

NEC



NEC Express5800 Series
NEC ESMPRO Manager Ver.4.2
User's Guide

5-2005
ONL-x64-COMMON-127-99-0505

PROPRIETARY NOTICE AND LIABILITY DISCLAIMER

The information disclosed in this document, including all designs and related materials, is the valuable property of NEC, Inc. (NEC) and/or its licensors. NEC and/or its licensors, as appropriate, reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use, and sales rights thereto, except to the extent said rights are expressly granted to others.

The NEC product(s) discussed in this document are warranted in accordance with the terms of the Warranty Statement accompanying each product. However, actual performance of each such product is dependent upon factors such as system configuration, customer data, and operator control. Since implementation by customers of each product may vary, the suitability of specific product configurations and applications must be determined by the customer and is not warranted by NEC.

To allow for design and specification improvements, the information in this document is subject to change at any time, without notice. Reproduction of this document or portions thereof without prior written approval of NEC is prohibited.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Mylex is a registered trademark of LSI Logic Corporations of the U.S.

"OpenView" and "HP OpenView" are registered trademarks of HEWLETT PACKARD.

All other product, brand, or trade names used in this publication are the trademarks or registered trademarks of their respective trademark owners.

Contents

Chapter 1 Introducing the NEC ESMPRO	1
Functions and Features	1
Configuration.....	2
System Requirements	3
Chapter 2 Installing the ESMPRO Manager	4
Before Installing	4
About a Virtual Directory the Web Component Creates	4
Setting of Network Services.....	4
Setting Up the NEC ESMPRO User Group	4
Installing IIS.....	5
Installing HP OpenView Network Node Manager	5
Installation	6
Installing the Manager Software	6
Adding/Removing the optional Component.....	9
Chapter 3 Using the ESMPRO Manager	10
Starting the ESMPRO Manager.....	10
Tool Bar and Menus	11
Detecting Agents Automatically.....	12
Changing Agent Properties.....	13
Adding an Icon Manually.....	13
Changing an Icon	14
Creating an Icon Type	15
Changing the Popup Menu.....	16
Setting Up Inter-Manager Communication	17
Monitoring Agents.....	22
Browsing MIF.....	23
Screen.....	23
Browsing MIB	25
Installing Vendor Extension MIB	26
Chapter 4 Alert Viewer	27
Accessing the Alert Viewer.....	27
Message Notification	29
Getting More Details	30
Finding and Sorting Alert Messages.....	31
Sorting Alert Messages.....	31
Filtering Alert Messages.....	32
Configuring the Alert Viewer	32
Setting Notification Options.....	33
Receiving SNMP Traps.....	35
Forwarding Alert Messages.....	36
Alert Log Auto Save Settings.....	36

Chapter 5 Data Viewer	37
Setting Threshold Limits.....	39
How Threshold Limits and Reset Values Work.....	40
Fatal and Warning Limits	40
Local Polling.....	41
Mylex GAM Launcher View	43
Creating Graphs	44
Automatic Data Collection	45
Setting Up Automatic Data Collection	45
Saving Data with the ODBC Interface	46
Printing Statistical Data	48
Chapter 6 Web Component.....	49
About the Web Component.....	49
Getting Started	50
Setting a User Authority	50
Checking the Operation of the Web Component	51
Before You Manage Server(s) via Web Browser	52
Re-creating the Virtual Directory for the Web Component	52
Operation Window	53
Starting the Operation Window	53
Registering a Server to be Managed.....	55
Monitoring the Server Status	62
AlertViewer.....	63
Starting the AlertViewer	63
Viewing a Detailed Alert Information	64
DataViewer	65
Displaying a Server Configuration Information	65
Customizing the Monitoring Item Set	67
Agent Control Panel.....	68
Starting the Agent Control Panel	68
Changing the Operational Settings	69
Remote Wake Up	81
Remote Shutdown.....	82
Remotely Shutting Down a Managed Server	82
Setting the Agent Settings.....	83
Chapter 7 HP OpenView Integration	84
ABOUT THE HP OPENVIEW INTEGRATION	84
GETTING STARTED.....	84
Setting a method of receiving SNMP traps.....	84
Before auto-discovering of NEC ESMPRO Agent.....	84

- USING HP OPENVIEW INTEGRATION 85
 - Auto-discovering NEC ESMPRO Agent..... 85
 - Monitoring the NEC ESMPRO Agent status 85
 - Deleting NEC ESMPRO Agent..... 85
 - Launching DataViewer 85
 - Launching Operation Window 85
 - Launching AlertViewer 86
 - Displaying NEC ESMPRO Agent traps 86
- Appendix A Inter-Manager Communication.....87**
- Appendix B Note.....89**
 - Manager 89
 - Web Component 97

About This Guide

The NEC ESMPRO monitors the configuration, failures, and performance of systems across a network. This user's guide is intended for the system administrator and describes ESMPRO capabilities, installation, features, and use.

This manual is comprised of the following chapters.

- Chapter 1, Introducing NEC ESMPRO, describes ESMPRO features, configuration and system requirements.
 - Chapter 2, Installing the ESMPRO Manager, provides instructions for getting the appropriate network protocols running, creating a user group called the NEC ESMPRO User Group, and installing the Manager software on the system to be used for monitoring Agents across the network.
 - Chapter 3, Using the ESMPRO Manager, explains how to start the ESMPRO Manager, set up a network maps, use toolbars and buttons, and get most out of the ESMPRO Manager.
 - Chapter 4, Alert Viewer, describes how to access and read the Alert Log, sort the Alert list, and interpret Alert data.
 - Chapter 5, Data Viewer, provides details about checking hardware and software features on Agents being monitored, printing reports and statistical data, setting thresholds, and creating graphs.
 - Chapter 6, Web Component, describes how to use the Web Component.
 - Chapter 7, HP OpenView Integration, explains how to use the HP OpenView Integration.
 - Appendix A, Inter-Manager Communication, describes the communication capabilities between network type and community levels.
 - Appendix B, Note
-

Chapter 1

Introducing the NEC ESMPRO

The NEC ESMPRO (referred to as ESMPRO hereafter) lets a system administrator manage remote servers across a network. ESMPRO monitors server hardware and software configurations, failures, and performance. With log data collected by ESMPRO, a system administrator can track long-term and short-term performance, monitor server usage, create graphs to record trends, and check server failure rates. The administrator can use the information collected to create more efficient data routing procedures and optimize server usage.

FUNCTIONS AND FEATURES

The ESMPRO offers many functions and features for managing remote servers across a network. These features help the system administrator perform daily system operation, system extension, and transfer tasks. Some features of ESMPRO Manager include:

- Hardware and software server configuration
 - Hardware resources mounted in servers, such as the CPU, memory, disks, disk arrays, and LAN boards.
 - Software resources, such as operating system information and drivers running on each server.
 - Server failures
 - On-screen real-time displays provide the system administrator with the failure type, location, cause, and suggested corrective action.
 - Failure data includes hardware failure information such as system board temperature, memory failure, crashes, and software failure information.
 - Performance
 - ESMPRO monitors server performance and displays server usage on the screen and displays information, such as the rate of CPU load, memory usage, disk usage, and LAN traffic. Usage threshold values can help the system administrator monitor and prevent server overloads.
-

CONFIGURATION

The ESMPRO consists of a Manager program that runs on a management computer and an Agent program that runs on servers to be managed.

- The Manager collects hardware, software, and firmware information from Agents connected to the network. The Manager displays Agent information, failures, and error logs on the screen.
- The Agent monitors server hardware, software, and firmware and transmits the information over the network to the Manager using SNMP. The Agent lets you view system settings and reset some ESMPRO thresholds locally.

Each managed server must have the Agent installed and running. Using SNMP, the Agent sends data across the network to the Manager, which collects the server information.

In addition, when you install both IIS and the Web Component on the Manager computer, you can manage servers through the web browser.

The following figure shows a sample Manager/Agent Configuration.

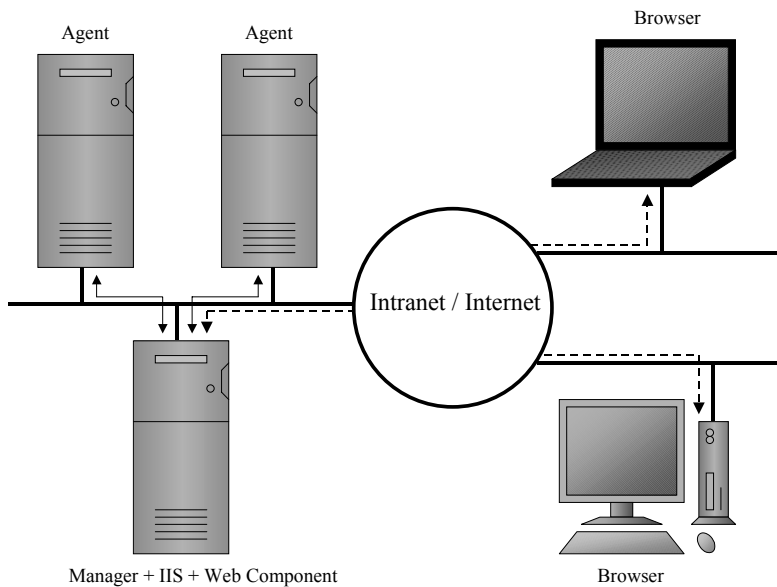


Figure 1-1 Manager/Agent Configuration

SYSTEM REQUIREMENTS

NEC ESMPRO Manager requires the following hardware and software:

■ Hardware

- Memory: 20MB of free memory for 32-bit and x64 systems or 230MB for 64-bit Itanium-based systems.
- Hard Disk space : 130MB (150MB with Web Component)
100MB (120MB with Web Component) is required for installing program.
In addition to the above, capacity of 30MB is required at installation as the area for creating work files in a temporary directory the operating system manages.
- Additional storage space
When operating ESMPRO, the files below are created.
Please confirm there is the capacity as well as the 100MB (120MB with Web Component) required for installing the program.
 - 1) Automatic Data Collection
Approx. 40KB per information collection.
 - 2) Alert information
Approx. 500 bytes per alert.
 - 3) Others
Approx. 10MB as the management area of server registered in Operation Window.
- Network Interface Card
- Display : a high-resolution monitor (Some dialog boxes do not fit on a display set to 640 x 480 pixels.)

■ Software

- Operating System :
Windows 2000 Server/Professional
Windows XP Professional/Home Edition
Windows XP Professional x64 Edition
Windows XP 64-bit Edition (Service Pack 1)
Windows Server 2003, Standard Edition/Enterprise Edition
Windows Server 2003, Standard x64 Edition/Enterprise x64 Edition
Windows Server 2003, Enterprise Edition for Itanium-based Systems
 - Communications Protocol : TCP/IP (comes standard with respective OS)
 - Web Server (required for the Web Component) : IIS 5.0 - 6.0
* Web Component doesn't run on Windows XP Home Edition.
 - Web Browser (required for the Web Component) : IE 6.0 (JavaScript must be enabled.)
-

Chapter 2

Installing the ESMPRO Manager

BEFORE INSTALLING

About a Virtual Directory the Web Component Creates

A virtual directory "esmpro" is created at the first web site (it is usually "Default Web Site") on the Web Server by installing the Web Component. If a virtual directory "esmpro" already exists, the setting will be overwritten. Therefore, please change the name to another name before installing the Web Component.

Setting of Network Services

The NEC ESMPRO Manager uses TCP/IP as its communication protocol. Please set up network services so that TCP/IP works properly.

Setting Up the NEC ESMPRO User Group

To use the NEC ESMPRO Manager, you must belong to a user group called the NEC ESMPRO User Group for security purpose.

NOTE: As for Windows XP Home Edition, which doesn't support creating optional user groups, Computer Administrator meets the requirement.

The NEC ESMPRO User Group should be determined during the installation, and the Manager setup shows "Administrators" for it by default.

If you want to specify other user group, you must create it before installing the NEC ESMPRO Manager and specify the group during installation. The NEC ESMPRO User Group is case sensitive.

Also, to make this security function effective, please install the NEC ESMPRO Manager on a hard drive formatted with NTFS.

NOTE: When you create the NEC ESMPRO User Group as a global group, make sure that there is no local group having the same name. Also, when you install the NEC ESMPRO Manager on a backup domain Controller, you must create it as a global group.

Installing IIS

If you use the Web Component, install IIS before installing the NEC ESMPRO Manager.

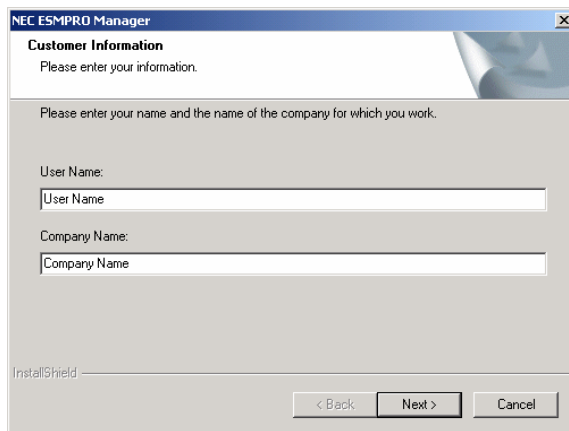
Installing HP OpenView Network Node Manager

If you use the HP OpenView Integration, install HP OpenView Network Node Manager before installing the NEC ESMPRO Manager..

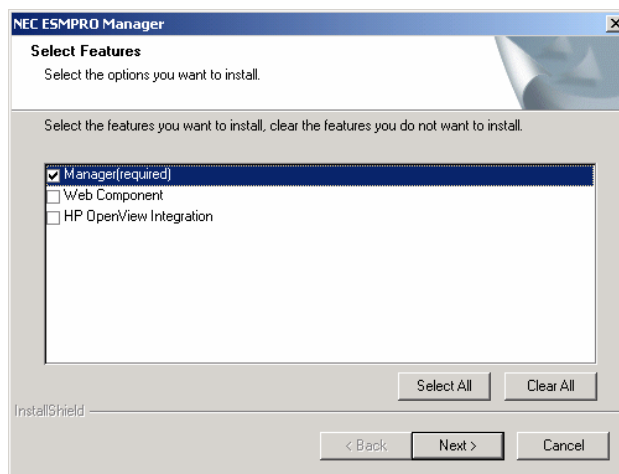
INSTALLATION

Installing the Manager Software

1. Log on as a user with administrative privilege. As for Windows XP Home Edition, log on as Computer Administrator.
2. Run SMx64.exe which you downloaded from the Web Site.
Setup files are extracted automatically and the NEC ESM PRO Manager Setup starts.
3. After verifying system conditions, setup prompts you to enter your name and your company name.

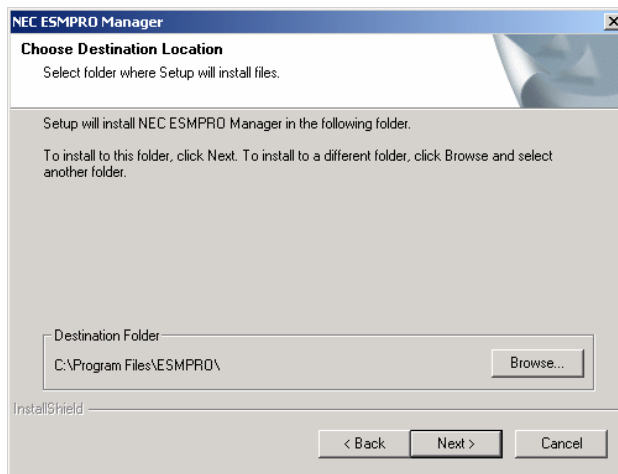


4. Depending on environment, a dialog box for selecting components may appear when you install NEC ESM PRO Manager. Select the item(s) you want to install to proceed.

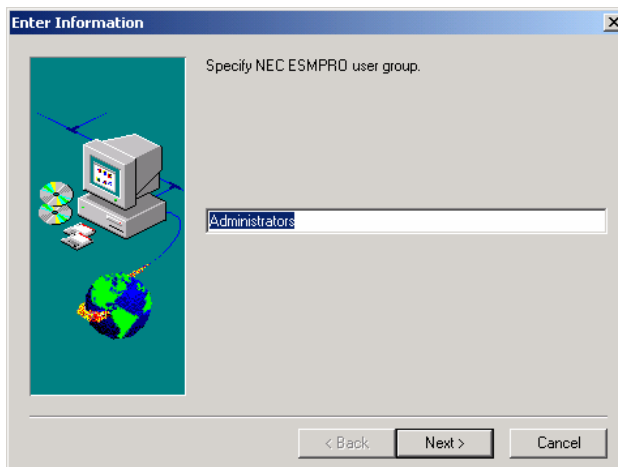


NOTE: The optional components can be added any time you want after this installation.

5. Enter the destination directory for the NEC ESMPRO Manager.



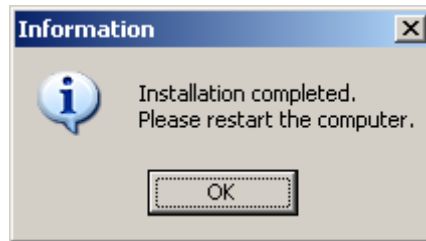
6. Specify the NEC ESMPRO User Group you determined.



NOTE: When you install the NEC ESMPRO Manager on Windows XP Home Edition, accept the default user group "Administrators" as the NEC ESMPRO User Group and proceed with installing.

8 Installing the ESMPRO Manager

7. When the installation is complete, restart the system.



IMPORTANT: Depending on environments, a setup window may remain on the screen after you click on the [OK] button. In such a case, follow the instructions below.

1. Click on the close button on the title bar of the setup window.
2. An End Program dialog appears. Click on the [End Now] button.
3. A confirmation dialog for sending an error report is displayed. Click on the [Don't Send] button.
4. A dialog which says "1628: Failed to complete installation." appears. Click on the [OK] button.

Installation of the NEC ESMPRO Manager has been successfully completed and there is no problem in later operations.

NOTE: Except for Windows XP Home Edition

When installing the NEC ESMPRO Manager in an already existing directory, the NEC ESMPRO Manager will not operate unless the access right required for the NEC ESMPRO Manager operation has been set.

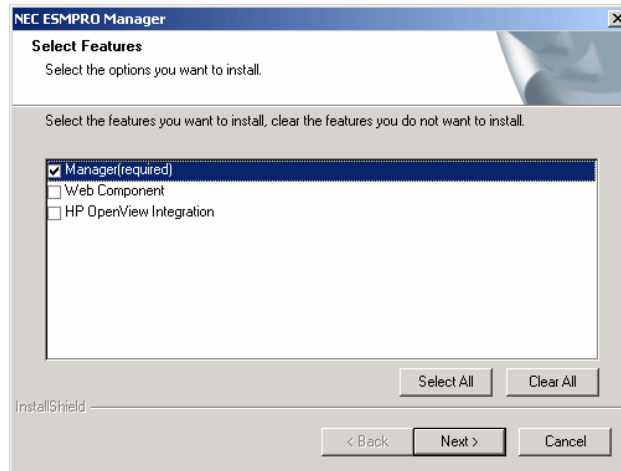
When installing the NEC ESMPRO Manager in a non-existing directory, the following access rights are set by an installer.

Administrators	Full Control (All)(All)
Everyone	Read (RX)(RX)
SYSTEM	Full Control (All)(All)

If you specified a user group other than the default (Administrators) as the NEC ESMPRO User Group at the installation, Full Control access right will be set for it.

Adding/Removing the optional Component

To add/remove the optional components, set up the NEC ESMPRO Manager again by following the "Installing the Manager Software."



Select the check box of the item you want to add, deselect the check box of the item you want to delete, and then click the Next button..

IMPORTANT: You cannot go to the next step with all checks cleared.

Chapter 3

Using the ESMPRO Manager

STARTING THE ESMPRO MANAGER

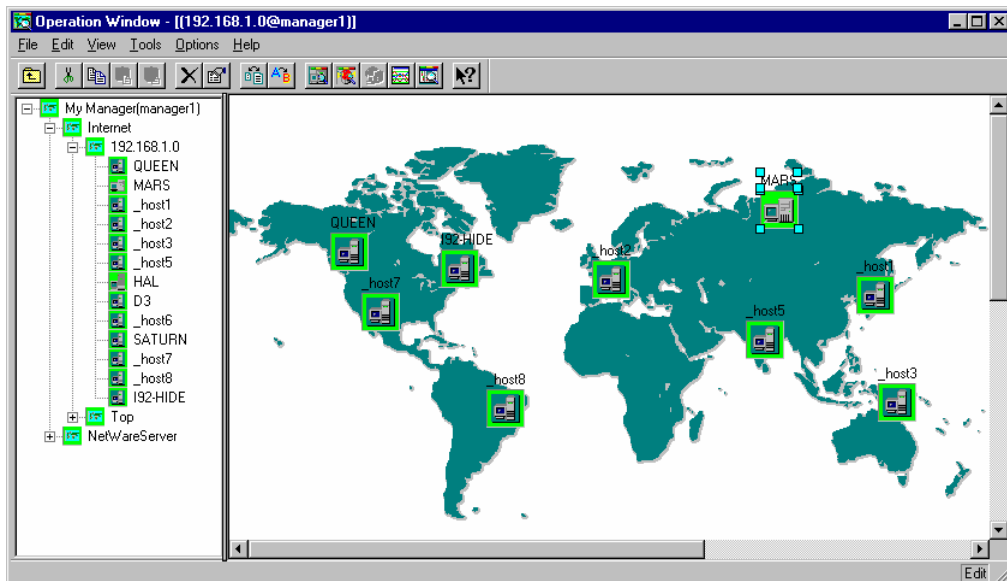
Start the ESMPRO Manager as follows:

- During ESMPRO Manager installation, an NEC ESMPRO Manager folder is created in the Start Menu. To start the ESMPRO Manager, click on the ESMPRO Manager icon.

