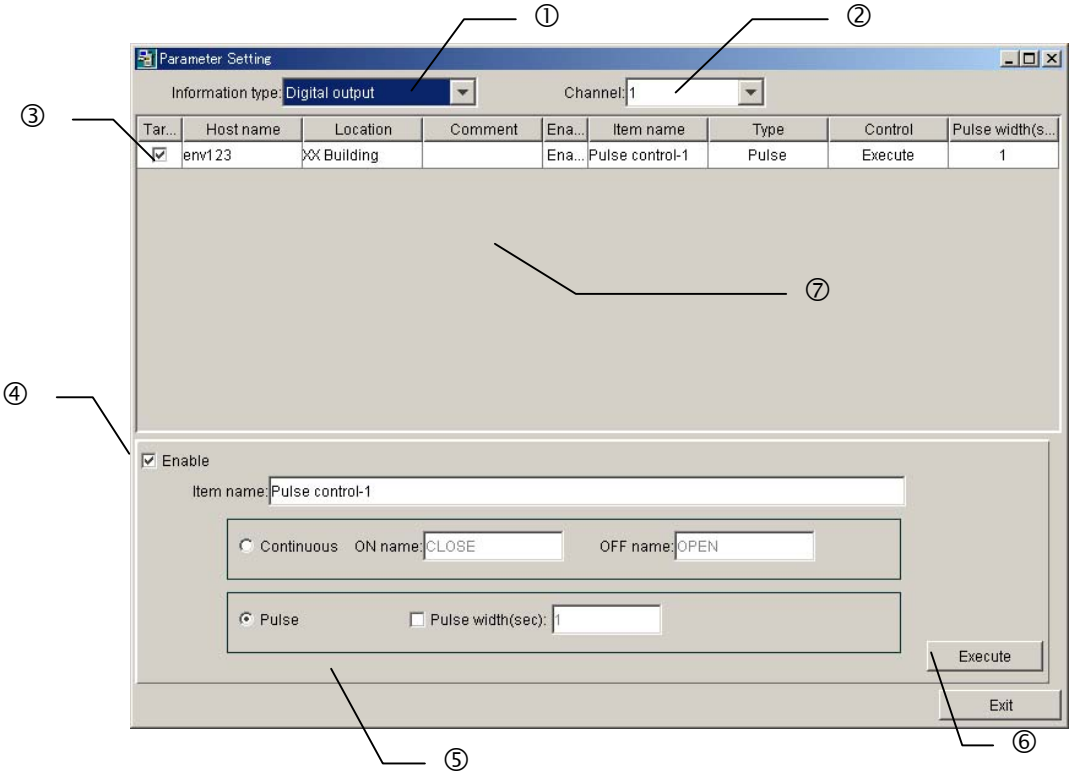
⑥ Make sure that you have entered the information correctly and the target devices are correct; then click the "Execute" button.

⑦ The target devices are updated with the changes.

<Note>

The types (MJ, MN, and ST) are used for function expansion in the future. It has no meaning in the current version in particular.

8.9.5 Digital output parameter setting procedure



① Using the "Parameter Setting" screen, select "Digital output" from the "Information type" drop-down list.

② From the "Channel" drop-down list, select a channel to change.

③ If there are devices in the target device list that you do not want to apply the settings to, clear their "Target" check boxes.

④ Select the "Enable" check box.

⑤ Specify the item name, pulse or continuous (for continuous signal, enter the ON name and OFF name for the signal). For detailed information on how to set each of these items, refer to the environment monitoring device's user guide.

⑥ Make sure that you have entered the information correctly and the target devices are correct; then click the "Execute" button.

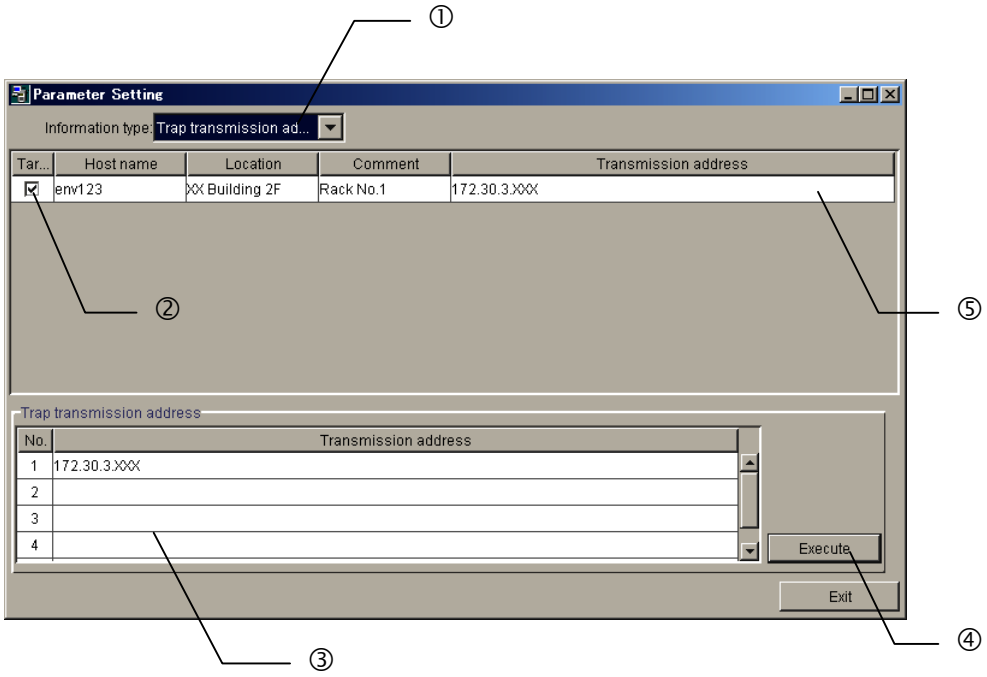
⑦ The target devices are updated with the changes.

8.9.6 Environment monitoring device's trap recipient setting procedure

When the analog input value deviates from the specified normal range and when the digital input signal changes, if you want the SNMP trap to be sent to a specific machine, you need to pre-set the IP address of the machine as the trap recipient.

Furthermore, to perform fault notification of the SANUPS IT Monitor Manager system, you also need to pre-set the IP address of the SANUPS IT Monitor Manager server machine as the trap recipient.

Use the following procedure to set the trap recipient:



① Using the "Parameter Setting" screen, select "Trap transmission address" from the "Information type" drop-down list.

② If there are devices in the target device list that you do not want to apply the settings to, clear their "Target" check boxes.

③ Enter the IP addresses of the trap recipients. You can register up to five trap recipients.

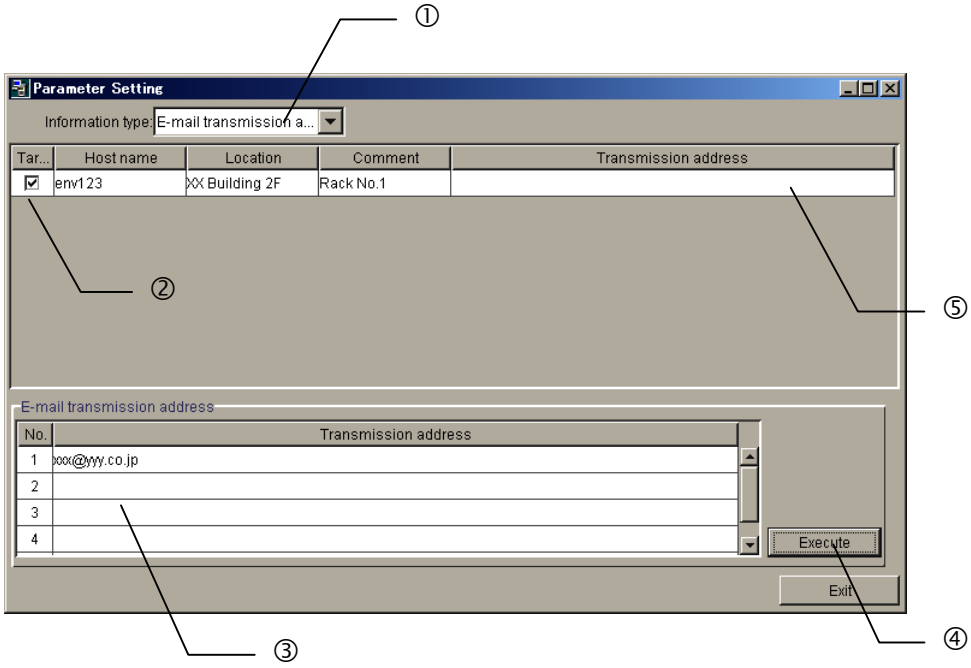
④ Make sure that you have entered the information correctly and the target devices are correct; then click the "Execute" button.

⑤ The target devices are updated with the changes.

8.9.7 E-mail transmission address setting procedure

When the analog input value deviates from the specified normal range and when the digital input signal changes to the state defined as fault handling, if you want to have an e-mail sent to specific addresses, you need to pre-set the e-mail addresses.

Use the following procedure to set the e-mail addresses:



① Using the "Parameter Setting" screen, select "E-mail transmission address" from the "Information type" drop-down list.

② If there are devices in the target device list that you do not want to apply the settings to, clear their "Target" check boxes.

③ In the "Transmission address" text boxes, enter the e-mail addresses of the machines for sending an e-mail when a device fault occurs. You can register up to five e-mail addresses.

④ Make sure that you have entered the information correctly and the target devices are correct; then click the "Execute" button.

⑤ The target devices are updated with the changes.

<Note>

To enable e-mail transmission, the e-mail address of the device itself must also be set. For information on how to set the e-mail address of a device, see the "Starting The Web Applet Of A Device" section on page 58.

8.10 Setting The Parameter Information Of A Device (UPS)

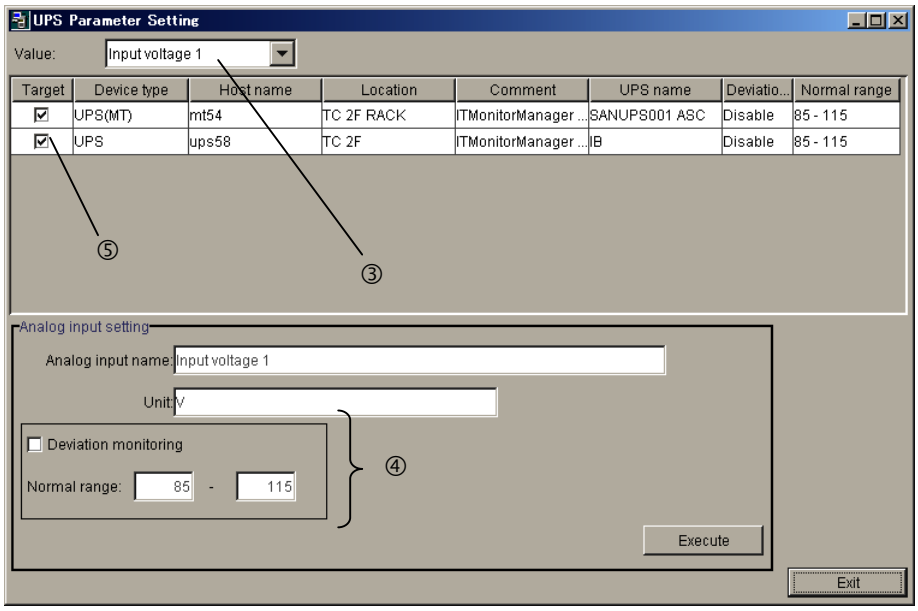
8.10.1 What is the UPS parameter information?

The UPS parameter information refers to the definition required to perform UPS analog input value deviation monitoring. This information is stored on the server.

8.10.2 Parameter information setting procedure

① Using the main screen, select a device from the device operation status list that you want to set the parameter information for. (You can select multiple devices). From the "Setting" menu or the short-cut menu, select "Parameter Setting".

② The "UPS Parameter Setting" screen appears.



③ Select a value for deviation monitoring.

④ Select the "Deviation monitoring" check box; then enter the normal range.

⑤ If there are devices in the target device list you do not want to apply the settings to, clear their "Target" check boxes.

⑥ Make sure that you have entered the information correctly and the target devices are correct; then click the "Execute" button.

<Note>

The normal range of analog input value specified here is reflected in the normal range of real-time display.

Even if the analog input value returns from the deviation state to the normal range, this is not determined to be a recovery immediately, but as a hysteresis with 10% of the normal range.

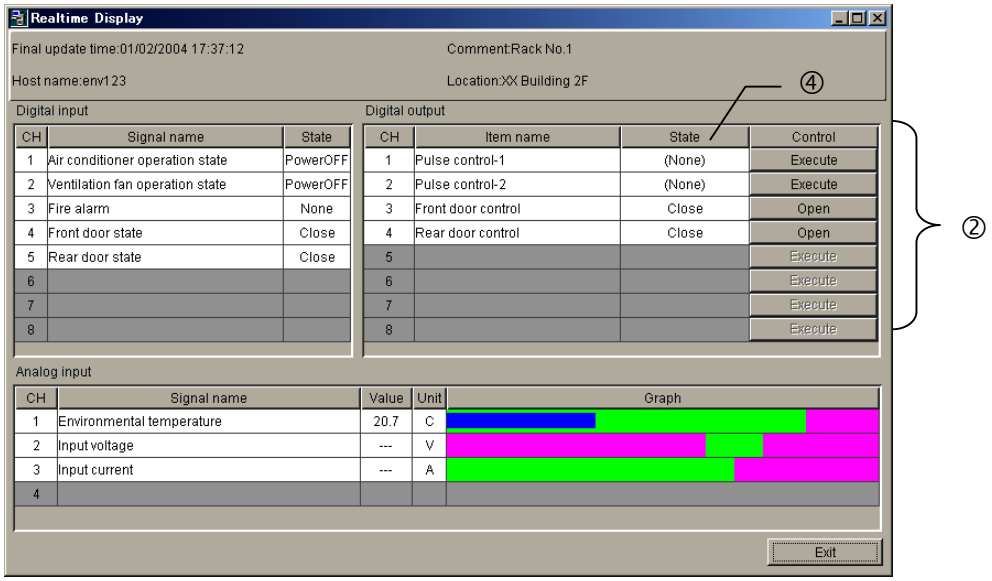
8.11 Performing Remote Control Of A Device (Environment Monitoring Device)

8.11.1 About remote control

Three methods are available for remote control: using the real-time display screen to control the output of a single device, using batch control to control the output of multiple devices, or using a schedule to control the output of multiple devices.

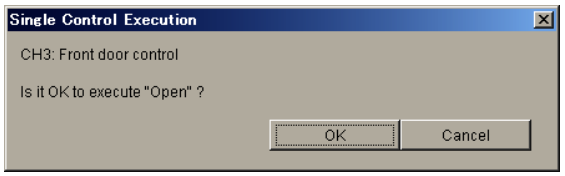
8.11.2 Using the procedure to control the output of a single device

① Using the main screen, double-click on a desired device from the device operation status list. Or, you can select "Realtime Display" from the "View" menu or the short-cut menu to display the "Realtime Display" screen.



② Click the control button of the channel that you want to control.

③ When the "Single Control Execution" screen appears, click the "OK" button to execute the control.

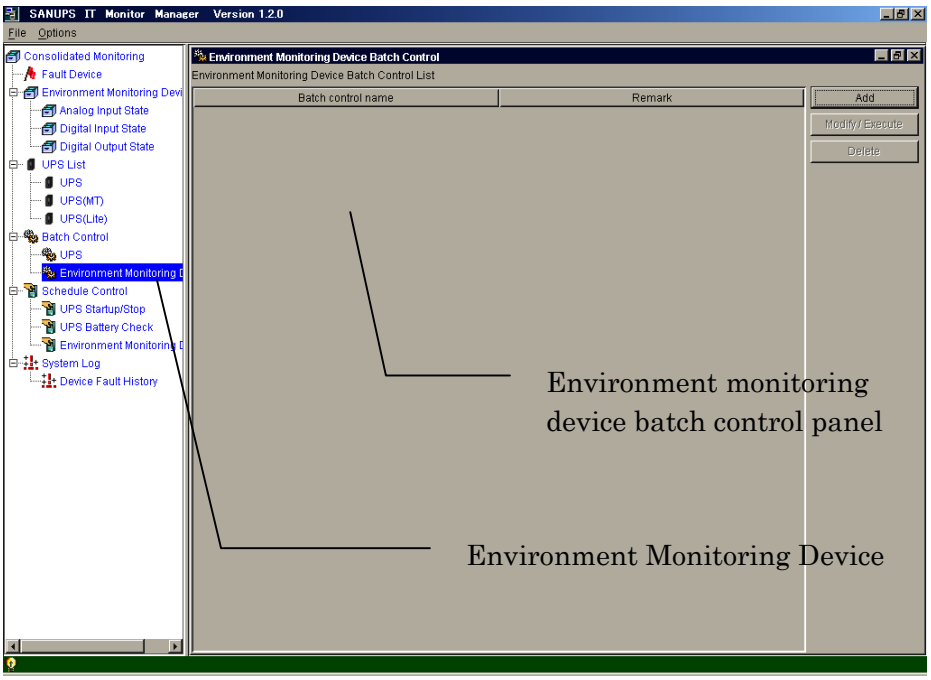


Example: The "Open" button of CH3 of the "Realtime Display" screen was clicked.

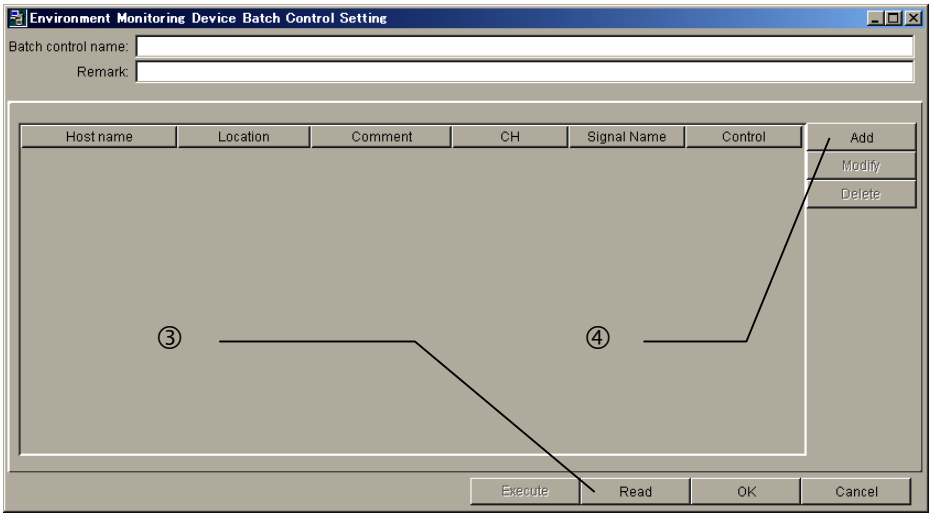
④ The result of the control execution is updated in the "State" column of the "Realtime Display" screen.

8.11.3 Batch control procedure

① Using the main screen, select "Environment Monitoring Device" below "Batch Control" on the "Consolidated Monitoring" tree.

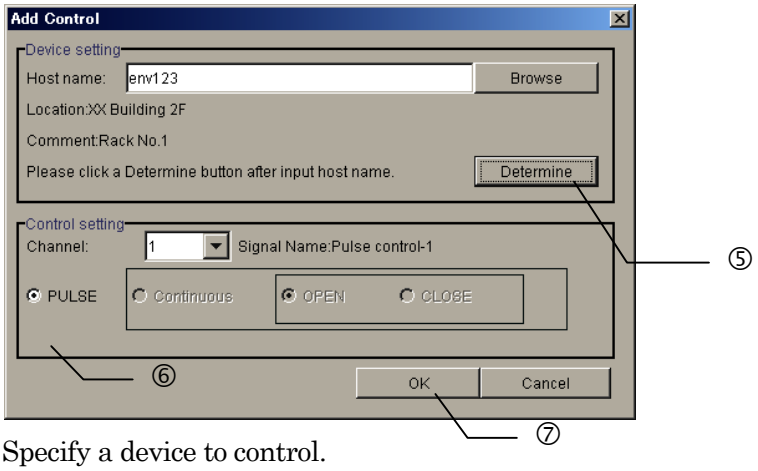


② From the environment monitoring device batch control panel, click the "Add" button. The "Environment Monitoring Device Batch Control Setting" screen appears.



③ If there is already batch control information saved on the server, click the "Read" button and select a batch control name; then read the contents of the selected control.

④ To perform a new control, click the "Add" button to display the "Add Control" screen.



⑤ Specify a device to control.

(a) In the "Host name" text box, enter the host name of the device. Or, click the "Browse" button and then select a device from the list of devices.
Furthermore, you can enter the IP address of the device instead of the host name.

(b) Click the "Determine" button. (If you have entered the IP address instead of the host name of a device, the IP address is converted to the registered host name of the device when you click the "Determine" button).

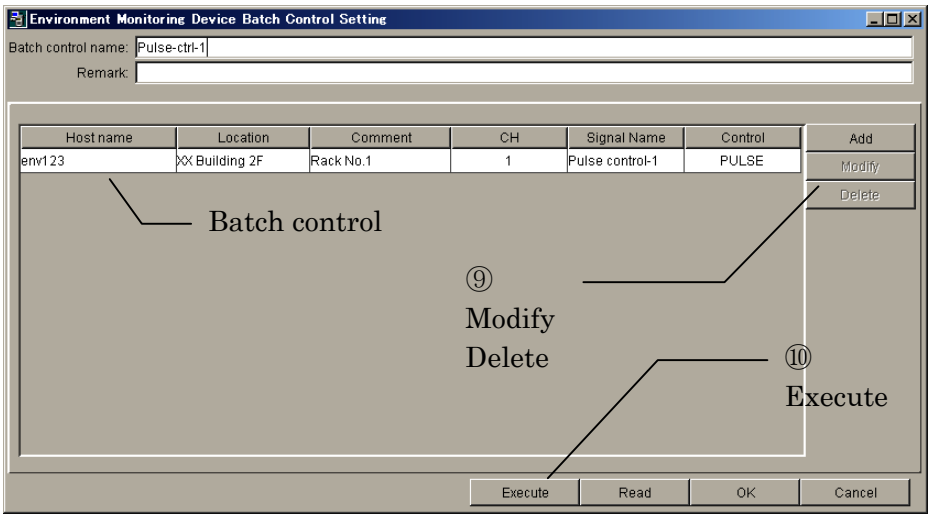
⑥ Specify the control content.

(a) Select a channel.

(b) If the signal of the selected channel is "Continuous", select the control content.

⑦ Click the "OK" button. The control content is added to the "Environment Monitoring Device Batch Control Setting" screen.

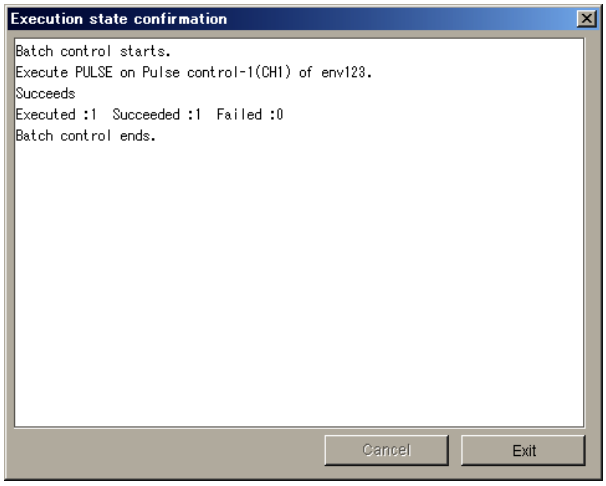
⑧ If there are other controls that you want to perform, repeat steps ⑤ to ⑧ to add the controls.



⑨ If there is a control in the list that is not needed, use the "Delete" button to delete it. If there is a control with incorrect control content, use the "Modify" button to modify the control content.

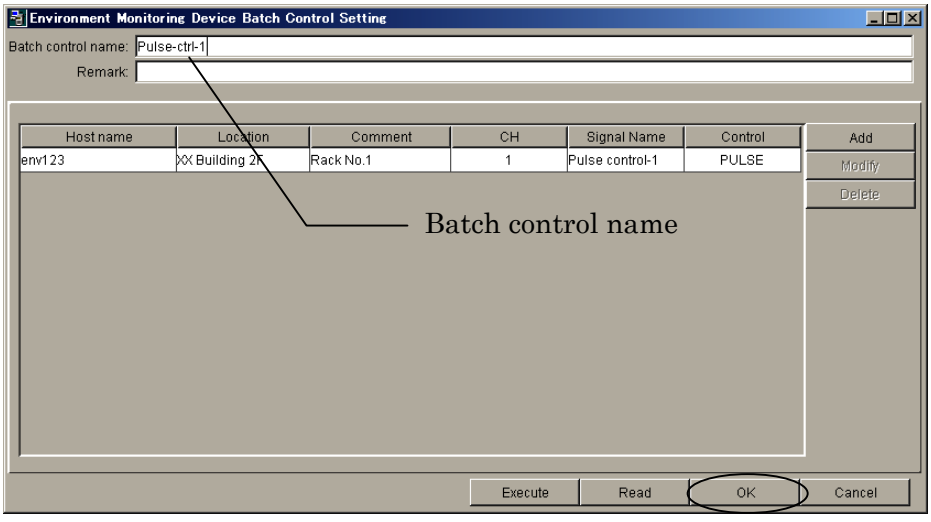
⑩ When everything you want to set in batch control is ready, click the "Execute" button.

⑪ The "Execution state confirmation" screen appears and displays the control execution progress.



⑫ After the control execution is finished, the following information appears: the number of executed devices, number of succeeded devices, and number of failed devices.
If there are devices that failed in the control, check the control content and try the control execution again.

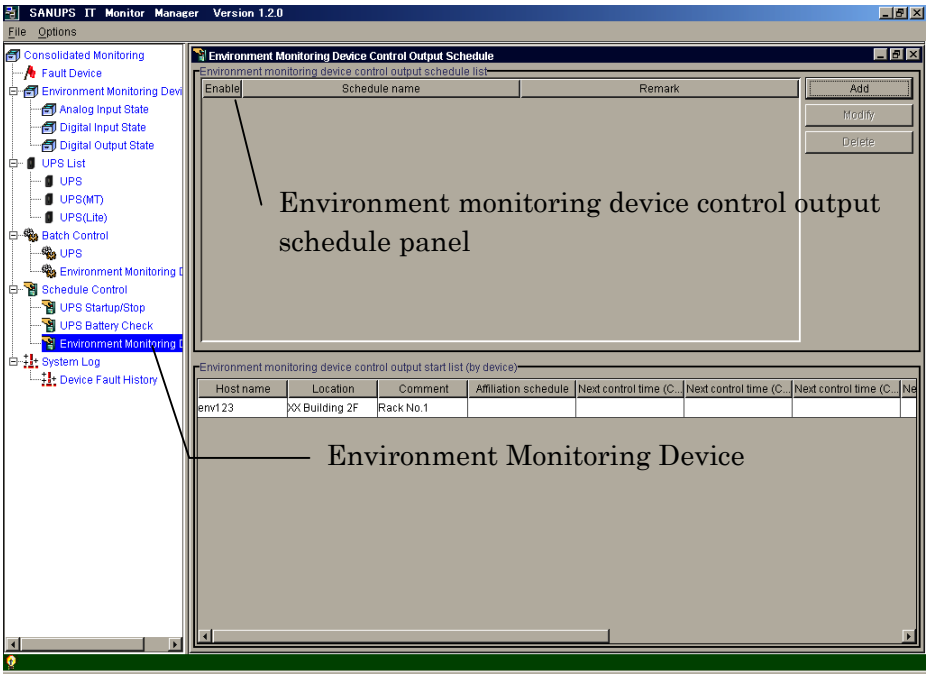
⑬ If you want to save the content of the batch control, enter a name in the "Batch control name" text box; then click the "OK" button.



