NEC

NEC Express5800 Series
NEC ESMPRO Manager
User's Guide

07-2008

PROPRIETARY NOTICE AND LIABILITY DISCLAIMER

Contents

About This Guide

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 NEC ESMPRO capabilities, installation, features, and use.
This manual is composed of the following chapters.

- Chapter 1, Introducing NEC ESMPRO, describes NEC ESMPRO features, configuration and system requirements.
- Chapter 2, Installing/Uninstalling the NEC ESMPRO Manager, provides instructions for getting the appropriate network protocols running, creating a user group called the NEC ESMPRO User Group, installing the Manager software on the system to be used for monitoring Agents across the network, and uninstalling the Manager software.
- Chapter 3, Using the NEC ESMPRO Manager, explains how to start the NEC ESMPRO Manager, set up network maps, use toolbars and buttons, and get the most out of the NEC ESMPRO Manager.
- Chapter 4, AlertViewer, describes how to access and read the Alert Log, sort the Alert list, and interpret Alert data.
- Chapter 5, DataViewer, 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 HP OpenView Integration.
- Appendix A, Inter-Manager Communication, describes the communication capabilities between network type and community levels.
- Appendix B, Notes, provides information and restrictions regarding NEC ESMPRO Manager.

Chapter 1

Introducing NEC ESMPRO

NEC ESMPRO lets a system administrator manage remote servers across a network. NEC ESMPRO monitors server hardware and software configurations, failures, and performance. With log data collected by NEC 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

NEC 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 NEC ESMPRO include:

- Hardware and software server configuration
  - Hardware resources mounted in servers, such as the CPU, memory, disks, disk array, 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
  - NEC ESMPRO monitors server performance 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

NEC 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 NEC ESMPRO thresholds locally. See the *NEC ESMPRO Agent User's Guide*.

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 management computer, you can manage servers through the web browser.

The following figure shows a sample Manager/Agent Configuration.

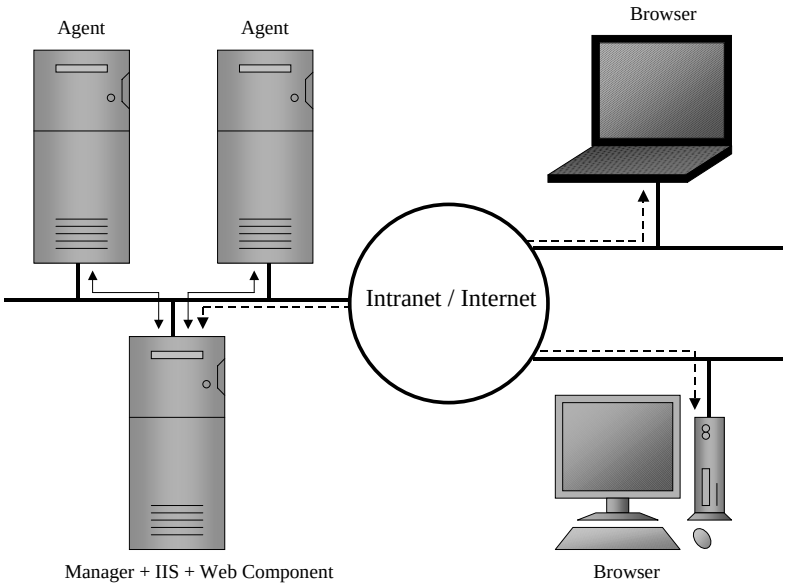


Figure 1-1 Manager/Agent Configuration

SYSTEM REQUIREMENTS

NEC ESMPRO Manager requires the following hardware and software:

- Hardware
  - Memory: 30MB of free memory for 32-bit and x64 systems or 230MB for 64-bit Itanium-based systems.
  - Hard Disk space: 130MB (170MB with Web Component)
    100MB (140MB with Web Component) is required for installing the program.
    In addition to the above, disk 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 in addition to the 100MB (140MB with Web Component) required for installing the program.
    1) Automatic Data Collection
       Approx. 40KB per information collection.
    2) Alert information
       Approx. 1KB per alert.
    3) Others
       Approx. 10MB as the management area of server registered in the 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 Advanced Server operating system
    Windows 2000 Server operating system
    Windows 2000 Professional operating system
    Windows XP Professional operating system
    Windows XP Professional x64 Edition operating system
    Windows Server 2003, Standard Edition
    Windows Server 2003, Enterprise Edition
    Windows Server 2003, Standard x64 Edition
    Windows Server 2003, Enterprise x64 Edition
    Windows Server 2003, Enterprise Edition for 64-bit Itanium-based systems
    Windows Server 2003 R2, Standard Edition
    Windows Server 2003 R2, Enterprise Edition
    Windows Server 2003 R2, Standard x64 Edition
    Windows Server 2003 R2, Enterprise x64 Edition
    Windows Vista Business
    Windows Vista Enterprise
    Windows Vista Ultimate
    Windows Server 2008 Standard

Windows Server 2008 Enterprise
Windows Server 2008 Datacenter
Windows Server 2008 for Itanium-based Systems

- Communications Protocol: TCP/IP (comes standard with the OS)
- Web Server (required for the Web Component): IIS 5.0 - 7.0
- Web Browser (required for the Web Component): IE 6.0 - 7.0 (JavaScript must be enabled.)

Chapter 2

Installing/Uninstalling the NEC ESMPRO Manager

BEFORE INSTALLING

Setting Up 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 purposes.

The NEC ESMPRO User Group name should be determined during the installation. The Manager setup names it "Administrators" by default.

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

Also, to make this security feature function effectively, 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.

In addition, to install the Web Component on Windows Vista or Windows Server 2008, you must install the CGI feature and set feature delegation in IIS Manager by following the procedures shown below:

- Installing the CGI feature

  Windows Vista

  1) Click [Start] - [Control Panel] - [Programs] - [Programs and Features] - [Turn Windows features on or off].
  2) Check the [Internet Information Services] checkbox in the Windows features list.
  3) Expand [Internet Information Services], [World Wide Web Service], and [Application Development Features] in turn, check the [CGI] checkbox, and click [OK].

  Windows Server 2008

  1) Click [Start] - [Control Panel] - [Programs] - [Programs and Features] - [Turn Windows features on or off] to start the [Server Manager] window.
  2) Click [Roles Summary] - [Add Roles] to start the [Add Roles Wizard] window.
  3) Click [Next] on [Before You Begin].
  4) Check the [Web Server (IIS)] checkbox from the [Server Roles] list.
  5) The message "Add features required for Web Server (IIS)?" appears. Click [Add Required Features], and click [Next].
  6) [Web Server (IIS)] appears. Click [Next].
  7) Check the [CGI] checkbox under [Application Development] in the [Role Services] list, and click [Next].
  8) [Confirmation] appears. Click [Install].

- Setting feature delegation in IIS Manager

  1) Click [Start] - [Control Panel] - [System and Maintenance] - [Administrative Tools].
  2) Double-click [Internet Information Services (IIS) Manager] (or [IIS Manager]) in the Administrative Tools list.
  3) Double-click [Feature Delegation] in the feature list on Home.
  4) Select [Handler Mappings] in the [Feature Delegation] list, and click [Read/Write] on the [Actions] pane or on the right-click menu.

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 directory will be overwritten. Therefore, please change the directory name before installing the Web Component.

Installing HP OpenView Network Node Manager

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

> **NOTE:** HP OpenView Integration does not support Windows Vista and Windows Server 2008.

Installation for multisession Terminal Server access

Perform the following operation to install the NEC ESMPRO Manager for multisession Terminal Server access:

- **For Windows 2000/Windows Server 2003**
  Use Add New Programs from Add or Remove Programs in Control Panel.
- **For Windows Server 2008**
  Use Install Application on Terminal Server in Control Panel.

About Sample of Script Component

When you changed a sample of the Script Component and saved it as the original file name, change the file name before performing update install.

If you perform update install without doing that, the sample will be overwritten and the changes might be initialized.

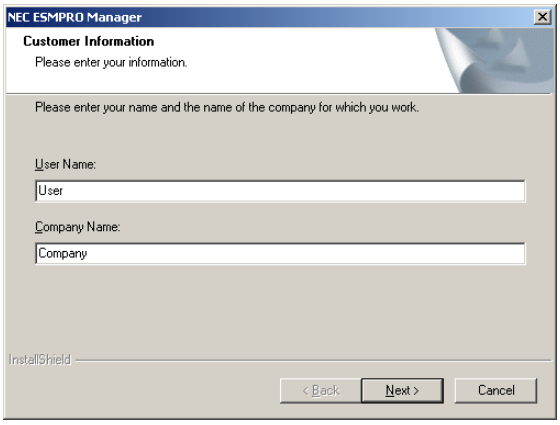
INSTALLATION

Installing the Manager Software

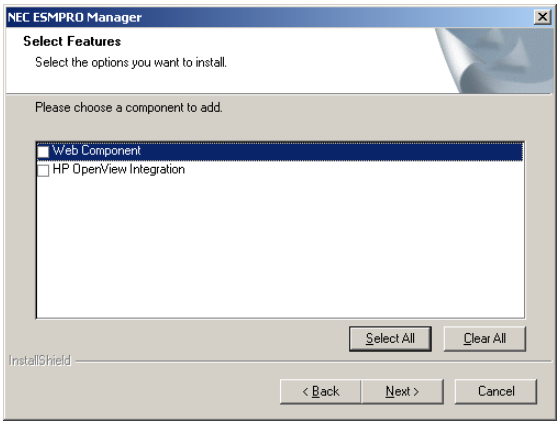
1. Log on as a user with administrative privileges.
2. Run the downloaded "SM2008.exe" file.

> **NOTE:** If User Account Control is enabled on Windows Vista or Windows Server 2008, the User Account Control window appears. Click [Continue] to proceed.

3. After verifying system conditions, the "Customer Information" screen is displayed. Enter your user name and company name, and then click [Next].



4. Features that can be added to NEC ESMPRO Manager are listed. Select features you want to add and click [Next].



Features to be displayed in the list vary depending on your environment (features that can be installed are listed). If no features can be added, this dialog box is not displayed.

[Features]

Web Component:

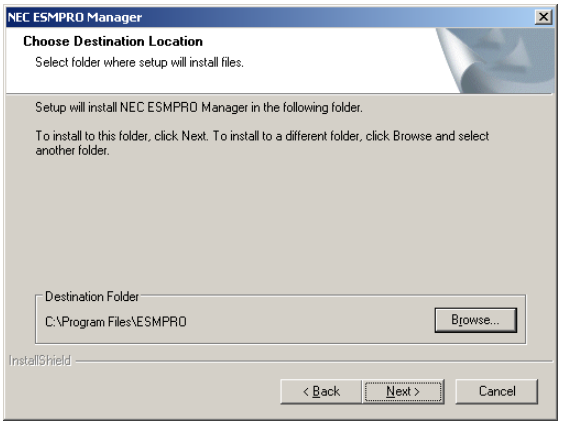
Enables you to access NEC ESMPRO Manager from Web Brower. Internet Information Services is required to install this feature.