When you start the ESMPRO Manager, an Operation Window similar to the following appears.

The left side of the Operation Window is the Tree View and contains a list of icons that represent Agents in the network or maps. The Tree View also displays Neighbor Managers if any are registered.

On the right side of the Operation Window is the Map or Information View, which shows additional details for the icon selected in the Tree View. Agents within your network are shown as icons on the network map. An example is shown in the previous figure. When the icons are displayed here, this side is called the Map View. On the other hand when the system information of a server is displayed, it is called the Information View.



Tree View

Map or Information View

When the Operation Window first appears, ESMPRO servers on the same network can be discovered and recorded on the Map View. (See Detecting Agents Automatically, page 12)

The ESMPRO Manager automatically monitors Agents at specific intervals. The background color of the icon indicates the Agent status. Normally, the icon background is green. If the status is red or yellow, use the Data Viewer and Alert Viewer to determine the problem.

Tool Bar and Menus

The tool and menu bars at the top of the Operation Window give you access to many ESMPRO functions. The tool bar gives you quick access to many frequently used menu items. Simply press the button and access the function. These buttons include the following:



Upper Map



Cut (short cut to Edit Menu/Cut)



Copy (short cut to Edit Menu/Copy)



Paste (short cut to Edit Menu/Paste)



Paste with a New Name (short cut to Edit Menu/Paste with New Name)



Delete (short cut to Edit Menu/Delete)



Properties (short cut to File Menu/Properties)



Shrink to Fit (short cut to View Menu/Shrink to Fit)



Alias (short cut to View Menu/Alias)



Data Viewer (short cut to Tools Menu/Data Viewer)



Alert Viewer (short cut to Tools Menu/Alert Viewer)



SMS (short cut to Tools Menu/SMS)



MIB Browser



MIF Browser



Help

To obtain more detail about a menu item, tool bar icon, or field, select the Help icon from the tool bar and click on the screen.

Detecting Agents Automatically

ESMPRO Manager can detect Agents automatically and register an icon on the Map View when it finds them. If you prefer, you can add Agents manually. (See Adding an Icon Manually, page 13.)

Initiate automatic Agent detection as follows.

1. Ensure that the SNMP service is running on the Agents.
2. Open the map where you want Agents registered automatically.
3. From the Tools Menu, select Autodiscover/Foreground.
4. Select TCP/IP Hosts.
5. Proceed as follows.

Enter the network address and network mask for the network you want to find. Also enter the value set for the Agent to be detected in the SNMP Community field. The default is public.

If you are entering more than one SNMP community name, separate the names with commas, as in public,xxx.

If Class A (255.0.0.0) or Class B (255.255.0.0) is specified, the number of addresses becomes enormous and the automatic detection takes a very long time. If the network in use is Class B, we recommend that you modify the network address and network mask appropriately and carry out a partial detection

If you want to access the details of auto discovery, press Details button and check the following items.

- Update properties
To update server's properties already been set, check this item.
- Discover DMI Agent
To detect DMI agent, check this item.
- Restrict the objects
To specify ESMPRO Agent, check this item.

Please refer to on-line help for more details.

6. Press the Start button.
7. When automatic detection is finished, press Close. Any Agents detected appear on the map as icons.

It is also possible to detect Agents periodically in the background by specifying the SNMP community name and the interval in Autodiscover/Background on Tools Menu.

Changing Agent Properties

After icons are added during Autodiscover, you may want to view and edit their properties.

1. Click on the icon with the right mouse button.
2. Select Properties from the pop up menu.
3. Make changes in the Properties window. Use the on-line help for details on field entries.

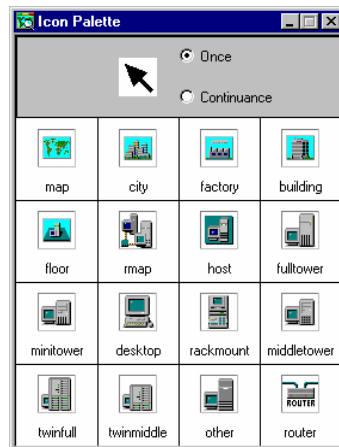
To delete an icon, select it and select Delete from the Edit Menu. If your attempt is denied, make sure that Enable Edit is selected in the Options Menu.

You can move an icon by dragging it.

Adding an Icon Manually

Follow this procedure to add an icon manually.

1. From the View Menu, select the Icon Palette. If it is already running, press Alt-Tab to access it.

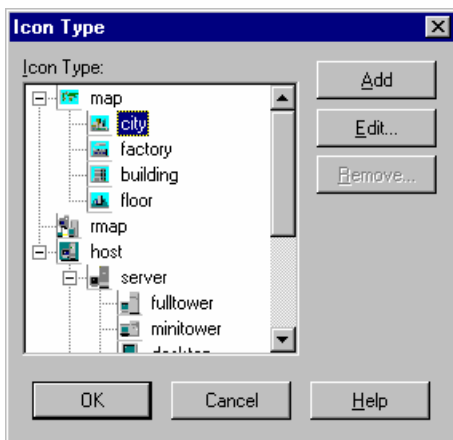


2. Click on the icon in the palette that best represents the Agent. If none of the icons is suitable, you can modify the standard ones or create your own. (See Changing an Icon in the next page or Creating an Icon Type, page 15 for details.)
 3. Move your cursor to the Map View side of the screen and press the mouse button to deposit the icon where you want it.
 4. When the Properties window appears, enter the appropriate information for the Agent or map being created. Use the on-line help for a description of the fields.
 5. When you finish, press OK. The icon is automatically added to the Tree View.
-

Changing an Icon

Follow this procedure to change an icon's image.

You can only change a map icon to another map icon or change a server icon to another server icon. You can determine which is a map icon and which is a server icon in the Icon Type window. (Select Customize and Icon Type from the Options Menu.) In the following figure, city, factory, building and floor are map icons. Fulltower and minitower are server icons. A floor icon can change to a building icon but cannot be changed to a full tower icon.



1. Highlight the icon that you want to change in the Map View.
2. Ensure that Icon Palette is selected in the View Menu.
3. Select Change Icon Type from the Edit Menu.
4. Ensure that the Icon Palette is visible. You may have to press [ALT][TAB] to display it again.
5. Click on an icon in the Icon Palette. The old icon changes to the new one selected.

Creating an Icon Type

You can create your own icon types and add them to the Icon Palette.

1. From the Options Menu, select Customize and Icon Type.
2. Highlight an icon.

Icons are listed hierarchically and by type. The new icon type will be placed under the one you highlight here.

There are several factors to consider when deciding where to add icons:

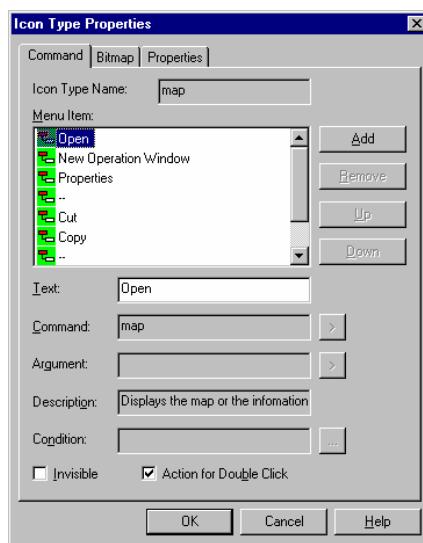
- a. The Properties window for the new icon will be based on the parent icon.
 - b. The icon's image can be changed later one they have been added to the map, but they can only be changed to another icon in the same group (that is, map or server).
3. Click on Add.
 4. Enter a name for the new icon.
 5. Click on Edit, select the Bitmap tab, and press Add.
 6. Enter the drive, path and filename to specify the bitmap.
 7. Press Open and the new bitmap file appears in the window with the existing bitmaps.

The icon appears in the Icon Palette when the Operation Window is restarted.

Changing the Popup Menu

These procedures will show you how to edit the popup menu for an icon type. Once these changes are made to the icon type, new icons created with the icon type have the new popup menu. Popup menus for icons created previously remain unchanged.

1. From the Options Menu, select Customize and Icon Type.
2. Highlight the icon type you want to change.
3. Click on Edit. The Icon Type Properties window displays. The Menu Item list on the Command tabs displays the items that appear in the popup menu.



➤ To add an item to the popup menu:

1. Click on Add.
2. Enter the new text to appear in the popup menu in the Text field.
3. Enter the command that starts the program in the Command field.
4. Enter any arguments needed to run the program in the Argument field. (This field is optional.)
5. If you want to activate the item with a double click instead of a single click, check Action for Double Click.
6. You can change the order that the items will appear by using the up and down arrow keys.

➤ To delete an item from the popup menu:

1. Items that you have added can be deleted with the Remove button.
 2. Standard items like Open and Properties can be eliminated by checking the Invisible check box.
-

Setting Up Inter-Manager Communication

These settings define the exchange of information between Managers on maps and agents registered in the remote manager.

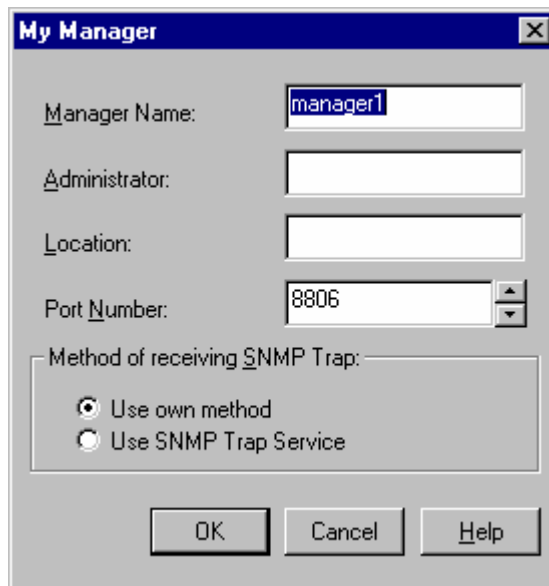
To establish the inter-Manager communication, you must specify the following.

- My Manager
- Neighbor Managers
- Routing
- Access rights
- Notification options

My Manager

Inter-Manager communication requires that each Manager have a unique name. Define My Manager as follows.

1. From the Options Menu, select Customize and then My Manager.



The screenshot shows a dialog box titled "My Manager" with the following fields and options:

- Manager Name:** A text box containing "manager1".
- Administrator:** An empty text box.
- Location:** An empty text box.
- Port Number:** A spin box containing "8806".
- Method of receiving SNMP Trap:** A group box containing two radio buttons:
 - Use own method
 - Use SNMP Trap Service
- Buttons:** "OK", "Cancel", and "Help" buttons at the bottom.

2. Set parameters for each field. Details are available in the on-line help.

NOTE: About Method of receiving SNMP Trap When there are other software's apart from ESMPRO Manager that receive SNMP Trap, for example, SMS Ver.1.2, ESMPRO Manager may not be able to receive SNMP Trap correctly due to the clash for SNMP Trap receive board.

In such case, select "Use SNMP Trap Service".

But when you select "Use SNMP Trap Service", there are the next restrictions.

- 1) When a trap by IPX protocol from NetWare server has been received, the name of the server that transmitted the trap cannot be identified.
- 2) The receive restriction function of Trap packet by SNMP community name set by [Options] - [Customize] - [Environment] of Operation Window cannot be used.

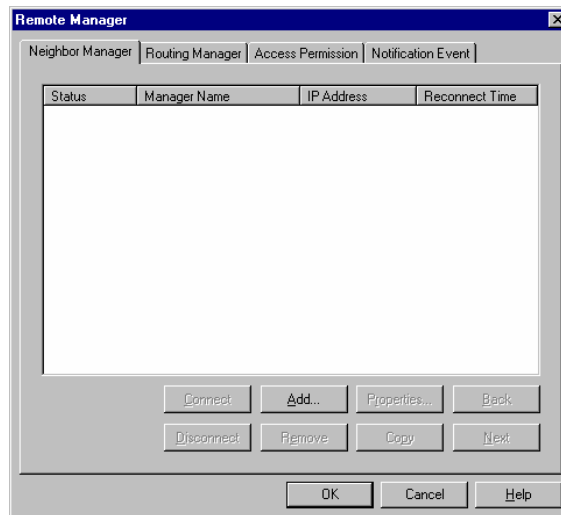
Also, when you select "Use SNMP Trap Service", "SNMP Trap Service" must be operating. "SNMP Trap Service" will be installed by incorporating SNMP Service, but the service is not started at initial condition. Activate Services in control panel and start "SNMP Trap Service". It is recommended that Startup Type of Startup is set to Automatic.

When you have selected "Use own method", be sure not to start up "SNMP Trap Service".

Neighbor Manager

The Neighbor Manager communicates directly with My Manager. The setting for the Neighbor Manager allows managers not registered as Neighbor Managers to communicate via the Neighbor Manager. Define the Neighbor Manager as follows.

1. From the Options Menu, select Customize/Remote Manager.



2. Select Neighbor Manager tab.
3. Click on the Add or Properties button.

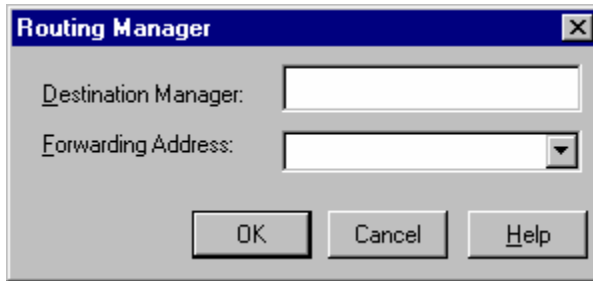


4. Enter the appropriate information in each field. Field details are available from the on-line help.

Routing

Inter-Manager communication to managers not directly connected (not neighboring) requires routing tables. Set up routing paths as follows.

1. From the Options Menu, select Customize/Remote Manager.
2. Select the Routing Manager tab and press the Add or Properties button.



3. Set the parameters for each field. Help is available from on-line help.

Access Rights

Defines read-only access or read/write access for inter-Manager communication from a specific Manager.

1. From the Options Menu, select Customize/Remote Manager.
2. Select the Access Permission tab and press the Add or Properties button.

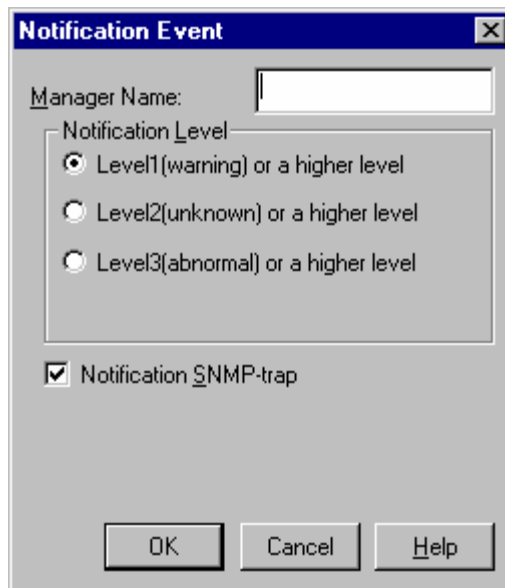


3. Enter the appropriate information in each field. Details about field entries is available in the on-line help.
-

Notification Options

Define notification options as follows.

1. From the Options Menu, select Customize/Remote Manager.
2. Select the Notification Event tab and press the Add or Properties button.



The screenshot shows a dialog box titled "Notification Event" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Manager Name:** A text input field.
- Notification Level:** A group box containing three radio button options:
 - Level1(warning) or a higher level
 - Level2(unknown) or a higher level
 - Level3(abnormal) or a higher level
- Notification SNMP-trap

At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

3. Fill in the appropriate information for each field. Details on field entries is available in the on-line help.
-

Monitoring Agents

After creating the network map, recording Agent icons, and establishing communications, the ESM PRO Manager automatically monitors the Agent status at specific intervals.

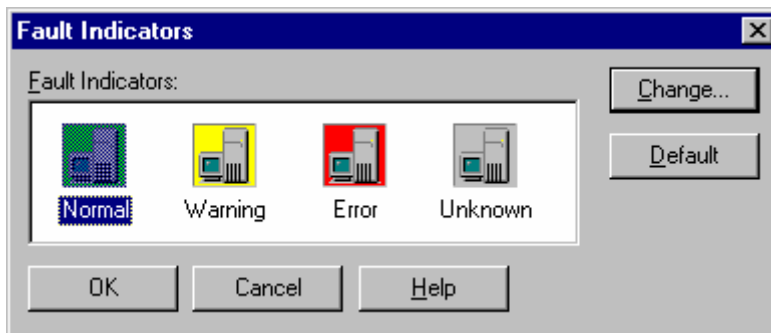
When the Manager detects a faulty Agent, the icon changes color according to the type of fault. Default colors are:

Table 3-1 Agent Status

Color	State	Description
Green	Normal	All Agent components are operating normally.
Red	Abnormal	A major error occurred in an Agent component.
Yellow	Warning	A minor error occurred in an Agent component.
Gray	Unknown	The Agent cannot be monitored or identified because the Agent is not started, the Agent software is not set up, or the server is down.

If the Agent status is red or yellow, use the Data Viewer and Alert Viewer to determine the problem.

You can change the fault indicators by selecting Fault Indicators from the Customize selections under the Options Menu. A screen similar to the following appears.

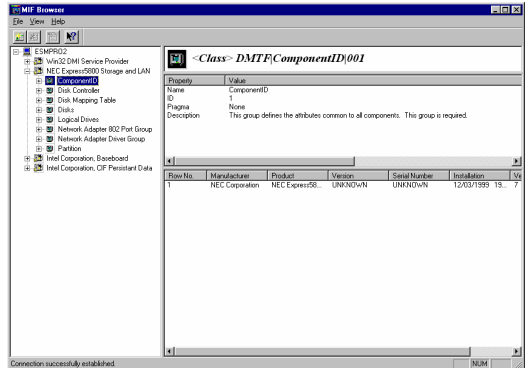
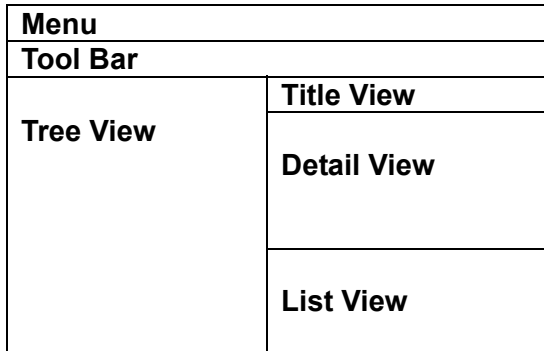


When a fault occurs in the agent which is managed by the remote manager, the background color of the rmap icon changes into the color indicating the condition, but it will turn back to the color showing normal condition after a certain time (30 seconds in the default).

BROWSING MIF

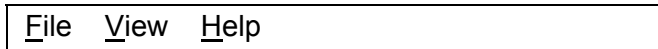
Screen

MIF Browser consists of the following views.



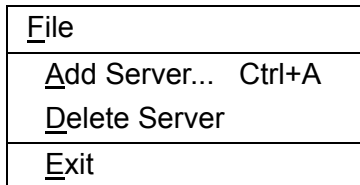
1. Menu

Displays the following menu on MIF Browser.



– File menu

Displays the following menu on the File Menu.



- Add Server : Add the server to be monitored.
- Delete Server : Delete the server to be monitored.
- Exit : Close the MIF Browser

– View menu

Displays the following menu on the View Menu.

<u>V</u> iew
<u>T</u> ool Bar
<u>S</u> tatus Bar
<u>R</u> efresh

Status Bar : When Status Bar is checked in the View menu, the Status Bar displays at the bottom of the screen.

Tool Bar : When Tool Bar is checked in the View Menu, the Tool Bar displays at the bottom of the screen

Refresh : Refresh the selected server information.

– Help menu

Displays the following menu on the Help Menu.

<u>H</u> elp
<u>H</u> elp Topics
<u>A</u> bout MIF Browser...

Help Topics : Accesses on-line help.

About MIF Browser : Provides revision information for the MIF Browser.

2. Tree View

The names of component, Group, Row, and Attribute are available from the Tree View.

3. Title View

The selected names (Component, Class, Row, Attribute) in the Tree View are available from the Title View.

4. Detail View

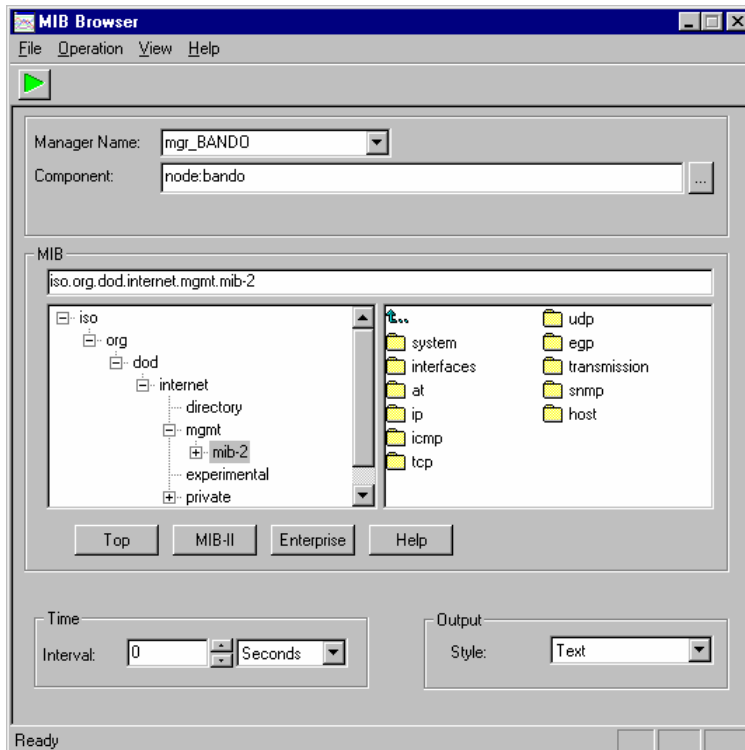
The details of the selected names in the Tree View are available from the Detail View.