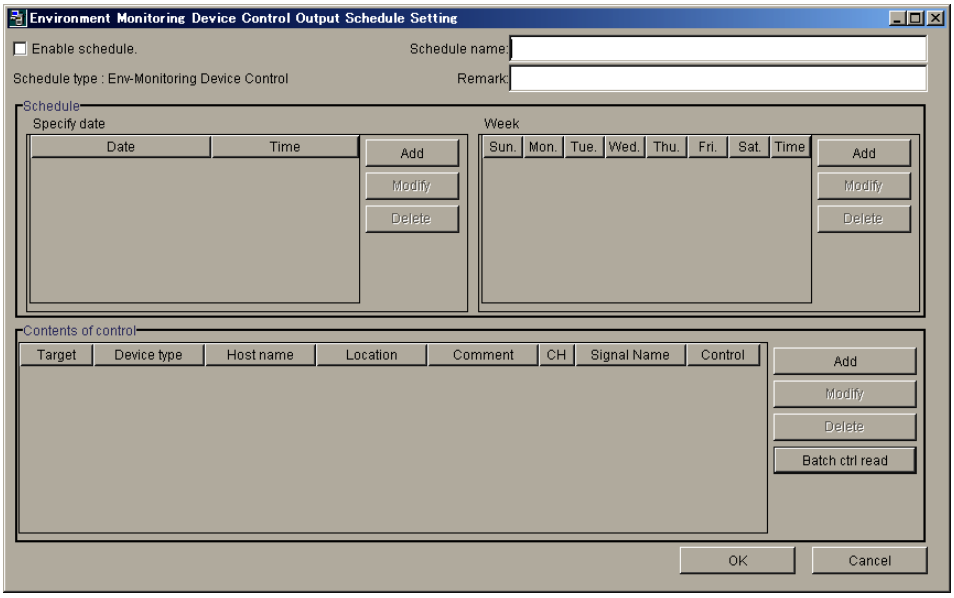
The batch control content is saved on the server.

8.11.4 Schedule control setting procedure

① Using the main screen, select "Environment Monitoring Device" from the "Consolidated Monitoring" tree.

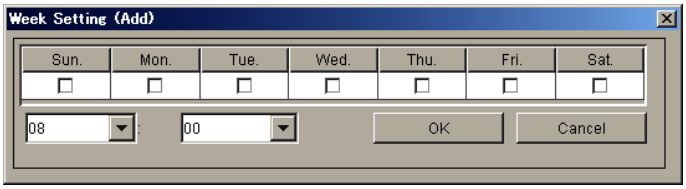


② From the "Environment Monitoring Device Control Output Schedule" panel, click the "Add" button. The "Environment Monitoring Device Control Output Schedule Setting" screen appears.

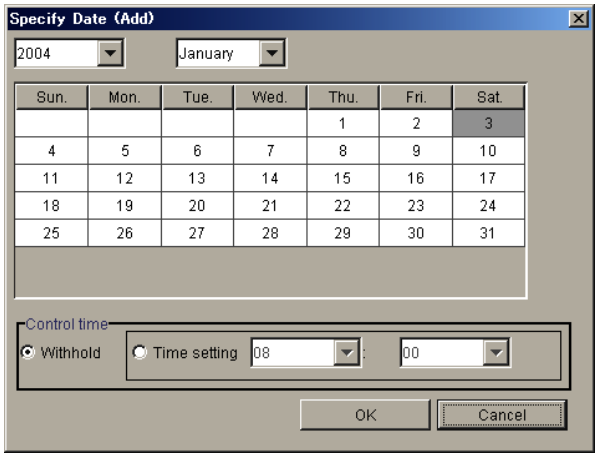


③ Set specific date schedules and weekly schedules.

(a) To specify a weekly schedule, click the "Add" button of the "Week" group.
When the following screen appears, specify what day of the week as well as what time of the day to run the schedule.



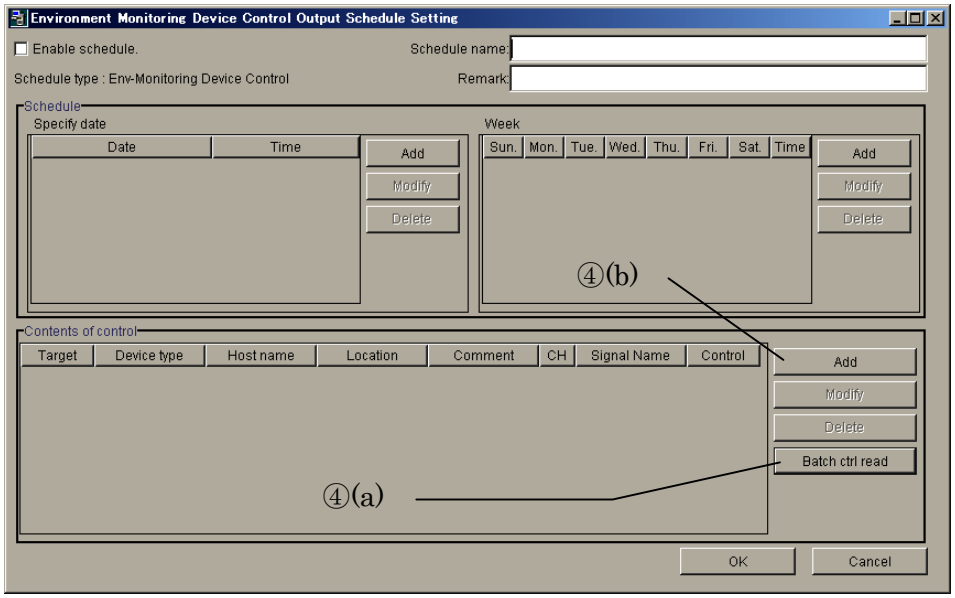
(b) To specify a specific date to run a schedule, click the "Add" button of the "Specify date" group.
When the following screen appears, specify a date to set up a schedule. Within the same schedule control, a specific date schedule takes priority over a weekly schedule.
Within a weekly schedule that you have set up, if there is a specific date that you want to exclude from the schedule, you can select the "Withhold" radio button.



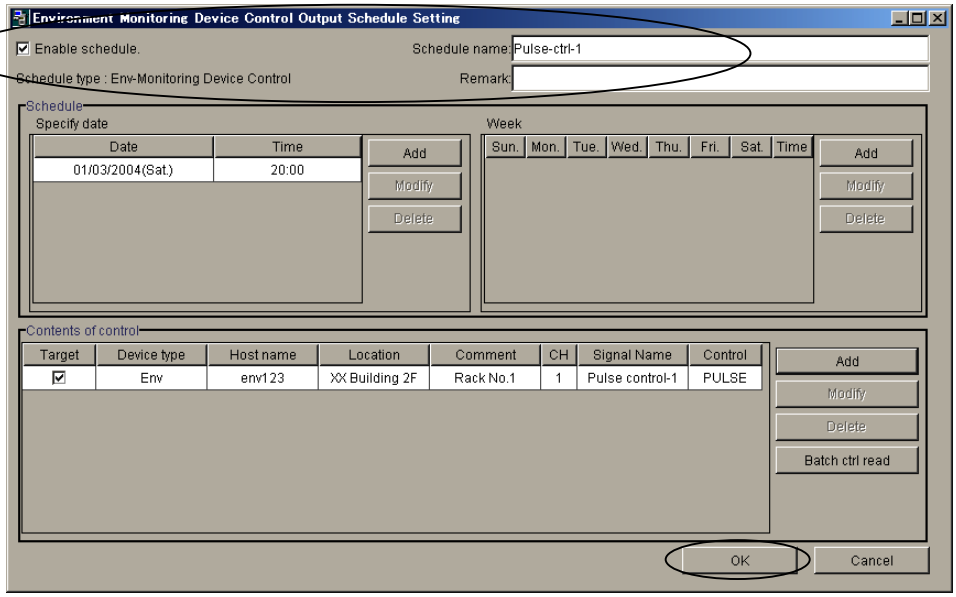
④ Specify contents of control.

(a) If there is already batch control information saved on the server, click the "Batch ctrl read" button, select a batch control name, and then read the contents of the selected control.

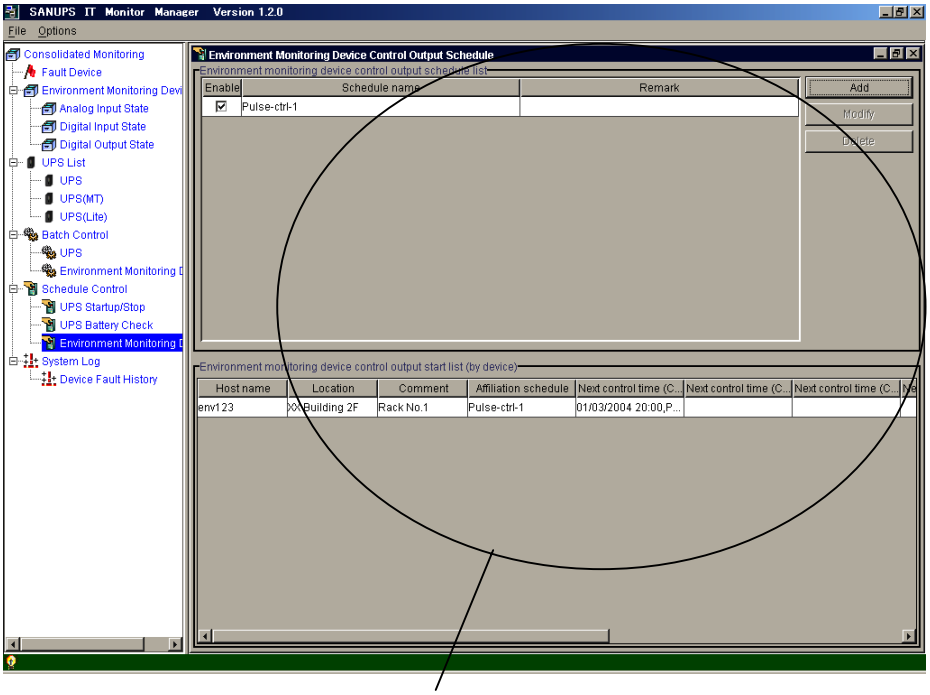
(b) To perform a new control, click the "Add" button to display the "Add Control" screen. (The operation on the "Add Control" screen is the same as that for batch control).



⑤ After setting up schedules and control contents, enter a schedule name and decide whether to enable this schedule. Finally, click the "OK" button.



⑥ After you click the "OK" button, the "Environment Monitoring Device Control Output Schedule" panel is updated with the contents of the added schedule. Furthermore, the schedule information is saved on the server.



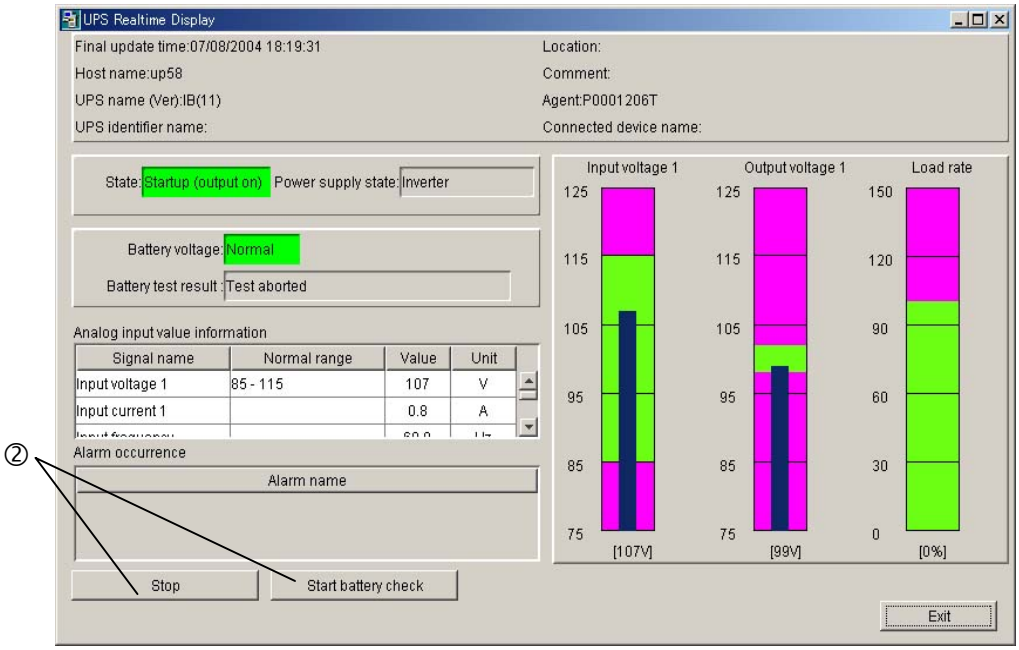
8.12 Performing Remote Control Of A Device (UPS)

8.12.1 About remote control

Three methods are available for remote control: using the real-time display screen to control the output of a single device, using batch control to control the output of multiple devices, or using a schedule to control the output of multiple devices.

8.12.2 Using the procedure to control the output of a single device

① Using the main screen, double-click on a desired device from the device operation status list. Or, you can select "Realtime Display" from the "View" menu or the short-cut menu to display the "Realtime Display" screen.

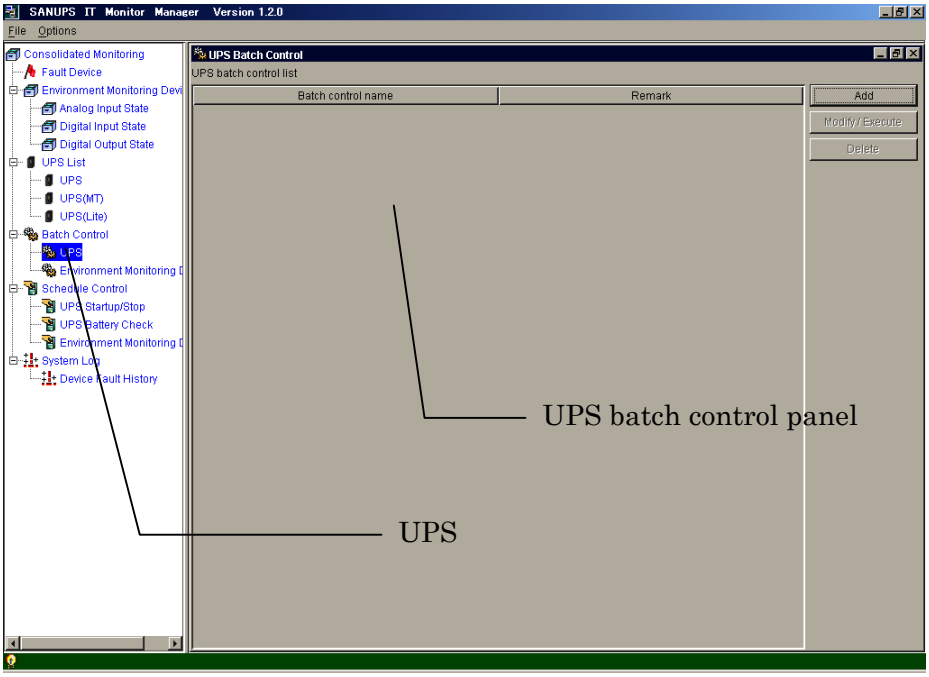


② Use the "Stop" and "Start battery check" buttons to perform the control.

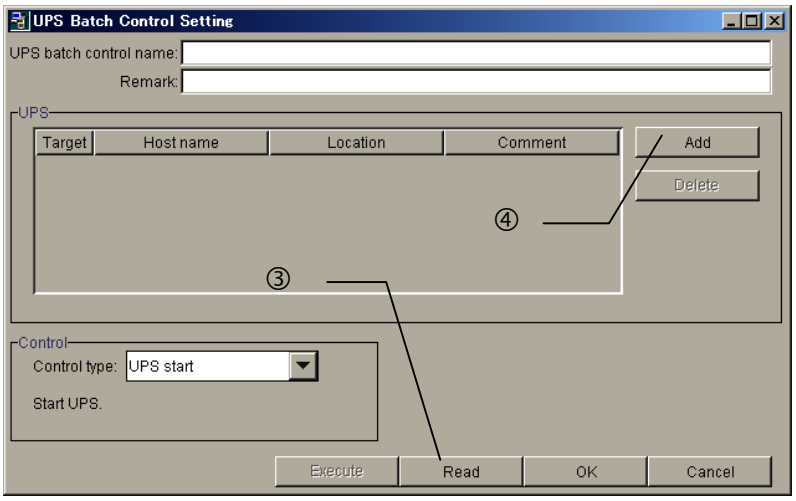
③ The result of the control execution is updated in the "Realtime Display" screen.

8.12.3 Batch control procedure

① Using the main screen, select "UPS" below "Batch Control" on the "Consolidated Monitoring" tree.

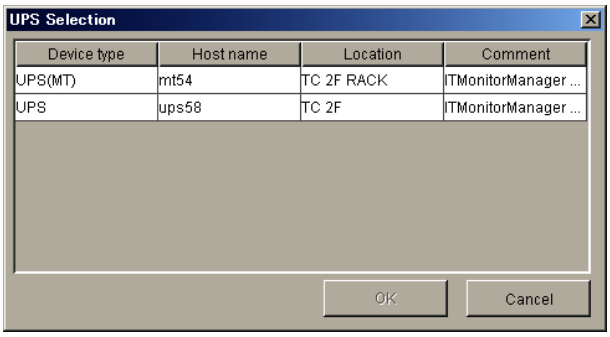


② From the UPS batch control panel, click the "Add" button. The "UPS Batch Control Setting" screen appears.

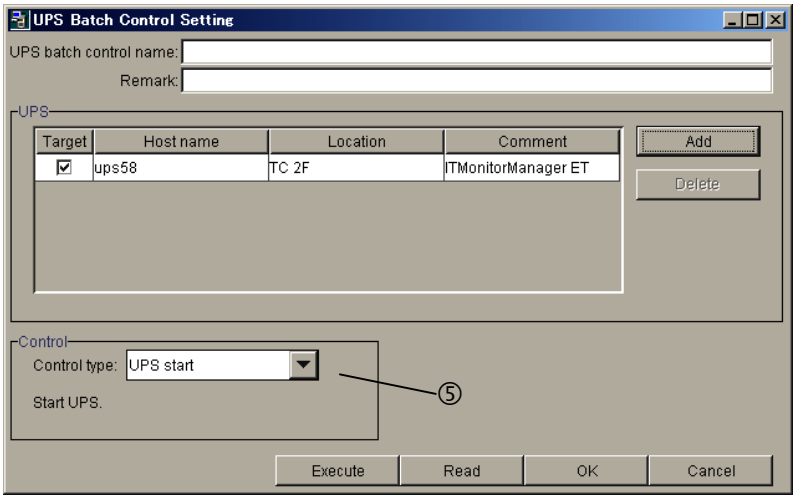


③ If there is already batch control information saved on the server, click the "Read" button, select a batch control name, and then read the contents of the selected UPS control.

④ To perform a new UPS control, click the "Add" button; then select a UPS control.

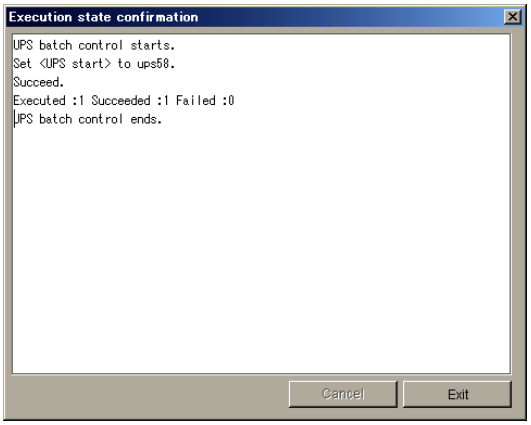


⑤ After specifying the targeted UPS control, select a control type from the "Control type" drop-down list.
The "Control type" drop-down list contains four control types: start UPS, stop UPS, start battery check, and stop battery check.



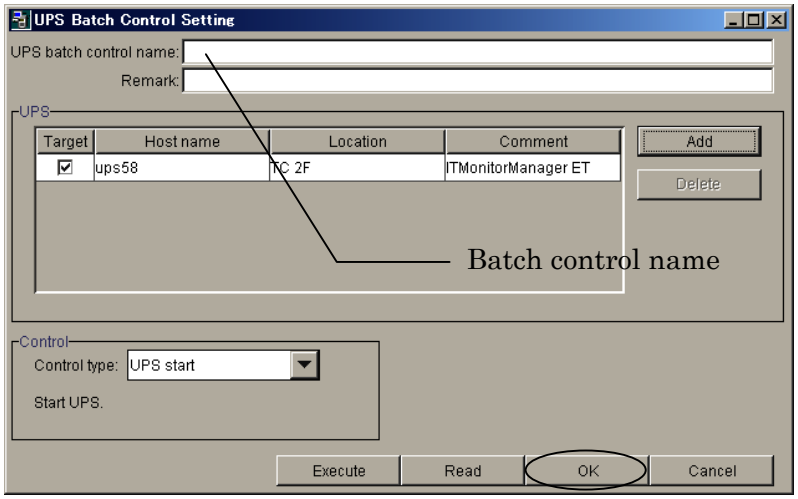
⑥ When everything that you want to set in batch control is ready, click the "Execute" button.

⑦ The "Execution state confirmation" screen appears and displays the control execution progress.



⑧ After the control execution is finished, the following information appears: the number of executed devices, number of succeeded devices, and number of failed devices.
If there are devices that failed in the control, check the control content and try the control execution again.

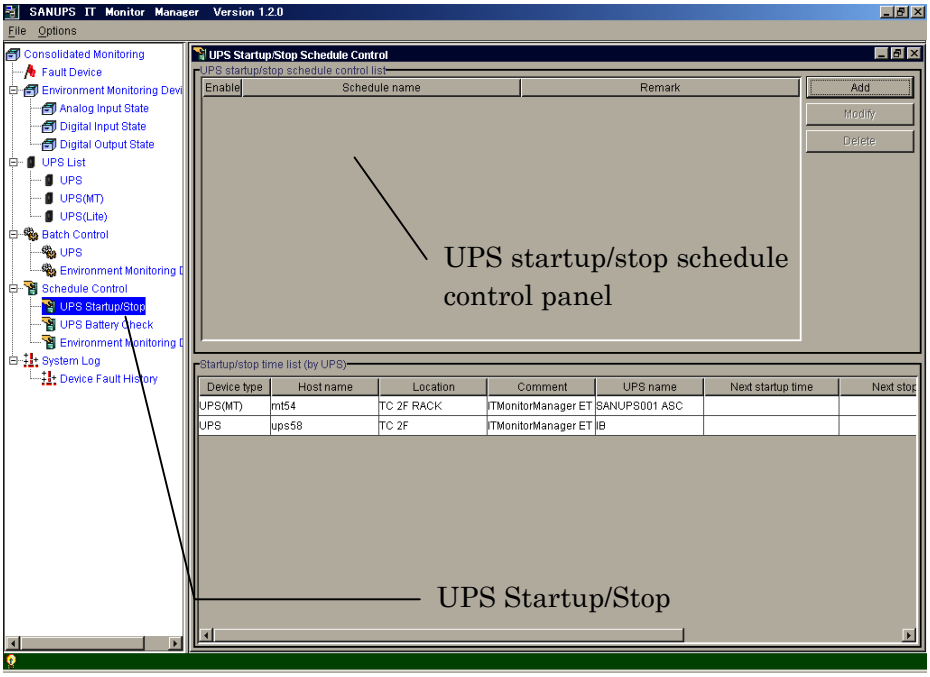
⑨ If you want to save the content of the batch control, enter a name in the "UPS batch control name" text box; then click the "OK" button.



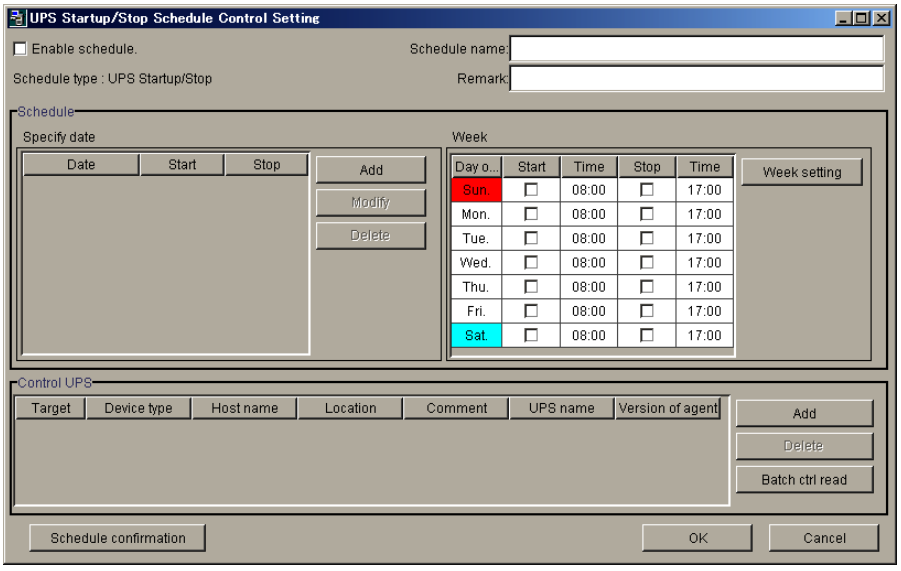
The batch control content is saved on the server.

8.12.4 Schedule control setting procedure

① Using the main screen, select "UPS Startup/Stop" or "UPS Battery Check" located below "Schedule Control" on the "Consolidated Monitoring" tree. "UPS Startup/Stop" is used as an example in the explanation here.



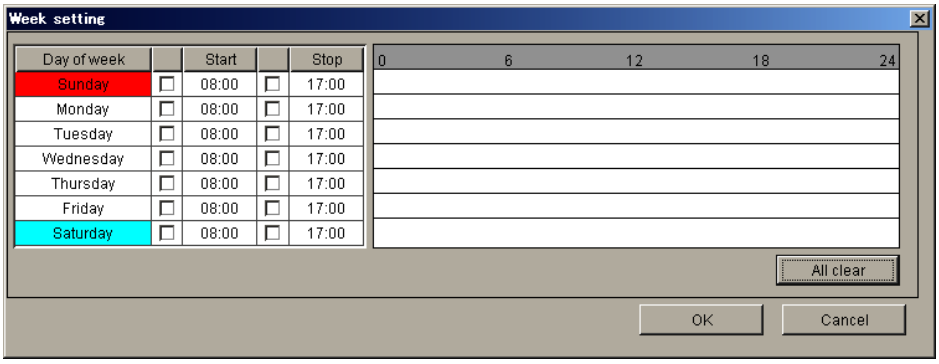
② When you click "Add" on the UPS startup/stop schedule control panel, the "UPS Startup/Stop Schedule Control Setting" screen appears.