HP OpenView Integration:

Integrates NEC ESMPRO Manager with HP OpenView. This feature is available when HP OpenView Network Node Manager is installed on the same computer.

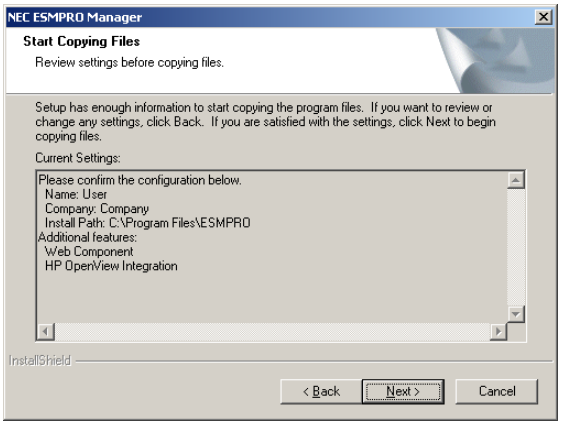
NOTE: The optional features can be added at any time after this installation.

5. The "Choose Destination Location" screen is displayed. Select the installation target folder, and then click [Next] (for update installation, this dialog box is not displayed).

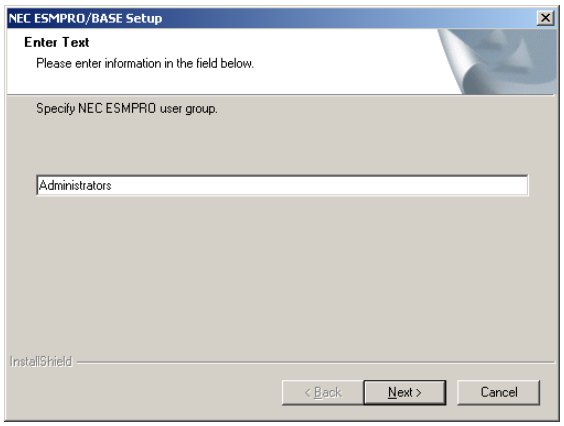


NOTE: In the case of 64bit OS, a location under SystemDrive:\Program Files cannot be specified.

6. The "Start Copying Files" screen is displayed. Click [Next].

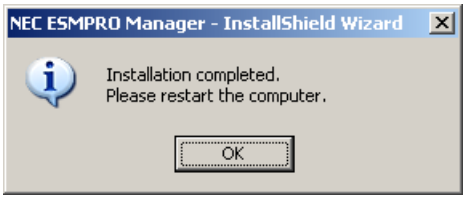


7. The "Enter Text" screen is displayed. Specify the NEC ESMPRO User Group, and then click [Next].



Wait a few minutes. As the software is installed, several windows open and then close automatically.

8. The "Installation Completed" screen appears. Click [OK].



The installation of the NEC ESMPRO Manager is complete. You may close the NEC ESMPRO Manager menu window manually.

Restart the computer before using the NEC ESMPRO Manager.

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

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

Installation of the NEC ESMPRO Manager has been successfully completed. There will be no problem in later operations.

NOTE: When installing the NEC ESMPRO Manager in an already existing directory, the NEC ESMPRO Manager will not operate unless the access permissions required for the NEC ESMPRO Manager operation have been set.

When installing the NEC ESMPRO Manager in a directory created by the installation software, the following access rights are set:

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 rights will be set for it.

UNINSTALLATION

Uninstalling the Manager Software

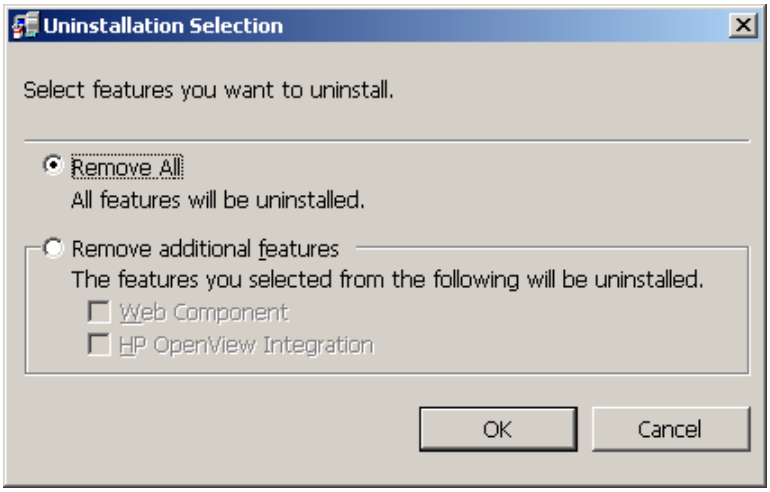
1. Close all opened NEC ESMPRO folders.
2. Start up **Programs and Features** (or **Add or Remove Programs**) from **Control Panel**.

   Select **NEC ESMPRO Manager** from the list of the installed programs, and click [Uninstall/Change] (or [Change/Remove]).
3. Select features you want to remove, and click [OK].

   Remove All: Removes NEC ESMPRO Manager and all added features.

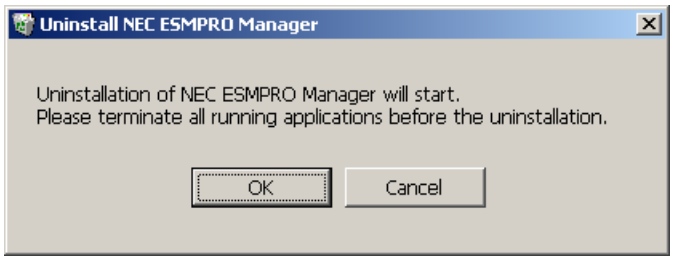
   Remove additional features: Removes features you selected.

   Features that were not added are grayed out and cannot be selected.



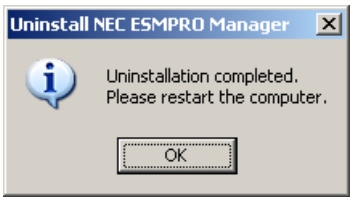
   If no features are added, this dialog box is not displayed.
4. Confirm that any applications related to NEC ESMPRO are not running, and click [OK].

   The selected features will be uninstalled.



Wait for a while until the uninstallation completes. During the uninstallation, some uninstallation dialogs will appear.

5. The "Uninstallation Completed" screen appears. Click [OK].



The uninstallation of the NEC ESMPRO Manager is complete.

Restart the computer.

NOTES:

After the uninstallation completes, pay attention to the following points:

[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, 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.

[Uninstallation where NEC ESMPRO Manager coexists with other NEC ESMPRO products]

If you uninstalled NEC ESMPRO Manager where other NEC ESMPRO products coexist, restart the system before using the products.

[Alarm Category of HP OpenView Network Node Manager]

If you uninstalled the HP OpenView Integration, "ESMPRO Alarms" remains in the alarm category of HP OpenView Network Node Manager. In such a case, delete it by hand.

Chapter 3

Using the NEC ESMPRO Manager

STARTING THE NEC ESMPRO MANAGER

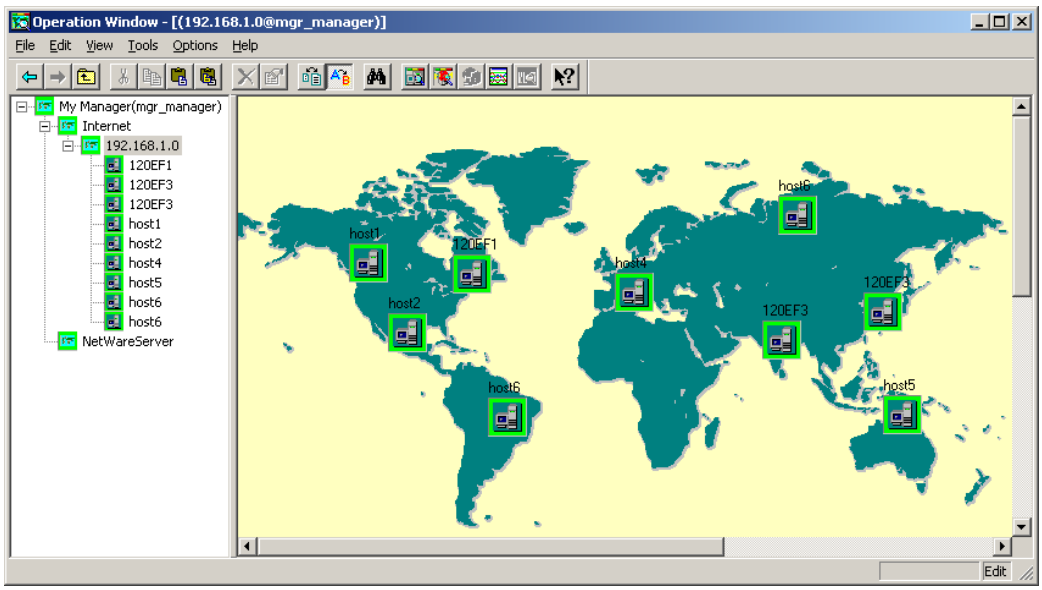
Start the NEC ESMPRO Manager as follows:

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

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

The left side of the Operation Window is the Tree View that 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 following figure. When the icons are displayed here, this side is called the Map View. On the other hand, when the system information for a server is displayed, it is called the Information View.



Tree View

Map or Information View

When the Operation Window first appears, servers on the same network can be detected and recorded on the Map View. (See Detecting Agents Automatically, page 17)

The NEC 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 DataViewer and AlertViewer to identify the problem.

Tool Bar and Menus

The tool and menu bars at the top of the Operation Window give you access to many NEC ESMPRO functions. The tool bar gives you quick access to many frequently used menu items. Simply click the button to access the function.

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

Detecting Agents Automatically

NEC 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 18.)

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 you want to access the details of auto discovery, click [Details] and check the following items.

   - Update properties

     To update server properties that have already been set, check this item.

   - Discover DMI Agent

     To detect DMI agent, check this item.

   - Restrict the objects

     To specify NEC ESMPRO Agent, check this item.

   Please refer to on-line help for more details.
6. Click [Start].
7. When automatic detection is finished, click [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 the Tools Menu.

> **NOTE:** To perform autodiscovery on Windows Vista, see "20. About Setting a Windows Firewall" described in the MANAGER section of the Appendix B Notes.

Changing Icon Properties

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

1. Right-click the icon.
2. Select Properties from the popup menu.
3. Make changes in the Properties window. Use the on-line help for details on field entries.