5. List View

List is available if the selected group in Tree View has multiple rows. Not available otherwise.

BROWSING MIB

1. Select MIB Browser from the Tools Menu or press MIB Browser icon on the Toolbar.



2. Select the destination Agent from the Manager Name and Component drop-down lists.
3. Specify the MIBs to be retrieved. You can specify several OIDs at one time. When the OID is not the last one in the directory, all entries under the OID are also selected.
4. Set the interval of retrieval. When interval is 0, the MIB Browser retrieves just once.
5. Select the output style for the information: Text, Line Chart, Bar Chart or Pie Chart.
6. Press  to start collection.

NOTE: When the version of the MSVCRT40.DLL file which is in the Windows\System directory is different between Managers engaged in inter-Manager communication, the retrieved time is sometimes not correct. If this occurs, please replace one so that all versions of the file are the same.

INSTALLING VENDOR EXTENSION MIB

The Operation Window allows you to install a vendor extension MIB. To install it you have to prepare a definition file that might be distributed by the agent vendor.

Chapter 4

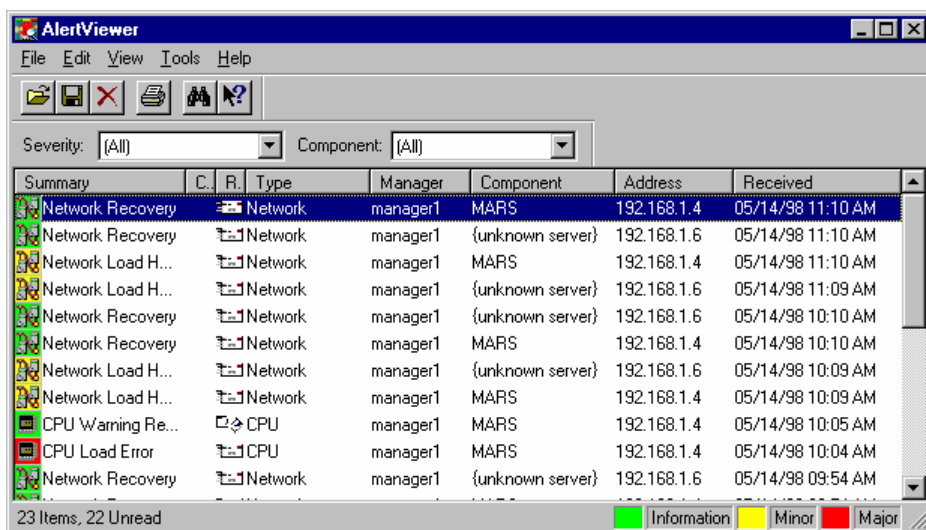
Alert Viewer

The Alert Viewer displays failures and warnings issued from servers running ESMPRO Agent software. The log provides the date and time of the alert, the server name, and a brief description of the problem. The icon in the Summary column is displayed in alert colors that indicate the severity of the problem.

ACCESSING THE ALERT VIEWER

To access the Alert Viewer from the Operation Window, select Alert Viewer from the Tools menu or the Alert Viewer icon in the tool bar. A screen similar to the following appears.

By clicking on any column title, alert messages are sorted by that column. You can also adjust the column widths by dragging the edge of a column title box to the left or right.



The central part of the Alert Viewer is the Alert Log which alert messages are displayed. New alert messages are added to the top of the list as they arrive.

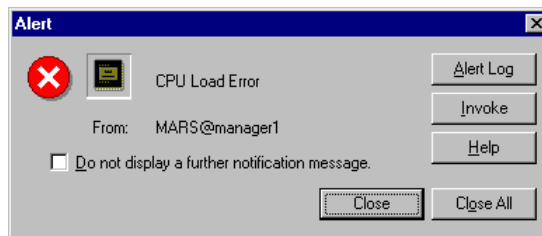
- **Summary** — gives a brief description of the alert message.
- **Icon (Summary column)** — displays the icon of the component in trouble. The icon color indicates the level of the alert. These colors include:
 - Green is informational and indicates a slight error or a warning recovery.
 - Yellow is a caution and indicates that the server has a problem that should be investigated.
 - Red is a warning and indicates a major problem with the server.

You can also use standard Windows icons without background color by checking "Use standard icons for alert list" in the Options dialog box.

- **Check** — lets you define and mark the status of an alert. Two marks are available, a cloud and lightning.
 - **Read/Unread** — indicates if the details of the alert message have been reviewed on the Alert Detail screen. The Read icon looks like an opened envelope. The Unread icon looks like a sealed envelope. (See Getting More Details, 30, for more information.)
 - **Type** — identifies the type of alert, such as FT Disk, System Reboot, or System Error.
 - **Manager** — identifies the remote manager where the alert originated.
 - **Component** — identifies the server that sent the alert.
 - **Address** — gives the TCP/IP address of the server that sent the alert. For a NetWare server, this address is the IPX address.
 - **Received** — shows the date and time when the alert was received by the Alert Viewer.
 - **Source** — identifies the service that sent the alert.
 - **Event ID** — the Event ID of the alert. (This column is not displayed in the default configuration. To display this column, select Columns in the View Menu.)
 - **Severity** — severity of the alert: major, minor, or information. (This column is not displayed in the default configuration. To display this column, select Columns in the View Menu.)
-

MESSAGE NOTIFICATION

When a new alert message arrives, you may hear a beep and see a notification message similar to the one shown next. (These options are set in the View Menu. See Setting Notification Options, page 33.) If your system has audio capability, you can also specify different sounds to signify different alert levels. Otherwise, the system sounds a beep through the internal speaker.

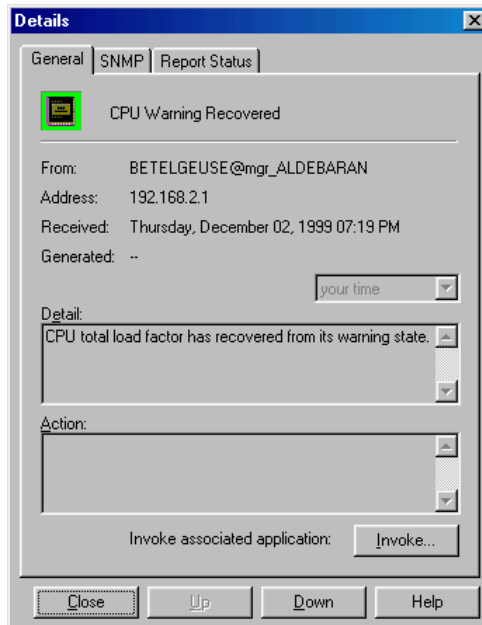


Click on the Alert Log button to open the Alert Log Detail screen or select the Invoke button to start the Data Viewer. If you do not wish to view alert messages or details, select Close.

Getting More Details

For details on an alert message, double click on the message line in the Alert Viewer. You can also select the Alert Log button on the notification message. A window similar to the following displays the details of the alert message, including corrective action to take.

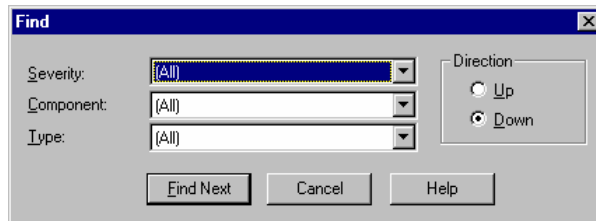
Once the Details window appears, the message is marked as Read in the Alert Log. (The symbol in the Read/Unread column changes to an opened envelope.) You can also mark messages as Read or Unread from the Edit Menu. Simply highlight the message and select Mark as Read or Mark as Unread.



Finding and Sorting Alert Messages

You can search for alert messages by specifying severity, component, or type. Do so as follows:

1. From the Tools menu, select Find.
2. In the dialog box that appears, enter the search criteria you want to use.

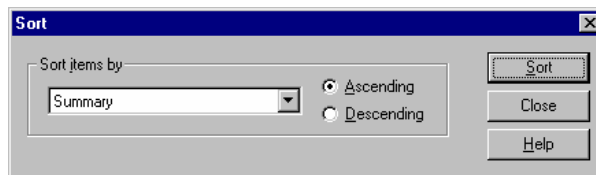


3. Click on the Find Next button. The next alert that matches the criteria is highlighted in the Alert Log. (Double click on the line to see the Details screen.)

Sorting Alert Messages

ESMPRO lets you sort alert messages in the Alert Log. This allows you to list a specific class of messages first, like all warning messages or those related to fan errors.

1. From the View menu, select Sort.



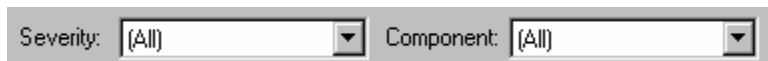
2. From the drop down "Sort items by" list, select the sort criteria to use. You can use any of the Alert Viewer columns as your sort criteria.
3. Select the circle next to Ascending or Descending to specify the order in which the messages should appear.
4. Select OK to sort the alert messages or Cancel to abort.

Another way to sort messages is to click on a column title in the Alert Log. Clicking once will sort all messages in ascending order using the selected column as the sorting criteria. Clicking again will sort in descending order.

Filtering Alert Messages

You can filter alert messages by specifying severity or component.

1. Specify severity or component by selecting drop-down list on Toolbar.



2. Check on Filter in the View menu. (Your selections here only affect what is displayed. All data is stored)

Configuring the Alert Viewer

You can configure the appearance of the Alert Viewer in a number of ways. You can select the information you want to appear in the Alert Log. You can also hide the tool and status bars from the screen if they are not needed.

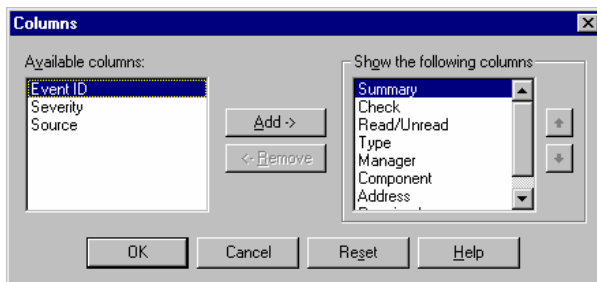
- To view or remove Tool Bar and Status Bar

You can display the Toolbar and Status Bar on the screen or remove them from the screen by checking or removing the check from the appropriate line under the View menu.

- A check next to the item indicates that it is displayed on the screen.
- No check next to the line, indicates that the toolbar or status bar will not appear.

- To add or delete columns from the Alert Log

You can choose the information to include in the Alert Viewer Log. From the View menu, select Columns. A window similar to the following appears:



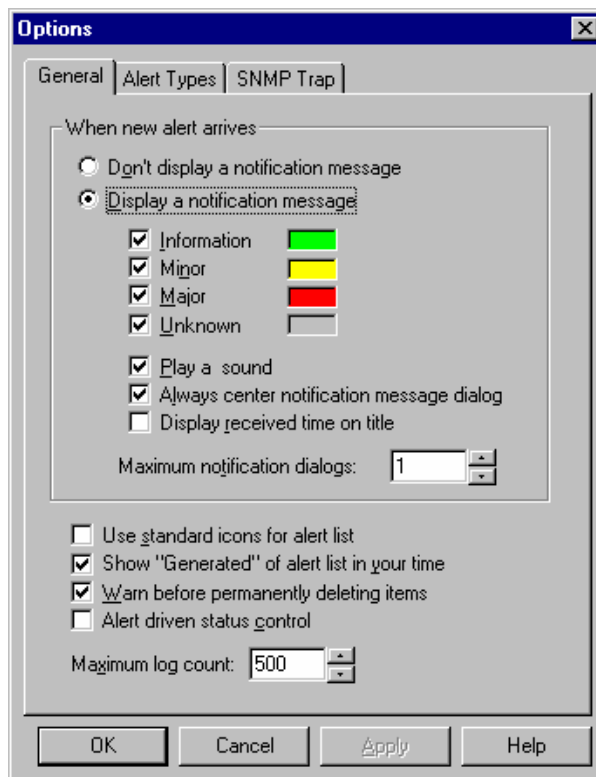
- Information that appears in the Alert Log is listed in the box "Show the following columns."
- Information under "Available Columns" can be added to the Alert Log.

To add a new column to your screen, highlight an item from the "Available Columns" box and select the Add button. To remove a column from the Alert Log, highlight an item in "Show the following columns" and select Remove.

Setting Notification Options

You can configure how you are notified of new alert messages. You can filter alert messages by severity and define the maximum size of the Alert Log.

From the Tools menu, select Options. A screen similar to the following appears.



Set up notification options as follows:

- If you don't want to receive any notification messages when alert messages arrive at the Alert Viewer, select "Don't display a notification message."
- If you choose to display notification messages (like the one on page 29), you can also select the type. For example, you may not want to be notified when informational messages arrive. To see a notification message when a new alert is received, select "Display a notification message." and check a severity level. If no boxes are checked, messages of all severity levels are not displayed.
- To hear a warning tone or .wav file when new messages arrive, check "Play a Sound." Wave files have already been assigned to error messages types. If you want to review or change these assignments, select the Alert Types tab.
- Check "Always center notification message dialog" if you want notification messages to be centered to desktop.

- Check "Display received time on title" if you want alert received time to be shown on title bar of notification message.
- "Maximum notification dialogs" allows you to define the maximum number of notification message displayed at one time.
- Check "Use standard icons for alert list" if you want to see the standard Windows icon in the Summary column. Leave this unchecked to use ESMPRO icons.
- Check "Show Generated of alert list in your time" to display "Generated" columns.
- Check "Warn before permanently deleting items" if you want to receive a confirmation message when deleting alert messages.
- Alert driven status control

When Alert Driven Status Control is not checked, the alert level is determined by the latest message from the Agent. For example, when a minor alert message is received, the icon changes to yellow. When a return to normal message is received from the Agent, the icon turns back to green.

When Alert Driven Status Control is checked, you have manual control over the appearance of the Agent icon. By marking a message as Read or Unread, you control the alert level. When an alert message is Unread, the icon takes on the status of that message. When all alert messages for a component are read, the status is normal.

For example, if you change a major alert message to unread, the alert status becomes Abnormal and the icon turns red. (If a component has several unread messages, the status is the most severe condition.) If all the messages for a component are marked read, its status returns to normal and the icon turns green.

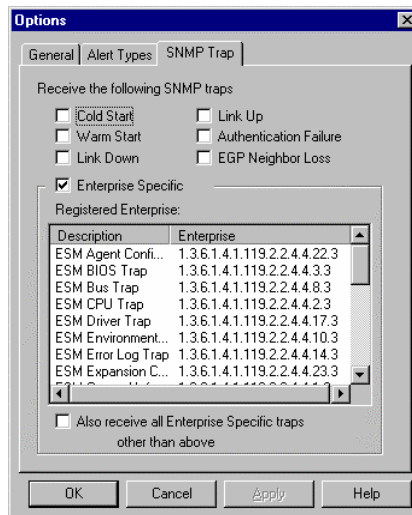
- "Maximum log count" allows you to define the size of the Alert Log.

Select the Apply button to refresh the Alert Log with the settings you entered.

Receiving SNMP Traps

By default, AlertViewer only receives and shows Enterprise Specific traps originating from ESMPRO Agent. You can configure AlertViewer to receive all other SNMP traps.

From the Tools menu, select Options and click "SNMP Trap" tab. A screen similar to the following appears.



Set up SNMP Trap options as follows:

- Check "Cold Start" if you want AlertViewer to receive cold start trap.
- Check "Warm Start" if you want AlertViewer to receive warm start trap.
- Check "Link Down" if you want AlertViewer to receive link down trap.
- Check "Link Up" if you want AlertViewer to receive link up trap.
- Check "Authentication Failure" if you want AlertViewer to receive authentication failure trap.
- Check "EGP Neighbor Loss" if you want AlertViewer to receive EGP neighbor loss trap.
- Check "Enterprise Specific" if you want AlertViewer to receive enterprise specific trap (like ESMPRO). This is checked by default. It is highly recommended you leave this option checked. Otherwise you cannot receive important alert message from ESMPRO agent.
- "Registered Enterprise" shows the list of trap enterprise for which AlertViewer can show detail and meaningful information.
- Check "Also receive all Enterprise Specific traps other than above" if you want AlertViewer to receive all enterprise specific traps.

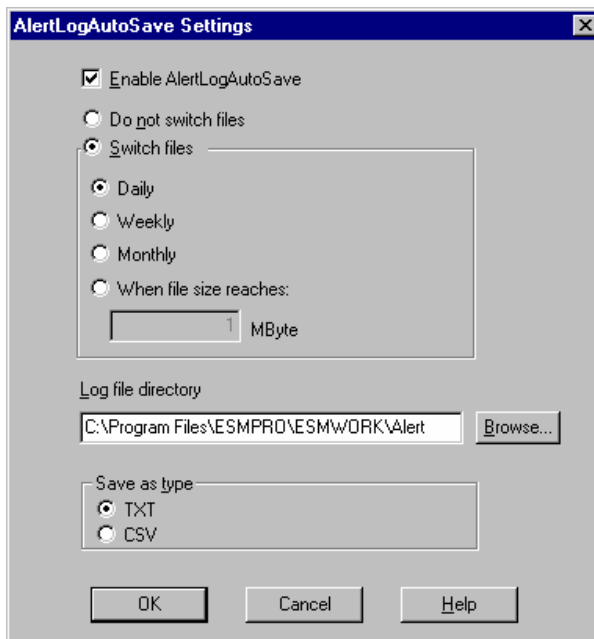
After setting up, you must restart the computer for the changes to take effect.

Forwarding Alert Messages

You can forward alert messages to various destinations by using Alert Manager. Click on Report Setting of Tools menu to invoke Alert Manager. As for the details of Alert Manager, please refer to NEC ESM^{PRO} AlertManager User's Guide.

Alert Log Auto Save Settings

The Alert Log Auto Save function automatically saves received alert data in files. The received alerts can be saved as long as disk capacity allows. You can set this function on this dialog box. After you have set it here, new alerts will be logged.



NOTE: This function consumes a few kilobytes of disk space per alert. Make sure to regularly create back up of or delete alert log files. You can not specify a network drive as the log file directory.

Chapter 5

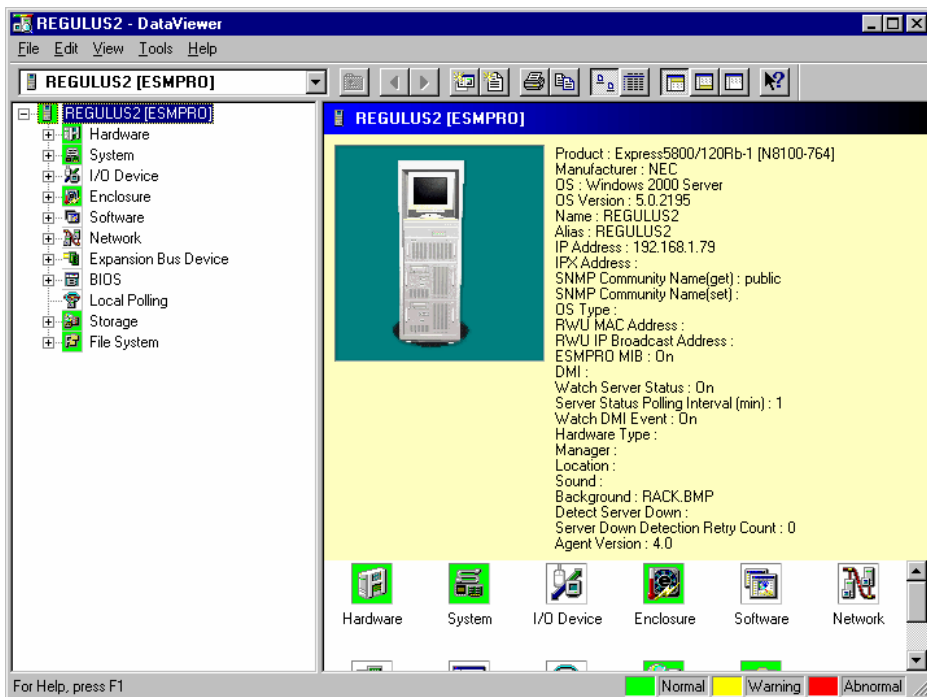
Data Viewer

This section describes the Data Viewer and its many options. The Data Viewer lets you check hardware and software features on Agents that are monitored by ESMPRO Manager.