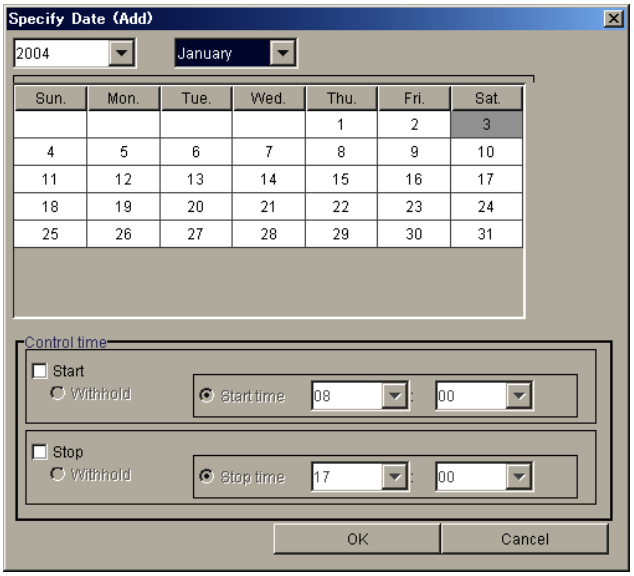
③ Set specific date schedules and weekly schedules.

(a) To specify a weekly schedule, click the "Week setting" button. Here, specify the UPS start and stop times for a day of the week.

Select the "Start" and "Stop" check boxes for a desired day of the week.
To change a start (or stop) time, select the "Start" (or "Stop") check box. The time is ready for editing.

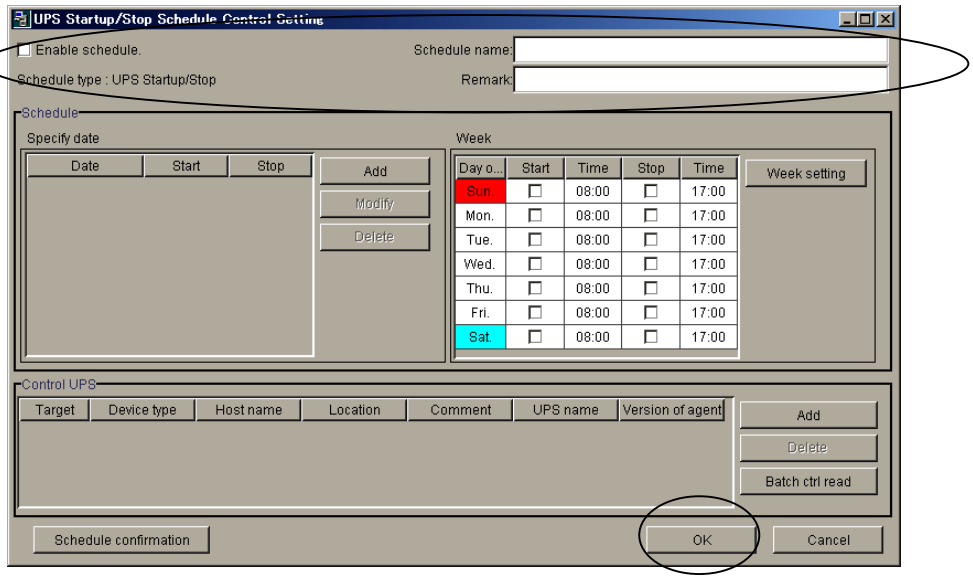


(b) To specify a specific date to run a schedule, click the "Add" button of the "Specify date" group.
When the following screen appears, specify a date to set up a schedule. Within the same schedule control, a specific date schedule takes priority over a weekly schedule.
Within a weekly schedule that you have set up, if there is a specific date that you want to exclude from the schedule, you can select the "Start" check box (followed by the "Withhold" radio button) or the "Stop" check box (followed by the "Withhold" radio button).



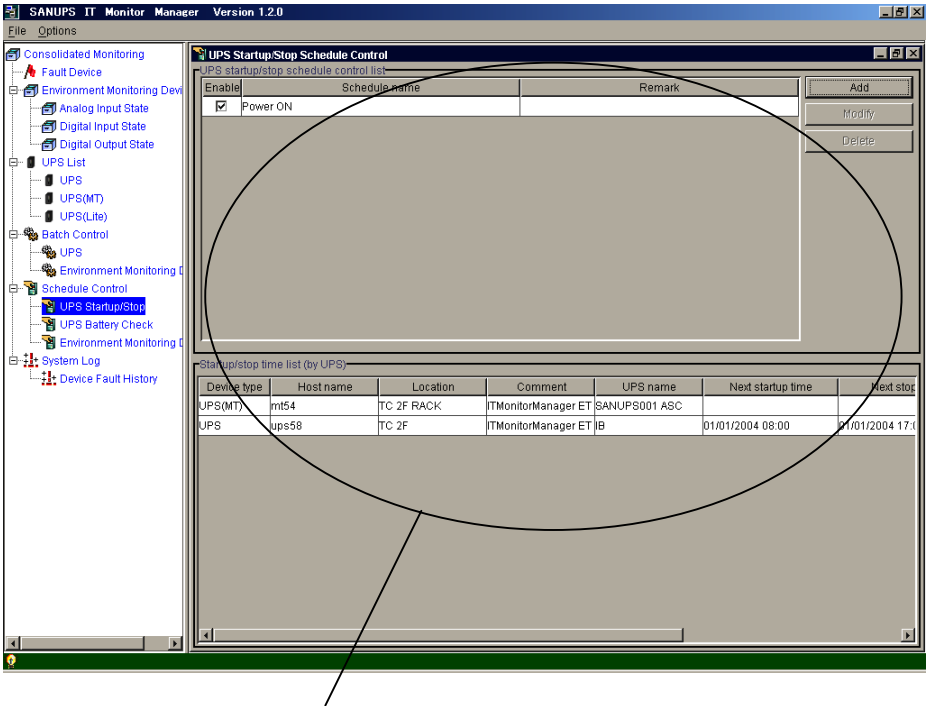
④ Set the targeted UPS control.
(a) If there is already batch control information saved on the server, click the "Batch ctrl read" button, select a batch control name, and then read the contents of the selected UPS control.
(b) To perform a new UPS control, click the "Add" button to display the "UPS Selection" screen. (The operation on the "UPS Selection" screen is the same as that for batch control).

⑤ After setting up schedules and target UPS control contents, enter a schedule name and decide whether to enable this schedule. Finally, click the "OK" button.



<Note>
When performing the UPS startup/stop schedule, the target UPS control cannot contain SG IV Lite. This is because SG IV Lite cannot start.

⑥ After you click the "OK" button, the "UPS Startup/Stop Schedule Control" panel is updated with the contents of the added schedule contents. Furthermore, the schedule information is saved on the server.



Schedule information is updated.

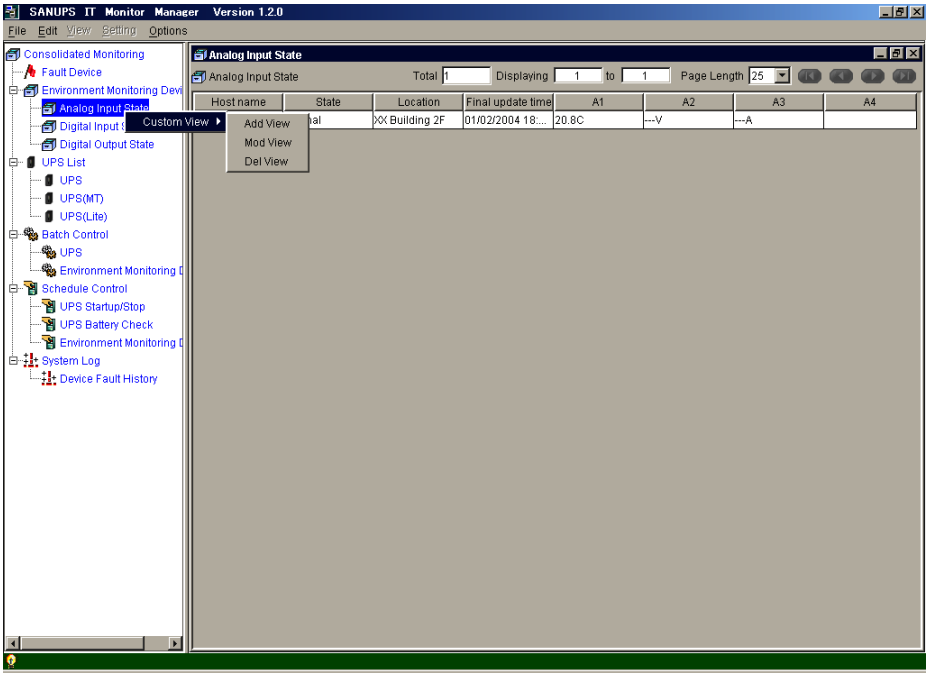
8.13 Viewing The Device Operation Status

The operation status of a device appears in the device operation status list. This section describes how to customize the display items.

8.13.1 Customizing content of the device operation status list display (environment monitoring device)

You can create custom views under each view. Also, by modifying the view filter criteria, you can customize items for display in the device operation status list.
Customizing views allows the administrator to manage devices more easily.

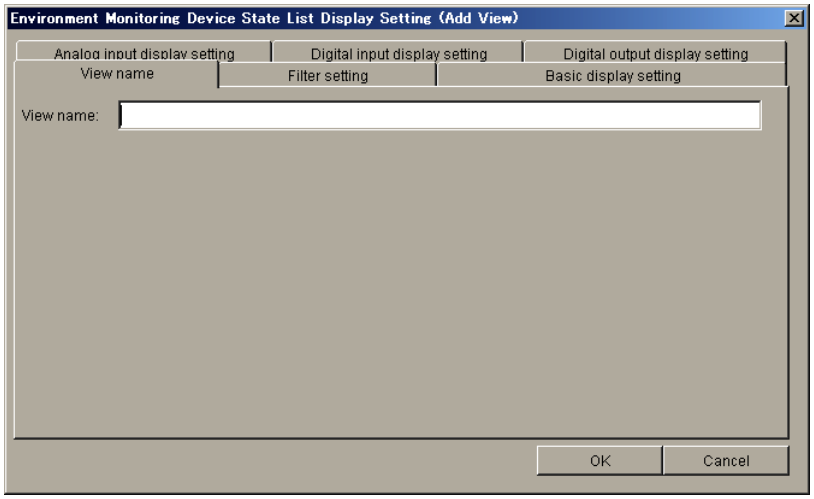
① To create a custom view, right-click any existing view. From the shortcut menu, select "Custom View". When its submenu appears, select "Add View".
From the same submenu, you can select "Mod View" to change the filter criteria of a view, or "Del View" to delete a view. If a view cannot be deleted, the "Del View" menu does not appear.



② The "Environment Monitoring Device State List Display Setting" appears.

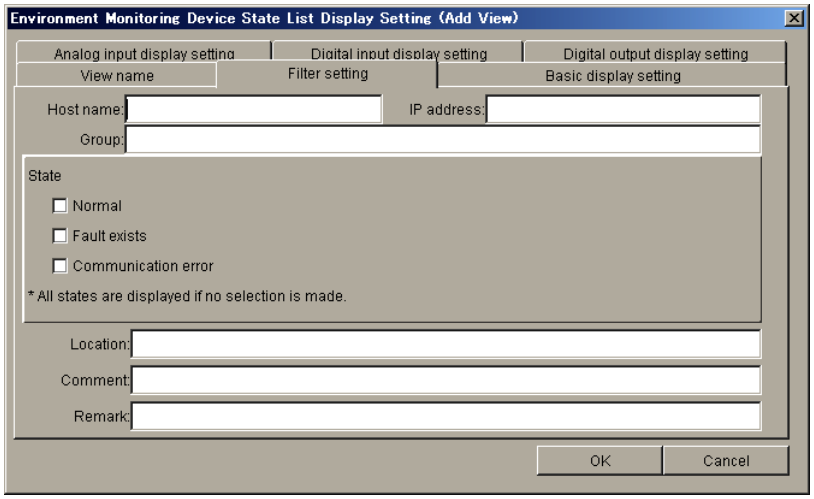
(a) "View name" tab

Use this tab to specify a name for the custom view.



(b) "Filter setting" tab

Use this tab to specify criteria to select and display environment monitoring devices.

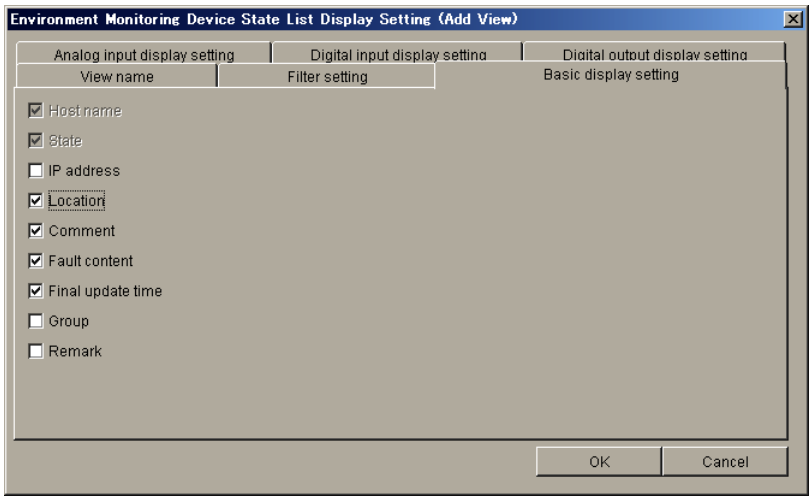


Individual conditions are combined using the logical AND to form the filter criteria.

For the host name, IP address, group, location, comment, and remark, you can use the wildcard characters. Wildcard characters available are * (any number of occurrences of any characters), and ? (any single character). However, if a character string containing ? is set, this is equivalent to having * added to the end of the character string.

(c) "Basic display setting" tab

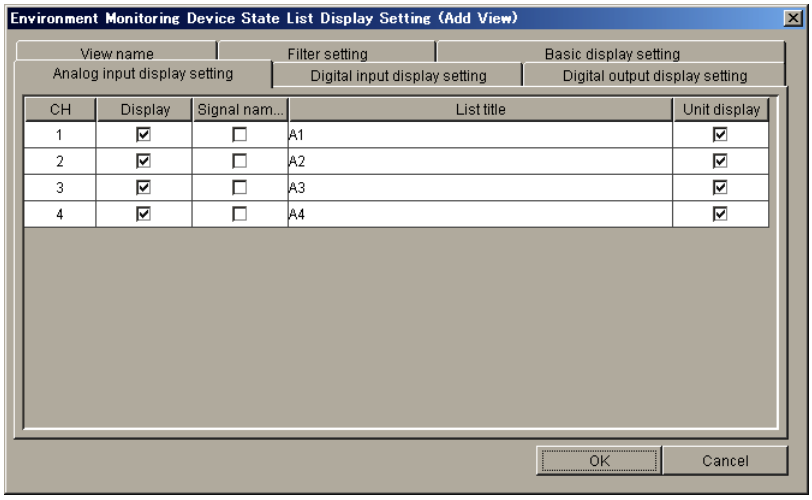
Use this tab to specify the basic display items in the device operation status list.



To include an item in the device operation status list for display, select its check box.

An item that appears dimmed is always included in the device operation status list for display and cannot be modified.

(d) "Analog input display setting" tab

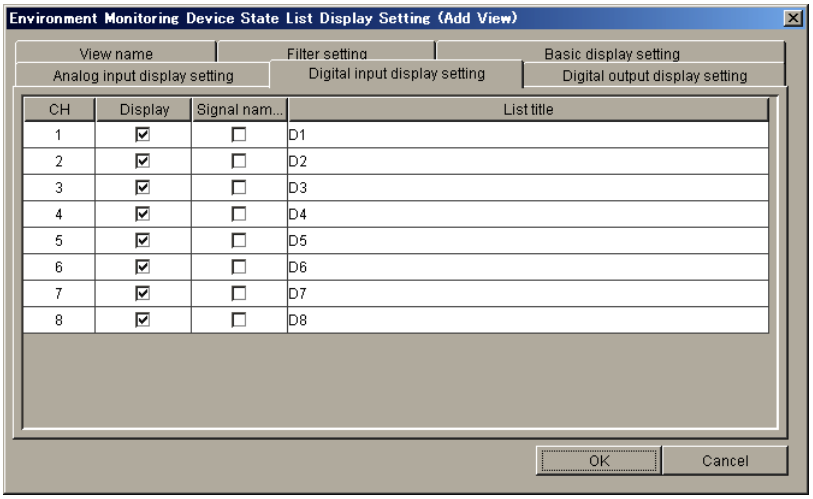


When you select the "Display" check box of a signal CH, the contents of this signal appear in a row in the device operation status list. If you clear the selection, the contents of this signal do not appear in the device operation status list.

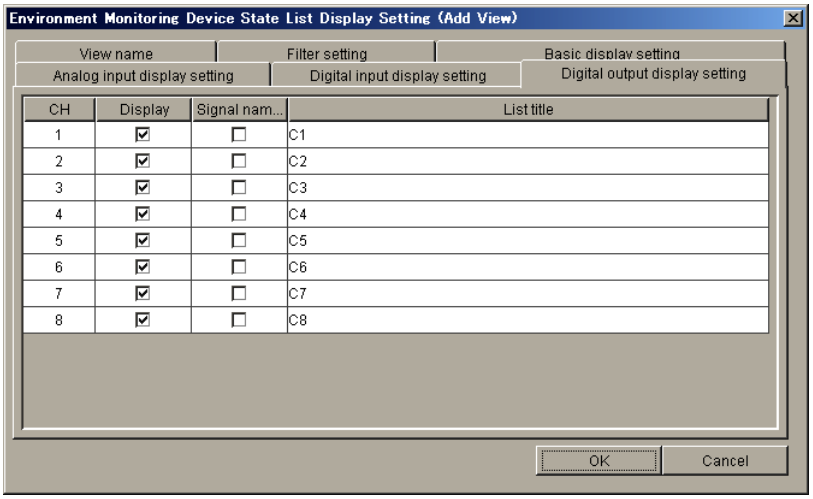
When you select the "Display" check box of a signal CH, you can then edit its signal name display, list title, and unit display.

If the "Signal name display" check box is selected, "Signal name:" is added in front of the analog input value.

(e) "Digital input display setting" tab
Use this tab in the same way as the "Analog input display setting" tab.
If the "Signal name display" check box is selected, "Signal name:" is added in front of the signal state.



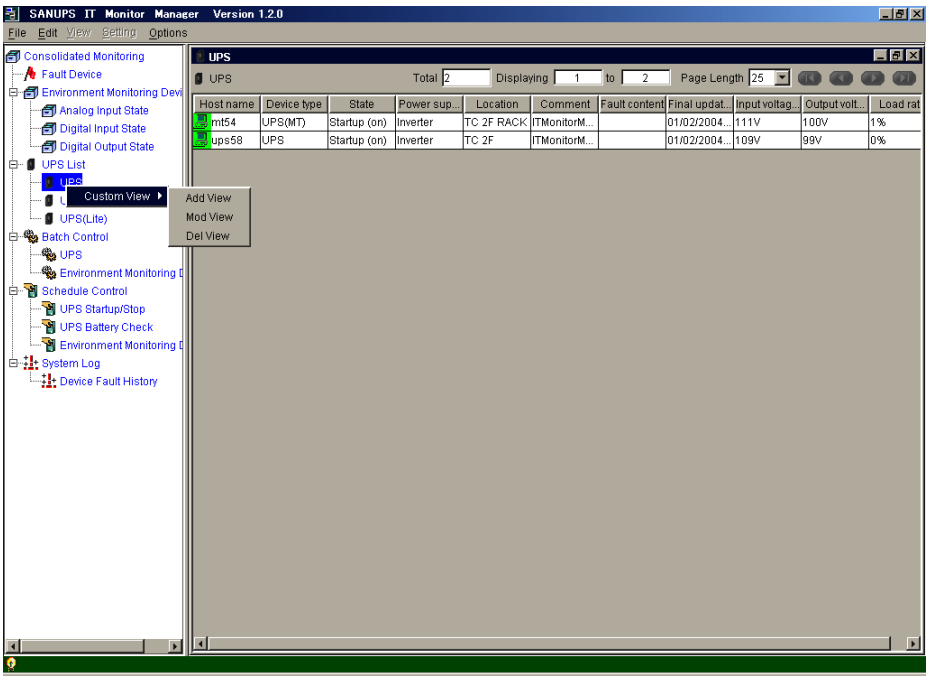
(f) "Digital output display setting" tab
Use this tab in the same way as the "Analog input display setting" tab.
If the "Signal name display" check box is selected, "Signal name:" is added in front of the signal state.



8.13.2 Customizing content of the device operation status list display (UPS)

You can create custom views under each view. Also, by modifying the view filter criteria, you can customize items for display in the device operation status list.
Customizing views allows the administrator to manage devices more easily.

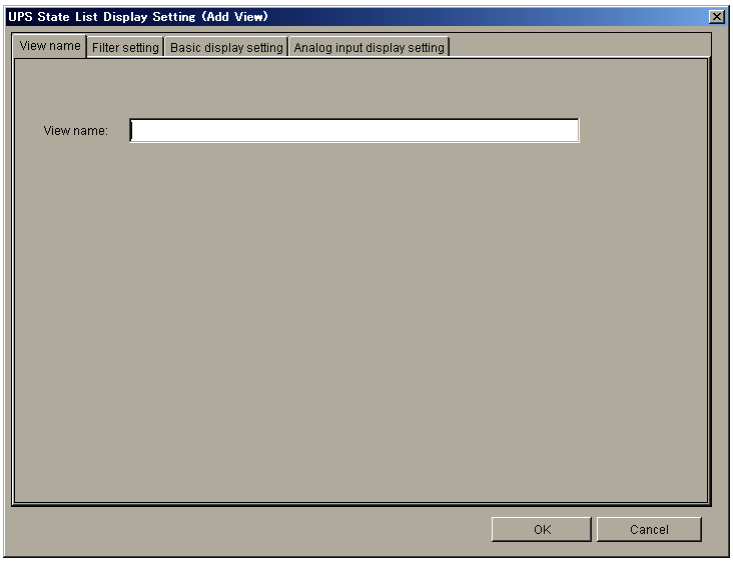
① To create a custom view, right-click any existing view. From the shortcut menu, select "Custom View". When its submenu appears, select "Add View". From the same submenu, you can select "Mod View" to change the filter criteria of a view, or "Del View" to delete a view. If a view cannot be deleted, the "Del View" menu does not appear.



② The "UPS State List Display Setting" appears.

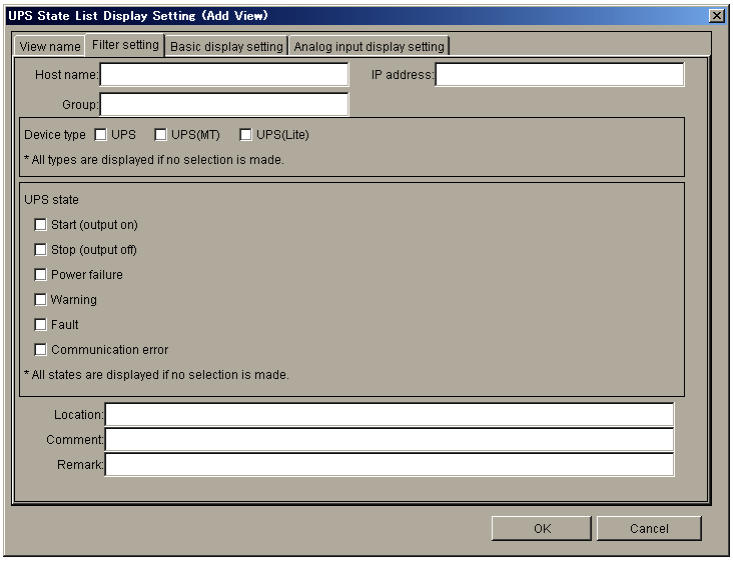
(a) "View name" tab

Use this tab to specify a name for the custom view.



(b) "Filter setting" tab

Use this tab to specify criteria to select and display UPS devices.

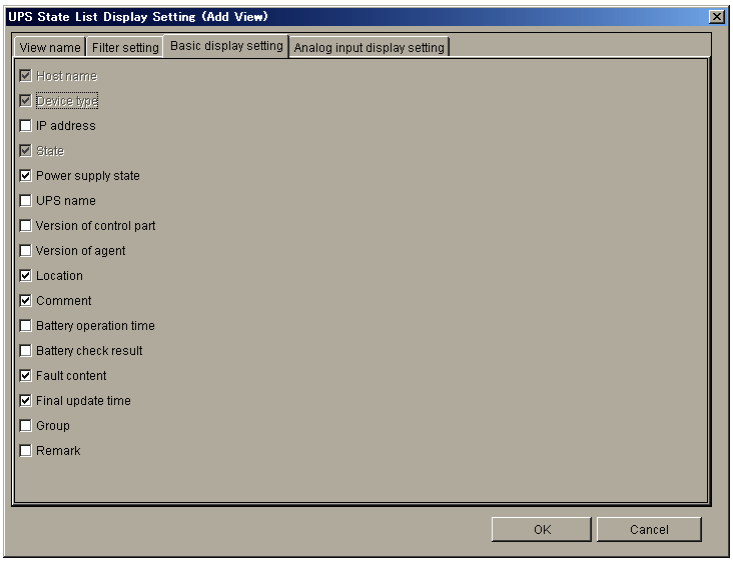


Individual conditions are combined using the logical AND to form the filter criteria.

For the host name, IP address, group, location, comment, and remark, you can use the wildcard characters. Wildcard characters available are * (any number of occurrences of any characters), and ? (any single character). However, if a character string containing ? is set, this is equivalent to having * added to the end of the character string.