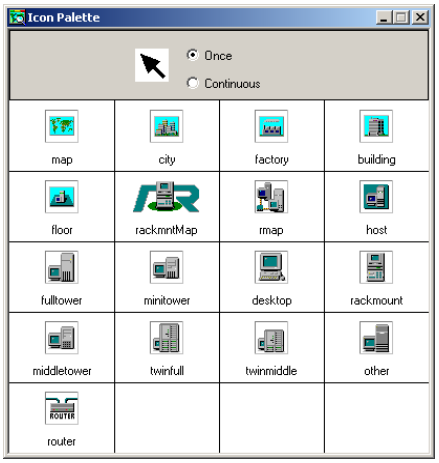
To delete an icon, select it and select Delete from the Edit Menu. If your attempt is denied, make sure that Enable Edit is selected in the Options Menu.

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.

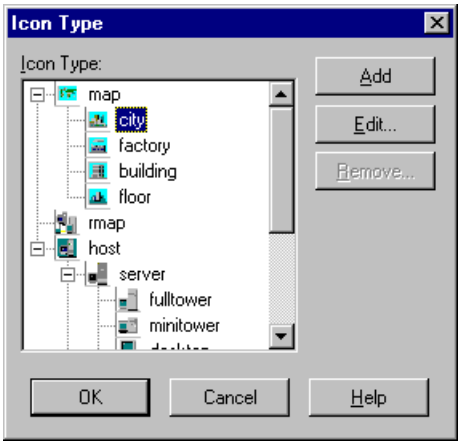


2. Click the icon in the palette that best represents the Agent.
3. Move your cursor to the Map View side of the screen and click to deposit the icon where you want it.
4. When the Properties window appears, enter the appropriate information for the Agent or map being created. Use the on-line help for a description of the fields.
5. When you finish, click [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. Select Change Icon Type from the Edit Menu.
3. Click an icon in the Icon Palette. The old icon changes to the new one selected.

Setting Up Inter-Manager Communication

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

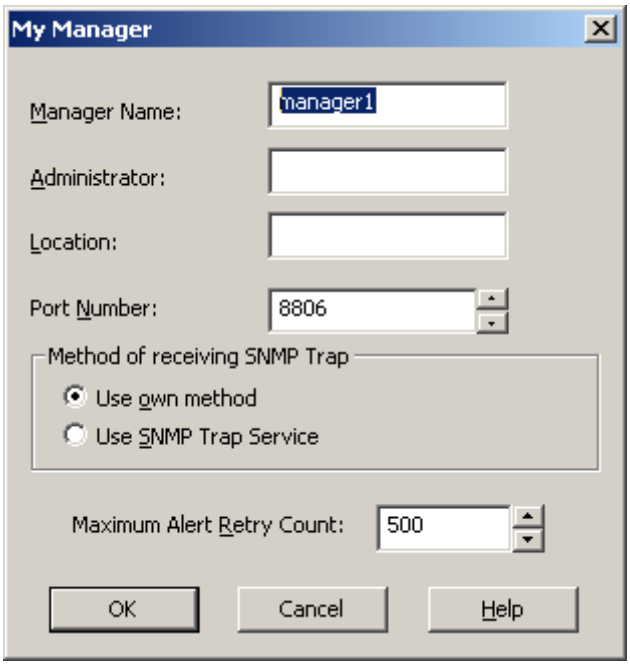
To establish the inter-Manager communication, you must specify the following.

- 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.



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

NOTE: Regarding the method of receiving an SNMP Trap, when software other than NEC ESMPRO Manager receives an SNMP Trap, NEC ESMPRO Manager may not be able to receive an SNMP Trap correctly due to the SNMP Trap port conflict.

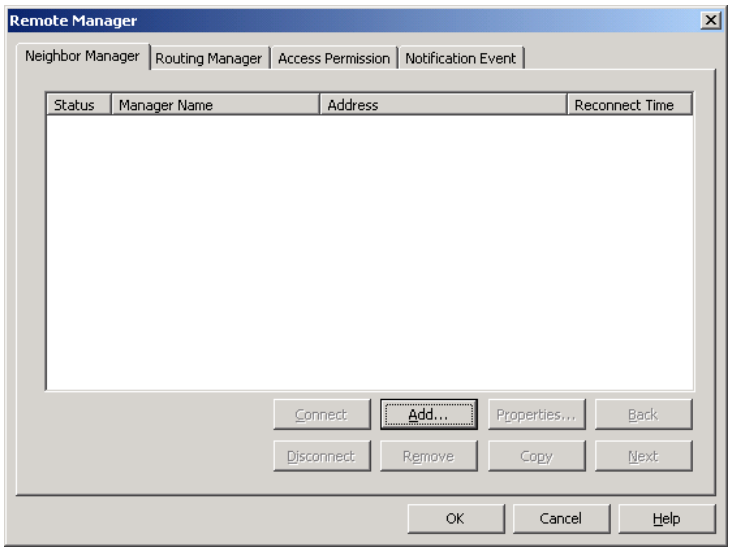
In this case, select "Use SNMP Trap Service".

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

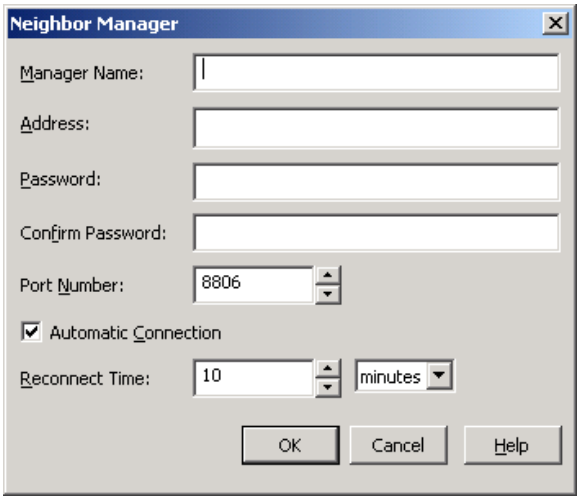
Neighbor Manager

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 the Neighbor Manager tab.
3. Click [Add] or [Properties].

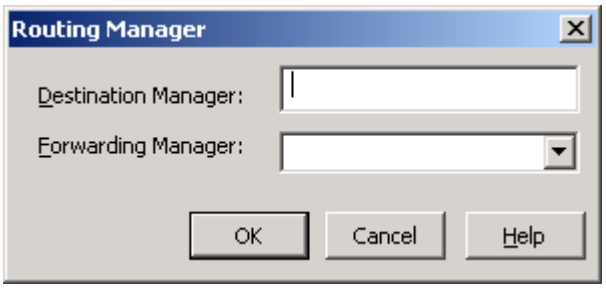


4. Enter the appropriate information in each field. Field details are available from the on-line help.
5. Click [OK].

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 click [Add] or [Properties].

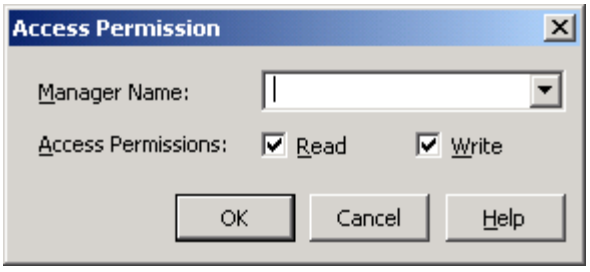


3. Set the parameters for each field. Help is available from on-line help.
4. Click [OK].

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 click [Add] or [Properties].

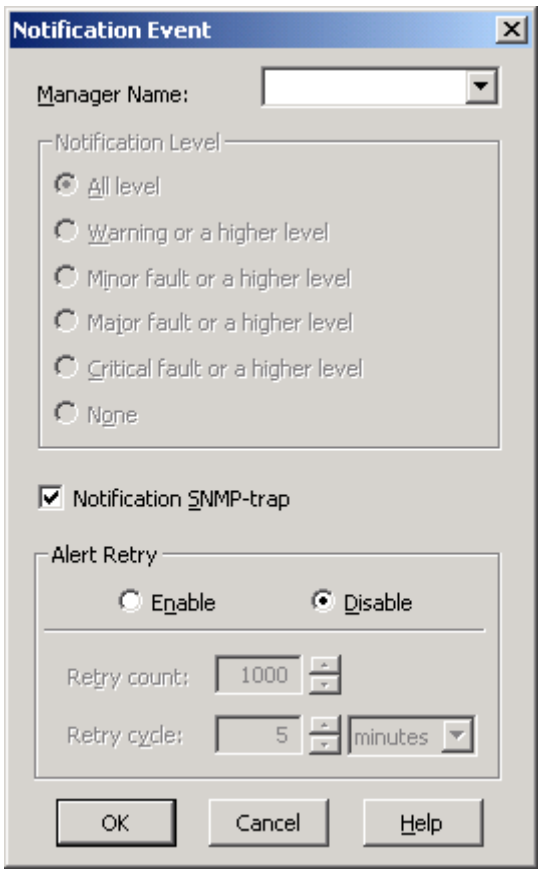


3. Enter the appropriate information in each field. Details about field entries are available in the on-line help.
4. Click [OK].

Notification Options

Define notification options as follows.

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



3. Fill in the appropriate information for each field. Details on field entries are available in the on-line help.
4. Click [OK].

Monitoring Agents

After creating the network map, registering Agent icons, and establishing communications, the NEC ESMPRO Manager automatically monitors the Agent status at specific intervals.

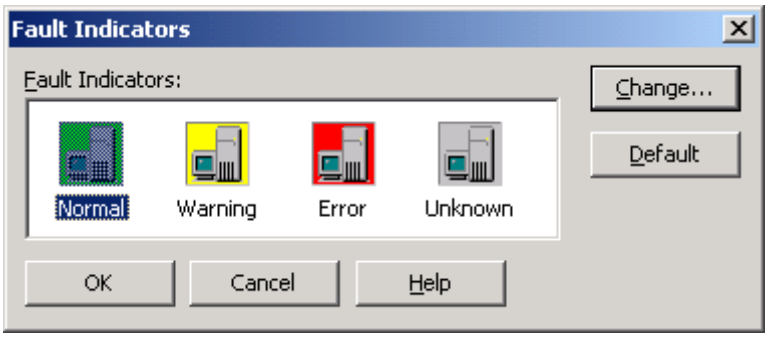
When the Manager detects a faulty Agent, the icon color changes according to the type of fault. Default colors are:

Table 3-1 Agent Status

Color	State	Description
Green	Normal	All Agent components are operating normally.
Yellow	Warning	A minor error occurred in an Agent component.
Red	Error	A major 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 DataViewer and AlertViewer 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.