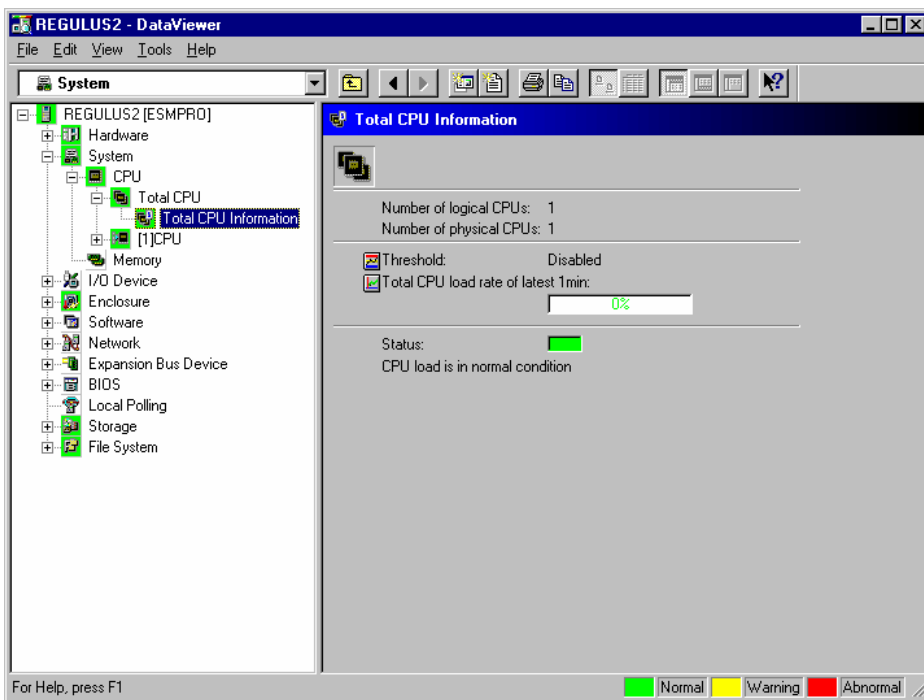
Access the Data Viewer as follows.

1. From the ESMPRO Manager Operation Window, click on an Agent icon to select it.
2. Once the Agent icon is selected, you can open the Data Viewer using any of the following methods.
 - Selecting Data Viewer from the Tools menu
 - Selecting the Data Viewer icon in the toolbar
 - Selecting Data Viewer from the Command menu (popup menu accessed with the right mouse button)

A screen similar to the following appears.



- The Tree View on the left side of the screen lists the folders.
 - The Information View on the right side of the screen displays the status or statistical information about the Agent
 - The status bar at the bottom of the window describes the current function and shows the alert color legend.
3. Double click on a folder entry in the tree view. A series of icons are displayed in the Information View and devices and device categories are listed under the entry.
 4. Click on a device or an icon. Data screens appear and provide detailed information about the device selected. The following screen is an example.



NOTE: Sometimes buttons or item names disappear when you start up graph or change screen size, but Data Viewer is operating correctly. In such case, you can change it to correct display by changing the screen size again.

SETTING THRESHOLD LIMITS



Thresholds can be set and viewed wherever you see the threshold button.

You can set threshold limits for:

- Server temperature (Enclosure folder)
- Voltage (Enclosure folder)
- Fan Speed (Enclosure folder)
- Rate of CPU load (System folder, CPU Total)
- Free Capacity (File System folder)

When an operation or device reaches the threshold setting, the Agent sends an alert message to the ESMPRO Manager. These messages are displayed in the Alert Viewer.

After you press the threshold button, a screen similar to the following appears. Set the limits and reset values in either the text fields or on the sliding bar.

When the limits are defined in terms of the number of errors counted, the Set Threshold window look similar to the following figure. Set the number of errors that trigger fatal and warning messages in the Fatal and Warning fields in the lower part of the screen.

NOTE: While the server is shutting down, an incorrect value can be shown if the threshold dialog box for temperature opened on Data Viewer.

In this case, close the threshold dialog box first and then reopen the threshold dialog box for server temperature on Data Viewer after restart the server.

HOW THRESHOLD LIMITS AND RESET VALUES WORK

When a parameter exceeds the threshold limit an alert message appears in the Alert Viewer. The corresponding icons in the Data Viewer and Operation Window turn red or yellow to show the warning or abnormal alert status. (The default colors red, yellow, and green are assumed here.)

The alert status returns to normal when the parameter falls below the reset value. A recover message appears in the Alert Viewer and the icons in the Data Viewer and Operation Window return to green.

Fatal and Warning Limits

Most parameters have two limits (Fatal and Warning or Major and Minor) and a reset value for each limit. When the parameter exceeds the Warning limit, a warning alert message (such as, CPU Load Warning) appears in the Alert Viewer. The Agent's icon in the Operation Window and the appropriate folder icon in the Data Viewer turn yellow to indicate the warning status.

The status continues to be warning until it falls below the Warning Reset value when the status returns to normal. A warning recover message (such as CPU Warning Recover) appears in the Alert Viewer and the icons in the Data Viewer and Operation Window return to green.

The Fatal limit is similar. As the parameter increases and reaches the fatal limit, an error message displays in the Alert Viewer (such as, CPU Load Error). Icons in the Data Viewer and Operation Window change to red to indicate the abnormal status.

When the parameter falls below the Fatal reset, the status is reset from Abnormal to Warning and an Error Recover message displays in the Alert Viewer. Icons change to yellow since the parameter still exceeds the Warning limit. Status is normal when the value falls below the Warning reset value.

1. Specify the OID in Item field. Some OIDs are selectable from the Browse button. And check the Enable Polling check box.

NOTE: In Item field, enter OID including Index.

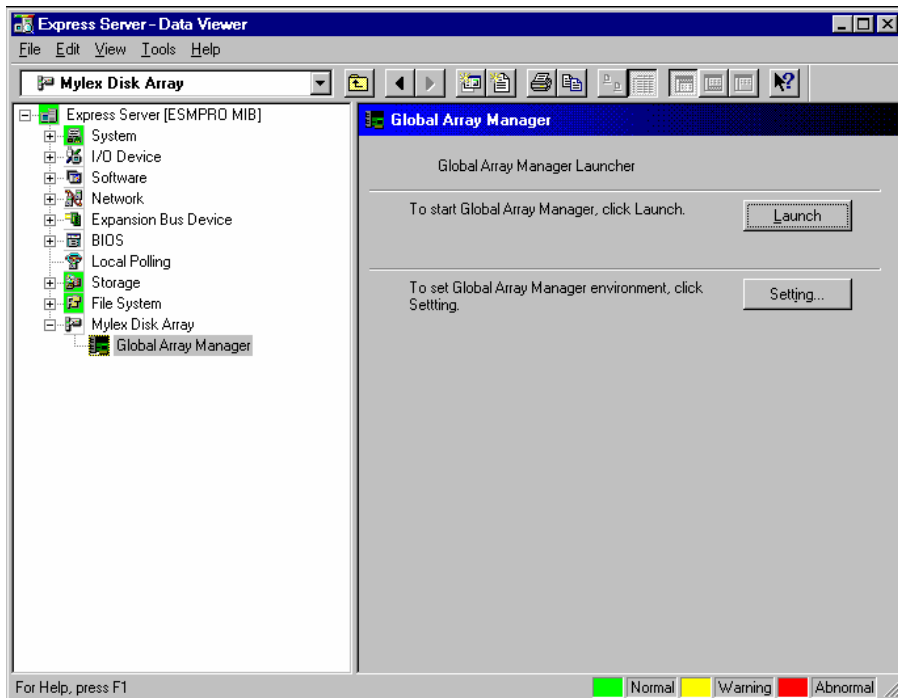
When entering using Browse button, where Index needs to be specified is shown by "Transmitted Error Packets. [%index%]" in the comment column.

When these OIDs are selected, character strings ending with "." such as "1.3.6.1.2.1.10." are set in the item field. Enter the index value after".".

2. Set duration and interval. When duration is 0, polling is continuous.
3. Set threshold limits and reset values for the OID. In addition to the text entry boxes, you can set the threshold using the sliding bars to the right.
4. Check Enable Sending Trap. This issues a trap corresponding to the current threshold settings.

MYLEX GAM LAUNCHER VIEW

"MYLEX GAM launcher view" launches a utility of disk array management "GAM client".



NOTES:

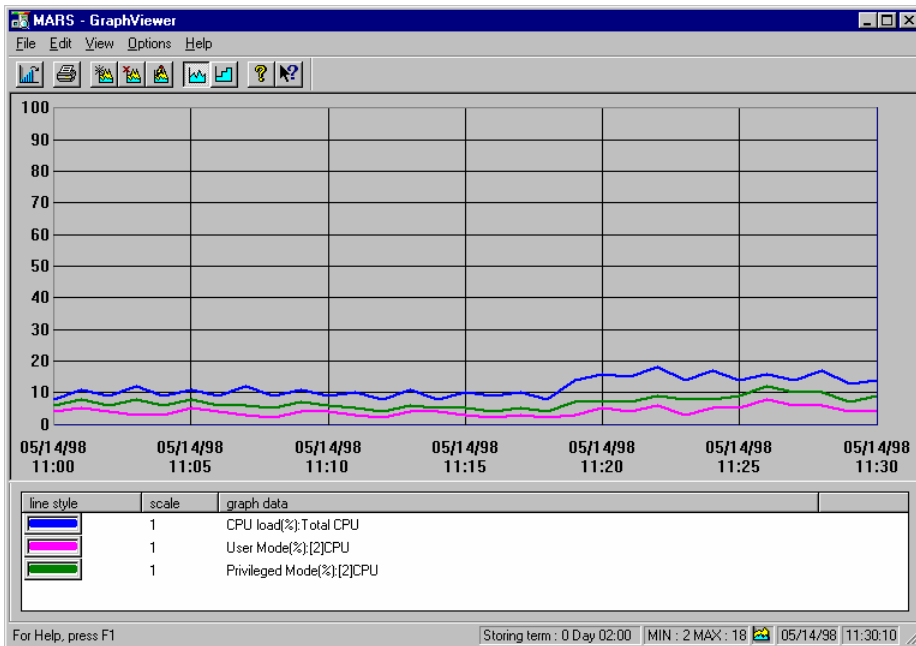
- "MYLEX GAM launcher view" launches GAM Client with following installation pass by default. If installation pass is different from real it of GAM Client, please change it using Setting Button.
C:\Program Files\Mylex\GAM CLIENT\gam2cl.exe.
 - If "GAM Server" doesn't exist in monitor server, this view isn't shown.
 - In case of using NEC ESM PRO Ver.3.8 agent or older version, this launcher view is to be displayed. With NEC ESM PRO Ver.4.0 agent or later version, this viewer is not to be displayed.
To start GAM client, launch from [Start Menu].
-

CREATING GRAPHS

The Data Viewer lets you create real-time graphs using the dynamic information collected from the Agent. The Graph window displays the change of values using the time increments specified.



A graph button appears next to parameters that can be graphed. Selecting the graph button displays a window similar to the following.



The Graph Viewer lets you define the appearance of the graph, including the type of graph (step or line), grid, line color, weight, and style. Additional information on creating graphs is provided in the on-line help.

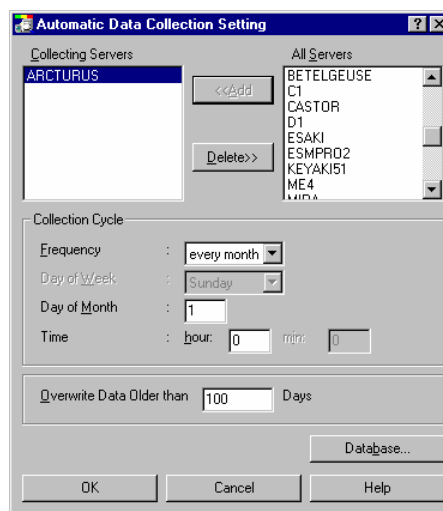
AUTOMATIC DATA COLLECTION

The NEC ESM PRO Manager has a function to collect statistical data automatically within a specific cycle.

Setting Up Automatic Data Collection

Set up data for automatic collection as follows:

1. On the Operation Window, right-click on the server icon and select "Automatic Data Collection Setting" from the pop-up menu.
2. Verify that your Agent is in the Collecting Servers list.



3. Set the Collection Cycle frequency to every month, week, day, hour, or every 30 minutes.
 - When the frequency is every month, you can set the day of the month and hour.
 - When the frequency is every week, you can set the day of the week and hour.
 - When the frequency is every day, you set the hour.
 - When the frequency is every hour, you can set minutes.
 - When the frequency is every 30 minutes, you can set minutes.
4. Enter a value of up to 9999 in the "Overwrite Data Older than" field to specify how many days the data is saved before being overwritten with new data.
5. Press OK to accept the data collection settings.

When you start Automatic Data Collection, the server icon on your network map changes to show a graph within the icon. This indicates that the Manager is collecting statistical data on the server.

Saving Data with the ODBC Interface

When you select ODBC as the data saving mode, a table for the Server Name is created in the specified database. The following information is recorded:

- DataName — saves the data name collected, for example, ABC Network Board.
- DataKind — stores the data type collected, for example, Total Send Packets.
- GetTime — stores the date and time (TIMESTAMP) of data collection in a DateTime field.
- GetValue — saves integer data collected.
- DataType — saves the data type that was collected as an integer.
 - 0: Indicates an item that has an unsigned value (e.g. Transmitted Total Packets).
 - 1: Indicates an item that has a value with a percent sign (e.g. CPU load).
 - 2: Indicates an item that has a signed value (e.g. Voltage Level).

NOTE: The server name is used as the table name, therefore, if the server name includes characters that cannot be used in ODBC, no data is stored. Check your database specifications for acceptable characters.

ODBC data collection must be specified in ESMPRO and matching information must be entered in your selected database. Initiate ODBC data collection in ESMPRO as follows:

1. Press the "Database ..." button on the Automatic Data Collection Setting window.
2. Select ODBC and enter an ODBC Data Source Name.

NOTE: Enter what you have set as System Data Source, in ODBC Data Source Name.

3. Click OK to save the setting and close the window.
4. Add servers to the Collecting Servers list as follows:
 - Highlight the servers in the All Servers list.
 - Click the Add button.
5. Specify collection cycles by selecting a Frequency, Day, Month, and Time for each server and press OK.

NOTE: If automatic statistical data collection is not executed, no data is stored in ODBC.

Set up your data base for ODBC collection as follows:

1. Install and configure the ODBC drive for your particular database.
 2. Set the environment in ODBC using the same Data Source Name used in the Statistical Data Saving Mode screen in ESMPRO. (Step 2 in the preceding procedure.)
 3. In your database manager software, create a database template or table with the following fields.
 - DataName
 - DataKind
 - GetTime
 - GetValue
 - DataType
 4. Save the database.
 5. Enter the name of this database into your ODBC driver's settings where appropriate.
-

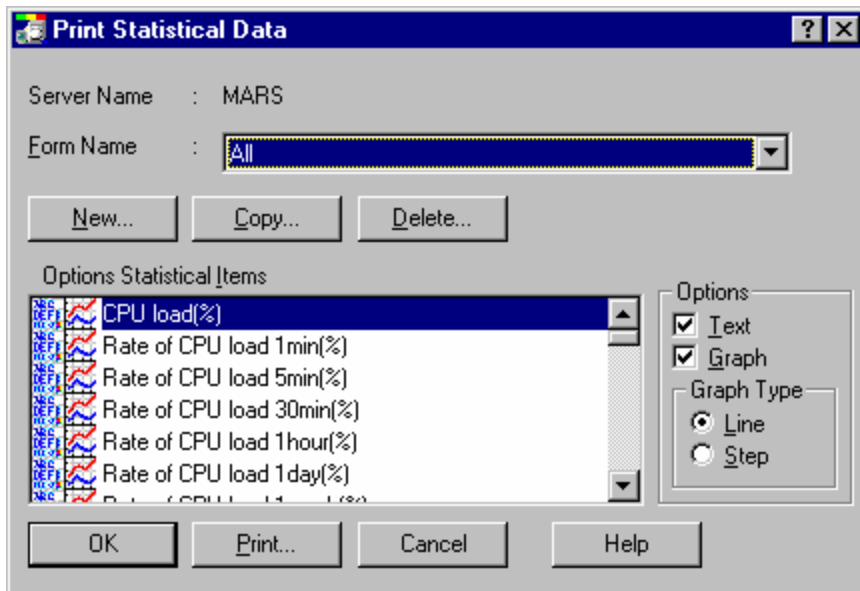
PRINTING STATISTICAL DATA

This section explains how to print the data collected through Automatic Data Collection.

1. On the Operation Window, right-click on the server icon and select "Print Statistical Data" from the pop-up menu.

NOTE: Data values and graphs are printed on separate sheets.

2. From the drop down list, select the form name to print. The NEC ESMPRO Manager comes with a number of forms already set up for you to use. A number of forms are available including options to print the forms with or without graphs.



Chapter 6

Web Component

ABOUT THE WEB COMPONENT

The Web Component allows you to use the main functions of the NEC ESMPRO Manager from your Web browser via Web server.

The Web Component consists of the following tools.

Operation Window

Adds, edits or deletes the managed servers, displays maps in a tree structure, and launches tools for managing servers.

AlertViewer

Displays alert messages issued by managed servers.

DataViewer

Displays a list of the detailed information on the NEC ESMPRO Agent (Version 3.7 or later for Windows).

Agent Control Panel

Allows you to set operational settings for the NEC ESMPRO Agent (Version 4.0 or later for Windows).

GETTING STARTED

When you use the Web Component, please follow the instructions below.

NOTE: When the Web Component has been installed on Windows XP 64-bit Edition, the installer may not create the virtual directory (esmpro). In such a case, refer to the later section "Re-creating the virtual directory for the Web Component" and create the virtual directory before proceed.

Setting a User Authority

To use the Web Component, you must set the appropriate user authority. Follow the instructions shown below to set the user authority.

The following procedure explains how to set the Web Component using IIS 5.0 on Windows 2000 Server. For other environments, see help of each Web server.

1. Start the Internet Services Manager on the Web server and display the virtual directory "esmpro" properties of the Default Web Site.
2. Click the Edit button of the Anonymous access and authentication control group on the Directory Security tab. Then set up the authentication methods.
3. Join the user with the authenticated access to the NEC ESMPRO User Group you specified during installation.
4. Restart the Web server computer.

NOTE:

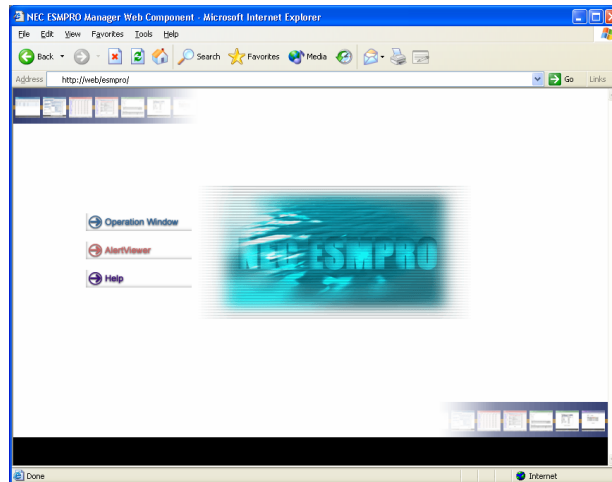
Considering your security, we do not recommend to allow an anonymous access. It is recommended to disable an anonymous access and use the authenticated access.

Checking the Operation of the Web Component

The initial URL for accessing the Web Component is:

<http://a web server name/esmpro/index.html>

Go to the above URL via your web browser to check that the following title page appears:



If the above title page does not appear, the authentication methods for the virtual directory may not have been correctly set up. Check that the setting has been correctly set again.

If starting the Operation Window from the above title page displays the following message:

'Failed to collect information. (No authorization was obtained. (5))'

the user that you accessed may not belong to the NEC ESMPRO User Group. Check that the setting is correct.

NOTE:

When you access the Web Component from a browser of a Web machine with the Integrated Windows authentication, the CGI window (command prompt), which is normally executed in the background, may be displayed. This is an issue of displaying, however, there are no problems in its operation.

If you access the Web Component from a browser of a remote machine, the CGI window will not be displayed.

Before You Manage Server(s) via Web Browser

- 1. Adding the server you want to manage**
There is no server registered in the NEC ESMPRO Manager right after the installation. Before you manage the server via your web browser, register the server you want to manage using the Manager (not web-based).
- 2. Updating Agent Version**
In order to run DataViewer or Agent Control Panel for the managed servers registered, the Agent Version property must be set properly.

To set the value, run Operation Window in Web Component and execute 'Agent Version Update' with the target servers.
- 3. Setting the number of the alerts to be stored**
To extend the number of the alert to be stored, specify the number of the alerts in the Manager (AlertViewer) beforehand. The default is 500 alerts.

Re-creating the Virtual Directory for the Web Component

Even if you perform overwrite installation, a virtual directory is not created.

If you have deleted the virtual directory for the Web Component, follow the instructions shown below to re-create it.

- 1.** Logon to the Web server as a user with administrative privilege, and open Command Prompt.
 - 2.** Type 'cd "C:\Program Files\ESMPRO\ESMBASE\ESMSMWEB"' to change the current directory.
* NEC ESMPRO Manager is assumed to be installed on "C:\Program Files\ESMPRO".
 - 3.** Type 'cscript sitelist.vbs'.