(c) "Basic display setting" tab

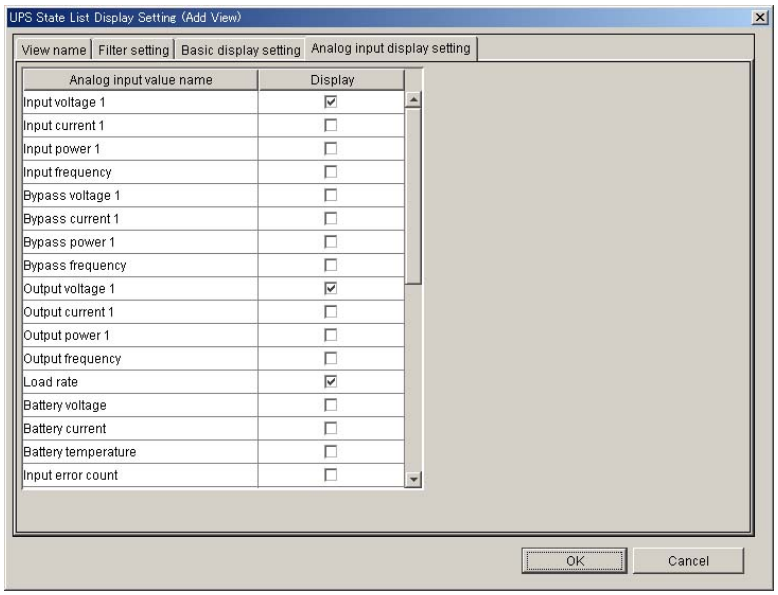
Use this tab to specify the basic display items in the device operation status list.



To include an item in the device operation status list for display, select its check box.

An item that appears dimmed is always included in the device operation status list for display and cannot be modified.

(d) "Analog input display setting" tab



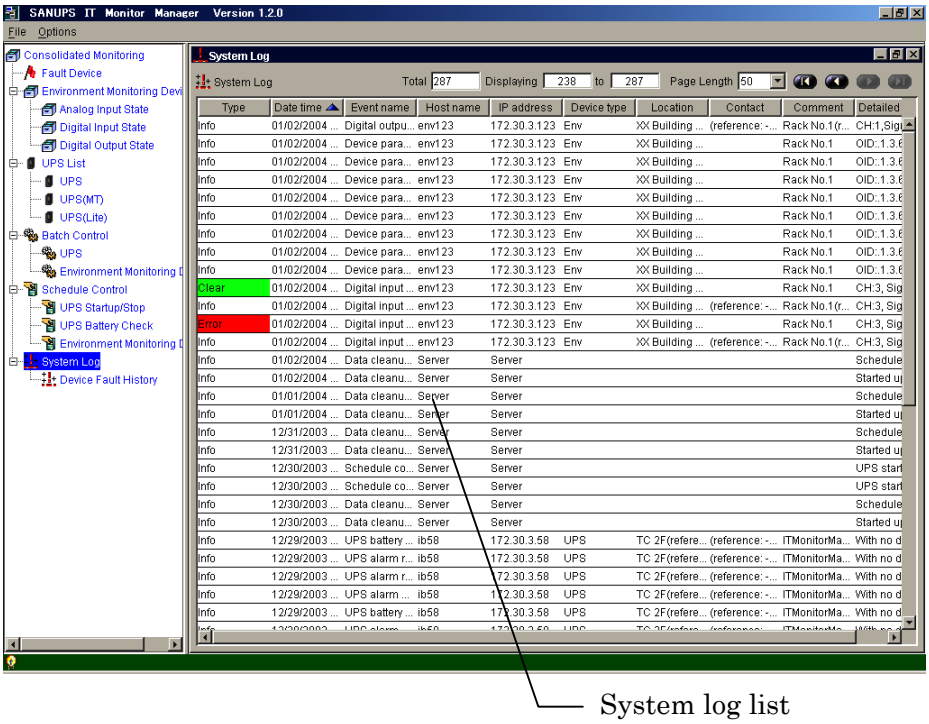
When you select the "Display" check box of an analog input value name, this analog input value name appears in the device operation status list.

8.14 Viewing The System Log

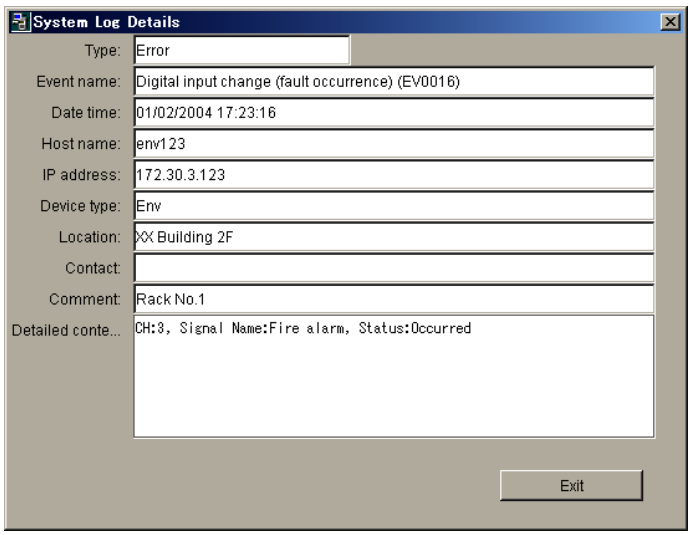
When you select the "System Log" view on the "Consolidated Monitoring" tree view, by default all logs kept by the SANUPS IT Monitor Manager system appear in the system log list.
Also, if you select the "Device Fault History" view, by default all fault occurrence and recovery logs (among the system logs) appear in the system log list.
Furthermore, this system log contains information kept by the SANUPS IT Monitor Manager system, and is different from the event log kept by a device.

8.14.1 Viewing details of the system log

① Using the main screen, double-click on a row in the system log list.



② The "System Log Details" screen appears so that you can look at the detailed information of the event.

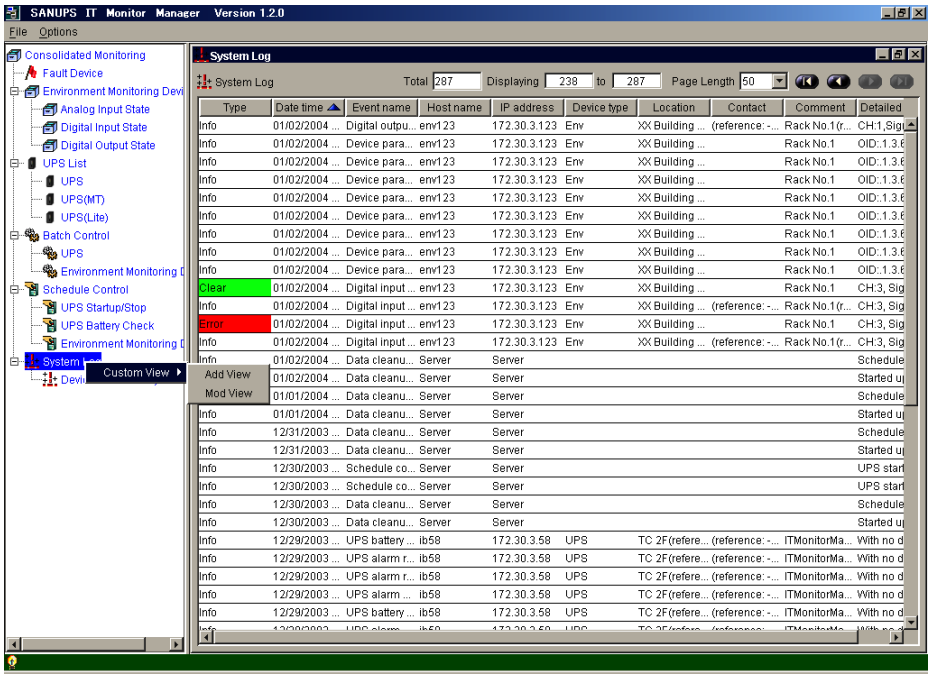


18.4.2 Customizing the system log list

You can create custom views under each view. Also, by modifying the view filter criteria, you can customize items for display in the system log list.

Customizing views allows the administrator to manage system log more easily.

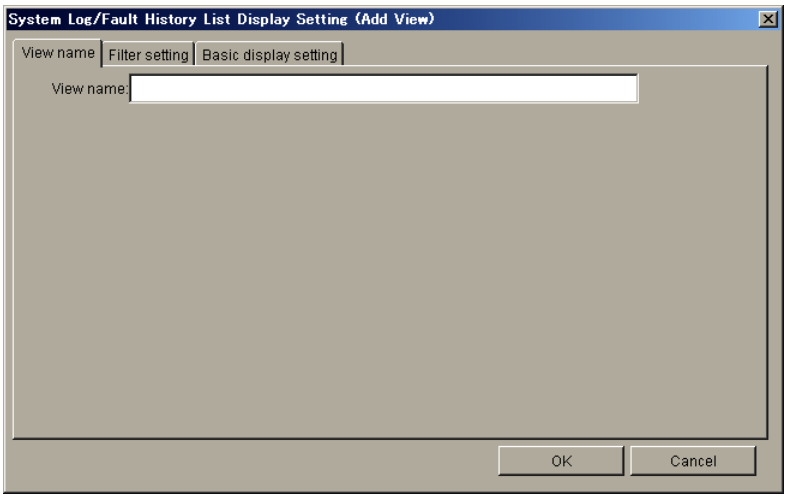
① To create a custom view, right-click any existing view. From the shortcut menu, select "Custom View". When its submenu appears, select "Add View". From the same submenu, you can select "Mod View" to change the filter criteria of a view, or "Del View" to delete a view. If a view cannot be deleted, the "Del View" menu does not appear.



② The "System Log/Fault History List Display Setting" screen appears.

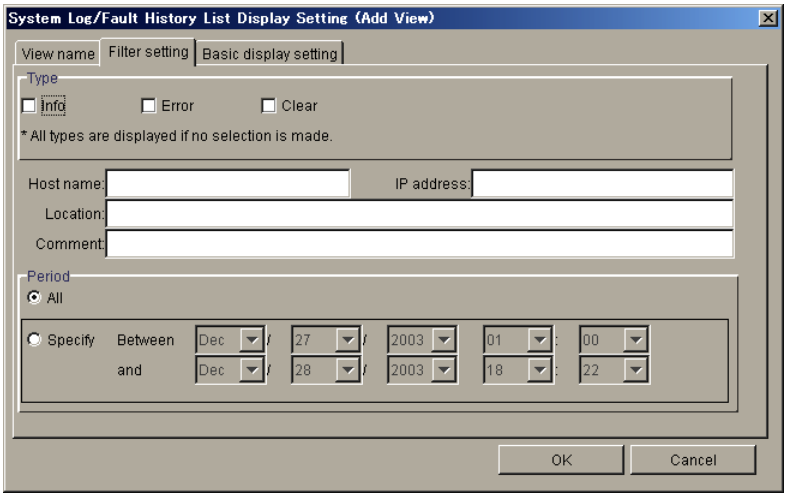
③ "View name" tab

Use this tab to specify a name for the custom view.



④ "Filter setting" tab

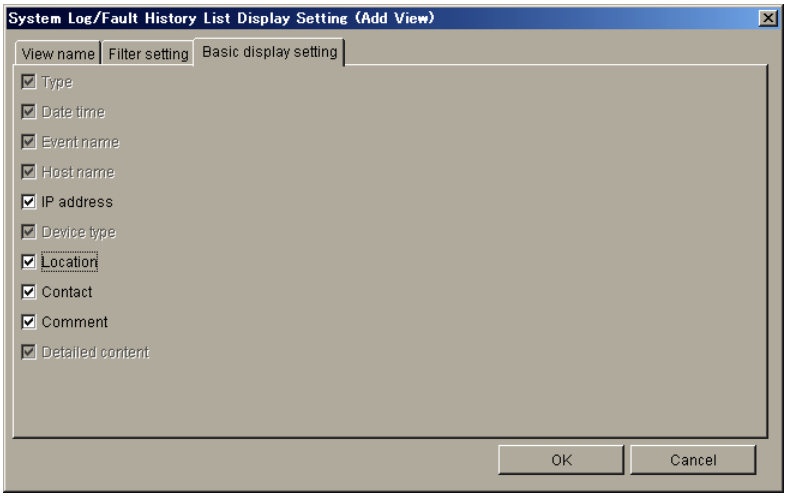
Use this tab to specify criteria to select and display some logs from the system log list.



Individual conditions are combined using the logical AND to form the filter criteria.

For the host name, IP address, location, comment, and remark, you can use the wildcard characters. Wildcard characters available are * (any number of occurrences of any characters), and ? (any single character). However, if a character string containing ? is set, this is equivalent to having * added to the end of the character string.

⑤ "Basic display setting" tab
Use this tab to specify the basic display items in the device operation status list.



To include an item in the device operation status list for display, select its check box.

8.14.3 Data storage period of system log

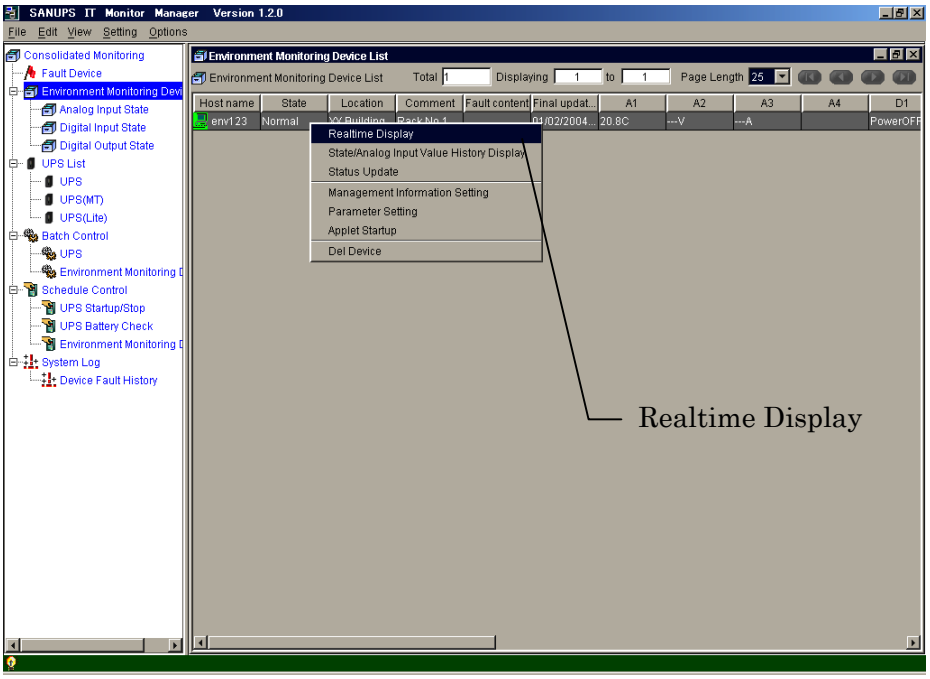
When a new event occurs, or when the server restarts, system log data older than 90 days is deleted automatically.

8.15 Enabling The Real-time Display Of A Device

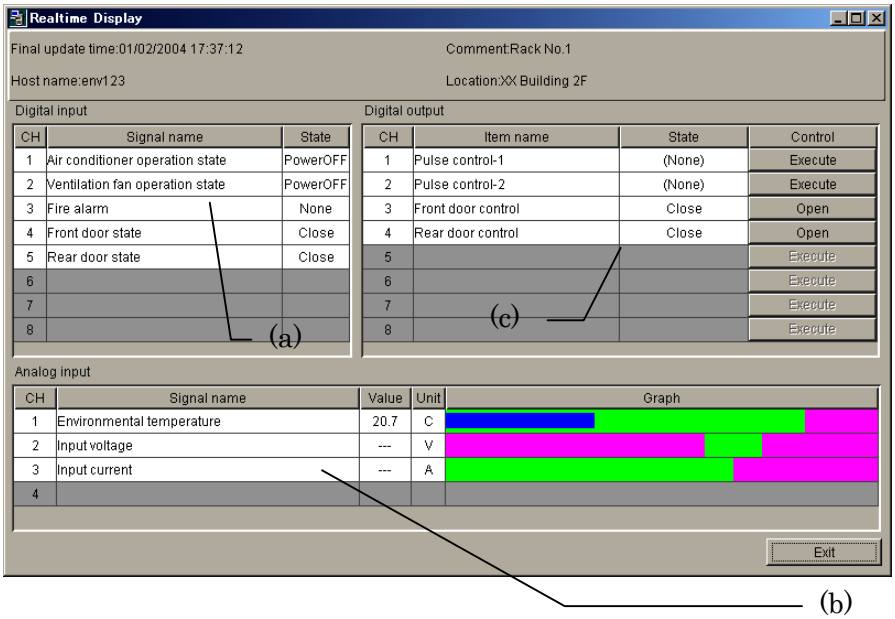
You can use this function to check the current state of the device specified by the administrator.
This information is automatically updated every five seconds.

8.15.1 Enabling the real-time display of an environment monitoring device

① Using the main screen, select an environment monitoring device from the device operation status list. From the "View" menu or the shortcut menu, select "Realtime Display".
(You can also double-click the device from the list).



② The "Realtime Display" screen appears.



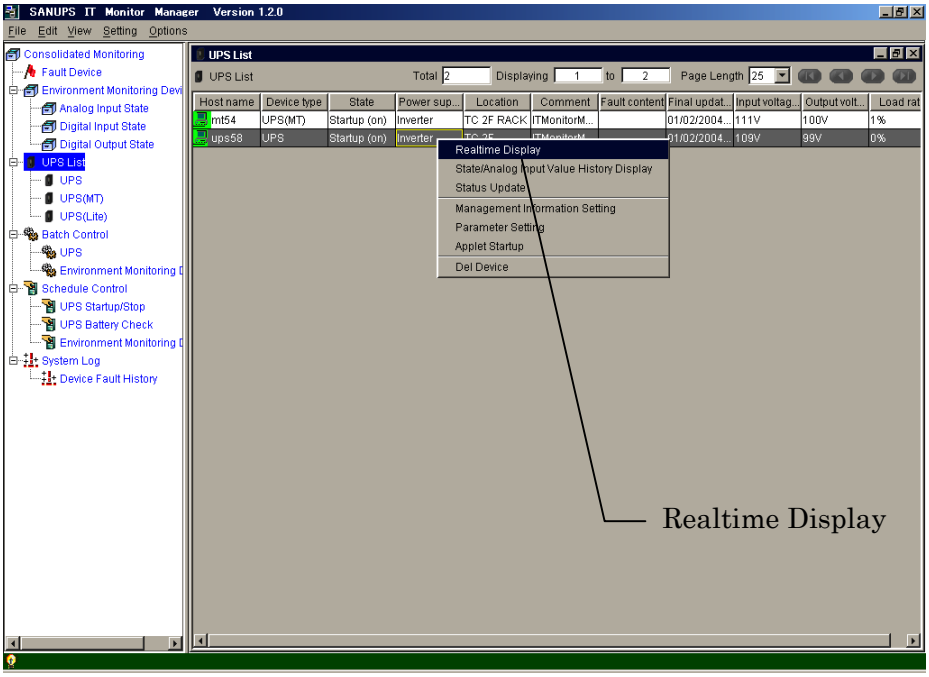
(a) Digital input signal state
The current state of each digital input signal is displayed.

(b) Analog input signal state
The current state of each analog input signal is displayed. In the graph, the blue area indicates the analog input value, the green area the normal range, and the magenta area the deviation range. (The signal which has alarm, displays a background color of red.)

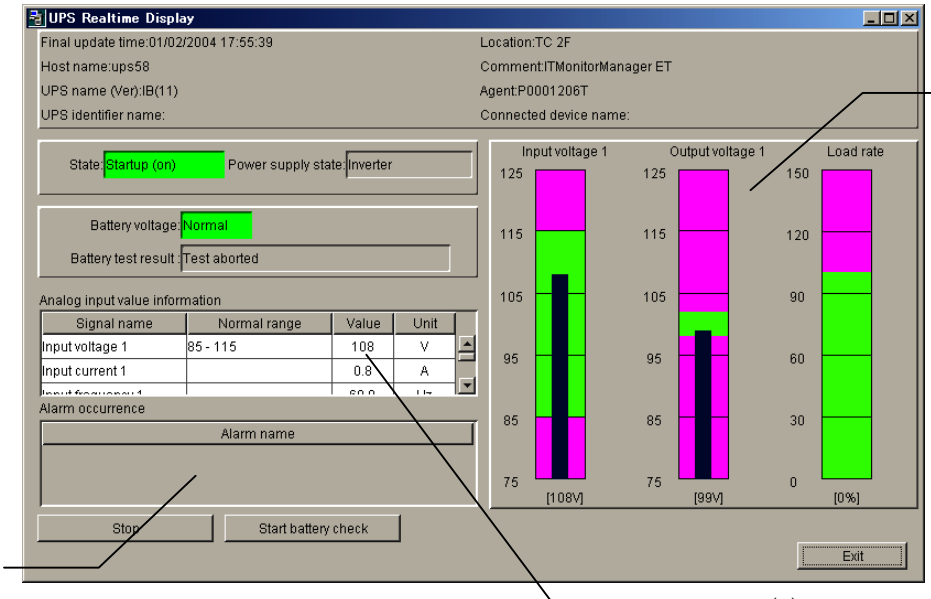
(c) Digital output signal state
The signal state of each digital output, as well as the active control button is displayed. (The signal which has alarm, displays a background color of red.)

8.15.2 Enabling the real-time display of UPS

① Using the main screen, select a UPS device from the device operation status list. From the "View" menu or the shortcut menu, select "Realtime Display". (You can also double-click the device from the list).



② The "UPS Realtime Display" screen appears.



(a) Alarm name
The name of the UPS alarm (RFC1628 alarm) that occurs on the device is displayed here.

(b) Analog input value information
The information displayed is the current analog input value of UPS device. Depending on the type of UPS device, the displayed analog input varies; analog input that cannot be obtained is not displayed.

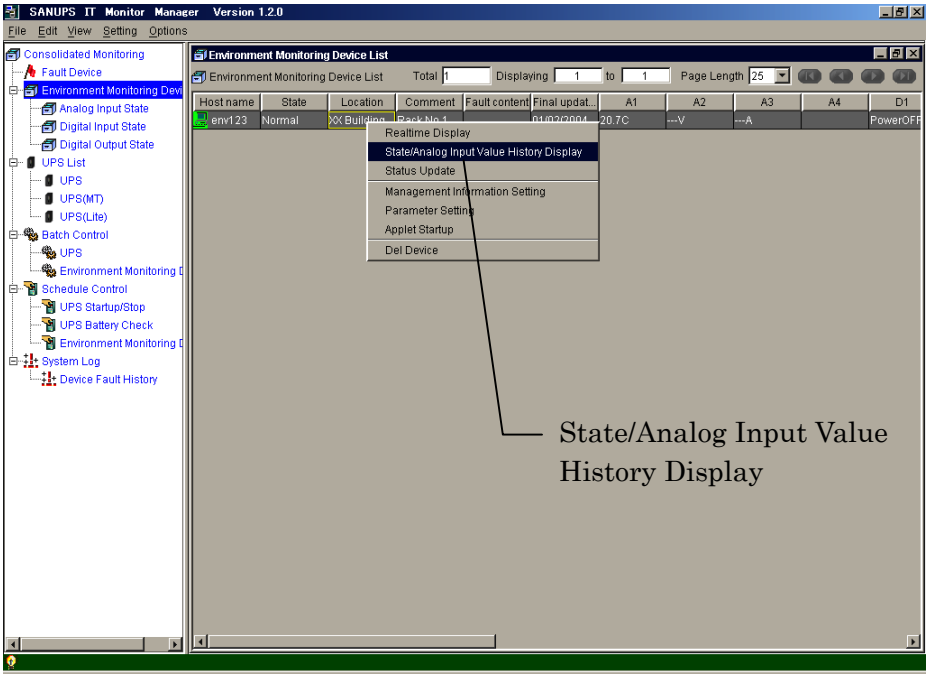
(c) Graphs
The current input voltage, output voltage, and load rate of the UPS device are displayed here.
For both the input voltage and output voltage, their first phase values are displayed.
Depending on the UPS device, you may not be able to obtain its analog input value; in this case, the analog input value displayed becomes blank.

8.16 Displaying The State/Analog Input Value History Of A Device

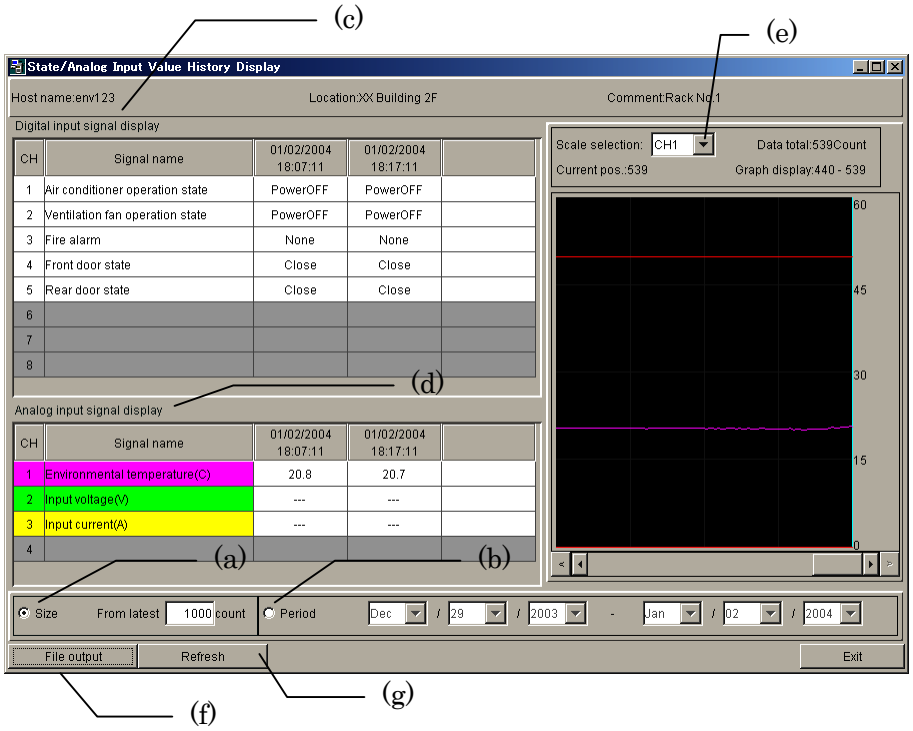
You can use this function to display the state/analog input value history of any device.
This is useful when you want to check the change in state of a device from the past to the present.
Furthermore, this state/analog input value history is kept by the server and is different from the state/analog input value history that is kept by a device.

8.16.1 Displaying the state/analog input value history of a device (environment monitoring device)

① Using the main screen, select a environment monitoring device from the device operation status list. From the "View" menu or the shortcut menu, select "State/Analog Input Value History Display".



② The "State/Analog Input Value History Display" screen appears.



(a) "Size" radio button
During startup, 1000 counts of data, starting from the latest, are displayed.
You can specify up to 10,000 counts of data.
After changing the setting, click the "Refresh" button. The appropriate data is displayed.

(b) "Period" radio button
The range of the state/analog input value history for the device saved on the server at the moment this screen appears is displayed. After changing the range, click the "Refresh" button. Only the appropriate data is displayed.

(c) "Digital input signal display" list
This list displays the appropriate digital input signal state history of the specified range. (The signal which has alarm, displays a background color of red.)

(d) "Analog input signal display" list
This list displays the appropriate analog input signal state history of the specified range. (The signal which has alarm, displays a background color of red.)

(e) "Scale selection" drop-down list
Use this drop-down list to select a channel. The analog input range of the selected channel is displayed as scale in a graph.