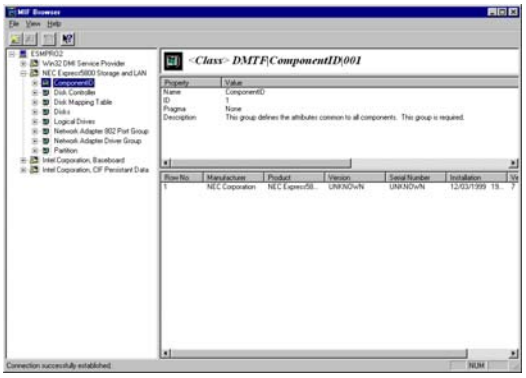


BROWSING MIF

Screen

MIF Browser consists of the following views.

<table>
<tr><td colspan="2">Menu</td></tr>
<tr><td colspan="2">Tool Bar</td></tr>
<tr><td rowspan="3">Tree View</td><td>Title View</td></tr>
<tr><td>Detail View</td></tr>
<tr><td>List View</td></tr>
</table>



1. Menu

Displays the following menu on MIF Browser.

File View Help

- File menu

  Displays the following menu on the File Menu.

File
Add Server... Ctrl+A Delete Server
Exit

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.

View
Tool Bar
Status Bar
Refresh

  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.

Help
Help Topics
About 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.

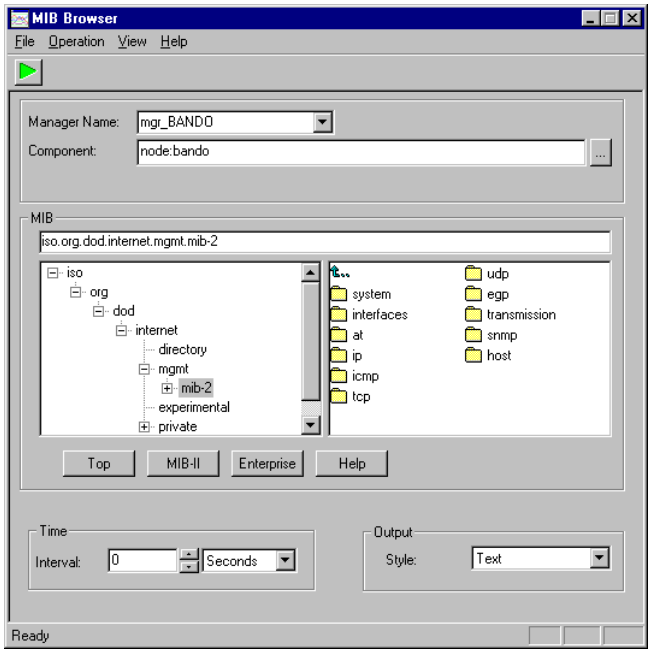
5. List View

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 click the MIB Browser icon on the Toolbar.

> **NOTE:** Browsing MIB (Management Information Base) needs expert knowledge about SNMP (Simple Network Management Protocol) and OID (Object Identifier).



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 the 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. Click  to start the collection.

Chapter 4

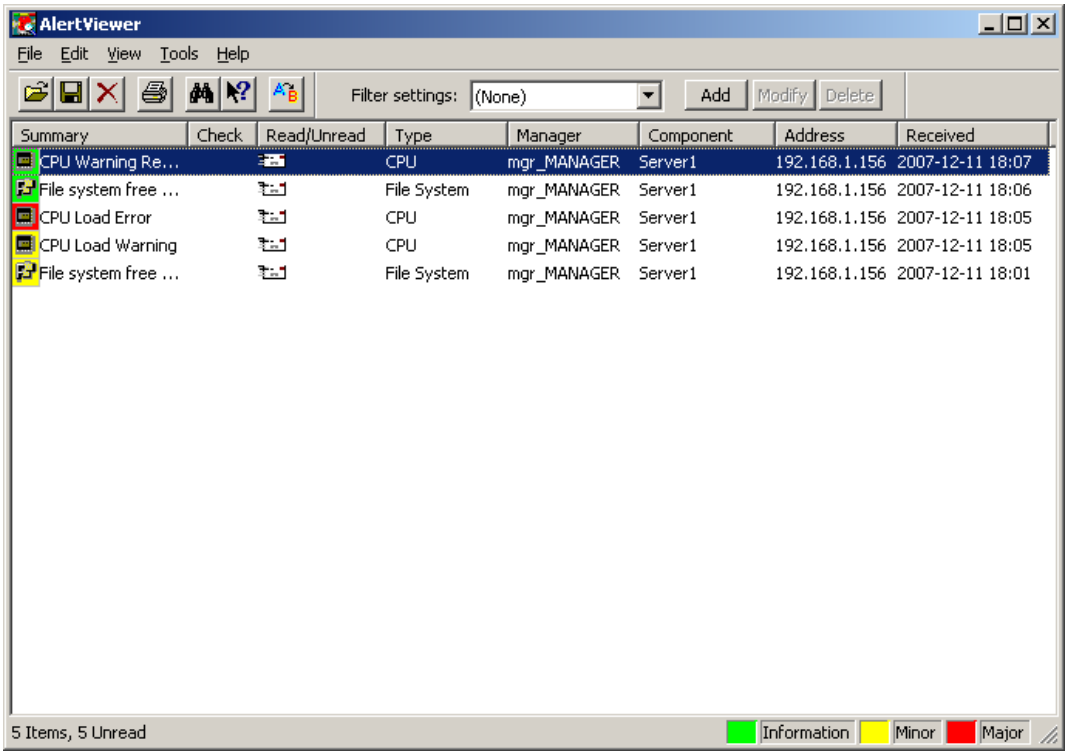
AlertViewer

The AlertViewer displays failures and warnings issued from servers running NEC 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 ALERTVIEWER

To access the AlertViewer from the Operation Window, select AlertViewer from the Tools menu or the AlertViewer 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.



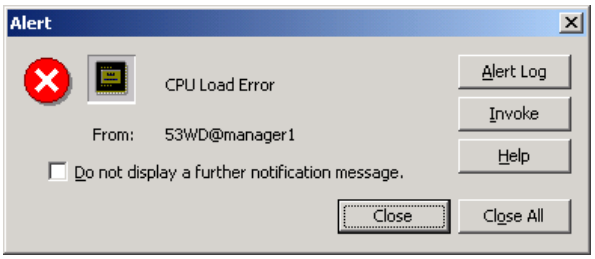
The central part of the AlertViewer is the Alert Log in which alert messages are displayed. New alert messages are added to the top of the list as they arrive. The following are columns of an alert message and their descriptions:

- 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 whether 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, page 32, 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 AlertViewer.
- Generated - shows the date and time when the alert was generated. (This column is not displayed in the default configuration. To display this column, select Columns in the View Menu.)
- Source - identifies the service that sent the alert. (This column is not displayed in the default configuration. To display this column, select Columns in the View Menu.)
- 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 - the 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 35.) 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.

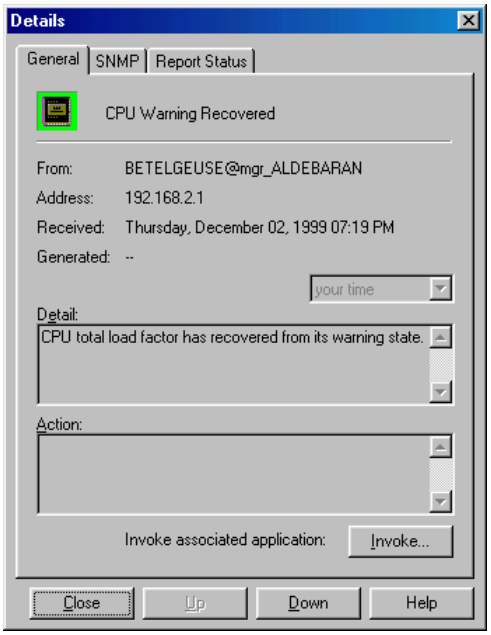


Click [Alert Log] to open the Alert Log Detail screen, or click [Invoke] to start the DataViewer. If you do not wish to view alert messages or details, click [Close].

Getting More Details

For details on an alert message, double-click the message line in the AlertViewer. You can also click [Alert Log] on the notification message. A window similar to the following displays the details of the alert message, including corrective actions to take.

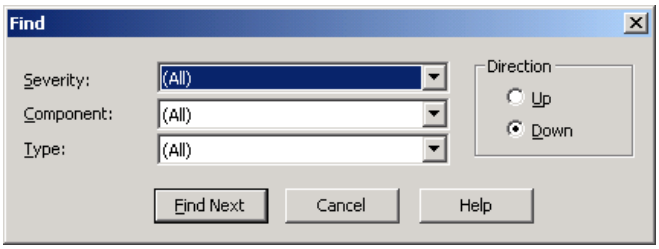
Once the Details window appears, the message is marked as Read in the Alert Log. (The symbol in the Read/Unread column changes to an opened envelope.) You can also mark messages as Read or Unread from the Edit Menu. Simply highlight the message and select Mark as Read or Mark as Unread.



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.

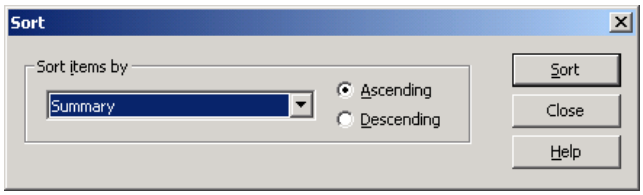


3. Click [Find Next]. The next alert that matches the criteria is highlighted in the Alert Log. (Double-click the line to see the Details screen.)

Sorting Alert Messages

The AlertViewer lets you sort alert messages in the Alert Log. This allows you to list a specific class of messages first, for example, 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 AlertViewer columns as your sort criteria.
3. Select the radio button next to Ascending or Descending to specify the order in which the messages should appear.
4. Select Sort to sort the alert messages or Close to abort.