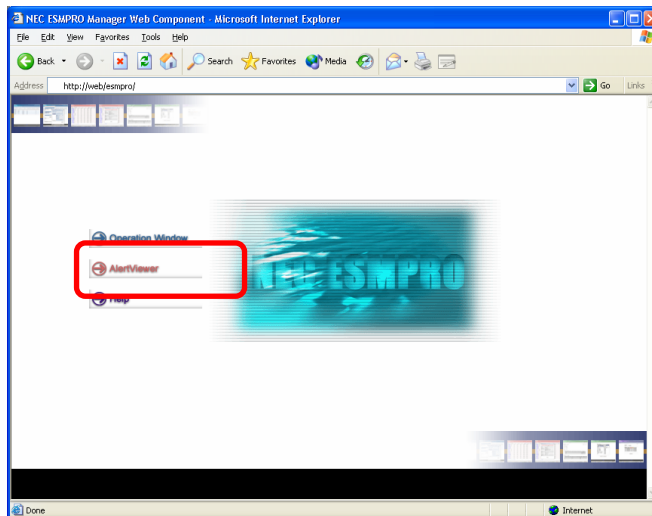
A list of Web sites that exist on the Web server will appear. The numbers displayed on the left are the Web site numbers. Confirm the web site number for which you want to create the virtual directory.
 - 4.** Type 'cscript websetup.vbs -s the site number -a the virtual directory name'.
* '-s 1 -a esmpro' is set up in initial setting.
-

OPERATION WINDOW

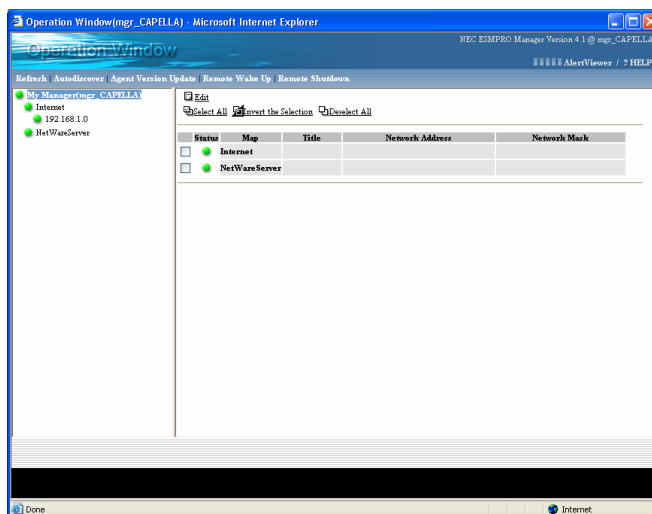
The Operation Window displays a list of the managed servers connected to the network on a map. Server monitor status and server properties can be accessed on the Operation Window. Additionally, tools for managing components can be launched from the Operation Window.

Starting the Operation Window

1. Click on "Operation Window" displayed on the Web Component title page.



2. The Operation Window starts.



NOTE:

The Web Component uses the same management information as the NEC ESMPRO Manager. Therefore, the maps and servers already registered in the Manager are displayed on the Web Component.

The Web Component does not support Inter-Manager communication. Thus, it does not display the Neighbor Manager information even if the Inter-Manager communication has been set in the NEC ESMPRO Manager.

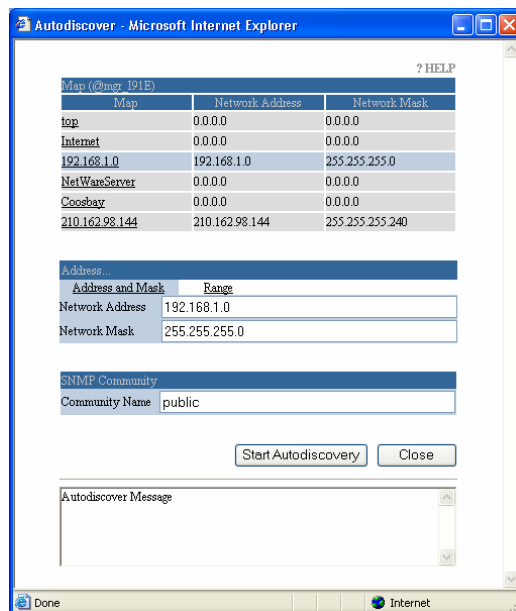
Registering a Server to be Managed

In order to register a server into an operation window, the Autodiscovery function of the Operation Window is used. If you already have managed server information in hand, you can manually input a host name, a map name, and required information, and register them.

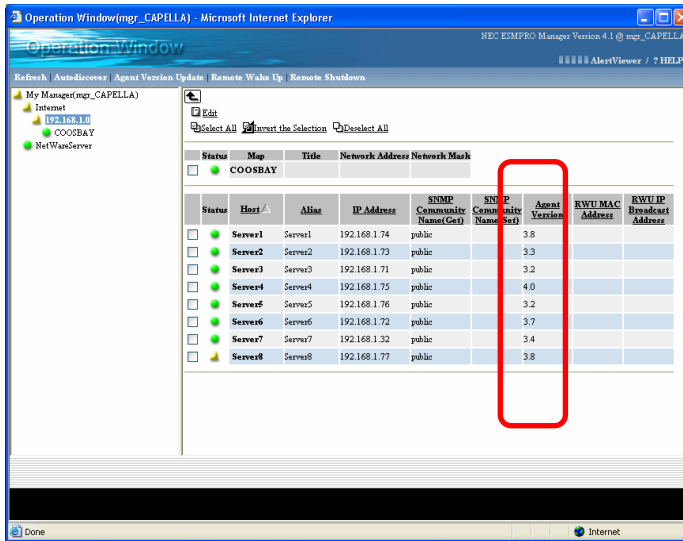
In addition, in order to start various tools from the Operation Window, it is necessary to set up the Agent Version property for the registered managed server appropriately.

Executing the Autodiscovery Function

1. Start the Operation Window, and select the Autodiscover menu from the Menu Bar.
2. Select the map for registering the discovered servers from the Map list.
3. Select Address and Mask from Address... to enter an appropriate value in the Network Address box and the Network Mask box, or select Range to enter the range of the address.
4. Type an appropriate community name in the SNMP Community Name box.
5. Click on the Start Autodiscovery button.



- After the Autodiscovery completes, execute Agent Version Update if the version of the registered host has not been set.



NOTE:

The map selected from the Tree Flame on the left of the Operation Window will be the default target map.

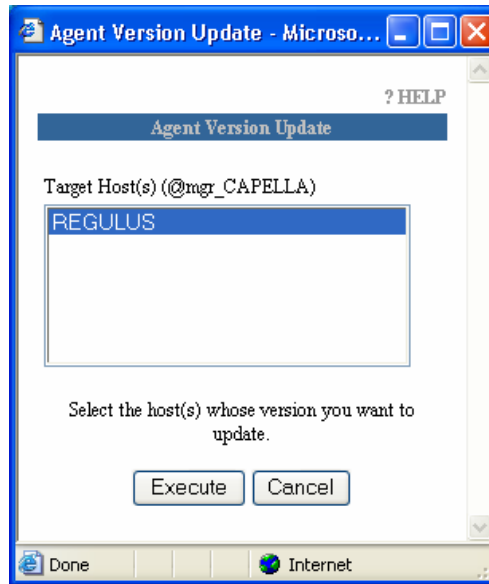
Keep in mind that the Web Component cannot perform Autodiscovery while the NEC ESMPRO Manager is performing Autodiscovery, or while performing automatic discovery from other browsers.

Autodiscovery does not obtain the Agent version of the discovered server. Some tools for a target host require the Agent version property to be set. Thus, run Agent Version Update to obtain the latest Agent version information after Autodiscovery completes.

It is recommended to edit the map configuration in the NEC ESMPRO Manager before editing the map configuration in the Web Component. Doing so helps you flexibly operate the map configuration.

Setting the Agent Version

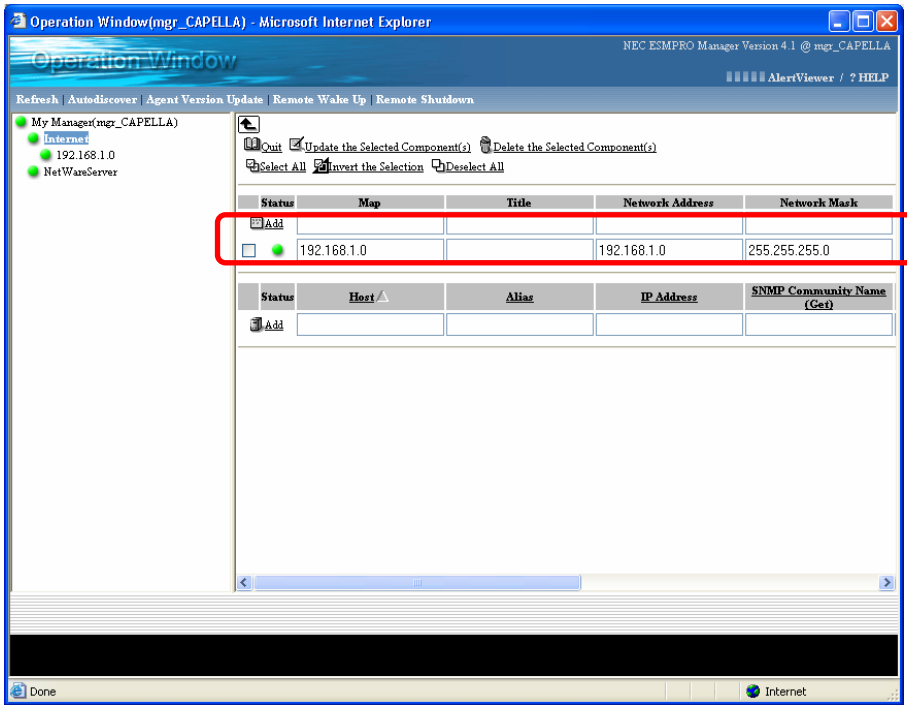
1. Turn on the check box of hosts or a maps containing hosts you want to update on the Operation Window, and select the Agent Version Update menu from Menu Bar.



2. Select hosts in the Target Host(s) List, and click on the Execute button.

Manually Adding a Map

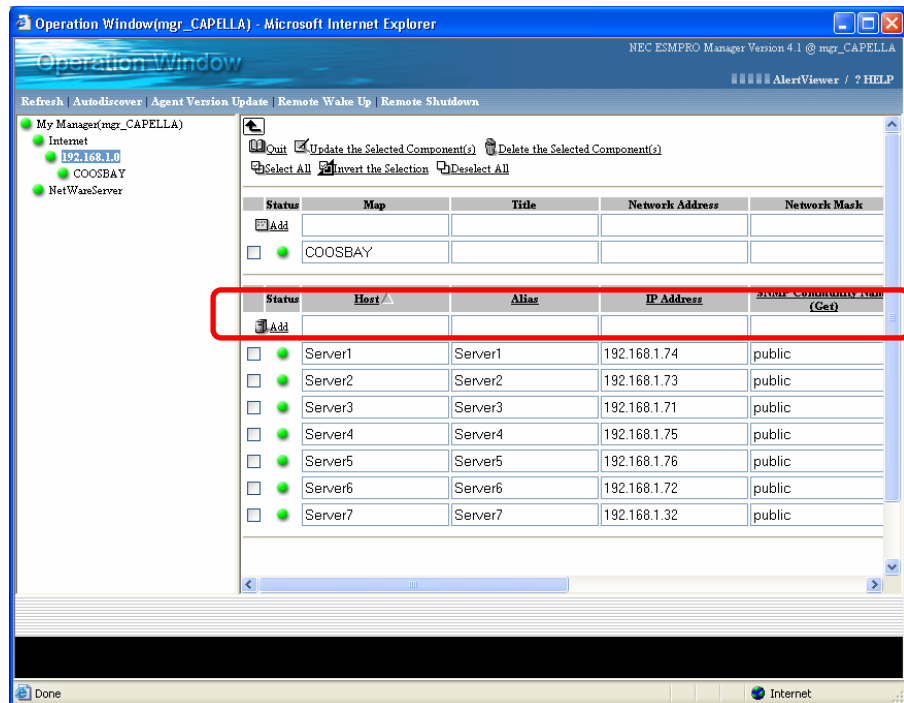
1. Select the map to which you want to add a new map.
2. Click on Edit above the Map List.
3. Enter an appropriate value in the each item box on the Area for adding a new map.



4. Click on Add on the Map List.

Manually Adding a Host

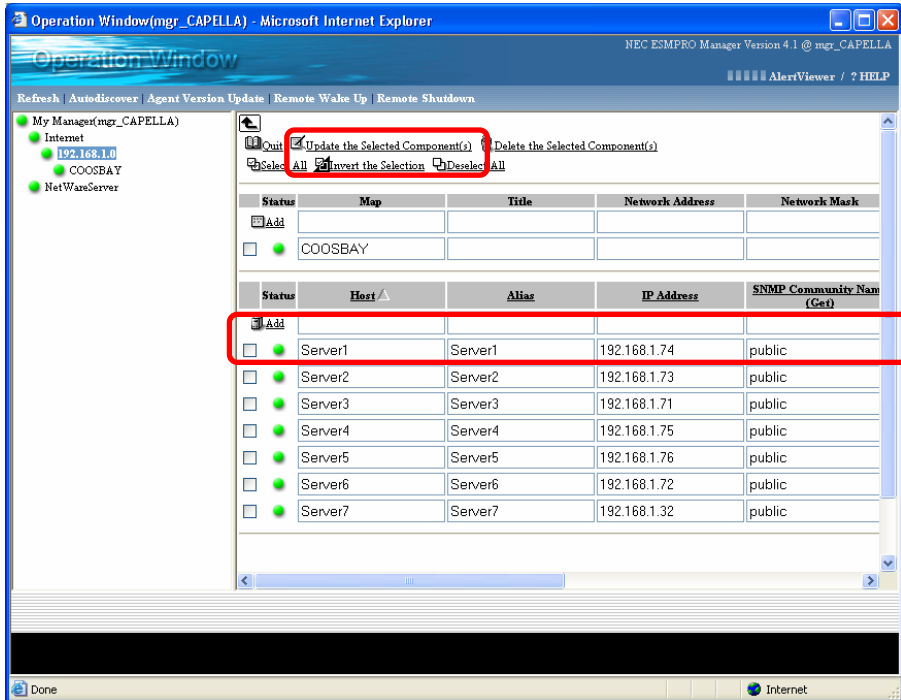
1. Select the map to which you want to add a new host.
2. Click on Edit above the Host List.
3. Enter an appropriate value in the each item box on the Area for adding a new host.



4. Click on Add on the Host List.

Editing Properties of Maps or Hosts

1. Select the map containing the map or host you want to edit.
2. Click on Edit above the Map or Host List.
3. Change the value on the properties of the map or host you want to edit.
4. Click on Update the Selected Component(s) above the Map or Host List.

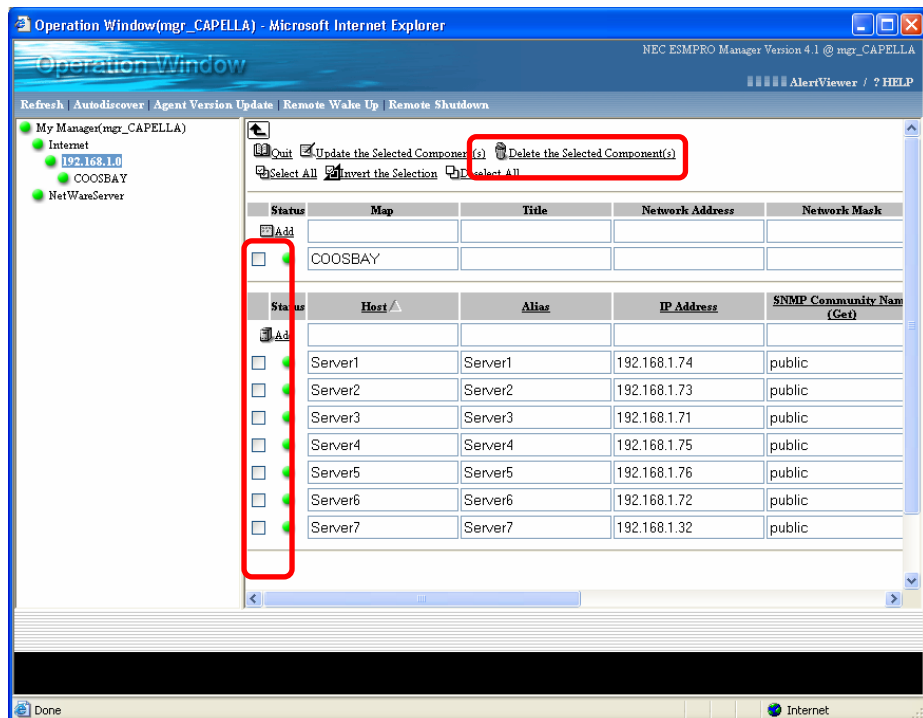


NOTE:

When you move to other entry item after changing a property of a map or host, the check box of the map or host is automatically turned on.

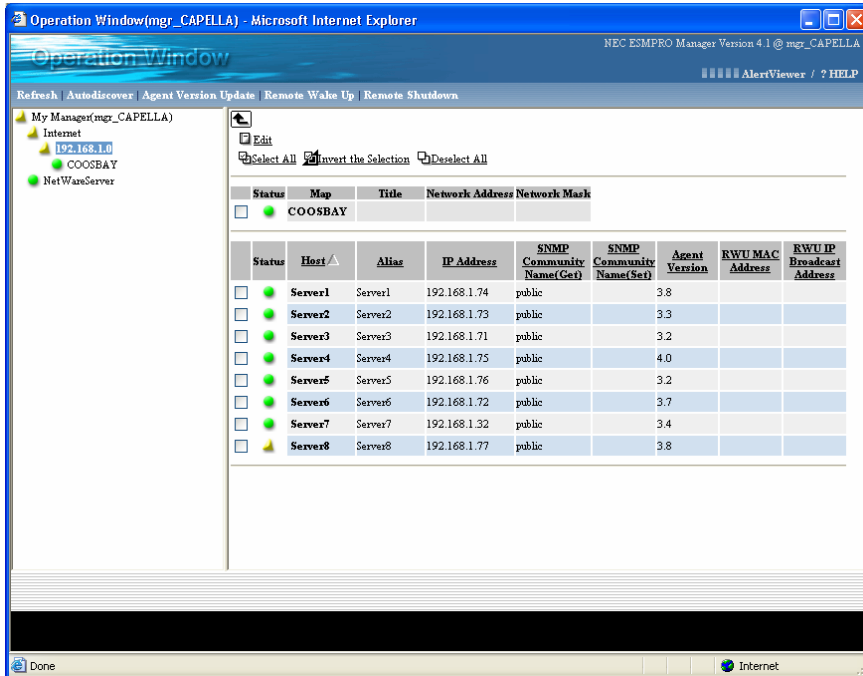
Deleting the Map or Host

1. Select the map containing the map or host you want to delete.
2. Click on Edit above the Map or Host List.
3. Turn on the check box of the map or host you want to delete.
4. Click on Delete the Selected Component(s) above the Map or Host List.



Monitoring the Server Status

The status of the registered server is automatically monitored, and icons on the Operation Window are changed according to the server status.



The following status icon is displayed to show the server status:

Status	Icon
Normal	
Warning	
Abnormal	
Unknown	

NOTE:

A list of the managed servers, and the status color are updated at one minute intervals. However, each property information needs to be updated by pressing the Refresh function.

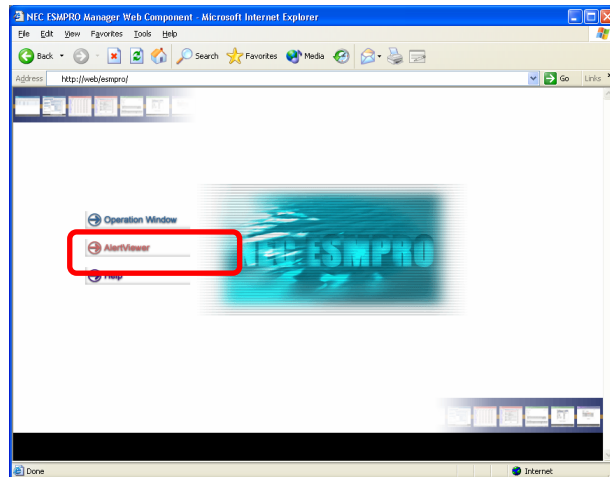
The status icon is displayed in gray (Unknown) when a target server is stopped or in sleep mode, or when any problems occur on the network.

ALERTVIEWER

The AlertViewer displays the alert messages sent to the NEC ESMPRO Manager.

Starting the AlertViewer

1. Click on "AlertViewer" displayed on the Web Component title page.



2. The AlertViewer starts, and a list of the received alert messages appears.

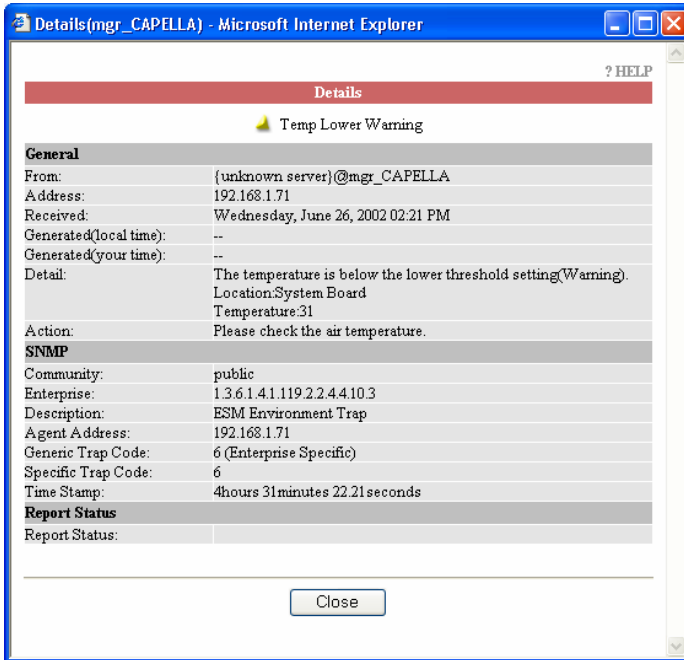
 A screenshot of the AlertViewer application window. The title bar reads 'AlertViewer (mgr_CAPELLA) - Microsoft Internet Explorer'. The interface includes a 'Reload' button and a table of alert messages. The table has columns for Summary, Type, Manager, Component, Address, and Received. There are five rows of data, each with a small icon to its left.