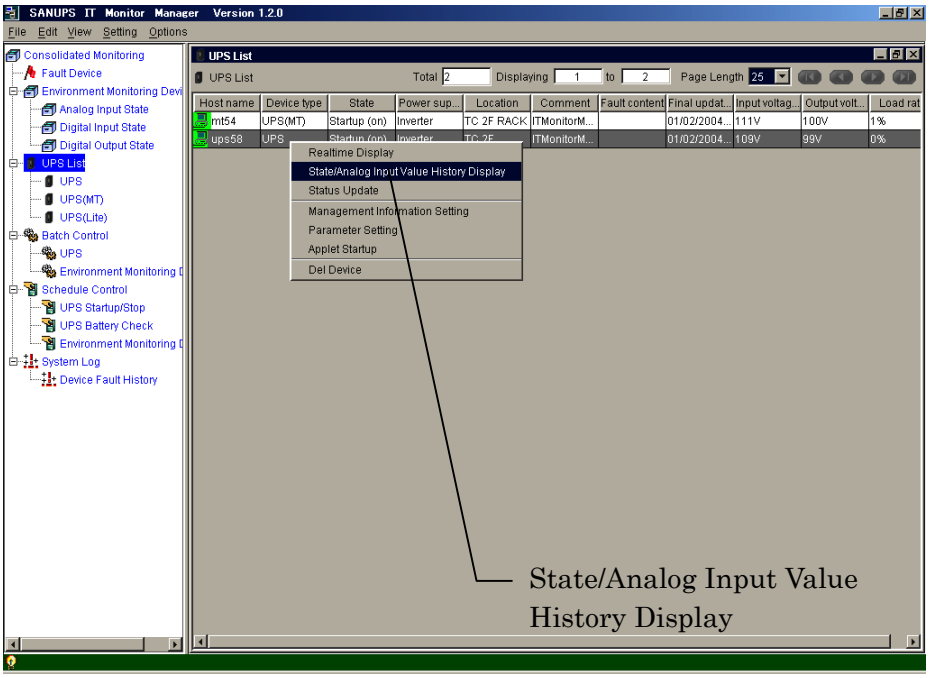
(f) "File output" button
Use this button to output the state/analog input value history of the current device to a file using the CSV format.

(g) "Refresh" button
Use this button to read the state/analog input value history

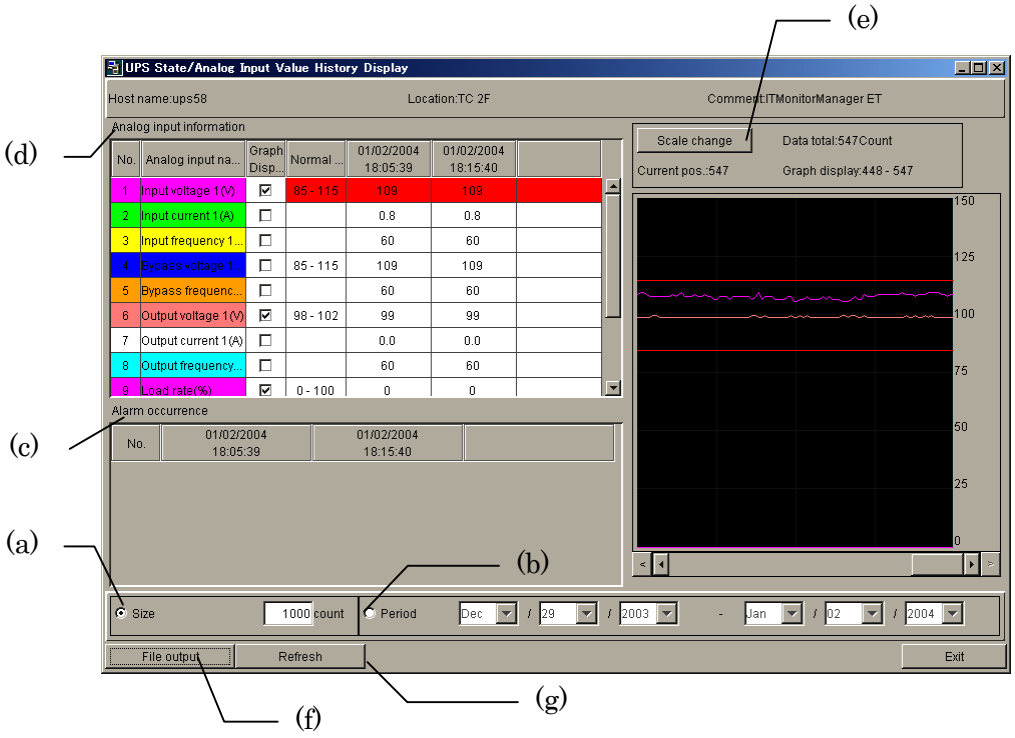
from the server, and then display this information again.

8.16.2 Displaying the state/analog input value history of a device (UPS)

① Using the main screen, select a UPS device from the device operation status list. From the "View" menu or the shortcut menu, select "State/Analog Input Value History Display".



② The "State/Analog Input Value History Display" screen appears.



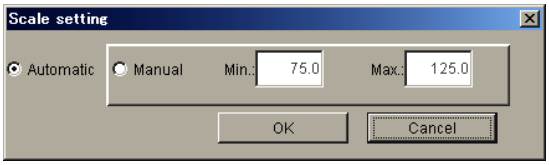
(a) "Size" radio button
During startup, 1000 counts of data, starting from the latest, are displayed.
You can specify up to 10,000 counts of data.
After changing the setting, click the "Refresh" button. The appropriate data is displayed.

(b) "Period" radio button
The range of the state/analog input value history for the device saved on the server at the moment this screen appears is displayed. After changing the range, click the "Refresh" button. Only the appropriate data is displayed.

(c) "Alarm occurrence" list
The alarm (RFC1628 alarm) that occurs at that moment is displayed here.

(d) "Analog input information" list
This list displays the analog input history for the appropriate range.

(e) "Scale change" button
Use this button if you want to change the display scale of the graph.
When you click this button, the following screen appears so that you can change the scale:



(f) "File output" button
Use this button to output the state/analog input value history of the current device to a file using the CSV format.

(g) "Refresh" button
Use this button to read the state/analog input value history from the server and then display this information again.

8.16.3 Notes on state/analog input value history display of a device

① The state/analog input value history display can display up to 10,000 counts of history. Also, a maximum of 65,535 counts of data can be output to a file.

② There is no restrictions on the number of counts of state/history information to keep. To clear the information, use the database cleanup function.
By default, 60 days of data is kept. If you do not use the database cleanup function to change the setting, all information is kept.
As a general rule, 50,000 counts of data require about 30 Mbytes.

Example: If the number of devices targeted for monitoring is 100 and the state/analog input value save interval is 600 seconds, data kept in one day takes up about 8 Mbytes.

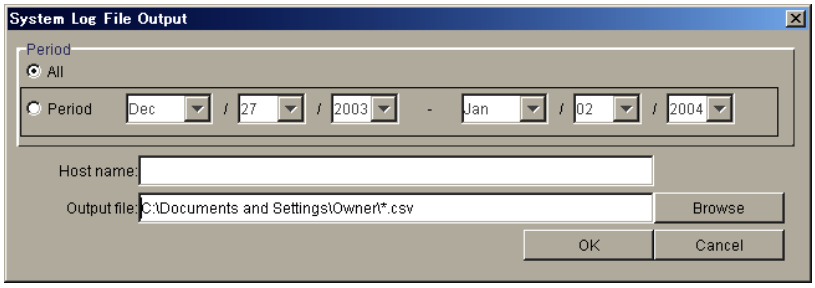
According to the free space available on the hard disk drive, perform the database cleanup settings.

8.17 Outputting The System Log To A File

You can output the system log kept on the server to a file in the CSV format. Data output to a CSV file can be used by other applications for further processing.

8.17.1 Using the procedure to output system log to a file

① Using the main screen, select "System Log File Output" from the "File" menu. The "System Log File Output" screen appears.



② Specify a period to select data for file output.

(a) If you select the "All" radio button, all of the system log kept by the server is output to a file.

(b) If you select the "Period" radio button, you can specify a period so that, among the system log kept by the server, only data in the specified period is output to a file. The default period displayed when the "System Log File Output" screen appears indicates the current period of data kept by the server. However, if there is no data kept by the server, then the period becomes the current system date.

③ In the "Host name" text box, enter a host name.
If you enter a host name, only system log related to this host name is output to a file. If no host name is specified, all system logs are output to a file.
For the host name, you can use wildcard characters. Wildcard characters available are * (any number of occurrences of any characters) and ? (any single character). However, if a character string containing ? is set, this is equivalent to having * added to the end of the character string.

④ Specify the location and name of a file for output.
You can also use the "Browse" button on the right side of this text box to specify a directory for outputting the file.

⑤ If you click the "OK" button, the system log is output to the specified file.

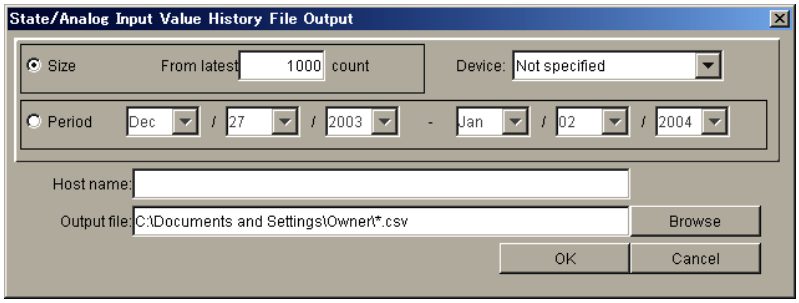
⑥ If you click the "Cancel" button instead, you can cancel the operation so that the system log is not output to a file.

8.18 Outputting The State/Analog Input Value History To A File

You can output the state/analog input value history to a file in the CSV format.
Data output to a CSV file can be used by other applications for further processing.

8.18.1 Using the procedure to output state/analog input value history to a file

① Using the main screen, select "State/Analog Input Value History File Output" from the "File" menu. The "State/Analog Input Value History File Output" screen appears.



② Select the "Size" or "Period" radio button.

(a) If you select the "Size" radio button, you can output the specified number of the counts of the latest state/analog input value history of the device specified by the "Device" drop-down list.
Three choices are available from the "Device" drop-down list: "Not specified", "Environment monitoring device", and "UPS".
If you select "Not specified", the specified number of the counts of data for the environment monitoring device is output, and then the specified number of the counts of data for UPS device is output.

(b) If you select the "Period" radio button, you can specify a period so that, among the state/analog input value history kept by the server, only data in the specified period is output to a file. The default period displayed when the "State/Analog Input Value History File Output" screen appears indicates the current period of all data kept by the server. However, if there is no data kept by the server, then the period becomes the current system date.

③ In the "Host name" text box, enter a host name.
If you enter a host name, only state/analog input value history related to this host name is output to a file. If no host name is specified, state/analog input value history of all devices is output to a file.
For the host name, you can use wildcard characters. Wildcard characters available are * (any number of occurrences of any characters), and ? (any single character). However, if a character string containing ? is set, this is equivalent to having * added to the end of the character string.

④ Specify the location and name of a file for output.
You can also use the "Browse" button on the right side of this text box to specify a directory for outputting the file.

⑤ If you click the "OK" button, the state/analog input value history is output to the specified file.

⑥ If you click the "Cancel" button instead, you can cancel the operation so that the state/analog input value history is not output to a file.

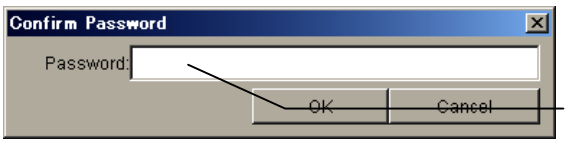
8.19 About The Security

To restrict operation by other users, you can set up a mode to force confirmation of a password to execute many functions.
Use the security setting to specify whether password confirmation is required for the execution of functions on each client machine.

8.19.1 Performing security setting

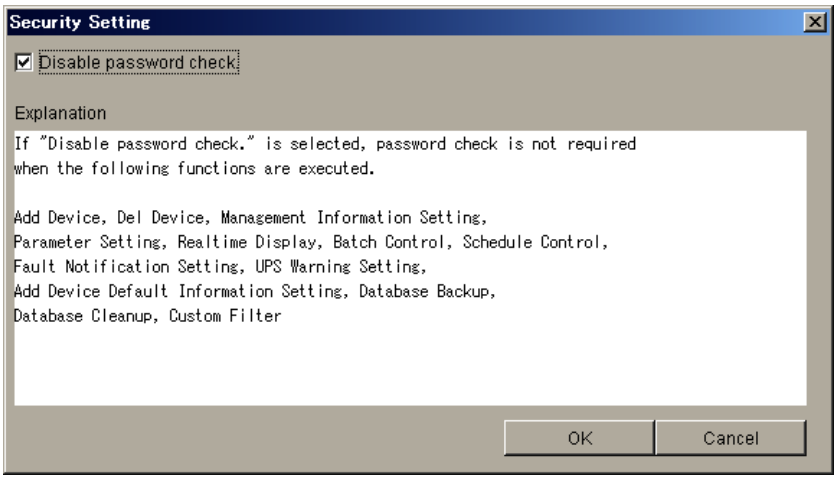
① From the "Options" menu, select "Security Setting".

② The "Confirm Password" screen appears.



Enter the current password.

③ The "Security Setting" screen appears.



④ Specify whether to disable password check in execution of functions on a client machine.

(a) If you select the "Disable password check" check box
No password check is performed when the functions are executed. However, the security setting and password setting always require password confirmation.

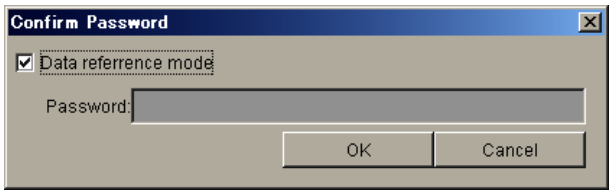
(b) If you clear the "Disable password check" check box
Password check is performed when the functions are executed. However, for the parameter setting and real-time display, information can be displayed in the data reference mode.

⑤ When you click the "OK" button, the setting becomes effective.

8.19.2 Functions that can have password confirmation

The functions that can have password confirmation are: device addition default information, adding device, deleting device, management information setting, parameter setting*, real-time display*, state/analog input value history display, batch control, schedule control, fault notification setting, UPS warning setting, database backup, database cleanup, custom filter (add, modify, delete).

* Indicates the function can be executed in the data reference mode. When you execute a function in the data reference mode, password input is not required and information can be read. However, the information cannot be changed, and the device cannot be controlled. If a function can be executed in the data reference mode, the following screen appears. If you clear the "Data reference mode" check box, then password input becomes necessary.

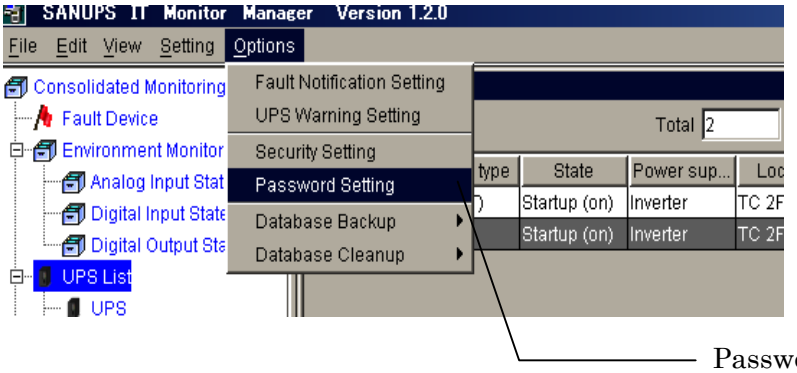


8.20 About The Password

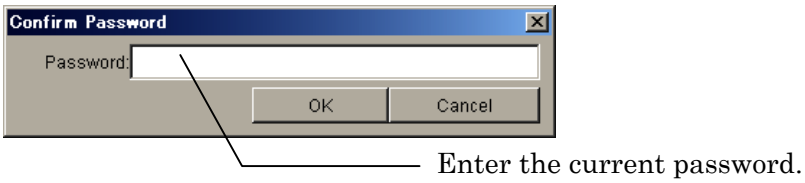
SANUPS IT Monitor Manager manages only one password that is used across all clients.
This password is used when you log on to the server, and when you execute the various functions.
By default, the password is "public". If necessary, change the password.

8.20.1 Changing the password

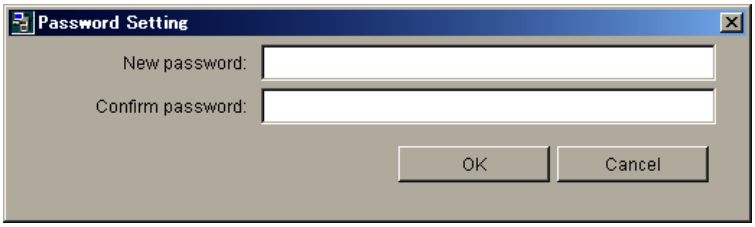
① Using the main screen, select "Password Setting" from the "Options" menu.



② The "Confirm Password" screen appears.



③ Enter the current password; then click the "OK" button. The "Password Setting" screen appears and then you can enter a new password.



④ Click the "OK" button. The new password becomes effective.

8.21 About Database Backup

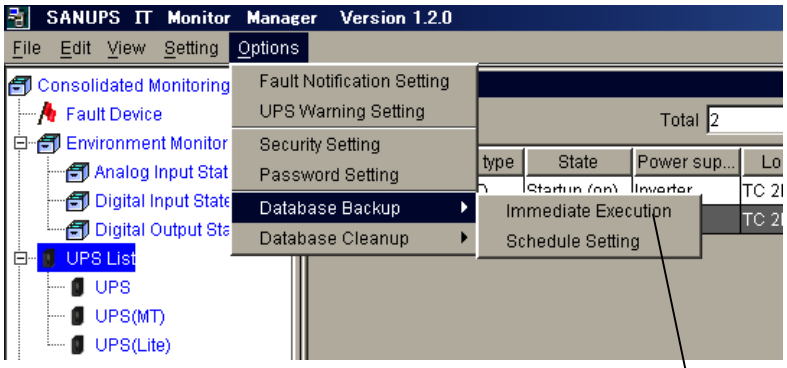
This is a function that you can use to save all information kept by the server to a backup file. In terms of the backup timing, two choices are available. You can back up immediately or back up according to a schedule.
The backup file is stored in the "backup" folder below the server install folder. The name of the backup file is backup__YYYYMMDD_HHMMSS.ZIP. The file name includes the date and time when the backup operation was performed. This file is used during a restore operation.

8.21.1 Backup target data

The target data for backup is all information kept by the server. (In other words, information of devices targeted for monitoring, view setting information, system log information, and state/analog input value history information are included).

8.21.2 Performing a database backup immediately

① Using the main screen, select "Database Backup" from the "Options" menu; then select "Immediate Execution".



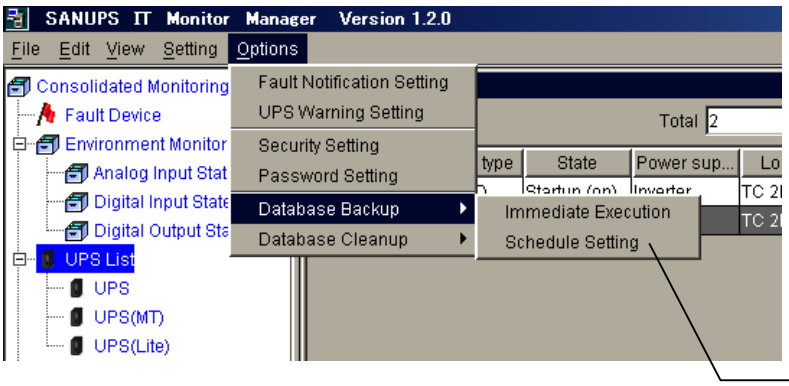
② The "Backup Start" screen appears.



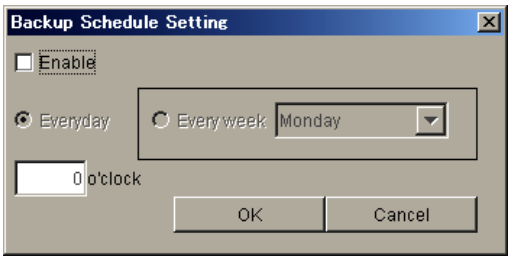
③ When you click the "Yes" button, the database backup operation starts. Furthermore, the backup start and stop information can be checked using the system log.

8.21.3 Setting up a backup schedule

① Using the main screen, select "Database Backup" from the "Options" menu; then select "Schedule Setting".



② The "Backup Schedule Setting" screen appears.
By default, the backup schedule has not been enabled during the install operation.



③ Specify whether to enable the backup schedule.
When you select the "Enable" check box, backup of the database is performed according to the specified schedule.
If you do not require periodic backup, clear the "Enable" check box.

④ Specify the backup timing.
(a) Select the "Everyday" radio button if you want to back up the database everyday.
(b) Select the "Everyweek" radio button and specify a day if you want to back up the database once every week on a specified day.
(c) In the text box, enter the time of day to back up the database.

⑤ Click the "OK" button. The backup schedule becomes effective.

8.21.4 Note on backing up the database

Because the backup operation greatly increases the load of the server, this may cause a delay in refreshing the display on the clients.

8.22 About The Database Restore

The backup file created by the Database Backup function is stored in the "backup" folder below the server install folder.
The name of the backup file is backup__YYYYMMDD_HHMMSS.ZIP. The file name includes the date and time when the backup operation was performed.
Use the following procedure to perform a database restore, using the backup file:

> <Note>
> Perform the following work as a user with administrator privileges. In Windows Vista and later operating systems, start Command prompt with "Run as administrator."
> In the case of an operating system that includes User Account Control (UAC), make sure you disable UAC before performing the work. For details on how to set UAC, see "Appendix J: User Account Control (UAC) Settings" on page 149.

① Stop the SANUPS IT Monitor Manager server. For information on how to stop the server, see the “Starting And Ending The Server” section on page 19.

② Open the MS-DOS command prompt; then change the current folder to the "bin" folder below the server install folder.

③ From the command prompt, run the following command:
`Sy_Restore BackupFileName`

> <Note>
> When specifying the backup file name, do not include the drive name, folder name, and file extension. Enter just the file name (in the form of backup__YYYYMMDD_HHMMSS).

④ When the restore operation is finished, the "Restore Complete!" message appears. After the restore operation, start the SANUPS IT Monitor Manager server, and then continue to operate it as usual.

8.23 About Database Cleanup

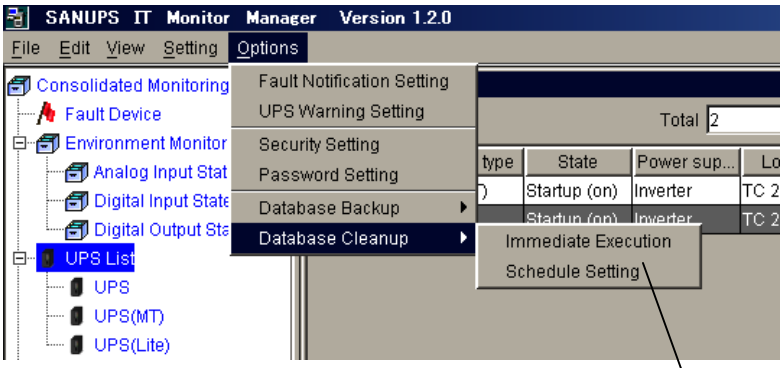
This function allows you to delete the state/analog input value history information kept by the server.
In terms of the cleanup timing, two choices are available. You can clean up immediately, or clean up according to a schedule.

8.23.1 Cleanup target data

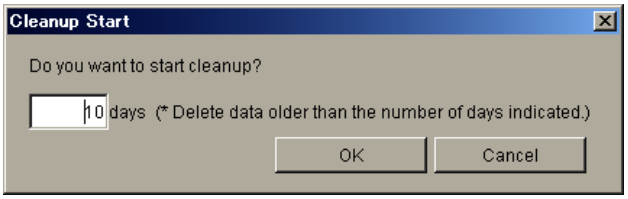
The data that you can delete is the state/analog input value history information only.

8.23.2 Performing a database cleanup immediately

① Using the main screen, select "Database Cleanup" from the "Options" menu; then select "Immediate Execution".



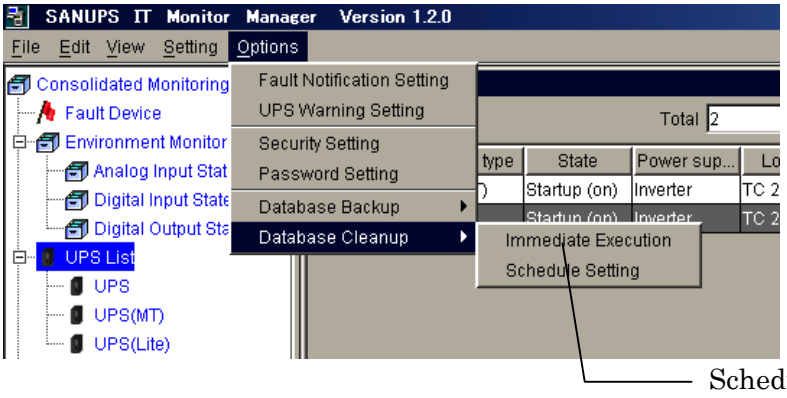
② The "Cleanup Start" screen appears.



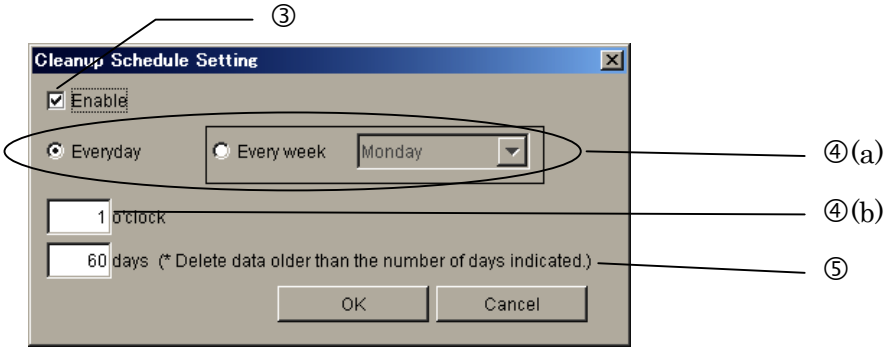
③ When you click the "OK" button, the state/analog input value history information older than the specified number of days (24H x specified number of days) counted from the cleanup operation is performed is deleted.
If you specify 0 days, then all data is deleted.

8.23.3 Setting up a cleanup schedule

① Using the main screen, select "Database Cleanup" from the "Options" menu; then select "Schedule Setting".



② The "Cleanup Schedule Setting" screen appears.
The default schedule set up during the install operation specifies that everyday at 1 o'clock, data older than 60 days is deleted.



③ Specify whether to enable the cleanup schedule.
(a) When you select the "Enable" check box, cleanup of the database is performed according to the specified schedule.
(b) If you do not require periodic cleanup, clear the "Enable" check box.