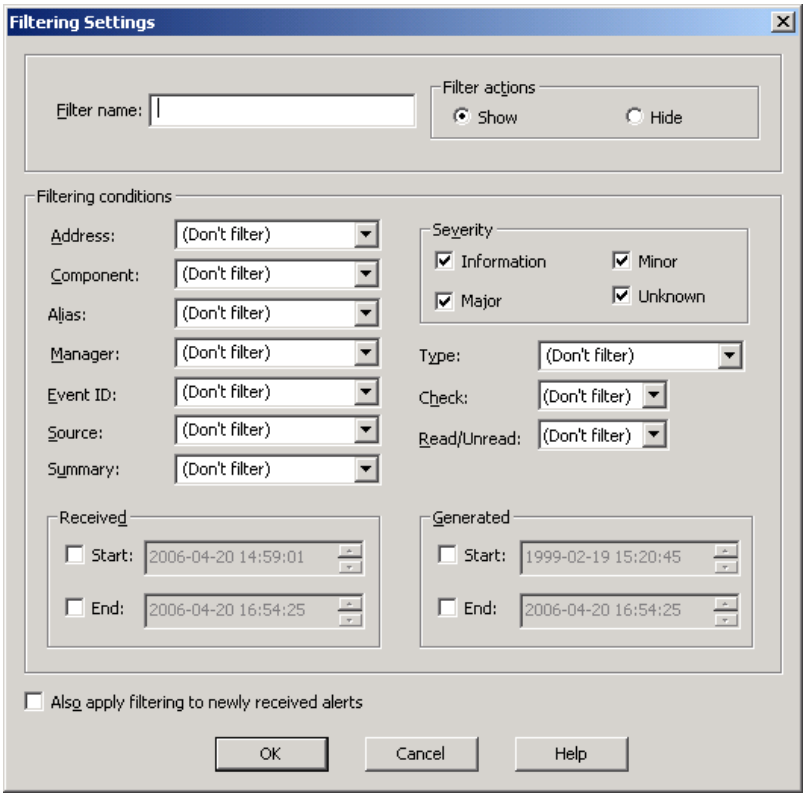
Another way to sort messages is to click a column title in the Alert Log. Clicking once will sort all messages in ascending order using the selected column as the sorting criteria. Clicking again will sort in descending order.

Filtering Alert Messages

You can filter alert messages by specifying a set of conditions.

1. On the filter bar, click [Add].

2. In the dialog box that appears, select filtering conditions and name the filter.



3. Click [OK] to save the setting and close the window.
4. Specify filter settings by selecting the drop-down list on the filter bar.

Please refer to on-line help for more details.

Configuring the AlertViewer

You can configure the appearance of the AlertViewer 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.

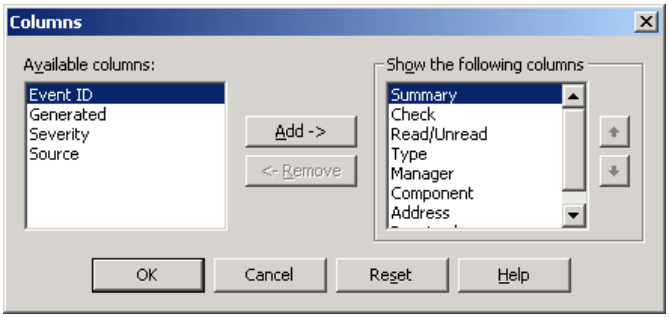
- To view or remove the Tool Bar and Status Bar

  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 AlertViewer Log. From the View menu, select Columns. A window similar to the following appears:



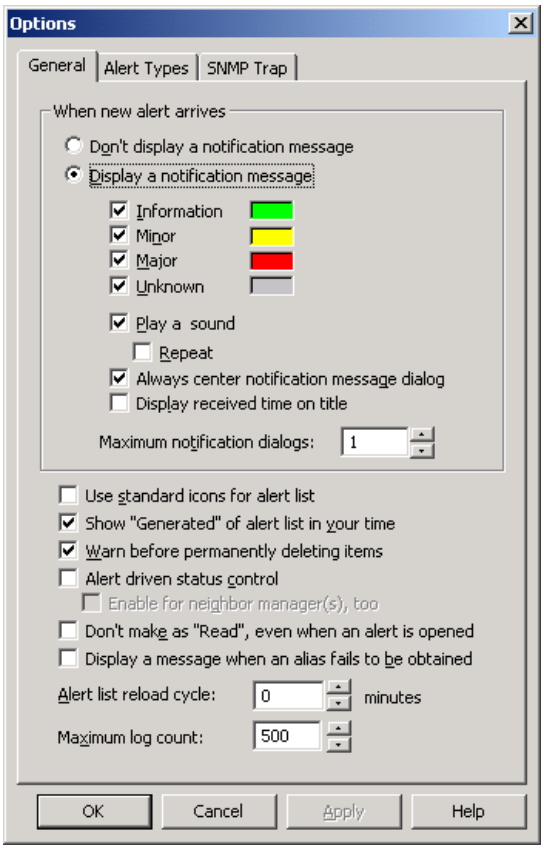
  - Information that appears in the Alert Log is listed in the box "Show the following columns."
  - Information under "Available Columns" can be added to the Alert Log.

  To add a new column to your screen, highlight an item from the "Available Columns" box and click [Add ->]. To remove a column from the Alert Log, highlight an item in "Show the following columns" and click [<- Remove].

Setting Notification Options

You can configure how you are notified of new alert messages. You can filter notification messages by severity.

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 AlertViewer, select "Don't display a notification message."
- If you choose to display notification messages (like the one on page 31), 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, no messages are 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 on the desktop.

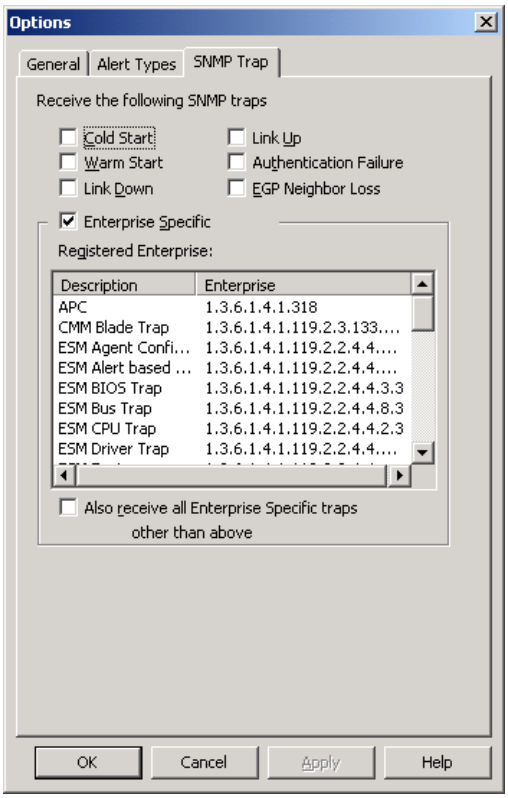
- Check "Display received time on title" if you want the time to be shown on the title bar of the notification message.
- "Maximum notification dialogs" allows you to define the maximum number of notification messages displayed at one time.

Please refer to on-line help for more details.

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 the "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 traps.
- Check "Warm Start" if you want AlertViewer to receive warm start traps.
- Check "Link Down" if you want AlertViewer to receive link down traps.
- Check "Link Up" if you want AlertViewer to receive link up traps.
- Check "Authentication Failure" if you want AlertViewer to receive authentication failure traps.
- Check "EGP Neighbor Loss" if you want AlertViewer to receive EGP neighbor loss traps.
- Check "Enterprise Specific" if you want AlertViewer to receive Enterprise Specific traps.

- "Registered Enterprise" shows the list of traps for which AlertViewer can show detailed and meaningful information.
- Check "Also receive all Enterprise Specific traps other than above" if you want AlertViewer to receive all Enterprise Specific traps.

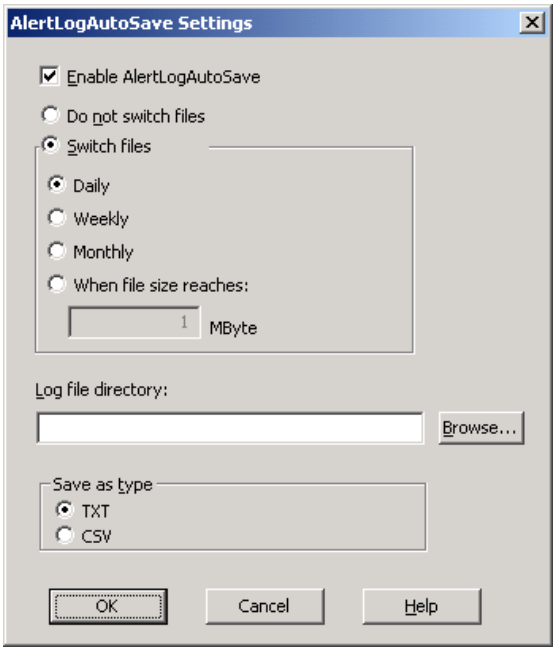
After setting the options, you must restart the computer for the changes to take effect.

Forwarding Alert Messages

You can forward alert messages to various destinations by using Alert Manager. Select Report Setting on the Tools menu to invoke Alert Manager. For details regarding Alert Manager, please refer to the *NEC ESMPRO Alert Manager User's Guide*.

Automatically Save Alert Log Settings

The Automatically Save Alert Log Settings function automatically saves received alert data in files. The received alerts can be saved as long as there is enough disk space. After you select this function, newly received alerts after you set here will be logged. From the Tools menu, select AlertLogAutoSave settings. A screen similar to the following appears.



NOTE: This function a portion (KB) of disk capacity whenever receiving a new alert. Make sure to regularly create back up of or delete alert log files. You cannot specify a network drive as the log file directory.

Chapter 5

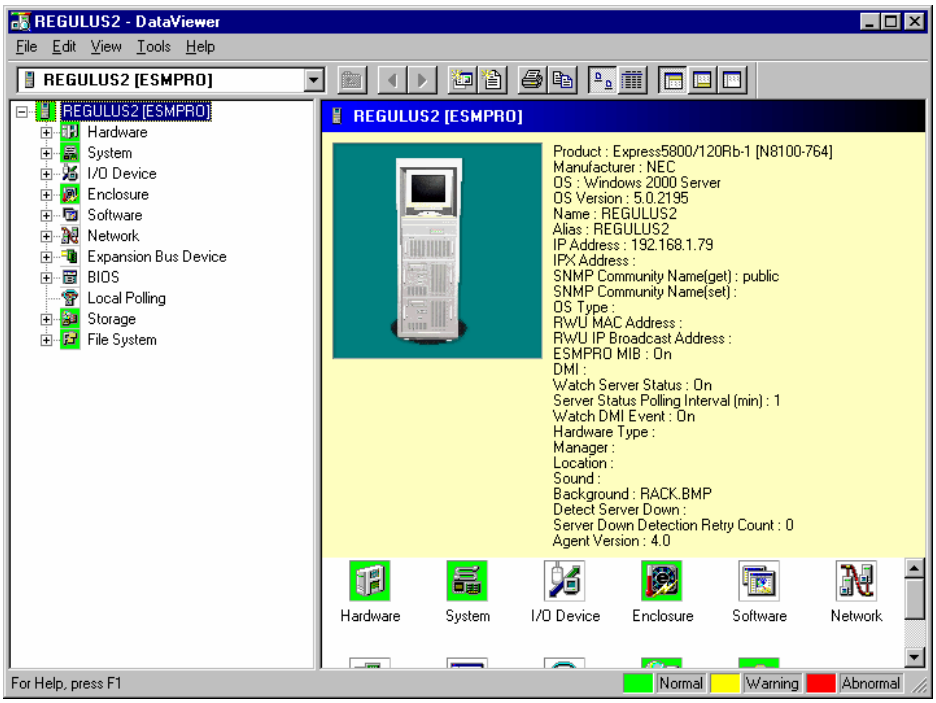
DataViewer

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

Access the DataViewer as follows.