Summary	Type	Manager	Component	Address	Received
Disk Space	Logical Drive	mgr_CAPELLA	FOMALHAUT	192.168.1.75	06/06/2002 02:35 PM
Recovered From The Low Temperature Warning State	Temperature	mgr_CAPELLA	BETELGRUSE	192.168.1.71	06/06/2002 02:34 PM
Temp. Lower Recovered	Temperature	mgr_CAPELLA	BETELGRUSE	192.168.1.71	06/06/2002 02:34 PM
Disk Space	Logical Drive	mgr_CAPELLA	FOMALHAUT	192.168.1.75	06/06/2002 02:30 PM
Temp. Lower Warning	Temperature	mgr_CAPELLA	(unknown server)	192.168.1.71	06/06/2002 02:23 PM

NOTE: A newly received message is not added to the current list. Click on the Reload button to obtain the latest alert information.

Viewing a Detailed Alert Information

1. Click on Summary of the alert you want to see the details.
2. The detailed alert information is displayed on the Details window.

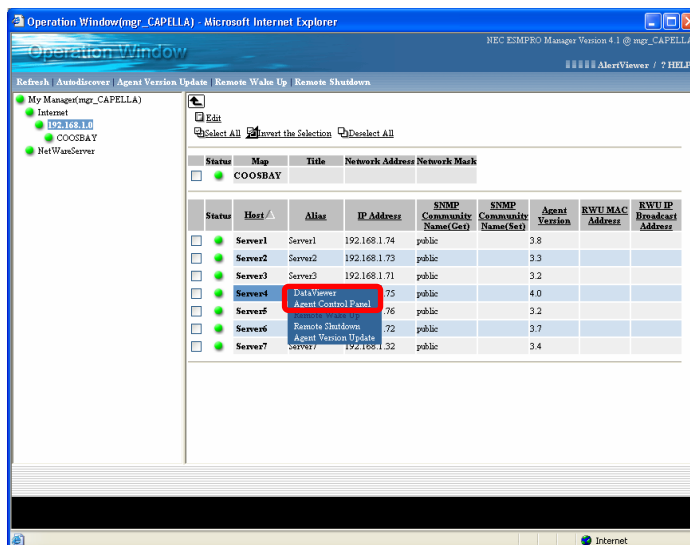


DATAVIEWER

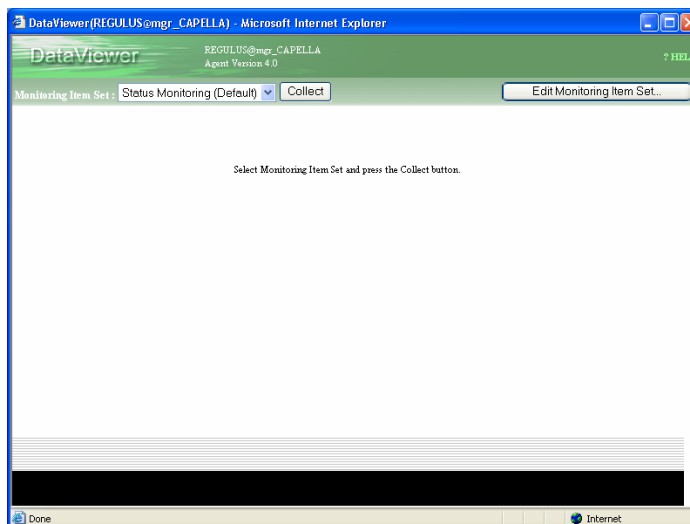
The DataViewer obtains the configuration information on the server in which the NEC ESMPRO Agent is installed and displays it in a tabular form.

Displaying a Server Configuration Information

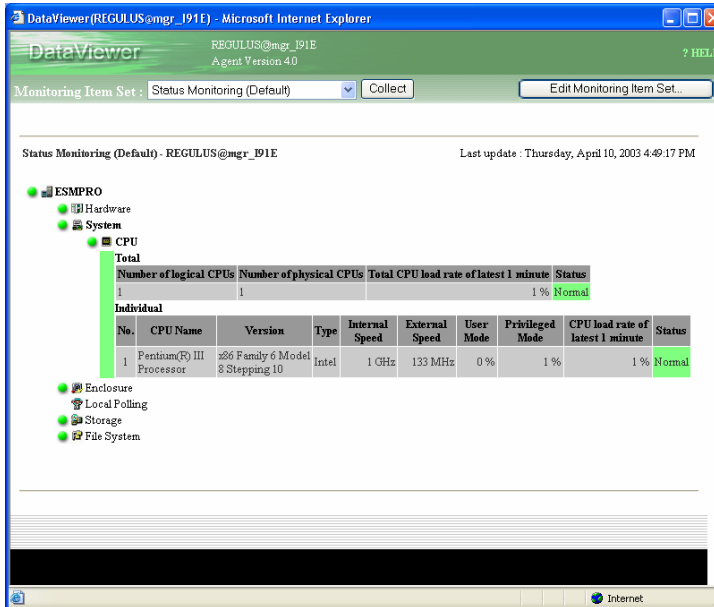
1. Position the cursor to a host on the Operation Window. Click on DataViewer when the pop-up menu appears.



2. The DataViewer starts.



3. Select the monitoring item set to be managed from the Monitoring Item list, and click on the Collect button.
4. The information on the selected monitoring item set is displayed.



NOTE:

The DataViewer of the Web Component supports the NEC ESMPRO Agent version 3.7 or later for Windows. Therefore, it does not display the information on the prior version.

The Agent Version of a target host must be properly set to start the DataViewer.

The information is not periodically updated. Click on the Collect button to obtain the latest information.

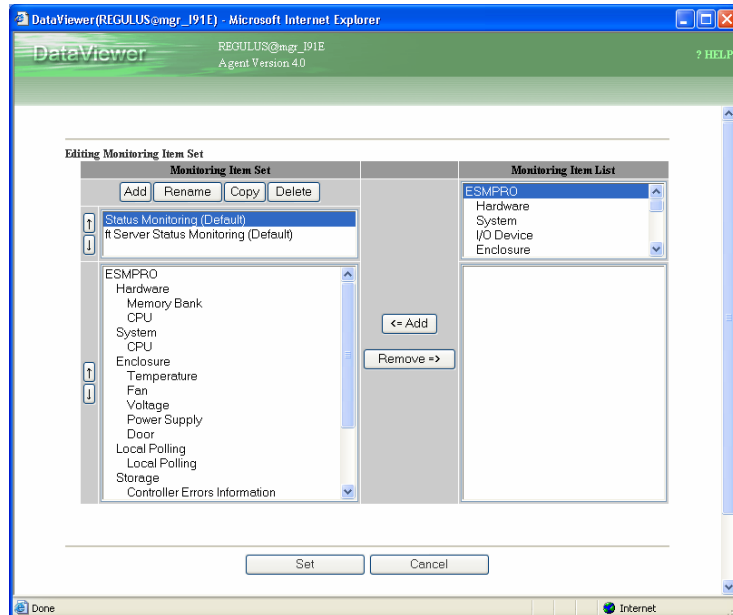
All or a part of the detailed information on some servers or some Agent versions may not be displayed.

An Item displayed in pale color and an item for which no values are displayed in the detailed information chart show that the NEC ESMPRO Agent did not return the information on that item due to some reasons, for example, the Agent does not support the item.

Customizing the Monitoring Item Set

The Monitoring Item Set can be customized. Defining it enables you to flexibly manage the servers.

1. Click on the Edit the Monitoring Item Set ...button on the upper right of the DataViewer window.
2. The Edit Monitoring Item Set window appears.



3. Click on the Add button of the Monitoring Item Set.
4. The Enter Motoring Item Set name to add dialog box appears. Type a monitoring item set name, and click on the OK button.
5. Select an item from the Monitoring Item List, and click on the <= Add button to add the item to the Monitoring Item Set List.
6. Add all items to be monitored, and click on the Set button.

NOTE:

Up to 100 monitoring item sets can be registered.

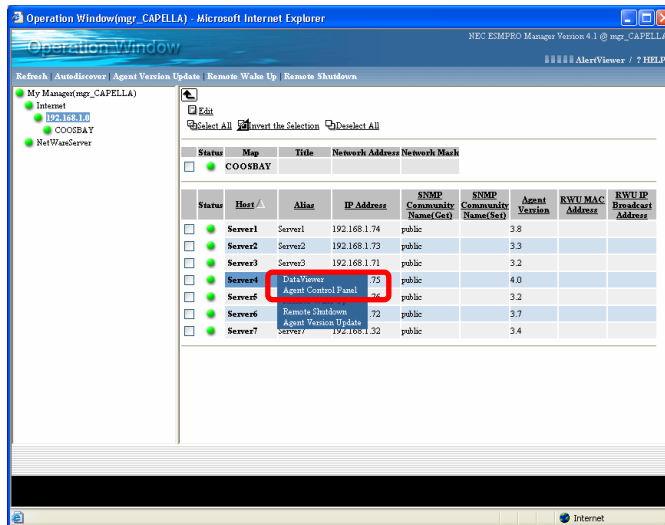
Pressing the Copy button enables you to create a new monitoring item set based on the existing monitoring item set.

AGENT CONTROL PANEL

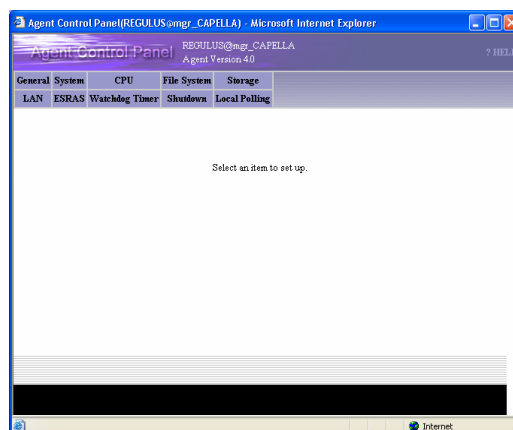
The Agent Control Panel allows you to change the operational settings of the NEC ESMPRO Agent.

Starting the Agent Control Panel

1. Position the cursor to a component on the Operation Window. Click on Agent Control Panel when the pop-up menu appears.



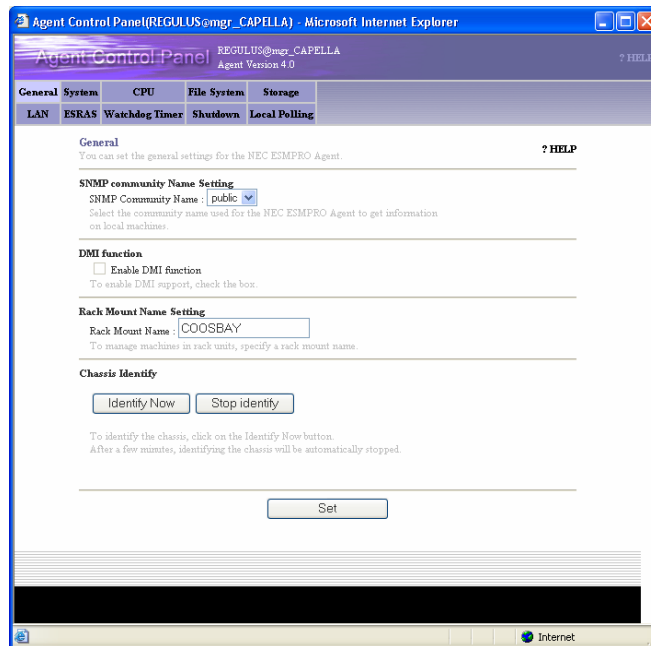
2. The Agent Control Panel starts.



NOTE: The Agent Version of a target host must be properly set to start the Agent Control Panel.

Changing the Operational Settings

1. In order to change settings, click on the tab of the item which you want to change in the upper part of the Agent Control Panel.



2. Enter or select the setting item on each tab.
3. Click on the Set button.

NOTE:

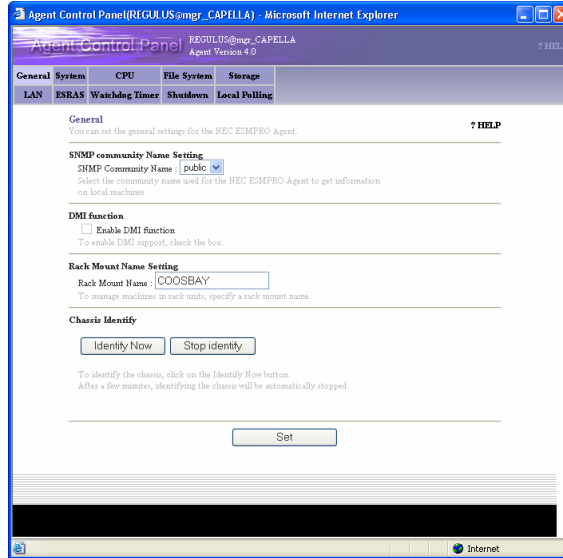
The information is not periodically updated. Click on the tab of the item again to obtain the latest information.

Depending on servers, some tabs may not be displayed or cannot be selected, or all or a part of the information may not be displayed or cannot be selected.

An item displayed in pale color shows that the NEC ESMFRO Agent did not return the information on that item due to some reasons that, for example, the server does not support the item.

The General Settings for the NEC ESMPRO Agent

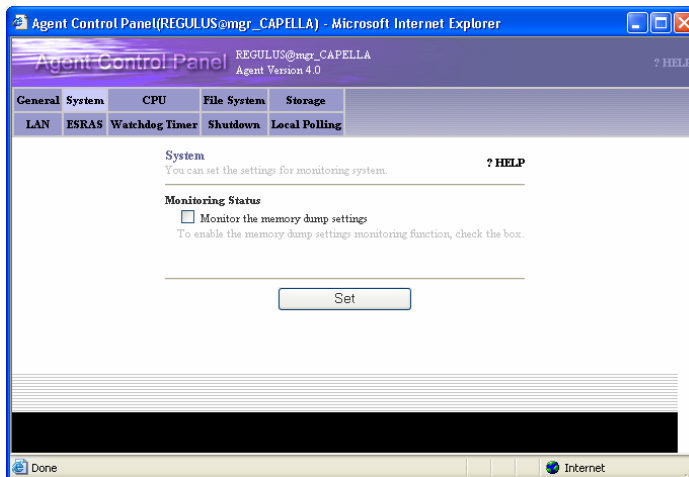
The General tab allows you to set the general settings for the Agent such as SNMP settings.



Monitor the Memory Dump Settings

Enabling "Monitor the memory dump settings" monitors the setting of the memory dump which is collected at the failure occurrence. Monitoring the memory dump setting helps avoid problems such that the necessary memory dump for investigating a failure cannot be collected.

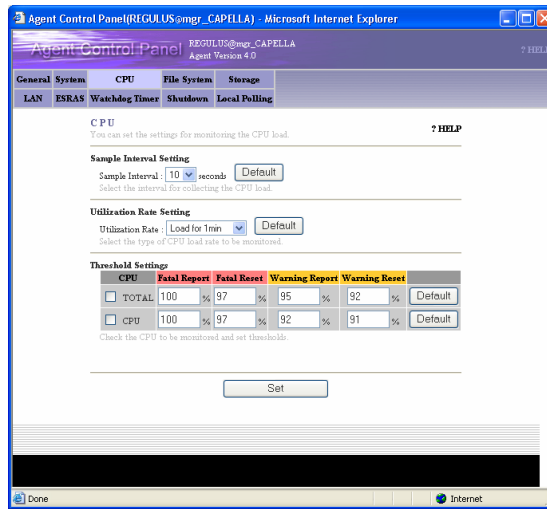
The dump setting which the memory dump can not be properly obtained is notified to the NEC ESMPRO Manager.



CPU

The CPU tab allows you to set the settings for monitoring CPU load. Monitoring CPU load can early detect high CPU load rate.

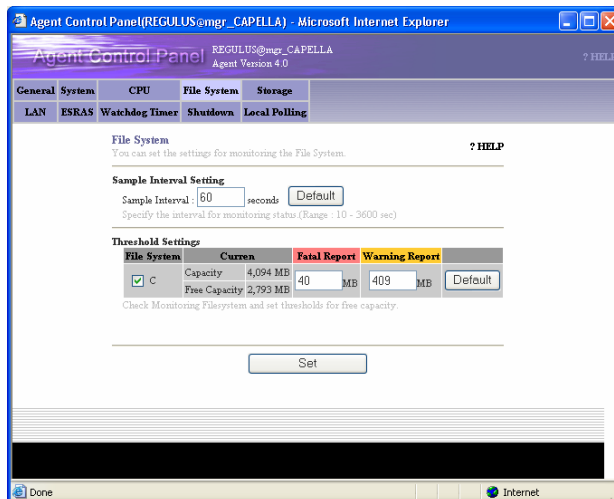
The CPU load status is displayed as the status color on the DataViewer and it is notified to the NEC ESMPRO Manager.



File System

The File System tab allows you to set settings for monitoring free capacity of the File System. Monitoring free capacity of the File System helps early detect the lack of free capacity.

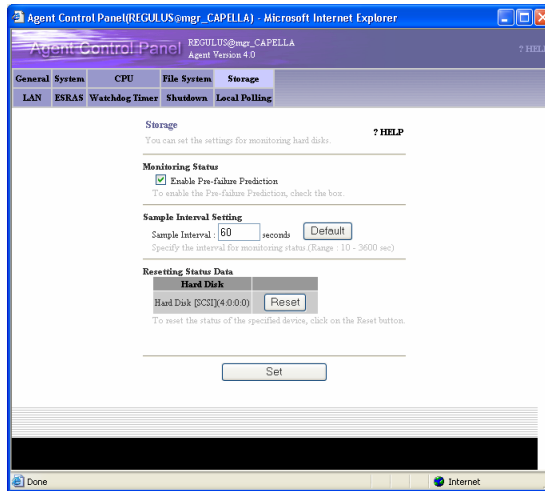
Lack of free capacity is shown as the status color on the DataViewer and it is notified to the NEC ESMPRO Manager.



Storage

The Storage tab allows you to set the settings for monitoring storage devices. The hard disk pre-failure prediction function monitors any failures in the hard disk. When monitoring storage devices is enabled, a failure can be detected before the hard disk breaks down. Therefore, you can take actions for it, for example, "replacing the hard disk with a new one before it breaks down. "

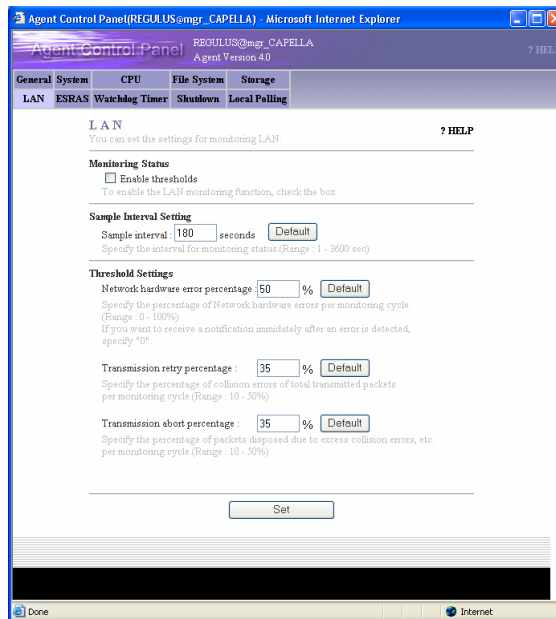
The failure status of the hard disk is notified to the NEC ESMPRO Manager.



LAN

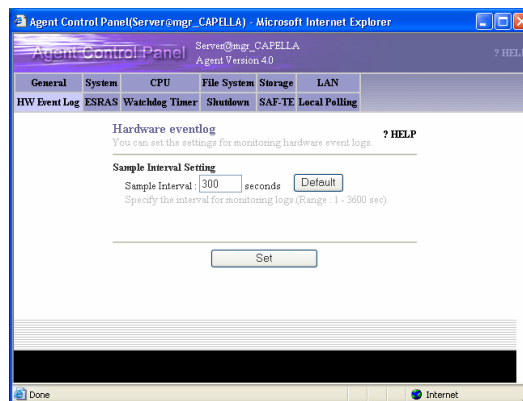
The LAN tab allows you to set the settings for monitoring packets received and sent from/to servers. When monitoring the packets is enabled, a failure on a line, the high load placed on a line, and lack of server resources can be detected.

A failure of LAN is notified to the NEC ESMPRO Manager or registered in the event log of the system.