④ Specify the cleanup timing.
(a) Select the "Everyday" radio button if you want to clean up the database everyday, or select the "Everyweek" radio button if you want to clean up the database once every week (on the specified day of the week).
(b) Specify the time of day to clean up the database.

⑤ Specify the cleanup range.
Specify the number of days (24H x specified number of days) counted from the cleanup operation is performed. The state/analog input value history information older than the specified number of days is deleted.
If you specify 0 days, then all data is deleted

⑥ Click the "OK" button. The cleanup schedule becomes effective.

Appendix A: Ports Used

The following shows the ports used by SANUPS IT Monitor Manager.

(1) Ports used by SNMP
The ports used by SNMP are fixed to 161 and 162.

(2) TCP/IP ports used by SANUPS IT Monitor Manager software application
The following TCP/IP port numbers are used for communication between the server and clients and server internal processing. If a firewall is set up between the server and clients, do not block these ports.

Port number	Description
9090	Apache server port
1099	RMI server port
3306	DBMS server port
2000	Server port for IT Monitor Manager framework
8009	Tomcat server port
Dynamic	Information exchange between server and clients, and server internal processing

* "Dynamic" refers to a port that is obtained as a result of a request for an unused port number made to the operating system. Therefore, the port number changes each time the server starts. For this reason, if a firewall is set up, do not block ports 1025 and higher.

<Note>
If the above ports are used by other applications, IT Monitor Manager will not operate properly.
To check whether the above ports are used by other applications, start Command Prompt and use "netstat –a /B" or "netstat –a /B /N." You can check how to use netstat commands with "netstat?."

(3) Port used by SMTP server
The port is fixed at 25.

Appendix B: Explanation Of Events

Event name	Description
Cold start [SNMP TRAP reception] (EV0001)	The SNMP trap of cold start is received.
Linkup [SNMP TRAP reception] (EV0002)	The SNMP trap of linkup is received.
Linkdown [SNMP TRAP reception] (EV0003)	The SNMP trap of linkdown is received.
Analog input threshold deviation occurrence [SNMP TRAP reception] (EV0012)	The SNMP trap of the analog input threshold deviation occurrence is received. (environment monitoring device only)
Analog input threshold deviation recovery [SNMP TRAP reception] (EV0013)	The SNMP trap of the analog input threshold deviation recovery is received. (environment monitoring device only)
Digital input change [SNMP TRAP reception] (EV0014)	The SNMP trap of input change in the digital input is received. (environment monitoring device only)
Digital output implementation [SNMP TRAP reception] (EV0015)	The digital output implementation SNMP trap is received. (environment monitoring device only)
Device parameter change [SNMP TRAP reception] (EV0041)	The device parameter change SNMP trap is received. (environment monitoring device only)
UPS alarm occurrence [SNMP TRAP reception] (EV0022)	The SNMP trap of UPS alarm occurrence is received.
UPS alarm recovery [SNMP TRAP reception] (EV0023)	The SNMP trap of UPS alarm recovery is received.
UPS error occurrence (EV0024)/UPS error recovery (EV0025)	A UPS fault occurrence or recovery is detected when the state is checked as forced upon by reception of the SNMP trap or as required in a regular interval.
UPS analog input threshold deviation occurrence (EV0026)/UPS analog input threshold deviation recovery (EV0027)	A UPS analog input threshold deviation occurrence or recovery is detected when the state is checked as forced upon by reception of the SNMP trap or as required in a regular interval.
UPS warning occurrence (EV0031)/UPS warning recovery (EV0032)	A warning occurrence or recovery is detected when the state is checked as forced upon by reception of the SNMP trap or as required in a regular interval.
UPS battery operation [SNMP TRAP reception] (EV0034)	The SNMP trap of UPS battery operation is received.
UPS battery check end [SNMP TRAP reception] (EV0033)	The SNMP trap of UPS battery check end is received.

Event name	Description
Authentication failure [SNMP TRAP reception] (EV0035)	The SNMP trap of authentication failure is received.
Communication error occurrence (EV0004)/Communication error recovery (EV0005)	A communication error occurrence or recovery is detected when the state is checked as forced upon by reception of the SNMP trap or as required in a regular interval.
Digital input change (fault occurrence) (EV0016)/Digital input change (fault recovery) (EV0017)	A digital input occurrence or recovery is detected when the state is checked as forced upon by reception of the SNMP trap or as required in a regular interval. (environment monitoring device only)
Digital input change (EV0030)	A digital input change (not treated as fault) is detected when the state is checked as forced upon by reception of the SNMP trap or as required in a regular interval. (environment monitoring device only)
Analog input threshold deviation occurrence (EV0018)/Analog input threshold deviation recovery (EV0019)	An analog input threshold deviation occurrence or recovery of the environment monitoring device is detected when the state is checked as forced upon by reception of the SNMP trap or as required in a regular interval. (environment monitoring device only)
Device parameter change detection (EV0011)	The data obtained by the device parameter is detected to be different from that obtained when the state is checked as forced upon by reception of the SNMP trap or as required in a regular interval. (environment monitoring device only)
Device parameter setting/control failure (CEV0021)	The client tries but fails to write to the MIB of the device.
Schedule control start (EV0037)/Schedule control end (EV0040)	The schedule control operation has started or ended on the server.
Schedule implementation (success) (EV0038)/Schedule implementation (failure) (EV0039)	Control of individual controls specified by schedule control succeeds or fails.

Event name	Description
Data backup start (EV0006)/Data backup end (EV0007)	The data backup operation has started or ended on the server.
Data cleanup start (EV0008)/Data cleanup end (EV0009)	The data cleanup operation has started or ended on the server.
Fault notification server command implementation (EV0010)	The fault occurrence or recovery notification command has been executed on the server.

Appendix C: Questions &Answers

Question	Answer
I want to change the community name of a device. What is a good procedure to use?	① Run the Web applet, and then give the device a new community name. ② Use the management information setting of the target device to change the community name.
I want to change the IP address of the machine where SANUPS IT Monitor Manager is installed. What are some points I need to take note of?	For all devices targeted for monitoring, on the machine permitting SNMP access setting, the IP address of the machine where SANUPS IT Monitor Manager is installed must be changed. Also, if the SANUPS IT Monitor Manager server is set as the SNMP trap transmission destination of a device, then its setting must also be changed.
How can I find out the version of firmware of a device?	From the "Consolidated Monitoring" tree view, select "Consolidated Monitoring". "Device Information" of the device operation status list indicates the version of firmware of the device. For an environment monitoring device, the version of firmware is displayed in the format of “ROM:Rom software version, WEB:WEB applet software version”. Also, for UPS, the version of firmware is displayed in the format of “UPS model name (control division version), IF:Agent version”.
What is the hysteresis percentage at deviation monitoring of analog input value?	In analog input deviation monitoring of UPS device, the hysteresis is 10% of the normal range when the device recovers from the deviation state.
What are the names of the SANUPS IT Monitor Manager executable files on the server?	The executable files of SANUPS IT monitor Manager for running on the server are listed below. JavaService.exe is the main service module. This main module starts the following modules: mysqld.exe apach.exe (two)

Appendix D: Troubleshooting

Problem	Solution
A device cannot be added.	See the following possible problems and corresponding solutions: (1) The device to add may not exist at the IP address (or the IP address of the device may be incorrect) -->See the “Adding A Device By Searching For It First” section on page 38 for solutions. (2) The community names set to the device may be different from the READ community name and WRITE community name input when the device was added. -->Start the Web browser, specify the IP address of the device, and then start the Web applet. Alternatively, connect the terminal to the device and then check the community names of the device. If the names are found to be different, perform the procedure described in the "Modifying The Settings Of A Device Added" section on page 42 and then add the device again. (3) In the settings of the device, the SNMP agent function may not be set to "Enable". -->Start the Web browser, specify the IP address of the device, and then start the Web applet. In the SNMP setting of the basic settings, enable the SNMP function. (4) It may be that in the SNMP setting of the device, access permission has not been granted to the machine where the SANUPS IT Monitor Manager software application is installed. -->Start the Web browser, specify the IP address of the device, and then start the Web applet. In the SNMP setting of the basic settings, select “Permit access from all terminals”. If you do not want to give access permission to all machines, set “Permit access only from terminals below” to the machine where the SANUPS IT Monitor Manager software application is installed.

Problem	Solution
The device is in the communication error state.	(1) The community names set at the device may not match the management information (READ community name and WRITE community name) in SANUPS IT Monitor Manager. -->Start the Web browser, specify the IP address of the device, and then start the Web applet. Alternatively, set up a terminal connection with the device and then check the community names of the device. If the names do not match, change the READ community name and WRITE community name. -->See the "Setting Management Information (Device Management Information)" section on page 54 for more information.
The SANUPS IT Monitor Manager software application cannot be uninstalled.	Follow the procedure described in the “Uninstall Procedure” section on page 18 and try to uninstall the software application.
After the IP address of a device is changed, a communication error for the device appears.	If you want to change the IP address of a device, you need to use SANUPS IT Monitor Manager to delete the device first, and then add it back. However, if the device has been registered with a host name, then this procedure is not required. (The new IP address is set automatically).
After the computer returns from the standby or suspend state, its connection to the server is terminated by force.	If the computer is, for example, a notebook computer, when you close its display unit, the computer enters the suspend state to save power. Because communication with the server is disconnected, the SANUPS IT Monitor Manager server deletes the connection with the client by force. In this case, you can solve the problem by connecting to the server again, or change the configuration of the computer so that it does not enter the standby and suspend states.
The server stops soon after being started.	If the IT Monitor Manager service ends abnormally soon after being started, check the settings of Data Execution Prevention (DEP). For details on how to check DEP, see "Appendix I: Data Execution Prevention (DEP) Settings" on page 147.
The client cannot connect to the server.	The reason why the client cannot connect to the server is likely to be due to a problem on the server, client, or network, so check the following. (1) Is the TCP port or UDP port used by the server conflicting with another application? For details on the ports used, see "Appendix A: Ports Used" on page 116. (2) Check whether the settings of Windows Firewall are correct. For details, see "Appendix H: Windows Firewall Settings" on page 132.

A database restore failed.	When you use the database restore function in Windows Vista or a later operating system, User Account Control needs to be disabled. Check whether User Account Control is enabled.
The fault notification popup screen is not displayed on the client.	The fault notification popup screen is not displayed if the client is not running. If the fault notification popup screen is not displayed even when the client is running, check the settings of Windows Firewall on the client. For details, see "Appendix H: Windows Firewall Settings" on page 132.

Appendix E: Glossary

Glossary	Description
Device targeted for monitoring	Refers to a device (environment monitoring device or UPS device) specified for monitoring.
Device operation status list	The device operation status list is a list of devices displayed when the fault device view, environment monitoring device list view, UPS list view or its following custom view is selected.
System log list	It is a list of system log that is displayed when the system log view, device fault history view or its following custom view is selected.
Device addition default information	This information is included by default when a device is added, and contains the following items: ① READ community name for accessing the device ② WRITE community name for accessing the device ③ Polling interval ④ State saving interval This information is used as the default value at the device addition screen and device search screen. This makes input of information when setting each device much easier.

Appendix F: Explanation Of Items Displayed On The Operation Status List

Displayed item	Displayed content
Icon of host name	Icons indicate the state of each device, using different colors. (a) Environment monitoring device icon color · Orange: Communication error · Red: Fault (digital input state or analog input value deviation state defined in the parameter setting function and treated as fault) · Green: Normal (b) UPS device icon color · Orange: Communication error · Red: Fault (fault or analog input value deviation state that is defined in the parameter setting function. The following faults are possible: abnormal battery temperature, charger fault, fan problem, blown fuse, serious fault, and slight fault) · Yellow: Warning (alarm occurrence state that is defined as warning in the UPS warning setting function) · Gray: Power failure · White: Stop (output off) · Green: Startup (output on)
Device type	The following four types are available: (a) For environment monitoring device: indicated as Env (b) For UPS LAN connection: indicated as UPS (c) For MT LAN connection: indicated as UPS (MT) (d) For SGIV Lite: indicated as UPS (Lite)
Installation location	Indicates the content of sysLocation of RFC-1213MIB. It can be changed using the management information setting.
Contact	Indicates the content of sysContact of RFC-1213MIB. It can be changed using the management information setting.
Comment	Indicates the content of sysDescr of RFC-1213MIB.
Polling interval	Indicates the setting content (10 to 65535 seconds) at the management information setting.

Displayed item	Displayed content
State save interval	Indicates the setting content (0 to 65535 seconds) at the management information setting. 0 has a special meaning; the information is saved only when the state of the device changes. For an environment monitoring device, the information is saved only when a change in the state of digital input or in the state of analog input value deviation is detected; for a UPS device, the information is saved only when a change in the state of the SNMP alarm or in the state of analog input value deviation is detected.
Fault content	(a) For environment monitoring device This information is displayed in the format of "Signal name: Deviation" for analog input value, or "Signal name: Status" for digital input. Also, if multiple faults occur, the displayed contents are delimited by a comma, and are displayed in the CH ascending order, starting from analog input, followed by digital input. (b) For UPS device This information is displayed in format of "Signal name: Deviation" for analog input value, or "Alarm name" for error or warning. Also, if multiple faults occur, the displayed contents are delimited by a comma; alarms are displayed first, followed by analog input value deviation. Furthermore, for a list of alarms, see "Appendix G: UPS Alarm List" on page 130.
Group	Indicates the contents of the setting at the management information setting.
Remark	Indicates the contents of the setting at the management information setting.
Digital input state in environment monitoring device list	Indicates the name of the digital input state obtained from the device. However, if the appropriate CH is not valid, then it is displayed as blank.
Digital output state in environment monitoring device list	Indicates the name of the digital output state obtained from the device. However, if the appropriate CH is not valid, then it is displayed as blank; if the signal attribute is pulse, "(None)" is always displayed.

Displayed item	Displayed content
Device information	(a) For an environment monitoring device, this information is displayed in the format of "ROM:ROM software version, WEB:WEB applet software version." (b) For UPS (LAN card connection), this information is displayed in the format of "UPS model name(control division version), IF:Agent version". (c) For UPS (Lite:UPS serial connection or MT:UPS serial connection), this information is displayed in the format of "UPS model name (control division version), IF:Agent version". (d) For UPS (Lite:UPS serial connection, no MT:UPS connection, or digital input connection with UPS), this information is displayed in the format of "IF:Agent version".
State	(a) For an environment monitoring device, "Normal", "Fault occurrence", or "Communication error" is displayed. (b) For UPS device, "Startup (output on)", "Stop (output off)", "Power failure", "Warning", "Fault", or "Communication error" is displayed.
Last update date time	Indicates the start time where the last polling was conducted.
Analog input value information in environment monitoring device list	Indicates the analog input value obtained from the device. However, if the appropriate CH is not valid, then it is displayed as blank. If analog input is not possible, then the value is displayed as "---". Analog input is not possible when the analog input signal is actually not connected.

Displayed item	Displayed content
Power supply state in UPS list	(a) For LAN card connection, Lite serial connection, or MT serial connection, “Inverter”, “Battery”, “Bypass”, or “Stop” is displayed. (b) For Lite digital input connection or MT digital input connection, “Normal”, “Battery”, or “Stop” is displayed. (c) For stand-alone MT, “Normal” or “Stop” is displayed.
UPS name in the UPS list	Indicates the content of upsIdentModel of RFC-1628MIB.
Control unit Ver in UPS list	Indicates the content of upsIdentUPSSoftwareVersion of RFC-1628MIB.
Agent Ver in UPS list	Indicates the content of upsIdentAgentSoftwareVersionof RFC-1628MIB.
Battery operation time in UPS list	Indicates the content of upsSecondsOnBattery of RFC-1628MIB. The unit of measurement is seconds. Furthermore, the display of the value is done when there is polling. (There are two types of polling. Once is a normal polling. The other is forced polling that is performed when TRAP from an appropriate device is received). Furthermore, for MT or Lite, the value remains at 0 and does not change when the following conditions are met: (a) There is a digital input connection with UPS and a battery test is in progress. (The value is updated if power failure occurs). (b) No connection with UPS.

Displayed item	Displayed content
Battery check result for list of UPS	(a) If upsTestResultsSummary of RFC-1628MIB is outside the 1 to 5 range, "Unknown" is displayed. (b) If upsTestResultsSummary of RFC-1628MIB is 1, “Ends with no error” is displayed. (c) If upsTestResultsSummary of RFC-1628MIB is 2, “Ends with error” is displayed. (d) If upsTestResultsSummary of RFC-1628MIB is 3, “Error” is displayed. (e) If upsTestResultsSummary of RFC-1628MIB is 4, “Test aborted” is displayed. (f) If upsTestResultsSummary of RFC-1628MIB is 5, “Test in progress” is displayed. * For cases from (b) to (e), only if the server detects an alarm (upsAlarmTestInProgress) indicating the battery check is in progress, it includes the server time at that moment in a message such as “Battery test start time:Test in progress”. Furthermore, "the server detects an alarm (upsAlarmTestInProgress) indicating the battery check is in progress" means addition of upsAlarmTestInProgress to upsAlarmTable is detected. If the LAN card, MT, and Lite have a cold start, the (a) state stays temporarily for a while and, therefore, the battery check start date time information is lost.

Appendix G: UPS Alarm List

Displayed content	Display condition (applicable alarm on upsAlarm of RFC1628MIB)
Battery life (AL0001)	Displayed when upsAlarmBatteryBad exists.
Battery operation (AL0002)	Displayed when upsAlarmOnBattery exists.
Low battery voltage (AL0003)	Displayed when upsAlarmLowBattery exists.
upsAlarmDepletedBattery (AL0019)	Displayed when upsAlarmDepletedBattery exists. Currently, this alarm does not occur on SANYO DENKI products.
Battery temperature trouble (AL0004)	Displayed when upsAlarmTempBad exists. This alarm is treated as a fault alarm.
Power failure (AL0005)	Displayed when upsAlarmInputBad exists.
upsAlarmOutputBad (AL0020)	Displayed when upsAlarmOutputBad exists. Currently, this alarm does not occur on SANYO DENKI products.
Overload (AL0007)	Displayed when upsAlarmOutputOverload exists.
Bypass operation (AL0008)	Displayed when upsAlarmOnBypass exists.
Bypass trouble (AL0006)	Displayed when upsAlarmBypassBad exists.
Waiting for UPS stop (AL0009)	Displayed when upsAlarmOutputOffAsRequested exists.
upsAlarmUpsOffAsRequested (AL0021)	Displayed when upsAlarmUpsOffAsRequested exists. Currently, this alarm does not occur on SANYO DENKI products.
Battery charger breakdown (AL0010)	Displayed when upsAlarmChargerFailed exists. This alarm is treated as a fault alarm.
Output OFF (AL0011)	Displayed when upsAlarmUpsOutputOff exists.
UPS system OFF (AL0012)	Displayed when upsAlarmUpsSystemOff exists.
Fan temperature trouble (AL0013)	Displayed when upsAlarmFanFailure exists. This alarm is treated as a fault alarm.
Bypass breaker OFF (Fuse Failure) (AL0014)	Displayed when upsAlarmFuseFailure exists. This alarm is treated as a fault alarm.
General Fault (AL0015) (alarms other than those treated as faults)	Displayed when upsAlarmGeneralFault exists. However, the display is withheld if alarms (other than this alarm) treated as fault alarms (such as abnormal battery temperature, charger fault, fan problem bypass breaker OFF) occur.

Displayed content	Display condition (applicable alarm on upsAlarm of RFC1628MIB)
upsAlarmDiagnosticTestFailed (AL0022)	Displayed when upsAlarmDiagnosticTestFailed exists. Currently, this alarm does not occur on SANYO DENKI products.
Internal com. Trouble (AL0017)	Displayed when upsAlarmCommunicationsLost exists.
Battery test (Test in Progress) (AL0016)	Displayed when upsAlarmTestInProgress exists.
upsAlarmAwaitingPower (AL0023)	Displayed when upsAlarmAwaitingPower exists. Currently, this alarm does not occur on SANYO DENKI products.
Reception of UPS stop request (AL0018)	Displayed when upsAlarmShutdownPending exists.
upsAlarmShutdownImminent (AL0024)	Displayed when upsAlarmShutdownImminent exists. Currently, this alarm does not occur on SANYO DENKI products.
Alarm Unknown (AL9999)	Displayed when the content of the alarm cannot be determined because the alarm number actually obtained is smaller than the counter value, after the counter of upsAlarm is looked up.

Appendix H: Windows Firewall Settings

Windows Firewall is a function that comes standard in the following operating systems.

- Windows XP: SP2 or later
- Windows Server 2003: SP1 or later
- Windows Vista
- Windows Server 2008
- Windows 7

When using IT Monitor Manager in any of the above operating systems, you need to change the settings of Windows Firewall for each of the server and clients.

(1) Settings on server

On the server, you need to ensure that the following five program files are not blocked by Windows Firewall. %WinDir% is an environment variable that indicates the location where the operating system is installed. Also, replace "*IT Monitor Manager installation folder*" with the path that matches your environment. This is usually "c:\Program files\SANYODENKI\SANUPS IT Monitor Manager".

- %WinDir%\JavaService.exe
- *IT Monitor Manager installation folder*\apache\apache.exe
- *IT Monitor Manager installation folder*\MySql\bin\mysqld.exe
- *IT Monitor Manager installation folder*\jre1.3\bin\java.exe
- *IT Monitor Manager installation folder*\jre1.3\bin\javaw.exe

For details on how to ensure program files are not targets for blocking by Windows Firewall, see "(3) How to ensure program files are not targets for blocking by Windows Firewall."

(2) Settings on client

On the client, you need to ensure that the following two program files are not blocked by Windows Firewall. Also, replace "*IT Monitor Manager installation folder*" with the path that matches your environment. This is usually "c:\Program files\SANYODENKI\SANUPS IT Monitor Manager".

- *IT Monitor Manager installation folder*\jre1.3\bin\java.exe
- *IT Monitor Manager installation folder*\jre1.3\bin\javaw.exe

For details on how to ensure program files are not targets for blocking by Windows Firewall, see "(3) How to ensure program files are not targets for blocking by Windows Firewall."

(3) How to ensure program files are not targets for blocking by Windows Firewall
There are two ways to ensure program files will not be blocked by Windows Firewall.

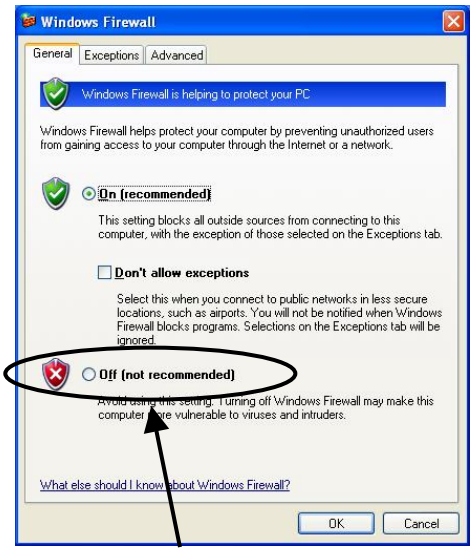
Method 1: Disable Windows Firewall
Method 2: Leave Windows Firewall enabled and add the program files to the Exceptions list

The following explains the operating procedure for each operating system. In any of these cases, stop the client and server of IT Monitor Manager beforehand.

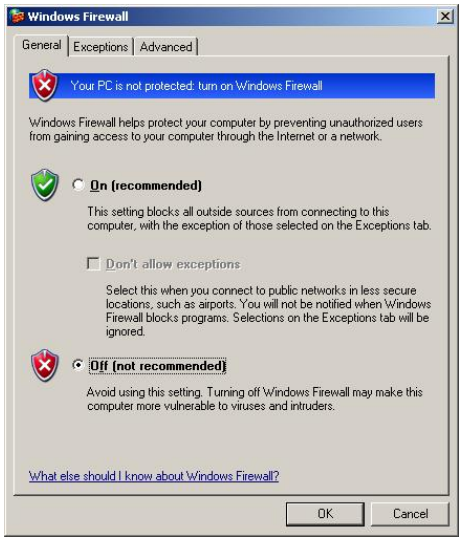
(A) Operation in Windows XP/Windows Server 2003

[Procedure for method 1]

① Start Windows Firewall from the Control Panel.



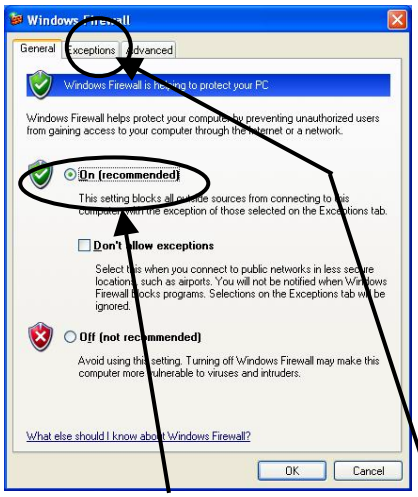
② Select "Off", and then select "OK".



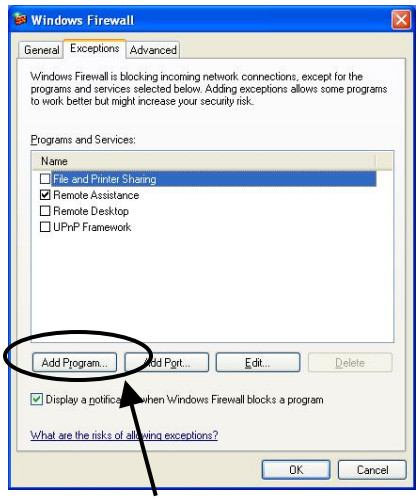
This completes the operation.

[Procedure for method 2]

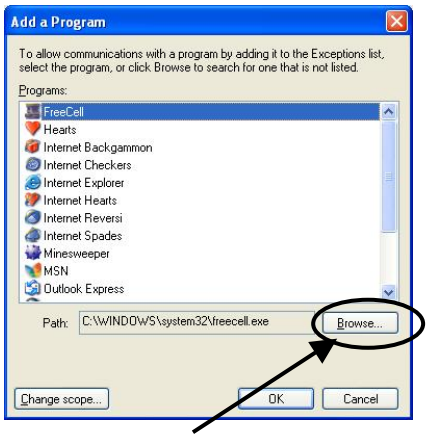
① Start Windows Firewall from the Control Panel.



② Select "On", and then select "Exceptions".