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

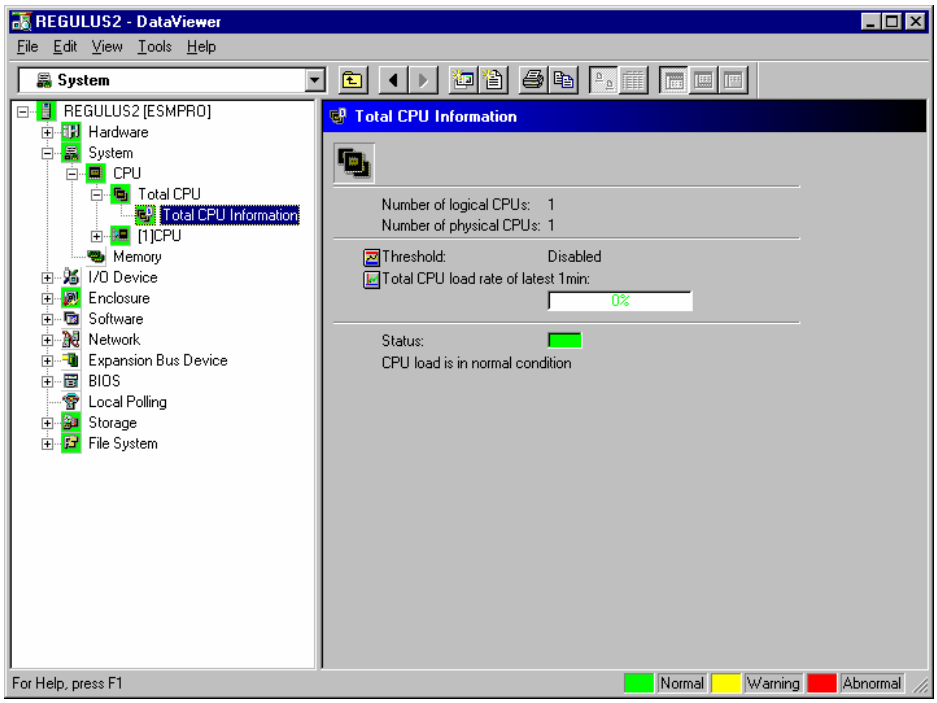
   A screen similar to the following appears.



- 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 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 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 a graph or change the screen size, but DataViewer is operating correctly. If this occurs, you can correct the display by changing the screen size again.

SETTING THRESHOLD LIMITS

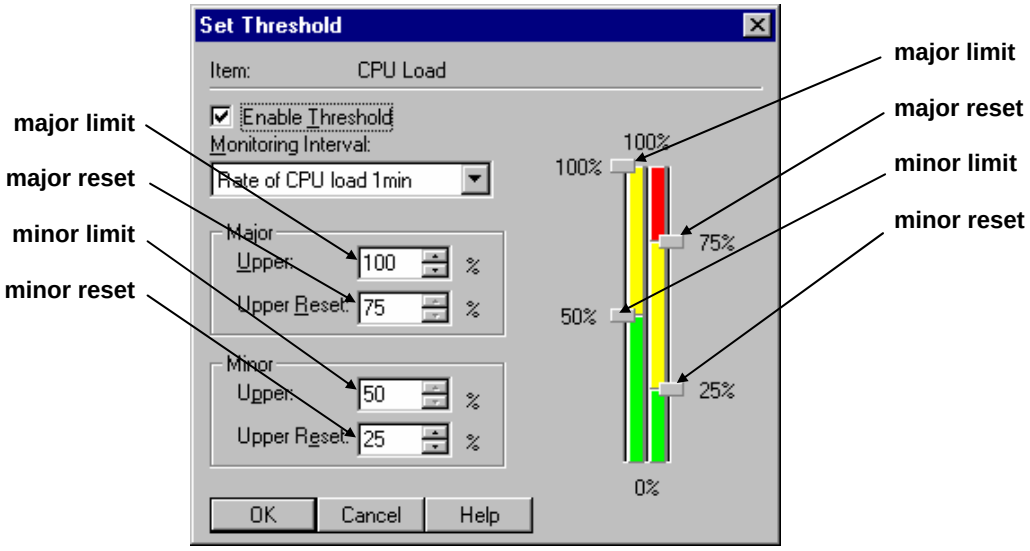
Thresholds can be set and viewed wherever you see the threshold button.

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 NEC ESMPRO Manager. These messages are displayed in the AlertViewer.

After you click 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. Click [OK].



HOW THRESHOLD LIMITS AND RESET VALUES WORK

When a parameter exceeds the threshold limit, an alert message appears in the AlertViewer. The corresponding icons in the DataViewer 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 AlertViewer, and the icons in the DataViewer 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 AlertViewer. The Agent's icon in the Operation Window and the appropriate folder icon in the DataViewer turn yellow to indicate the warning status.

The warning status continues until it falls below the Warning Reset value, at which time the status returns to normal. A warning recover message (such as CPU Warning Recover) appears in the AlertViewer, and the icons in the DataViewer and Operation Window return to green.

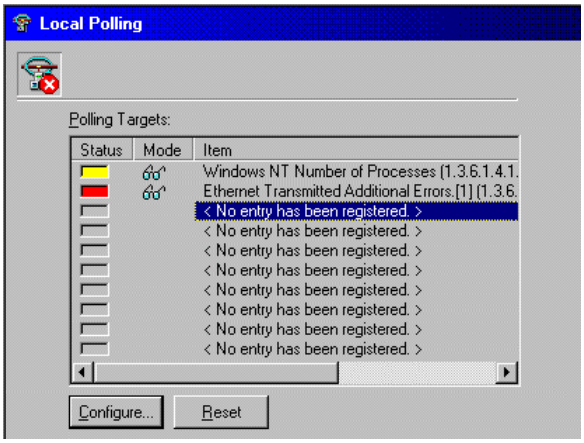
The Fatal limit is similar. As the parameter increases and reaches the fatal limit, an error message displays in the AlertViewer (such as CPU Load Error). Icons in the DataViewer and Operation Window change to red to indicate the abnormal status.

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

LOCAL POLLING

> **NOTE:** Using the Local Polling function requires expert knowledge about SNMP (Simple Network Management Protocol) and OID (Object Identifier).

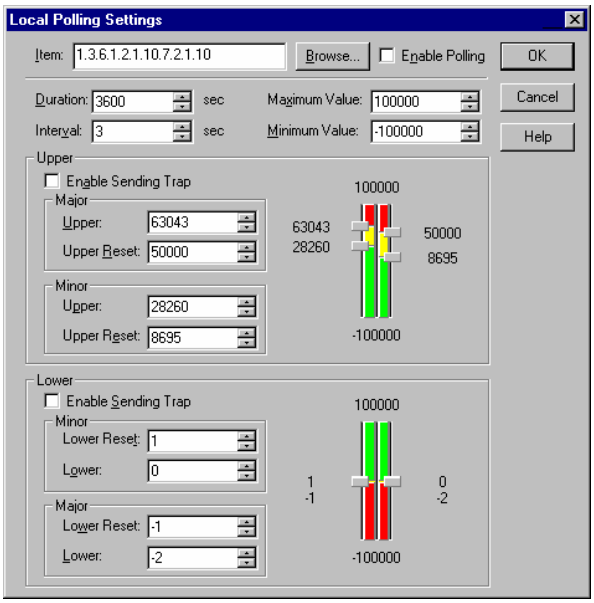
Selecting the Local Polling item on the Tree View shows the following screen.



The Local Polling window allows you to monitor data that has an Integer attribute. You can set or change the monitoring data and threshold levels.

- The [Configure…] button configures local polling settings for the selected item.
- The [Reset] button resets local polling settings for the selected item.

Select an item and click [Configure…]. A dialog box similar to the one below appears.



1. Specify the OID in the Item field. Some OIDs are selectable from the [Browse…] button. Then check the Enable Polling check box.

> **NOTE:** In Item field, enter the OID including the Index. When using the [Browse…] button, the location where the 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 the duration and the interval. When the duration is 0, polling is continuous.

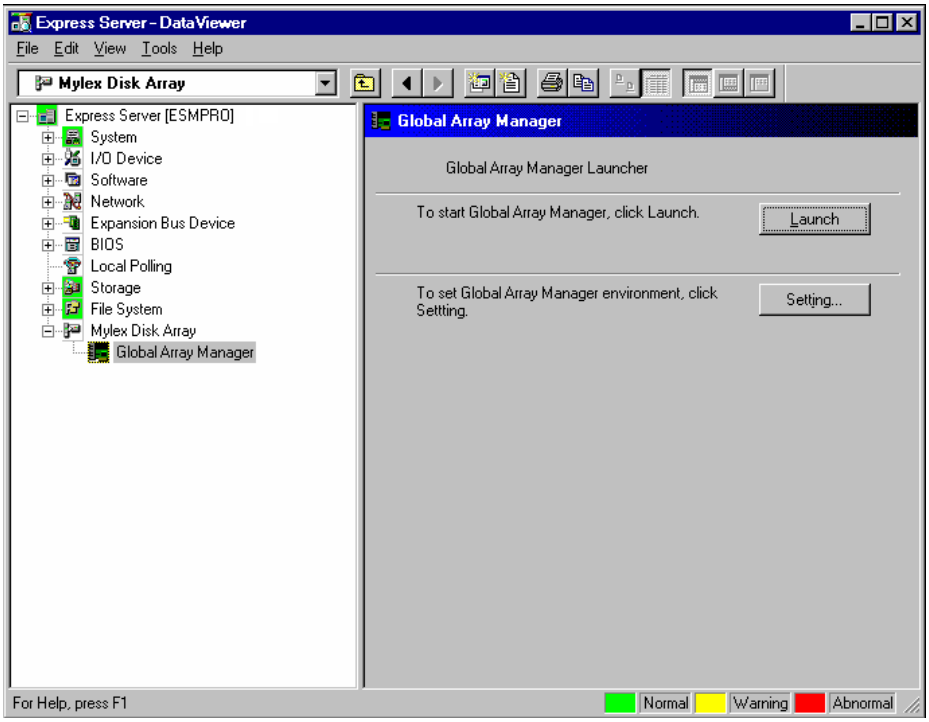
3. Set the threshold limits and reset values for the OID. In addition to the text entry boxes, you can set the threshold using the sliding bars to the right.

4. Check Enable Sending Trap. This issues a trap corresponding to the current threshold settings.

5. Click [OK].

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.