HW Event Log

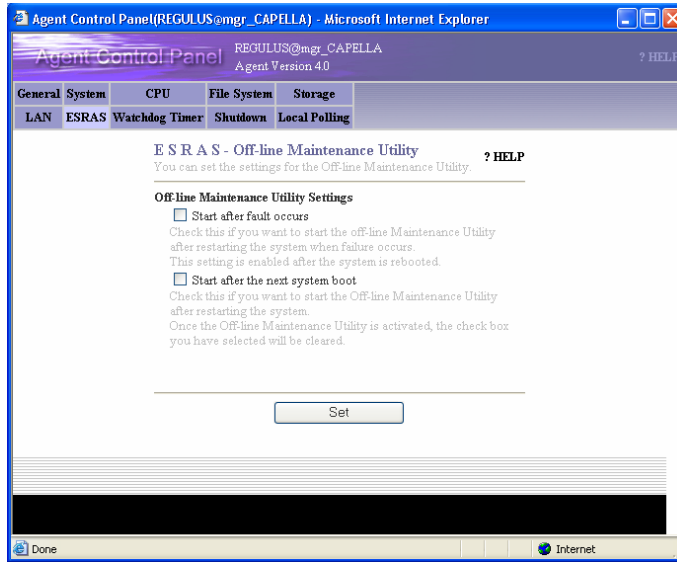
The HW Event Log tab allows you to set the settings for the hardware event log.



ESRAS

The ESRA S tab allows you to set the settings for activating the Off-line Maintenance Utility.

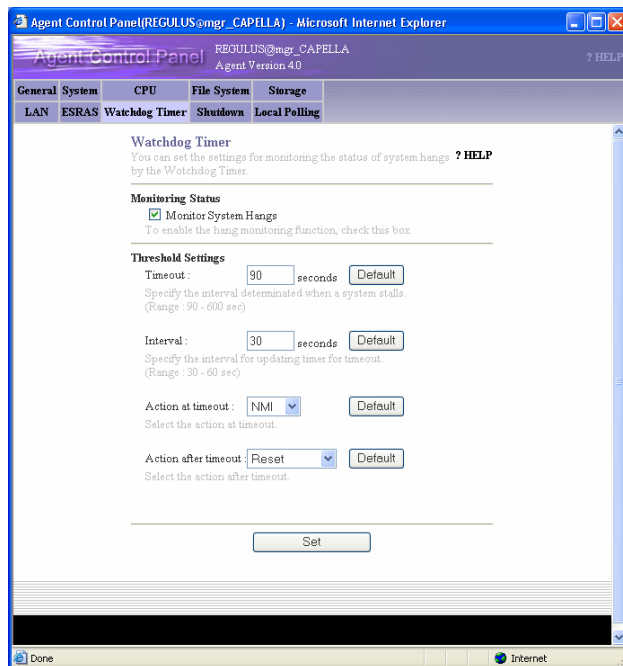
You can execute the preventive maintenance of hardware, isolate a failure, and restore the system according to the events detected from the hardware with the off-line utility.



Watchdog Timer

The Watchdog Timer tab allows you to set the settings for monitoring system hangs. Monitoring system hangs helps minimize the server stop time and negative effect on the business at the system hangs in automated/unmanned systems.

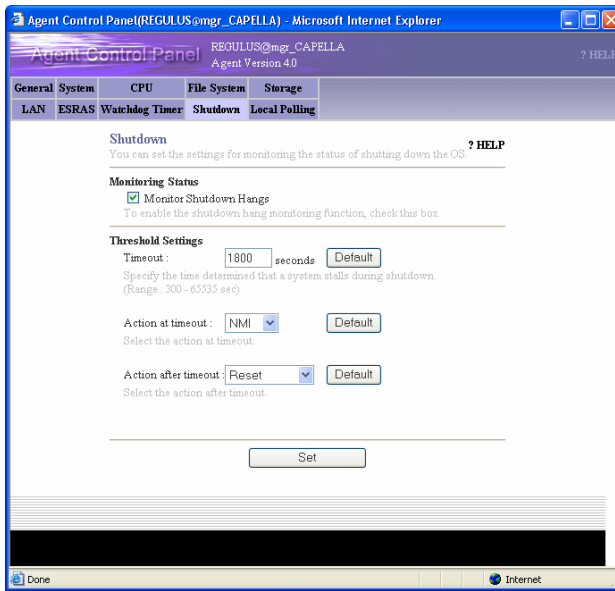
The monitored system hangs is notified to the NEC ESMPRO Manager.



Shutdown

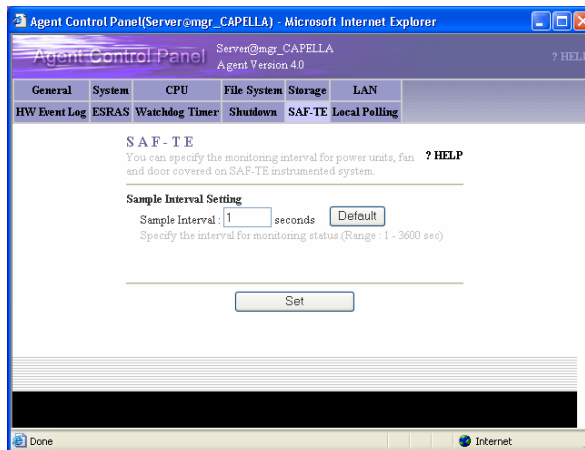
The Shutdown tab allows you to set the settings for monitoring the status of shutting-down the OS.

When monitoring the status of shutting-down is enabled, whether or not the OS is correctly shutdown can be monitored. The monitored system hangs at shutdown is notified to the NEC ESMPRO Manager.



SAF-TE

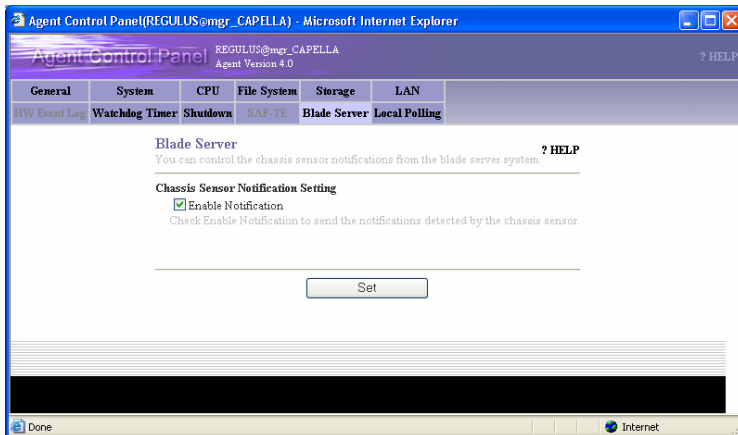
The SAF-TE tab allows you to specify the monitoring interval for power units, fan and door covered on the SAF-TE instrumented system.



Blade Server

The Blade Server tab allows you to set whether or not to report chassis events on a Blade server.

The Blade Server has a sensor which is shared by all blades. Therefore, the same chassis event is reported by the agent on each blade, resulting in multiple alerts from a single event. You can control the notifications from the all blades to avoid this when you set the notification settings here.

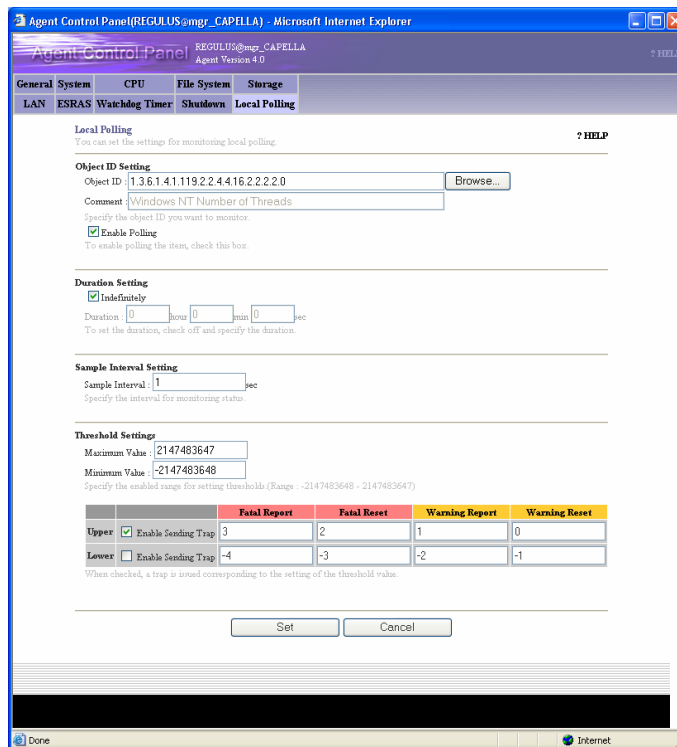


Local Polling

The Local Polling tab allows you to set the settings for monitoring local polling.

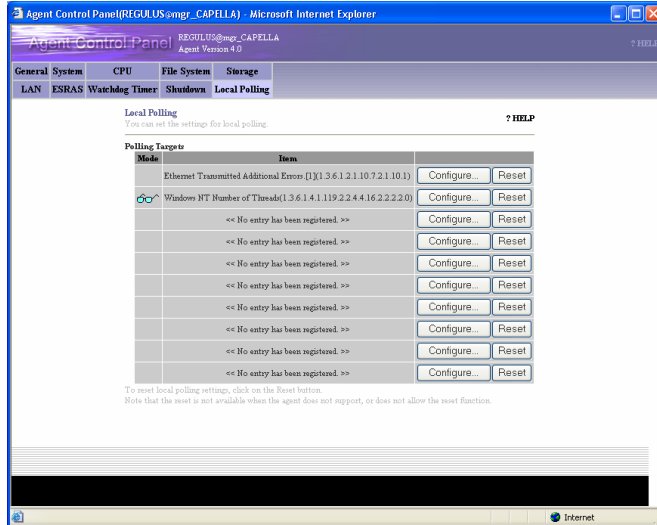
Using this function, you can monitor the items for which threshold setting function is not supported (e.g. network traffic information and used physical memory). Thus, an alert for the items will be sent when the monitored values are outside of the threshold range.

The monitoring status of managed servers is displayed as the status color on the DataViewer and it can be seen with the alert notification function of the NEC ESMPRO Manager.

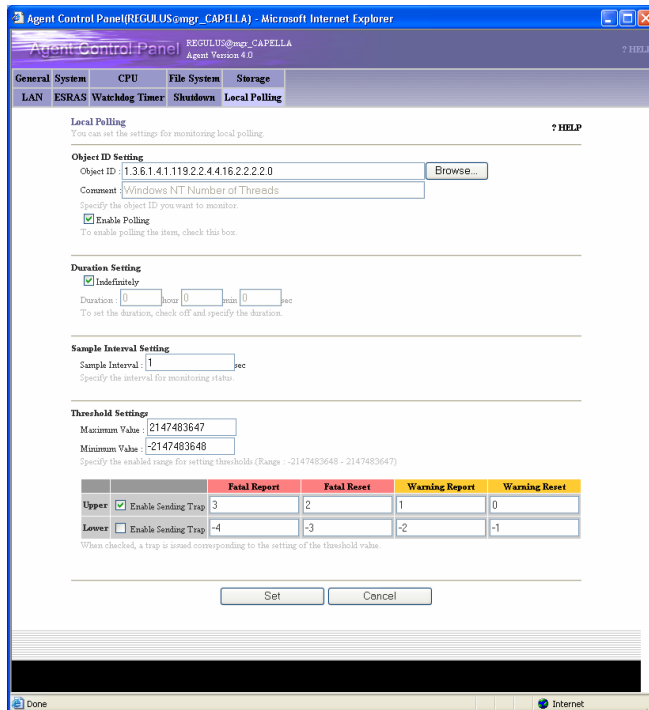


To use the Local Polling function, follow the instructions below.

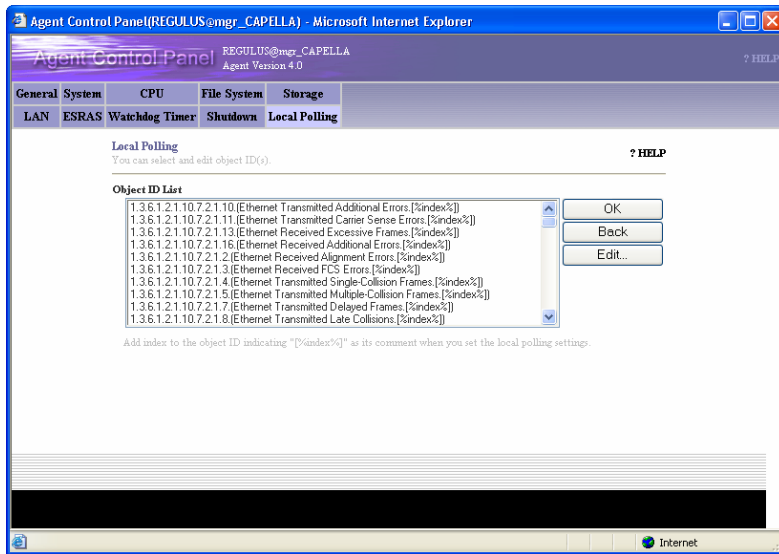
1. Click on the Local Polling tab.



2. Click on the Configure... button of the target to be registered or changed from the Polling Targets list.



3. Enter the object ID in the Object ID box. The object ID can be selected from the Object ID List by clicking the Browse... button if needed.



4. Set Duration, Interval, Maximum Value and Minimum Value.
5. Set appropriate threshold values.
6. Enable Polling allows you to set whether or not to monitor MIB. The value set in Interval is enabled only when this is checked.

NOTE:

Local Polling is a function for monitoring any items (only integers). This function is called "Local Polling" because the server status is monitored in the agent side (local) according to the values set. With this function, you can monitor the managed servers according to your system by setting a threshold, for example, the server status color will change and/or an alert will be sent when the monitored values are out of the threshold range.

If other SNMP products (SNMP Agent) is installed on the server to be managed, the MIB defined in that product can be monitored in the same way as the above.

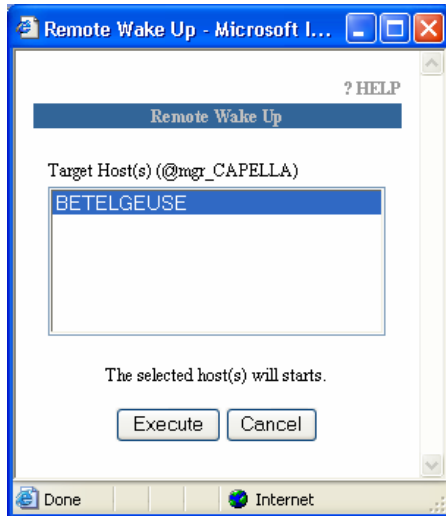
Note that an understanding of the managed server MIB information is required to determine appropriate local polling settings.

REMOTE WAKE UP

The Remote Wake Up function allows you to power on systems on the network.

To use the Remote Wake Up function, follow the instructions below.

1. Turn on the check box of the host or a map containing the host you want to start on the Operation Window, and select the Remote Wake Up menu.



2. Select hosts you want to start from the Target Host(s) List, and click on the Execute button.

NOTE:

To use the Remote Wake Up function, the "RWU MAC Address" and "RWU IP Broadcast Address" must be set.

The Remote Wake Up function needs to be enabled on the target host to use this function. See manual of each component for how to set it up.

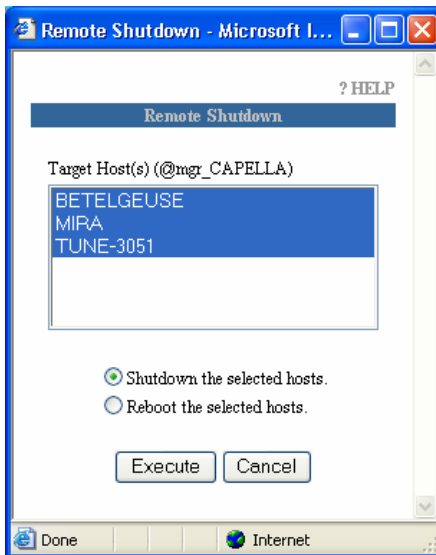
Additionally, the direct broadcast needs to be enabled in a router to use this function over the network via the router. See the router manual for details.

REMOTE SHUTDOWN

The Remote Shutdown function allows you to remotely shut down the system running on the network.

Remotely Shutting Down a Managed Server

1. Turn on the check box of a target host or a map containing the target host to be shut down on the Operation Window, and select the Remote Shutdown menu from the Menu Bar.



2. Select hosts to be shutdown from the Target Host(s) List, and click on the Execute button.

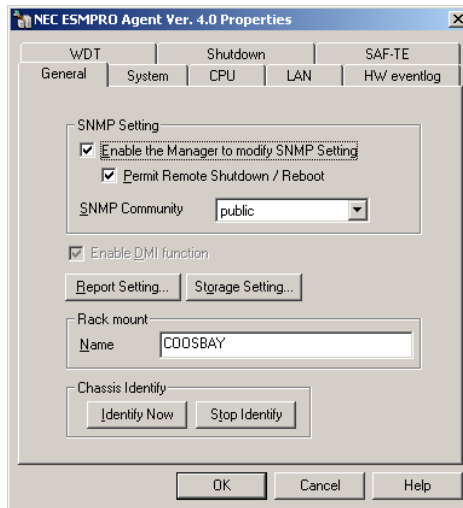
NOTE:

To use the Remote Shutdown function, the NEC ESM PRO Agent version 3.0 or later needs to be installed on the target host and its version also needs to be properly set on the properties on the target host.

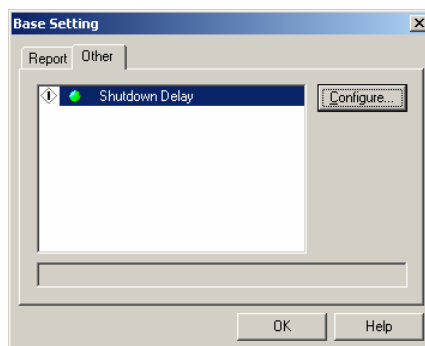
Setting the Agent Settings

The NEC ESMPRO Agent settings must be set on the target server to run the Remote Shutdown function.

1. Select NEC ESMPRO Agent from the Control Panel.
2. Select "Permit Remote Shutdown /Reboot " on the General tab.



3. Click on the Report Setting button on the General tab to open the Alert Manager window.
4. Select Base Setting from the Setting menu to open the Base Setting window. Select Other tab and check whether the green icon displayed on the left of the "Shutdown Delay" item as shown below or not. If not, click the icon to change to green.



5. Press the OK button to exit the menu.

Chapter 7

HP OpenView Integration

ABOUT THE HP OPENVIEW INTEGRATION

NEC ESMPRO Manager-HP OpenView Integration (HP OpenView Integration) is an application for using the server management functions provided in NEC ESMPRO Manager on HP OpenView Network Node Manager.

HP OpenView Integration includes the following functions:

- Auto-discovering and deleting NEC ESMPRO Agent
- Monitoring the NEC ESMPRO Agent status
- Launching DataViewer
- Launching Operation Window
- Launching AlertViewer
- Displaying NEC ESMPRO Agent traps

GETTING STARTED

Before you use the HP OpenView Integration, follow the instructions below.

Setting a method of receiving SNMP traps

To receive SNMP traps in the environment where NEC ESMPRO Manager and HP OpenView Network Node Manager coexist, select [Options] - [Customize] - [My Manager] on Operation Window and set Method of receiving SNMP Trap to "Use SNMP Trap Service" on the My Manager dialog.

Before auto-discovering of NEC ESMPRO Agent

Before you execute auto-discovery of NEC ESMPRO Agent to be managed, the sub map of the managed host needs to be registered on HP Open View Network Node Manager. If not, auto-discovery cannot be executed for the host. Therefore, be sure that the host is registered before executing auto-discovery.

USING HP OPENVIEW INTEGRATION

Auto-discovering NEC ESMPRO Agent

To register NEC ESMPRO Agent to be managed, select [Tools] - [NEC ESMPRO Manager] - [Agent Discovery] to display the NEC ESMPRO Agent Discovery wizard.

This function finds nodes which support SNMP from those registered on HP OpenView Network Node Manager, and then discovers NEC ESMPRO Agent from those nodes. When NEC ESMPRO Agent is discovered, an NEC ESMPRO Agent symbol is registered on a node sub map corresponding to it.

Monitoring the NEC ESMPRO Agent status

The HP OpenView Integration function collects the status information obtained by NEC ESMPRO Manager and sets it as the status of the NEC ESMPRO Agent symbol. Thus, the status color of the managed NEC ESMPRO Agent is reflected to the NEC ESMPRO Agent symbol.

Deleting NEC ESMPRO Agent

To delete a registered NEC ESMPRO Agent symbol, select [Tools]-[NEC ESMPRO Manager] - [Delete Agent] to display the Delete NEC ESMPRO Agent dialog.

At first, the process finding NEC ESMPRO Agent symbols from the selected network symbol is performed, and then component names set in the NEC ESMPRO Agent Component Name field and sub map names on which symbols are registered are listed.

Select NEC ESMPRO Agent you want to delete from the list, and press the [Delete] button to delete it. When you select the [Select All] button, all symbols of the list can be selected.

Launching DataViewer

To launch DataViewer, double-click an NEC ESMPRO Agent symbol or select DataViewer from the pop-up menu displayed by right-clicking the symbol.

Launching Operation Window

To launch Operation Window, select [Tools] - [NEC ESMPRO Manager] - [Operation Window].

Launching AlertViewer

To launch AlertViewer, select [Tools] - [NEC ESMPRO Manager] - [AlertViewer].