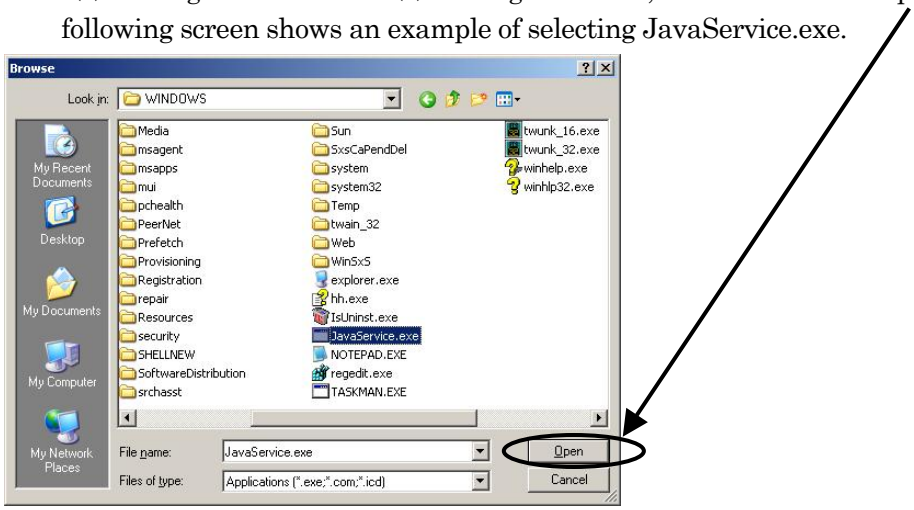


③ Select "Add Program".

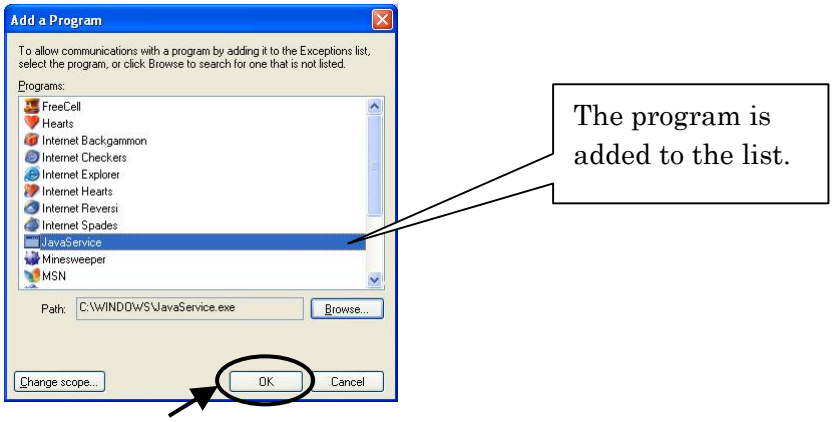


④ Select "Browse".

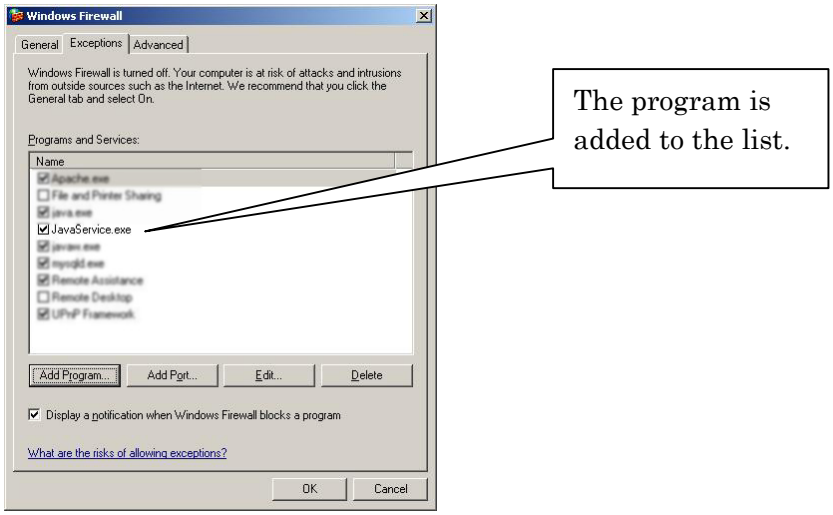
⑤ In the Browse dialog box, select one of the program files specified previously in "(1) Settings on server" or "(2) Settings on client," and then select "Open". (The following screen shows an example of selecting JavaService.exe.



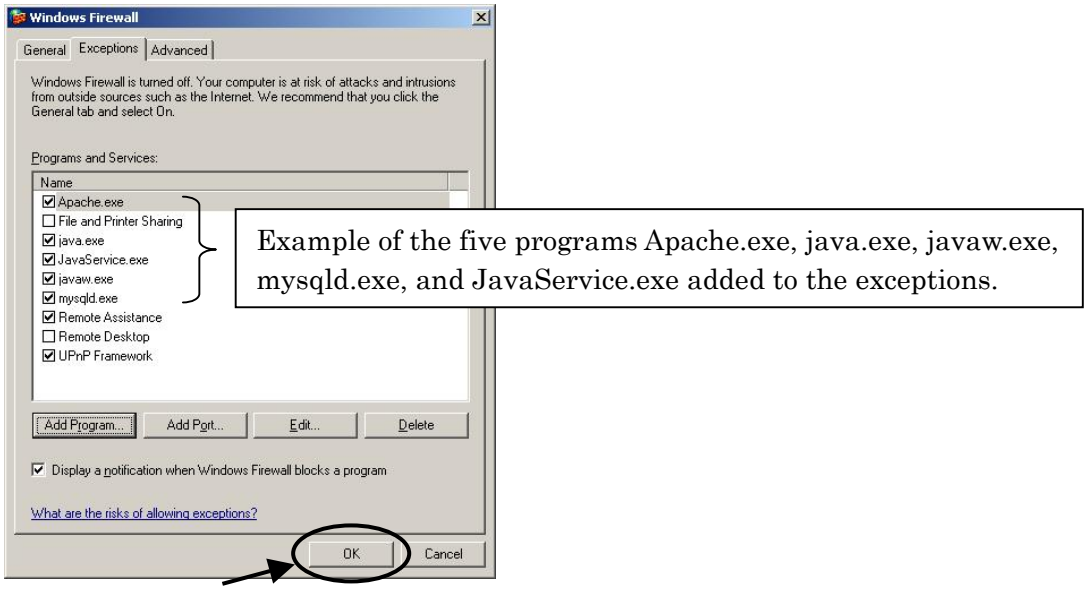
⑥ The file selection dialog closes and the Add a Program screen is redisplayed. (The following screen shows an example of the JavaService.exe program added to the Add a Program screen.)



⑦ Select "OK". This operation adds the program file to the Exceptions list of Windows Firewall.



⑧ Perform steps ③ to ⑦ for all of the program files specified previously in "(1) Settings on server" or "(2) Settings on client."



⑨ Select "OK".

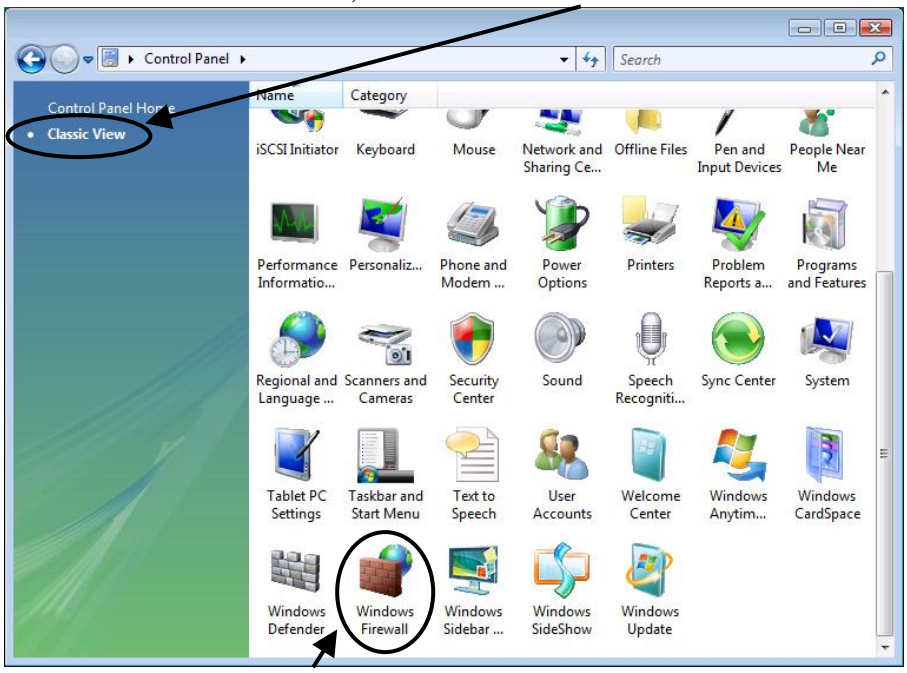
This completes the operation.

(B) Operation in Windows Vista/Windows Server 2008

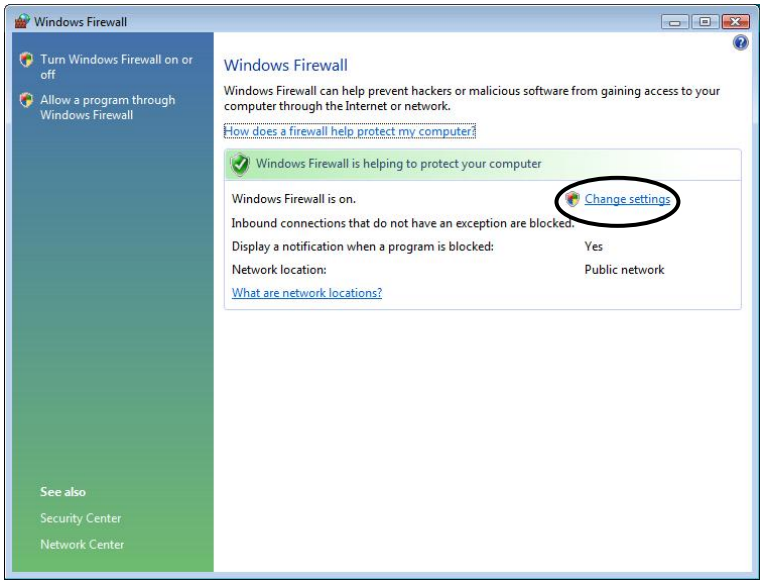
In Windows Vista/Windows Server 2008, the operation up until displaying the Windows Firewall screen differs, but the operation in the Windows Firewall screen is the same as that of Windows XP. Therefore, the following explains the procedure up until displaying the Windows Firewall screen.

[Procedure]

① Start the Control Panel, and then select "Classic View".

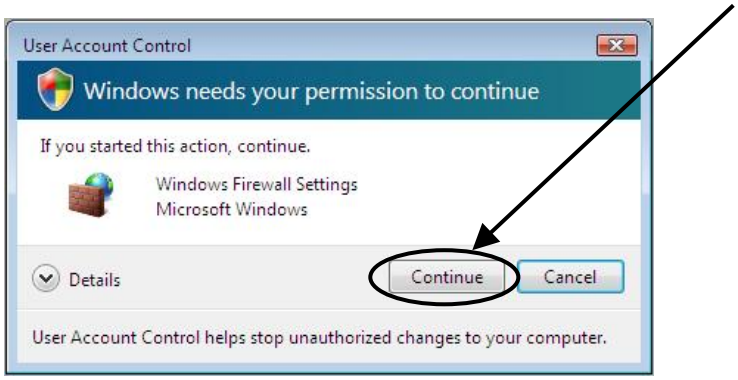


② Select "Windows Firewall".



③ Select "Change settings".

④ When the confirmation dialog box appears, select "Continue".



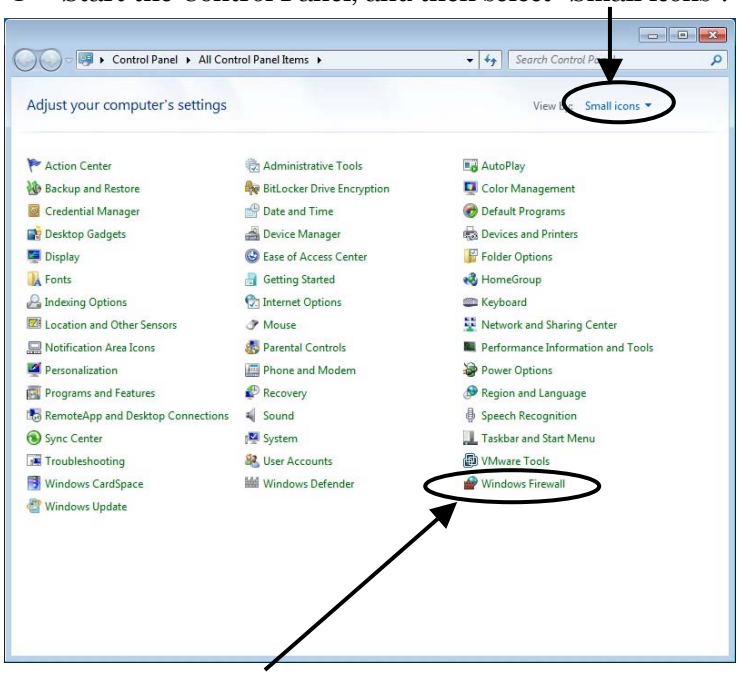
⑤ The Windows Firewall screen appears.

⑥ The subsequent operation is the same as that described in the procedure for Windows XP above.

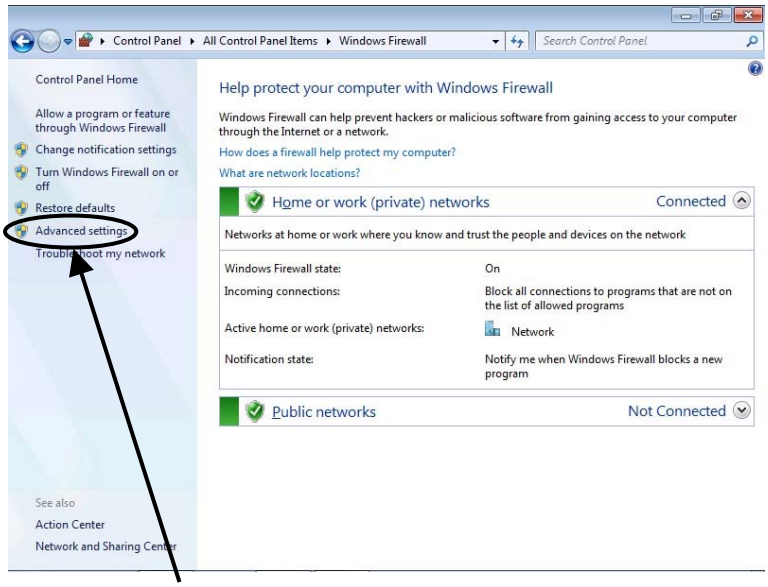
(C) Operation in Windows 7/Windows Server 2008 R2

[Procedure for method 1]

① Start the Control Panel, and then select "Small icons".

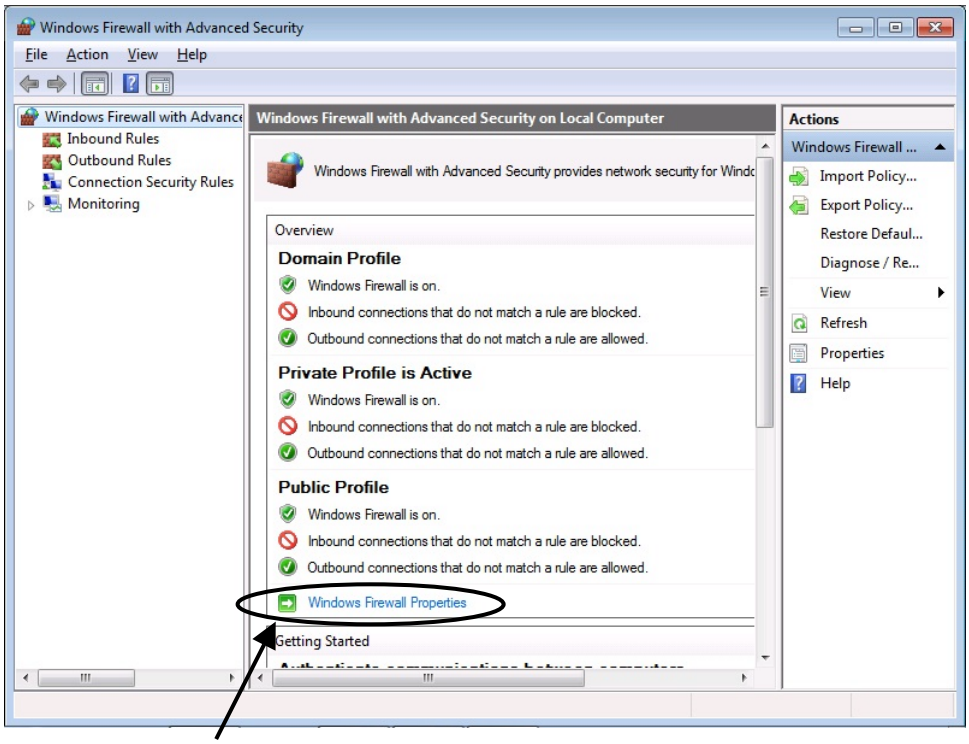


② Select "Windows Firewall".

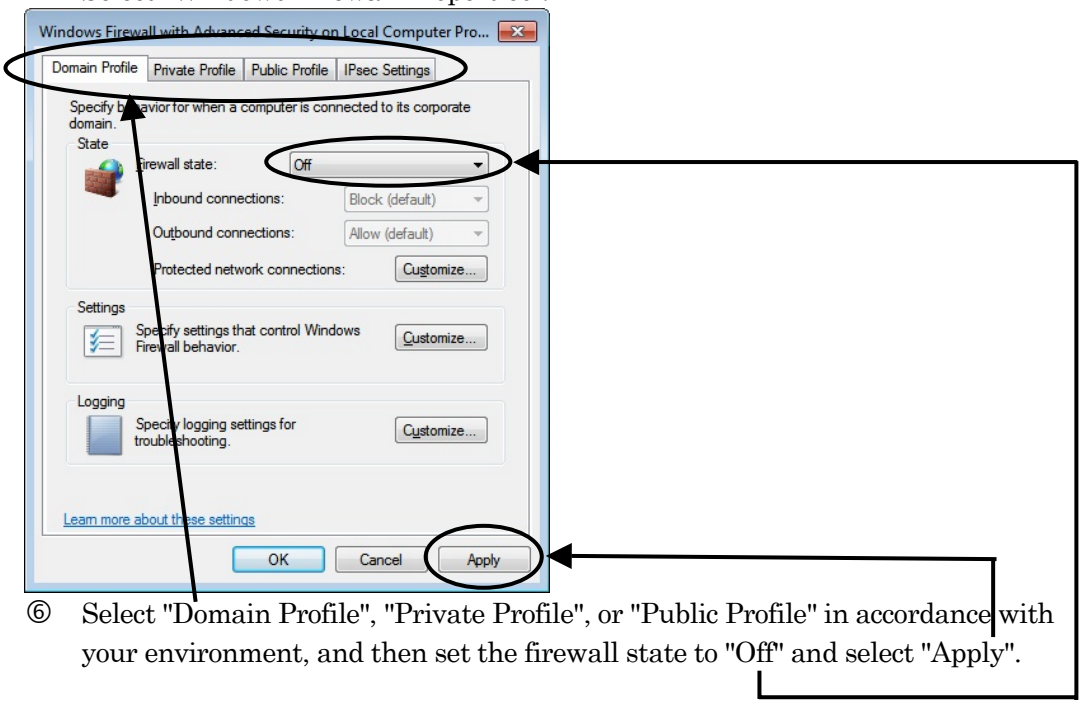


③ Select "Advanced settings".

④ The "Windows Firewall with Advanced Security" screen appears.



⑤ Select "Windows Firewall Properties".

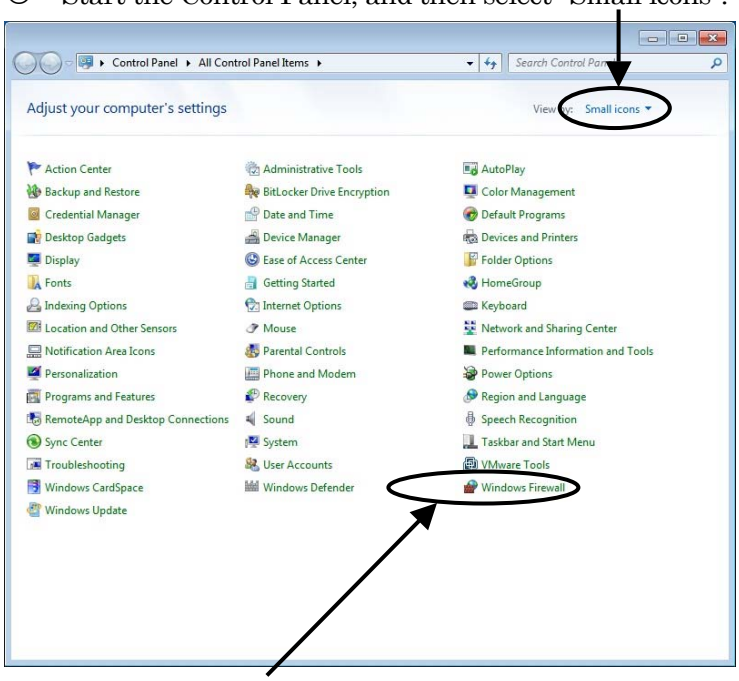


⑥ Select "Domain Profile", "Private Profile", or "Public Profile" in accordance with your environment, and then set the firewall state to "Off" and select "Apply".

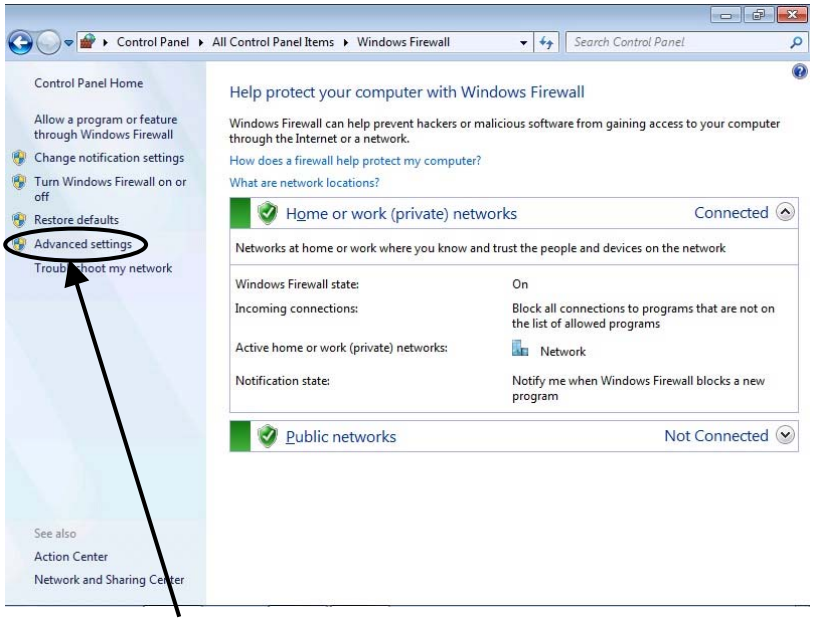
This completes the operation.

[Procedure for method 2]

① Start the Control Panel, and then select "Small icons".

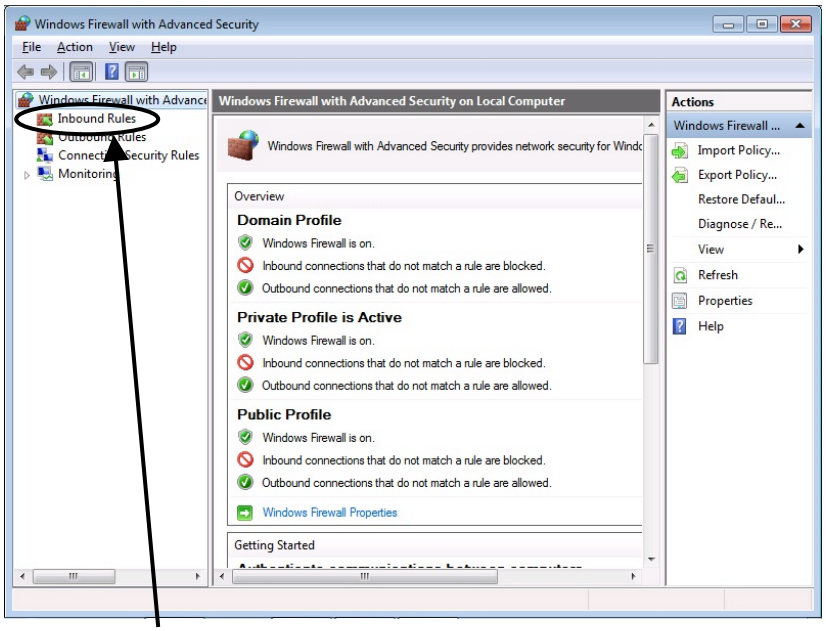


② Select "Windows Firewall".

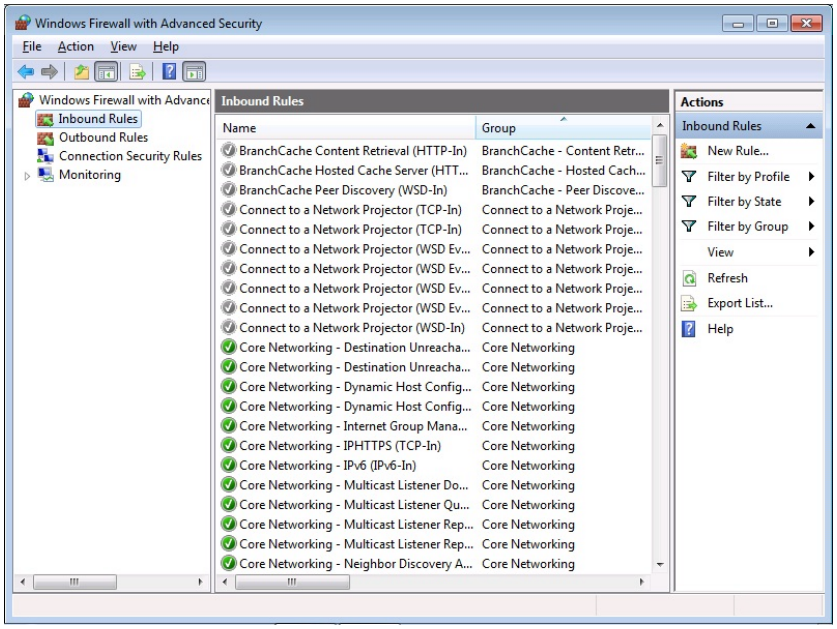


③ Select "Advanced settings".