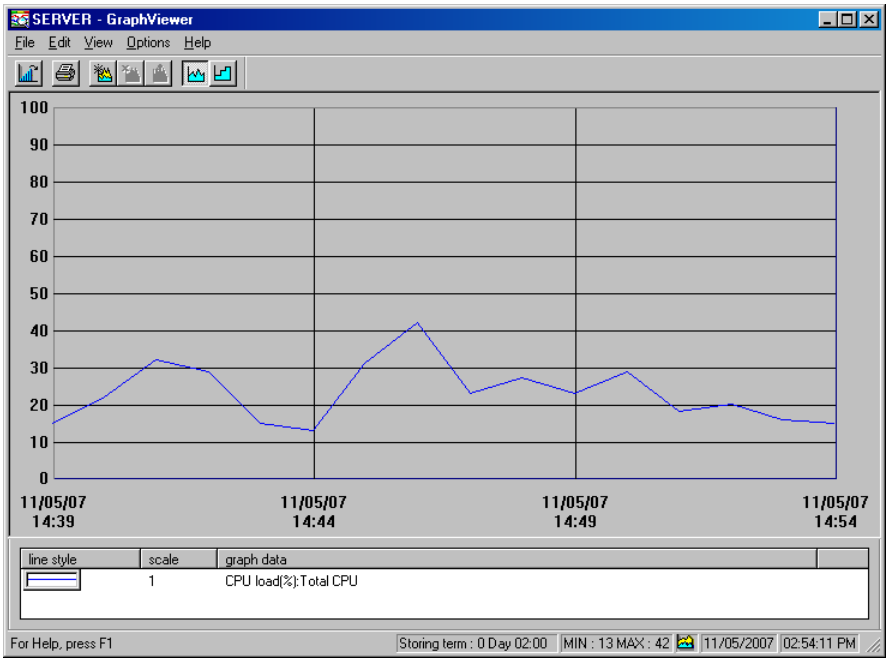
If "GAM Server" doesn't exist in monitor server, this view isn't shown.

In case of using NEC ESMPRO Ver.3.8 agent or older version, this launcher view is to be displayed. With NEC ESMPRO 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 DataViewer 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. Clicking the graph button displays a window similar to the following.



The GraphViewer 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.

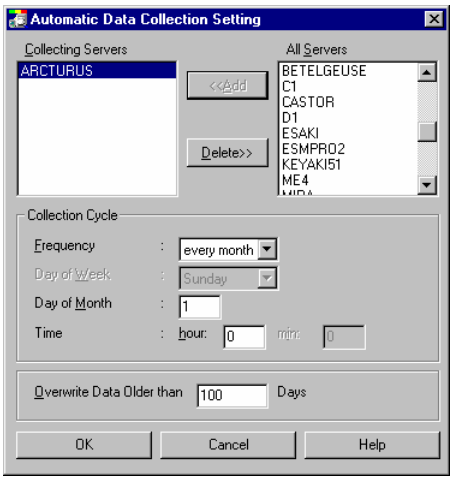
AUTOMATIC DATA COLLECTION

The NEC ESMPRO 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 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 the hour.
   - When the frequency is every week, you can set the day of the week and the 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. Click [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.

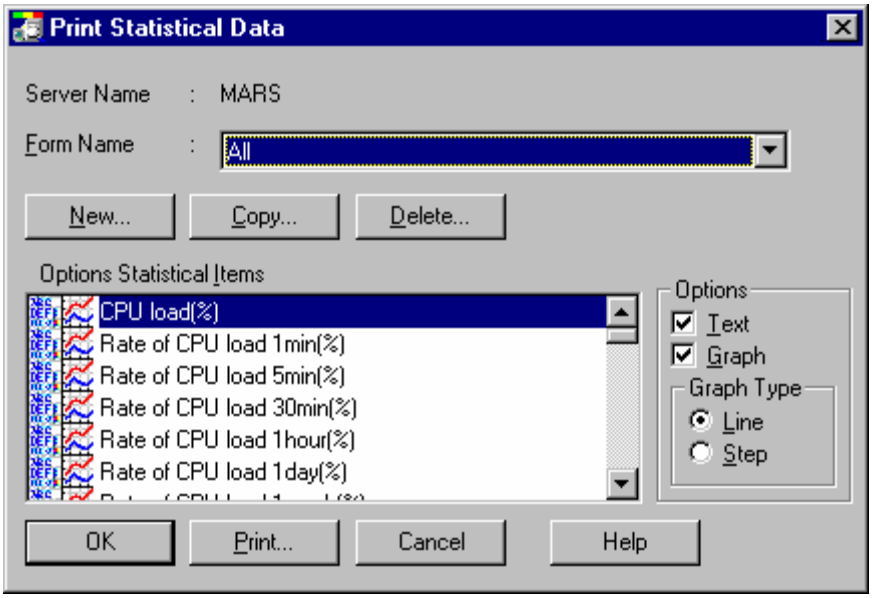
PRINTING STATISTICAL DATA

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

1. On the Operation Window, right-click 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).

Agent Control Panel

- Allows you to set operational settings for the NEC ESMPRO Agent. (Version 4.0 or later for Windows, Version 4.2 or later for Linux).

GETTING STARTED

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

Setting 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 6.0 on Windows Server 2003 R2 and IIS 7.0 on Windows Vista or Windows Server 2008. For other environments, see the help for each Web server.

For Windows Server 2003 R2

1. Start the Internet Information Services (IIS) Manager on the Web server and display the virtual directory "esmpro" properties of the Default Web Site.
2. Click [Edit] of the Authentication and access 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.

For Windows Vista

1. Start the Turn Windows features on or off window on the Web server, expand Internet Information Services, World Wide Web Service, and Security in turn, check the checkbox of the desired authentication method, and then click [OK].
2. Start Internet Information Services (IIS) Manager, double-click Authentication from the virtual directory "esmpro" properties list to display the Authentication window. 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.

For Windows Server 2008

1. Start the [Server Manager] window on the Web server, and display the [Web Server (IIS)] information from the [Roles] list.
2. Select [Add Role Service] from [Role Service].
3. Check the checkbox of the desired authentication method under [Security], and click [Install].

4. Start the Internet Information Services (IIS) Manager, double-click [Authentication] from the virtual directory "esmpro" properties list to display the [Authentication] window. Then set up the authentication methods.
5. Join the user with the authenticated access to the NEC ESMPRO User Group (by default, Administrators) you specified during installation.
6. Restart the Web server computer.

NOTE: Considering your security, we do not recommend that you allow anonymous access. It is recommended that you disable anonymous access and use the authenticated access.

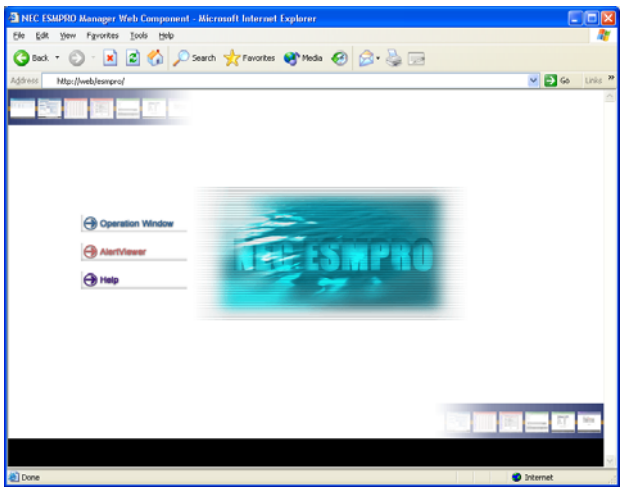
Note that there are limitations on users to be used when you use the Windows Authentication on Windows Vista or Windows Server 2008. For details, see Notes.

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 the settings.

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 might not belong to the NEC ESMPRO User Group. Check that the setting is correct.

NOTE: When you access the Web Component from the 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 only a display issue. There are no problems in its operation.

If you access the Web Component from the 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 the 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, open the Operation Window in the Web Component and execute 'Agent Version Update' with the target servers.

3. Setting the number of the alerts to be stored
   To increase the number of alerts 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 an 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. Log on to the Web server as a user with administrative privileges, and open the Command Prompt.

   NOTE: In the case of Windows Vista and Windows Server 2008, open Command Prompt as Administrator. To do so, log on to the system as Administrator and open Command Prompt, or select Command Prompt from the Start menu and click Run as administrator on the right-click menu.

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 websetup.vbs -default**'.

   The following settings are configured (the same as the default settings at installation.)

OS	Web site	Virtual directory name
Windows 2000/XP/Server 2003	1*	esmpro
Windows Vista/Server 2008	Default Web Site	esmpro

* The site number of the Web site

When you want to configure settings other than the default ones, follow the procedure below:

1. Log on to the Web server as a user with administrative privileges, and open Command Prompt.

   NOTE: In the case of Windows Vista and Windows Server 2008, open Command Prompt as Administrator. To do so, log on to the system as Administrator and open Command Prompt, or select Command Prompt from the Start menu and click Run as administrator on the right-click menu.

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 is displayed.

   Windows 2000/XP/Server 2003: The Web site information is displayed. A number displayed on the left is a site number of each Web site.

   Windows Vista/Server 2008: The Web site name is displayed.

4. Type '**cscript websetup.vbs -s *Web site* -a *virtual directory name***'.

   Web site: In the case of Windows 2000/XP/Server 2003, set a 'site number'. In the case of Windows Vista/Server 2008, set a 'site name'.

   virtual directory name: Set the virtual directory name (alias) to be added to the Web site.