Displaying NEC ESMPRO Agent traps

The HP OpenView Integration enables SNMP traps sent by NEC ESMPRO Agent to be displayed on Alarm Browser of HP OpenView.

The ESMPRO/SM Trap Redirection service receives an SNMP trap sent by NEC ESMPRO Agent, and sends it to HP OpenView Network Node Manager (local host).

Then, the SNMP trap is displayed on Alarm Browser.

This forwarding setting is always automatically made at installation, however, you may have to manually set it after the installation if:

- 'public' is not registered as the SNMP community name that HP OpenView accepts.
- Some kind of settings have been already set for the ESMPRO/SM Trap Redirection service.

In such cases, select [NEC ESMPRO Manager]-[SNMP Trap Redirection Setting] from the Start menu to launch SNMP Trap Redirection Setting and change or add the items of Destination Setting as follows:

Host name or IP address: 127.0.0.1

Community name: A name of an SNMP community that HP OpenView accepts

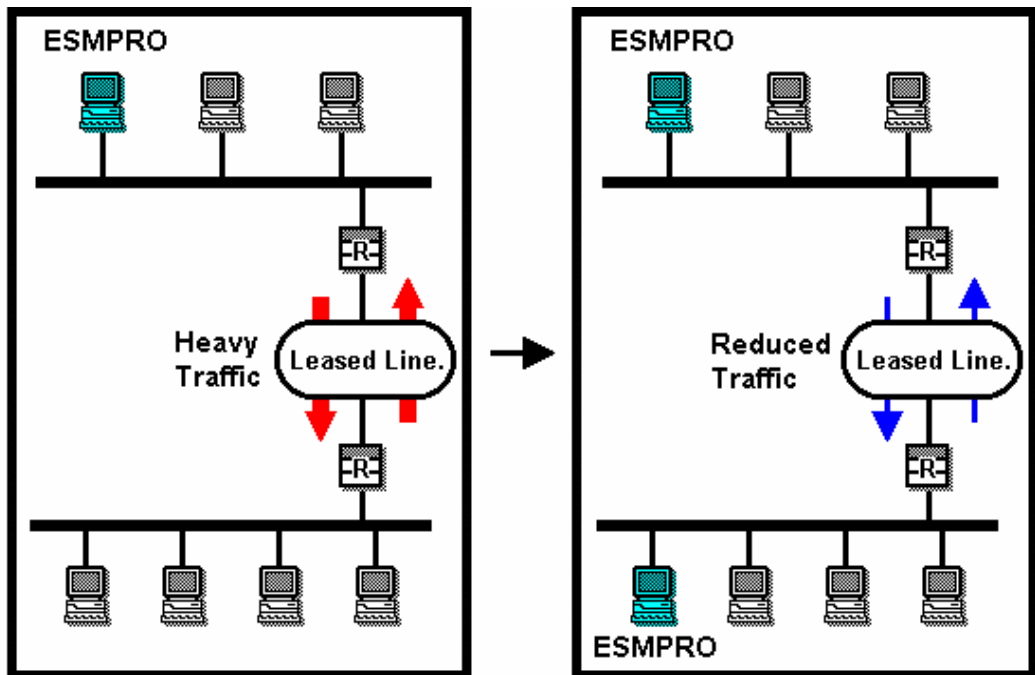
Appendix A

Inter-Manager Communication

ESMPRO software in a Manager can monitor approximately 100 units, although this number varies according to what is monitored. You can register more than 100 units in the configuration information on the screen. The number of units that can be managed depends on the performance of managers and routers. Limitations occur when availability management is carried out on all managed units within a short interval.

The ESMPRO system exchanges packets with the SNMP Agent. To monitor many Agents over a thin line, such as a private line, you should divide them into communities for the best results.

Figure A-1 shows two different routing configurations.



Managing with a single Manager

Managing with multiple Managers

Figure A-1 Routing Configurations

Each Manager is recognized by a Manager name that consists of up to 63 characters including the hyphen (-), underscore (_), and period (.). The Manager name can be changed in the My Manager Dialog screen by selecting My Manager from Customize menu in the Option menu.

You can group communities by network, level, or a combination of the two for the inter-Manager communication. Figures A-2 and A-3 show the two types of configurations. In Figure A-2, foo, bar, and the shina are Manager names. If you group communities by level, you may want to name the communities using the Domain Name System (DNS).

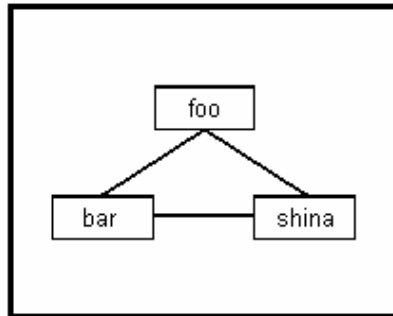


Figure A-2 Network Manager Group

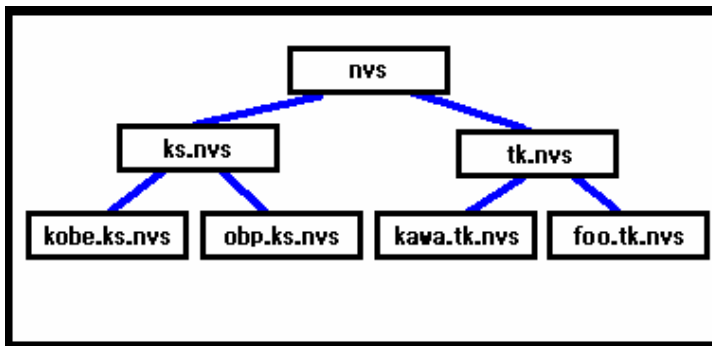


Figure A-3 Ladder Manager Group

In Figure A-3, the three communities, nvs, kawa.tk.nvs, and foo.tk.nvs, are directly connected to each other. Both ks.nvs and tk.nvs are adjacent communities. The TCP/IP connection is always established to adjacent communities. However, establishing a connection between two adjacent communities requires making some settings in the Remote Manager dialog.

Indirect communication to a non-adjacent Manager can be made available with the Manager routing function. For details about these procedures, see Setting Up Inter-Manager Communication, in Chapter 3, Using the ESM PRO Manager.

Appendix B

Note

MANAGER

1. About versions of NEC ESMPRO Manager and NEC ESMPRO Agent

If a version of NEC ESMPRO Manager is older than that of NEC ESMPRO Agent, a problem may occur such as the configuration information cannot be displayed, or received alerts are not correctly displayed, and so forth. Update NEC ESMPRO Manager to the version equal to or later than that of NEC ESMPRO Agent.

2. About coexistence of ESMPRO Manager with Non-NEC Made SNMP Management Application

In case when other vendor's SNMP management application which receives SNMP trap is used as well as NEC ESMPRO Manager at the same time, one of them may fail to receive SNMP trap due to conflict between the two applications. Through the following procedures, such situation can be avoided.

<Work Around 1>

If the other vendor's SNMP management application supports the trap reception of standard SNMP Trap Service, you can change the setting of NEC ESMPRO Manager according to the instruction below.

By selecting [Option]→[Customize]→[My Manager] of the Operation Window, change [Method of receiving SNMP Trap] to [Use SNMP Trap Service].

NOTE: SNMP Trap service can be installed by installing the SNMP service, however, the service will not start in the default state. Start SNMP Trap Service by starting Service of the Control Panel. (More convenient if startup type is set "Automatic".)

However, the following restrictions exist.

- If the trap by IPX protocol from NetWare server is received, host name of the sender (server name) cannot be identified.
- Restriction for receiving trap packet by SNMP Community name specified by selecting [Option]→[Customize]→[Environment] on the Operation Window will be disabled.

< Work Around 2 >

By utilizing "TCP/IP report to Manager" of NEC ESMPRO Agent, alert reception function of NEC ESMPRO Manager operates normally.

TCP/IP report to Manager: By transferring alert from server to NEC ESMPRO Manager using original protocol, alert can be transferred without fail.

However, the following restrictions exist.

- The operability of SNMP Trap reception function of other vendor's SNMP management application cannot be guaranteed.

3. About the operation of machine with Suspend/Resume function

With the use of Suspend/Resume function, the performance of manager might become unstable. In such case, do not use this function.

4. About transfer of DMI events on Inter-Manager Communication

DMI events are not transferred between the Inter-Manager Communication.

5. Installing other DMI management application and manager on the same machine

In case when other DMI management application (such as Intel LANDesk Client Manager, etc.) is installed to the same machine, receiving DMI events with AlertViewer may not work properly.

Be sure not to install Manager and DMI management application on the same machine.

6. Receiving DMI events from the machine belonging to multiple networks

Receiving DMI events from the machine (with multiple IP addresses) belonging to multiple networks may not be available. In such cases, use SNMP trap or TCP/IP In-Band for notification from Agent to Manager.

7. About using NEC ESMPRO Manager on a machine with high load

- When a machine on which the NEC ESMPRO Manager is installed is under high load

If you use the machine with extremely high load such as when 100% of the CPU has been used for a long time period, the following message may appear:

Communication with NVBASE System Service became invalid.

Manager applications communicate with a service (NVBase System Service) by design. The above message appears when the communication is timed-out due to high load.

In such a case, decrease the load on the machine and restart the application.

- When a machine on which the NEC ESMPRO Agent is installed is under high load

If a machine on which the NEC ESMPRO Agent is installed is under high load, NEC ESMPRO Agent does not respond to the query from the NEC ESMPRO Manager. Therefore, the following problems may occur:

- The icon for the machine is grayed out on the Operation Window.
-

- The following error messages are displayed when the DataViewer is started.

Could not collect information on the server.

Please refer to Recovery Action for errors in DataViewer Help.

- The machine information becomes "Unknown" on the DataViewer.
- The following message is registered in the AlertViewer when the "Detect Server Down" property is "On".

Summary: No response from the server.

Detail: Alert generation time ...

The server doesn't respond to SNMP access from Manager. There is the possibility that the server is down, the load on the server has been excessively increased or the network is not functioning properly.

8. About usage of DHCP

As NEC ESMPRO Manager manages system according to IP Address, DHCP which assign IP address dynamically cannot be used.

9. About transmitting and receiving of packet between NEC ESMPRO Manager and NEC ESMPRO Agent

Packets will be transmitted/received between NEC ESMPRO Manager and Agent in the following timing.

We recommend reasonable care in operating in the system which charges you such as connection on WAN.

- At autodiscovery of servers on Operation Window.
 - At specified interval after specifying regular autodiscovery on Operation Window.
 - When deleted server where DMI agent is checked for its properties on Operation Window.
 - When DMI Agent is registered on Operation Window.
 - When the DMI Agent is turned OFF on Operation Window.
 - When the DMI Agent is turned ON on Operation Window.
 - When Remote Wake UP is executed on Operation Window.
 - Irregularly, after specifying inter-manager communication on Operation Window.
 - At receiving SNMP Trap.
 - At receiving DMI event.
 - At startup of Operation Window, for all the DMI agents registered at Operation Window.
 - About every one minute after DataViewer is started.
 - About every one minute after GraphViewer is started.
 - At specified interval for specified server, after setting Automatic Data Collection.
 - Regular polling at about every one minute to monitor server status.*
-

* Can be avoided by turning "Watch Server Status" off at Properties of Operation Window's server icon, however, the server status will not be reflected to the color of icon on the Operation Window.

10. Setting a SNMP trap destination

When you install NEC ESMPRO Manager and NEC ESMPRO Agent on the same computer, specify the IP address assigned to the network card or the host name as the SNMP trap destination for the computer, instead of the loop back address 127.0.0.1.

If you specify 127.0.0.1, "unknown server" may be displayed on the AlertViewer.

On the other hand, you may need to specify 127.0.0.1 for a computer not to be connected to the network. For more information, "Settings on standalone environments without network connections" below.

If the following is displayed on the AlertViewer even when you have specified as above,

Component: {unknown server}

Address: 127.0.0.1

change the IP address to 127.0.0.1 on the properties of the server icon on the Operation Window.

11. Settings on standalone environments without network connections

When you install the NEC ESMPRO Manager and the NEC ESMPRO Agent on a machine together and if the machine is not connected to the network, take the following steps to monitor the machine itself:

- Select to specify addresses on the AutoDiscover dialog of the Operation Window, and specify 127.0.0.1 for Start Address and End Address.
- Specify 127.0.0.1 for the SNMP trap destination.

If you have already registered server icons, execute AutoDiscover after deleting the icons.

12. About the NEC ESMPRO User Group

Since security for the NEC ESMPRO Manager is managed by the NEC ESMPRO User Group, the NEC ESMPRO Manager never starts without accessing to this group.

Note on the followings:

- 1) Do not delete/change the NEC ESMPRO User Group after installing the NEC ESMPRO Manager.
- 2) When the NEC ESMPRO User Group is registered as global group member, it is necessary to start Domain Controller before Manager machine boots.

13. About the threshold dialog for temperature sensor

For some servers, only the Fatal status may be displayed on the dialog for setting threshold values of temperature sensor. In this case, the sliders show yellow as normal status, but green is displayed as the actual status color when temperature of a target machine is lower than the specified Fatal limit.

14. About versions when using Inter-Manager Communication

If you use Inter-Manager Communication between different versions of the NEC ESMPRO Manager, the following problems may occur.

- The alerts will not be sent to the neighbor manager.
- Part of the information will not be displayed in the DataViewer.

When you use Inter-Manager Communication, in advance, be sure to use same version of the NEC ESMPRO Manager by performing update installation if needed.

15. About versions of NEC ESMPRO Agent and NEC ESMPRO Manager when ft servers are monitored

Policies for deciding the status colors of ft servers vary depending on versions of NEC ESMPRO Agent and NEC ESMPRO Manager. Therefore, use NEC ESMPRO Agent Ver. 3.8a (or later) or NEC ESMPRO Agent Ver. 4.07 (or later) when this version of NEC ESMPRO Manager monitors ft servers, otherwise inappropriate status colors will be displayed.

16. To upgrade your operating system

Please uninstall NEC ESMPRO Manager before upgrading Operating System.

For Windows Server 2003, however, upgrade the NEC ESMPRO Manager to Ver. 4.1 first, and then upgrade the operating system. Doing so allows you to go on using the NEC ESMPRO Manager.

If the Web component has been installed in this case, you may not use it because the World Wide Web Publishing Service is disabled. In such a case, start up IIS (Internet Information Service) Manager on a Web server, and then start Default Web Site (Stopped).

17. About Specifying option of AlertViewer

After changing the option setting of AlertViewer and pressing OK button, if Operation System is shut down while AlertViewer remains running, the changed setting will not be stored.

Please exit from AlertViewer prior to shutting down the Operation System after changing the setting.

18. About the operation of the NEC ESMPRO Manager on Terminal Client

The NEC ESMPRO Manager does not support operations on a terminal client / a remote desktop.

19. About the alert message in AlertViewer

In the AlertViewer, the alert message containing characters other than English (e.g. Chinese) cannot be displayed correctly. Therefore, keep in mind that even if the alert message which contains those characters is watched and notified by the event log monitoring function of NEC ESMPRO Agent, it cannot be checked in the AlertViewer.

20. About monitoring DMI Agents

The DMI monitoring function has been removed from the NEC ESMPRO Manager Ver. 4.1 or later. As a result, the Manager behaves as follows.

- DMI Agents are discovered by the auto-discovery function, and displayed as icons on the Operation Window.
- DMI events are received, and displayed on the AlertViewer.
- Status of DMI Agents are not monitored through DMI even if the "Watch Server Status" properties are "On".
- The information of the DMI Agents is not viewed on the DataViewer or the GraphViewer, and not collected by the Automatic Data Collection function.

21. Maps to be specified at autodiscovery

After you execute Autodiscover on Operation Window, maps may be displayed as if they were registered infinitely as shown below:

```
Ex.) My Manager
    + Internet
      + 192.168.1.0
        + mapA
          + mapA .....(*)
            + mapA
              :
```

This problem occurs when you execute Autodiscover on maps which were created at autodiscovery, such as rackmount maps, cluster maps and blade maps. In such a case, delete the second mapA marked with (*) in this example to resolve the situation.

If you re-execute Autodiscover with icons already registered, do not specify maps which were automatically created at the previous autodiscovery, such as rackmount maps, cluster maps and blade maps.

22. Note on using NEC ESMPRO Manager on Windows XP Service Pack 2

NOTE:

NEC ESMPRO Manager on Windows XP Service Pack 2 does not support receiving DMI events. You need not use DMI for managing Express servers because DMI is a protocol for managing other companies' servers.

On Windows XP Service Pack 2, communication between NEC ESMPRO Manager and NEC ESMPRO Agent will be interrupted due to Windows Firewall. Do the following to avoid this issue:

■ Setting Windows Firewall Port

[Problem]

By default, Windows Firewall is enabled in Windows XP Service Pack 2.

When you use NEC ESMPRO Manager and NEC ESMPRO Agent on Windows XP Service Pack 2, they cannot communicate with each other due to Windows Firewall. Thus, servers cannot be managed.

[Steps to open Windows Firewall Port]

- 1) Open [Control Panel], and click [Security Center].
- 2) On the [Windows Security Center] dialog box, click [Windows Firewall].
- 3) On the [Windows Firewall] dialog box, click [Exceptions] tab and click [Add Port...].
- 4) On the [Add a Port] dialog box, enter values in the [Name] and [Port number] fields, select [TCP] or [UDP], and click [OK].

[Target Ports]

The following table shows the ports for Windows Firewall to be set on the [Add a Port] dialog box on a machine on which NEC ESMPRO is installed.

Name (can be changed)	Port number	Protocol	Environment
Inter-Manager communication	8806	TCP	When Inter-Manager communication is used.
SNMP Trap	162	UDP	When Manager Notification (SNMP) is used (default).
High Reliable Notification	31134	TCP	When Manager Notification (TCP/IP in Band) is used.
Express Notification via Manager	31136	TCP	When Express Notification Service is used via Manager.
Web Component	80	TCP	When Web Component is used.

■ Monitoring a server where multiple IP addresses are set for its single network card.

[Problem]

If a monitored server has multiple IP addresses for its single network card, the IP address of the SNMP Response packet from NEC ESMPRO Agent may differ from the source address in the IP header of the SNMP Request packet from NEC ESMPRO Manager.

In such a case, if NEC ESMPRO Manager receives the Response packet from NEC ESMPRO Agent before Windows Firewall Service starts, the server cannot be monitored thereafter.

[Steps to avoid this issue]

On Operation Window, open [Properties] on the server icon, change the IP address to other one that is set on the monitored server, and reboot the Manager computer.

23. Autodiscovery of Blade Servers

When you execute Autodiscover and register blade servers, the number of slots for storing blades may be displayed differently from the actual one, and icons may be placed outside of the frame.

In such a case, follow the steps below to change map properties on Operation Window of the main NEC ESMPRO Manager:

- 1) Right-click the target blade map icon, and select [Properties] from the pop-up menu.
- 2) Double-click [Background], and select an appropriate background image.
- 3) Double-click [Maximum Number of Blade Slot in Chassis], and set an appropriate maximum number of slots.
- 4) Click [OK] to complete the settings.

24. About a value that displayed in "Rebuild Status" when LSI Logic's disk array controller is used

When a physical device is rebuilt, an incorrect value may appear in "Rebuild Status" of the [Physical Device] window from [Disk Array] of DataViewer. In such a case, use "Power Console Plus" (Management Utility of a disk array RAID system) to check the actual rebuild status. You can check the rebuild completion with the [Physical Device] window. When the rebuild successfully completes, "Status" is turned from "Rebuild" to "Online".

WEB COMPONENT

1. About the virtual directory for the Web Component after uninstalling

If you have changed the default virtual directory name (esmpro) of IIS used by the Web Component, or if you have installed the Web Component on Windows XP 64-bit Edition, the virtual directory is not deleted even when you uninstall the Web Component. In such a case, uninstall the Web component, and then manually delete the virtual directory.

2. About display of SCSI Slot General on the Web Component

If you are trying to see the ft server information "SCSI Slot General" of the NEC ESMPRO Agent Ver. 3.8 series on DataViewer of the Web Component installed on NEC ESMPRO Manager Ver. 4.07 or later, the following items may not be correctly displayed:

- Vendor
- Model
- Revision
- Serial Number

3. Security levels of Internet Explorer when the Web Component is used

The Web Component uses the JavaScript function of Internet Explorer.

Therefore, set the security level of Internet Explorer for the Web Component to "Medium" or lower.

Note that the Security level for the Internet zone of Internet Explorer is set to "High" on Windows Server 2003 by default. In such a case, set the security level to "Medium" or lower, or add the Web Component site in the Trusted Sites list.

4. When you use the Web Component through Internet Explorer on Windows Server 2003

If you use the Web Component through Internet Explorer on Windows Server 2003, titles (e.g. tool name, host name and manager name) may not be correctly displayed on the title bar. In such a case, see information displayed within the window.

5. About the Disk Array information

The Web Component does not support the Disk Array information.

6. Autodiscovery of Blade Servers

When you execute Autodiscover and register blade servers, the number of slots for storing blades may be displayed differently from the actual one, and some blade images may not be displayed.

In such a case, follow the steps below to change amp properties on Operation Window of the main NEC ESMPRO Manager:

- 1) Right-click the target blade map icon, and select [Properties] from the pop-up menu.
 - 2) Double-click [Background], and select an appropriate background image.
 - 3) Double-click [Maximum Number of Blade Slot in Chassis], and set an appropriate maximum number of slots.
 - 4) Click [OK] to complete the settings.
-