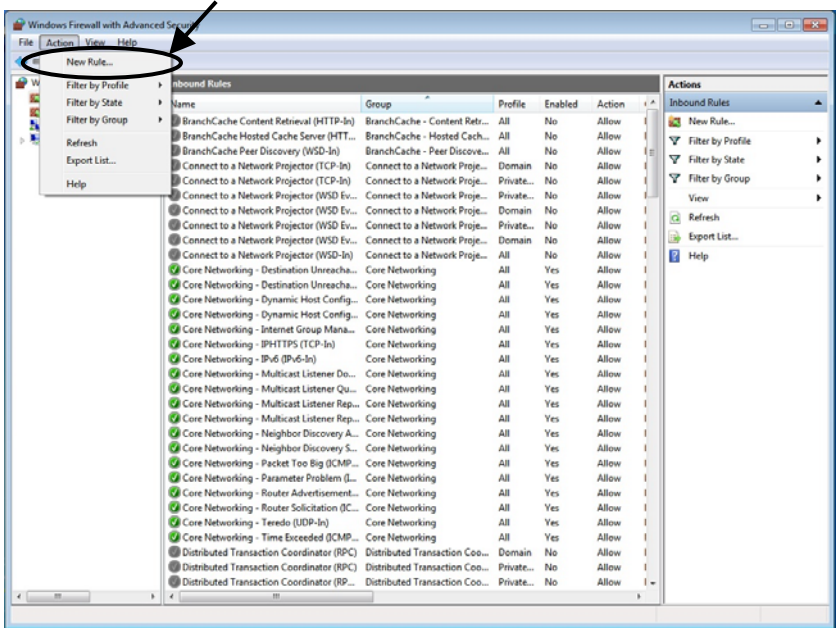
④ The "Windows Firewall with Advanced Security" screen appears.



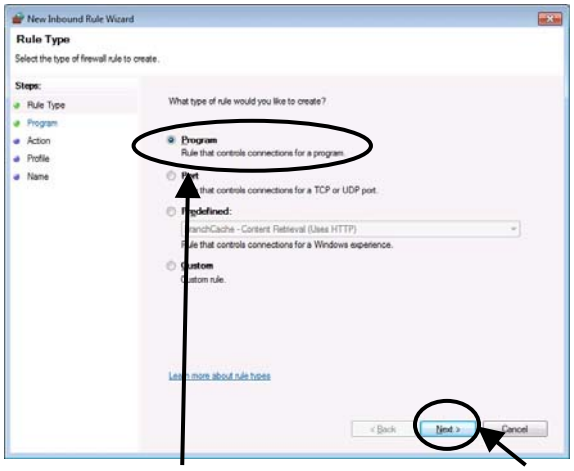
⑤ Select "Inbound Rules".



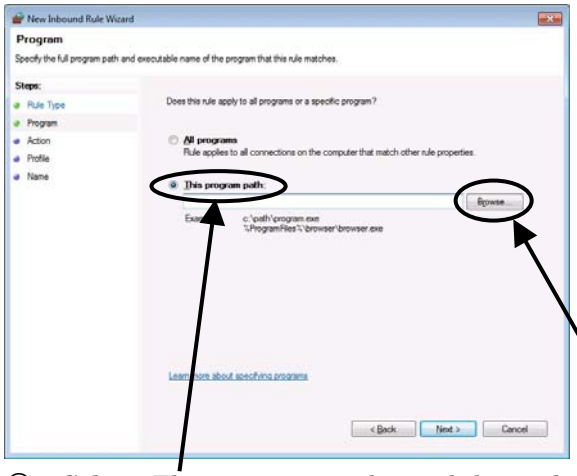
⑥ Select "New Rules" from the Action menu.



⑦ The New Inbound Rule Wizard appears.

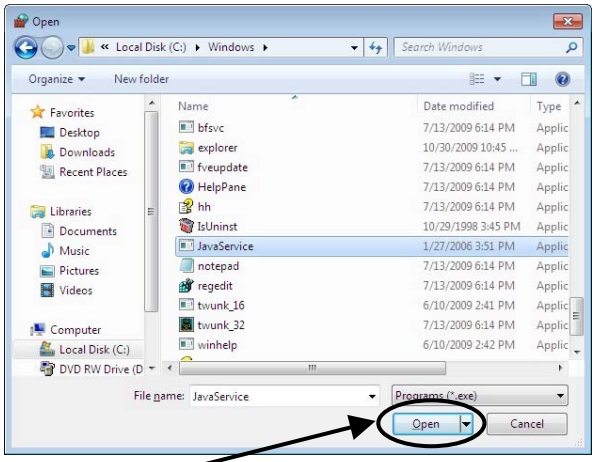


⑧ Select "Program", and then select "Next".

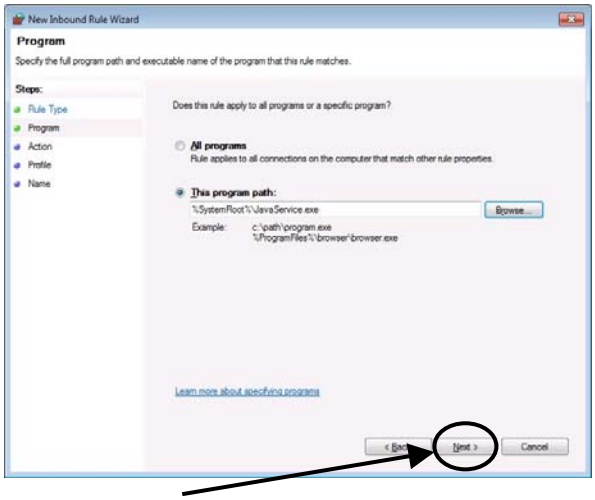


⑨ Select "This program path", and then select "Browse".

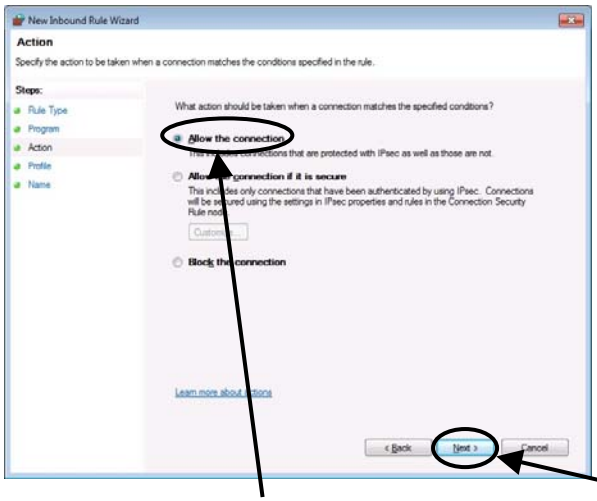
⑩ In the file browse dialog box, select one of the program files specified previously in "(1) Settings on server" or "(2) Settings on client," and then select "Open". (The following screen shows an example of selecting JavaService.exe.



⑪ Select "Open".

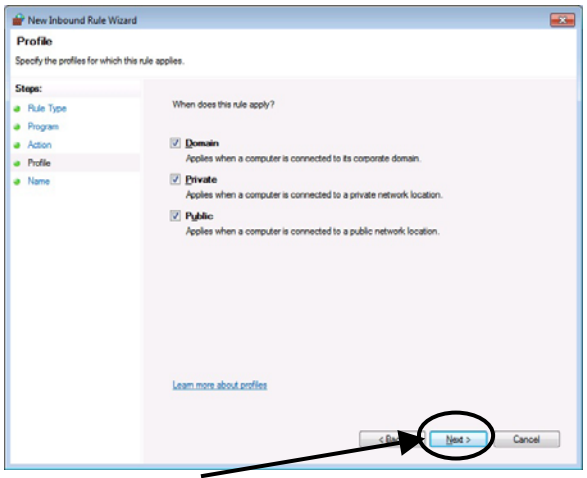


⑫ Select "Next".

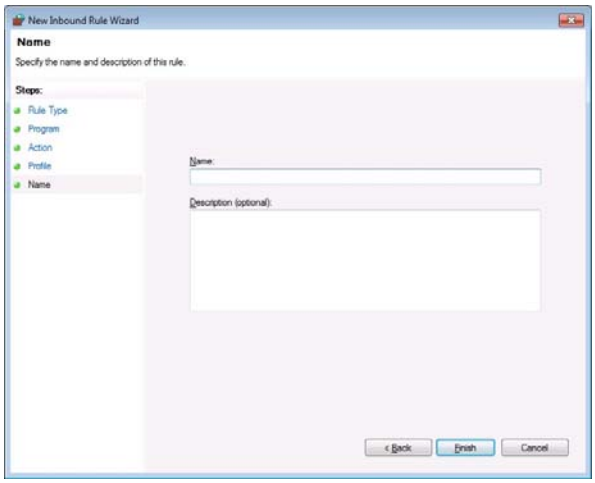


⑬ Select "Allow the connection", and then select "Next".

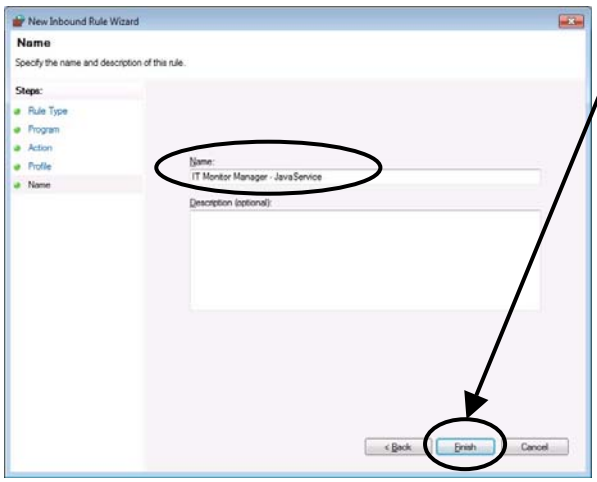
⑭ Select the check boxes for when to apply this rule in accordance with your environment.



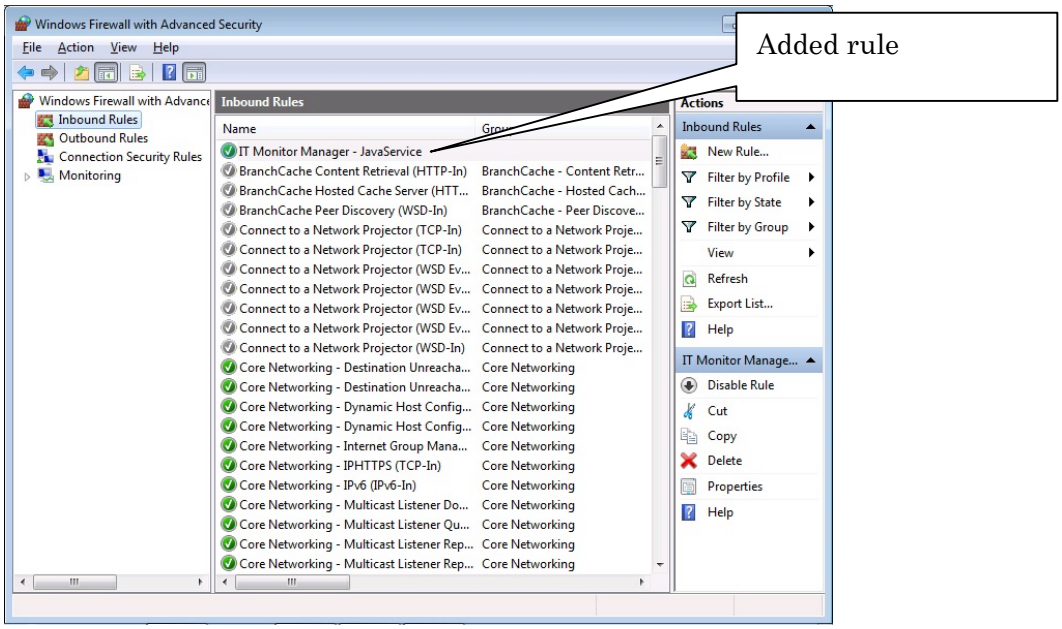
⑮ Select "Next".



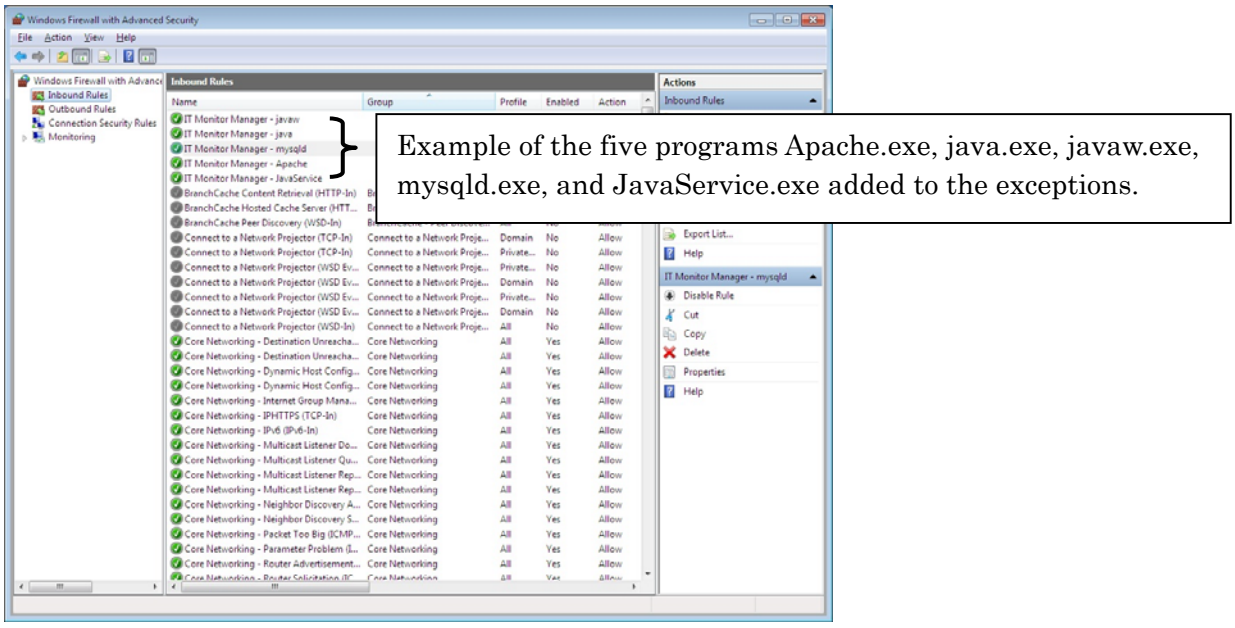
⑯ Enter any name for the rule, and then select "Finish".



⑰ The rule is added when step ⑯ is performed.



⑱ Perform steps ⑥ to ⑯ for all of the program files specified previously in "(1) Settings on server" or "(2) Settings on client."



This completes the operation.

Appendix I: Data Execution Prevention (DEP) Settings

Data Execution Prevention is a function that comes standard in the following operating systems.

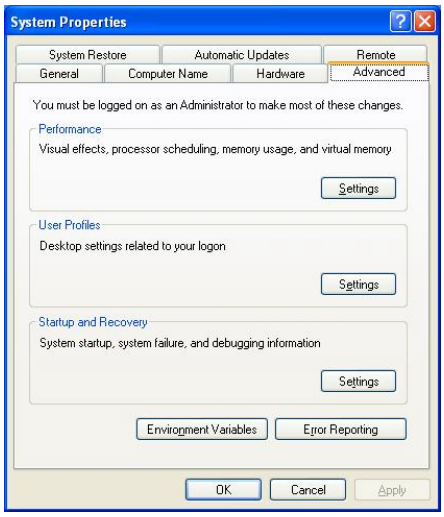
- Windows XP: SP2 or later
- Windows Server 2003: SP1 or later (including R2)
- Windows Vista
- Windows Server 2008 (including R2)
- Windows 7

When using IT Monitor Manager in any of the above operating systems, you need to change the settings of Data Execution Prevention for each of the server and clients.

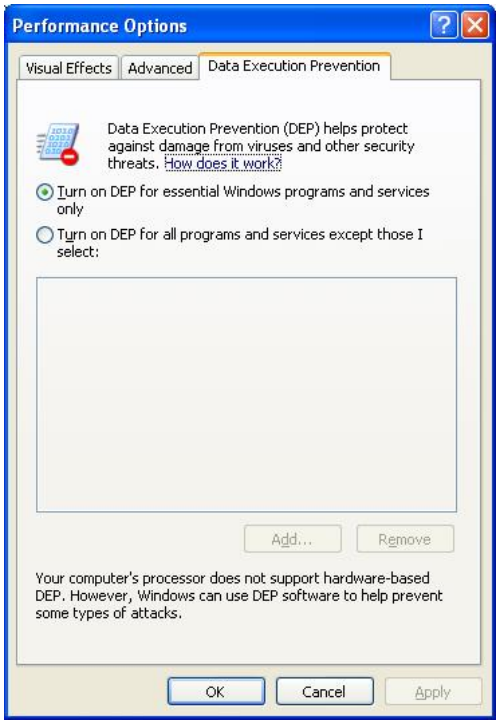
The following explanation uses Windows XP as an example. Perform the equivalent operation in another operating system.

[Procedure]

① Start "System" from the Control Panel, and then display the advanced settings.



② Select "Settings" of Performance, and then display Data Execution Prevention.



③ Select "Turn on DEP for essential Windows programs and services only", and then select "OK".

This completes the operation.

Appendix J: User Account Control (UAC) Settings

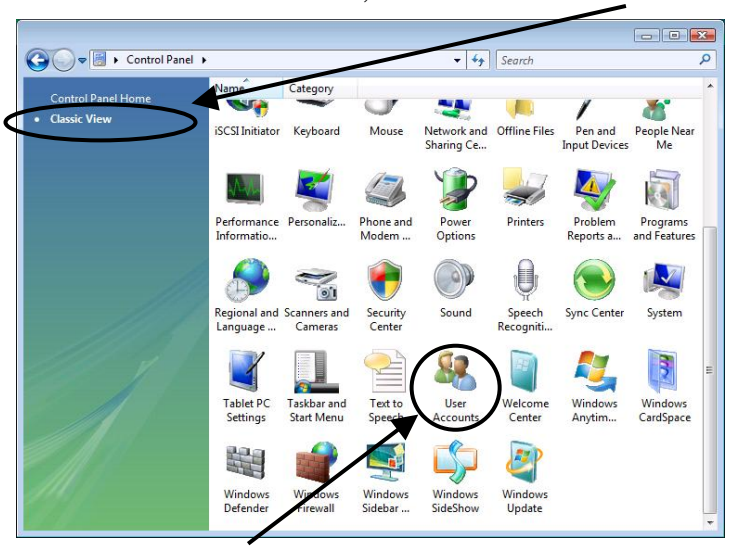
User Account Control is a function that comes standard in the following operating systems.

- Windows Vista
- Windows Server 2008 (including R2)
- Windows 7

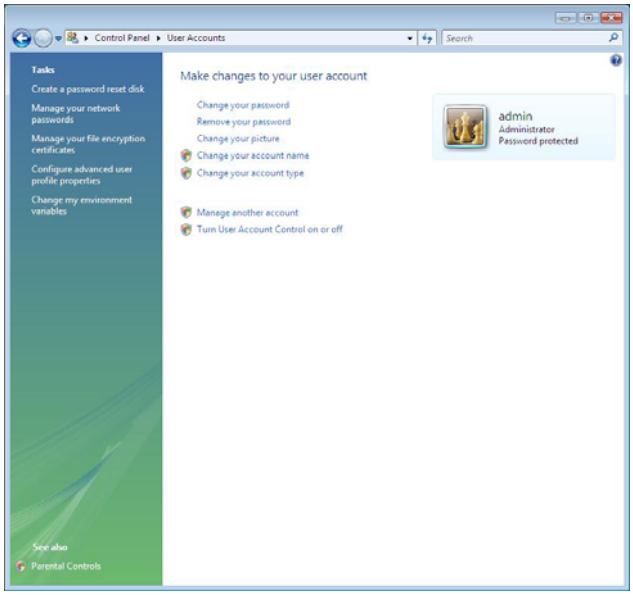
When using IT Monitor Manager in any of the above operating systems and performing a database restore, you need to change the settings of User Account Control on the server.

[Procedure in Windows Vista or Windows Server 2008]

① Start the Control Panel, and then select "Classic View".

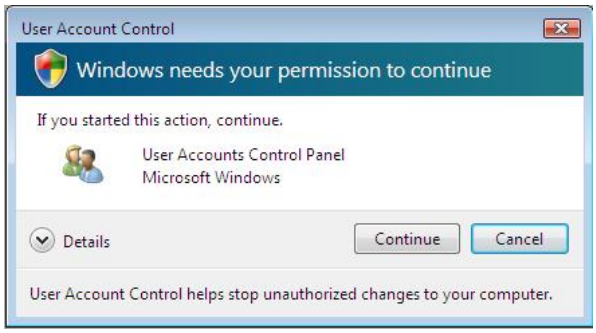


② Select "User Accounts".

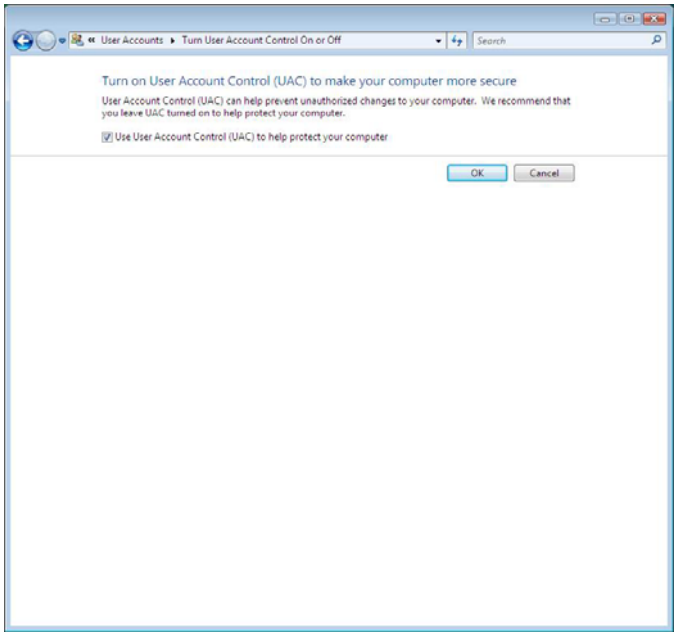


③ Select "Turn User Account Control on or off".

④ When the confirmation dialog box appears, select "Continue".



⑤ Clear the check mark from the "Use User Account Control (UAC) to help protect your computer" check box, and then select "OK".

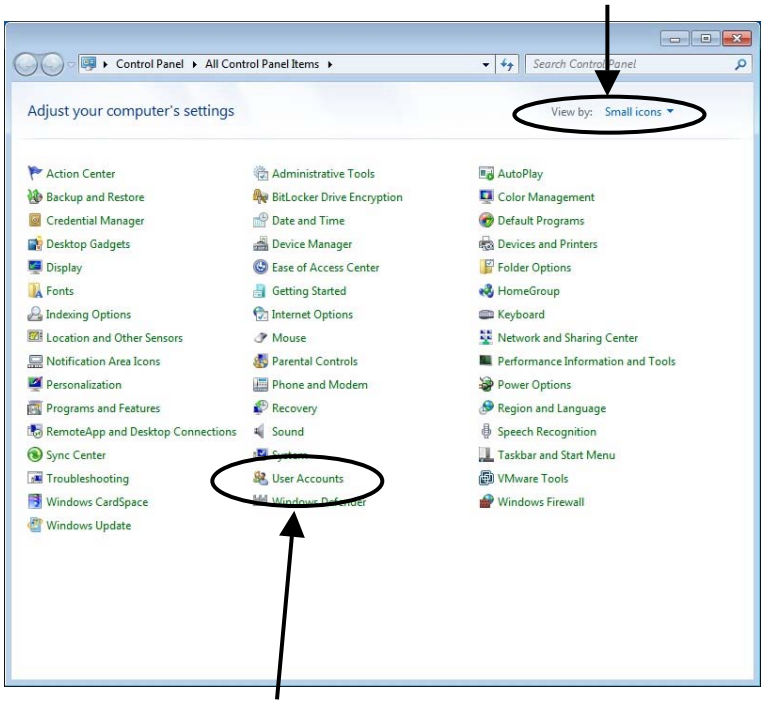


⑥ Restart the operating system.

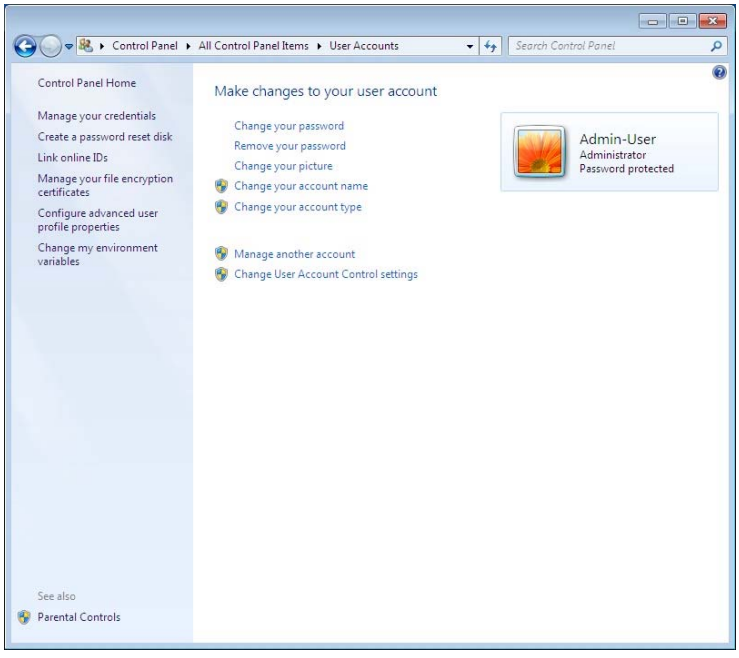
This completes the operation.

[Procedure in Windows 7 or Windows Server 2008 R2]

① Start the Control Panel, and then select "Small icons".



② Select "User Accounts".

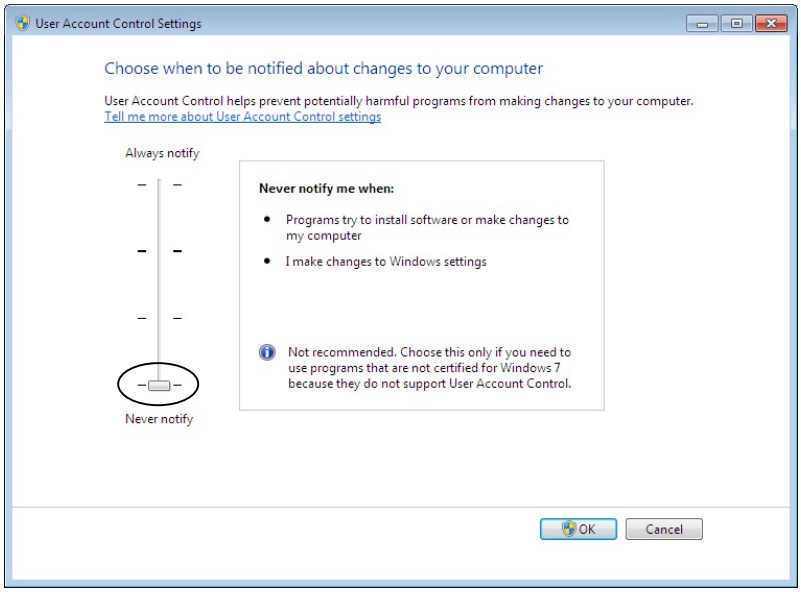


③ Select "Change User Account Control settings".

④ When the confirmation dialog box appears, select "Yes".



⑤ Drag the bar to move it to the bottom, and then select "OK".



⑥ Restart the operating system.

This completes the operation.