   The default setting ('cscript websetup.vbs -default') is the same as below:

   Windows 2000/XP/Server 2003: 'cscript websetup.vbs -s 1 -a esmpro'

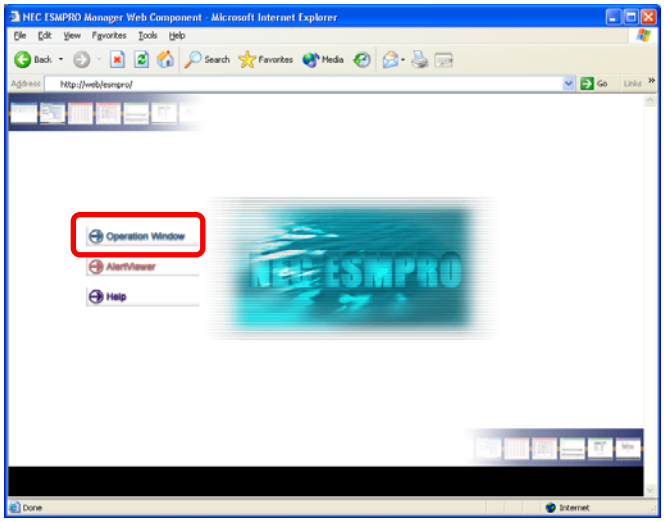
   Windows Vista/Server 2008: 'cscript websetup.vbs -s "Default Web Site" -a esmpro'

OPERATION WINDOW

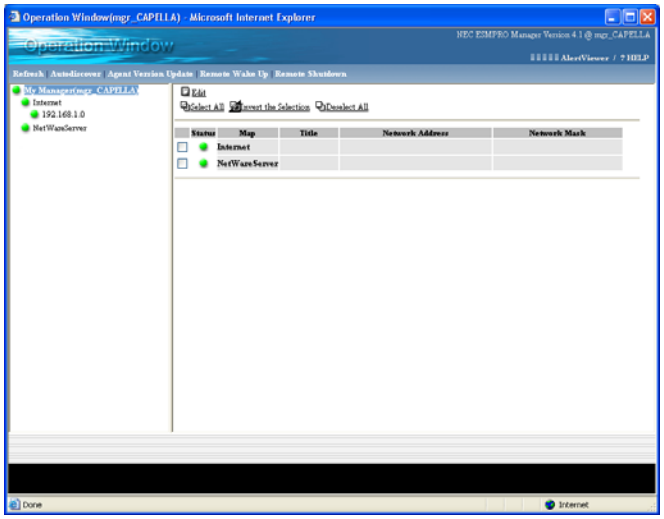
The Operation Window displays a list of the managed servers connected to the network on a map. Server monitor status and server properties can be accessed on the Operation Window. Additionally, tools for managing components can be launched from the Operation Window.

Starting the Operation Window

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



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.

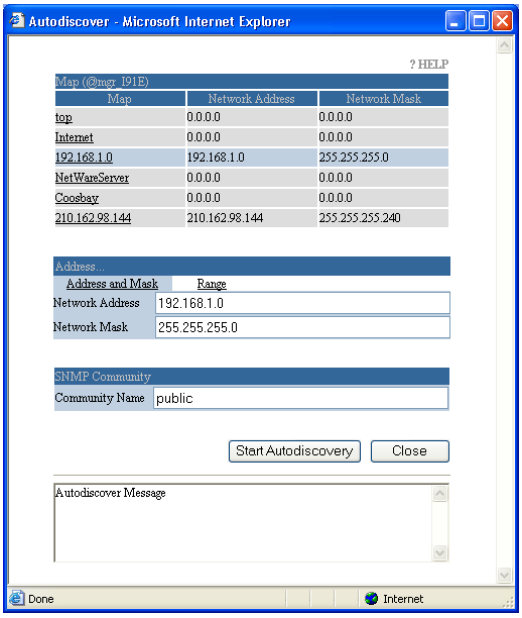
Registering a Server to be Managed

To register a server to the Operation Window, use the Autodiscovery function. If you already have the managed server information in hand, you can manually input a host name, a map name, and required information to 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 [Start Autodiscovery].



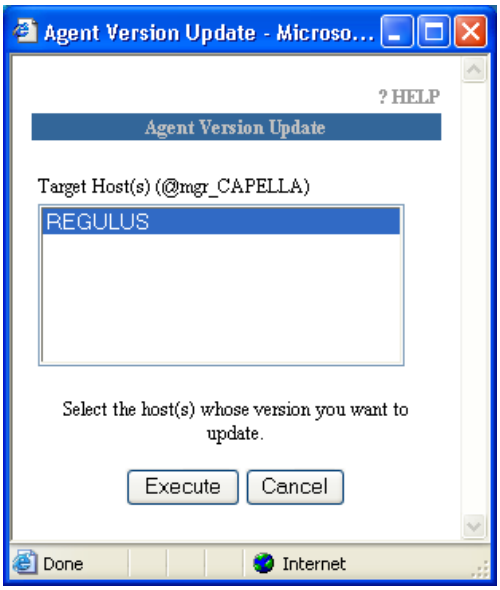
NOTE: The map selected from the tree frame on the left of the Operation Window will be the default target map.

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

It is recommended that you 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

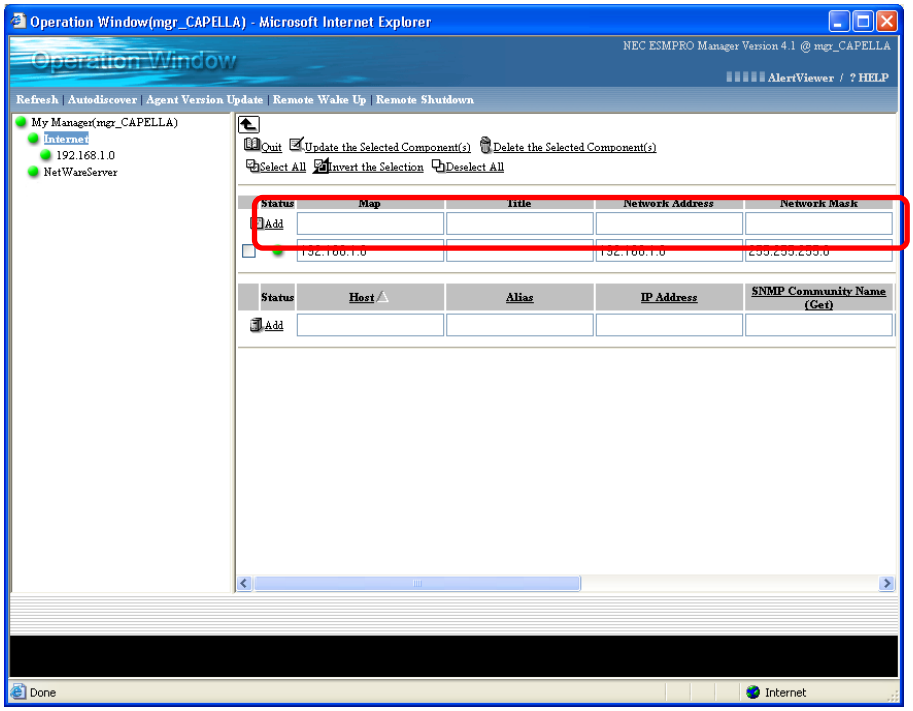
1. Select the check box of hosts or maps containing hosts you want to update on the Operation Window, and select the Agent Version Update menu from the Menu Bar.



2. Select hosts in the Target Host(s) list and click [Execute].

Manually Adding a Map

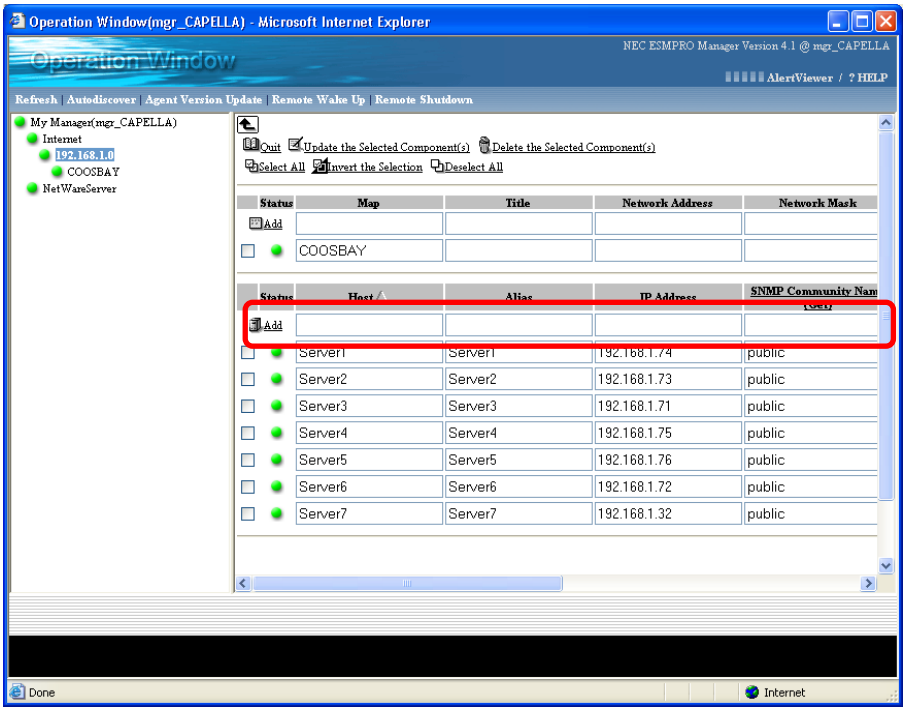
1. Select the map to which you want to add a new map.
2. Click "Edit" above the Map List.
3. Enter an appropriate value in each box on the Area for adding a new map.



4. Click "Add" on the Map List.

Manually Adding a Host

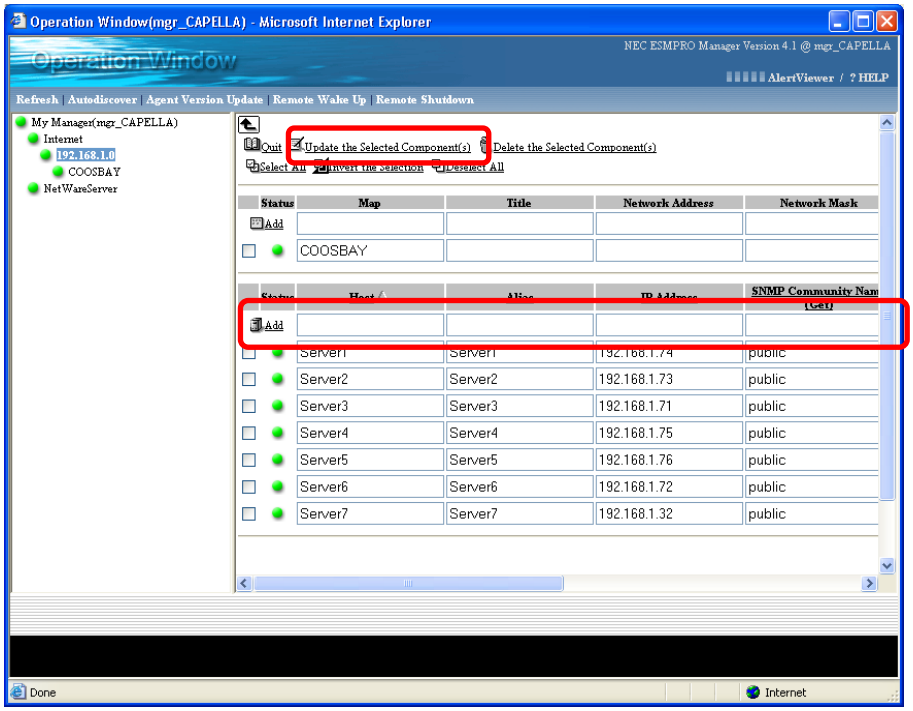
1. Select the map to which you want to add a new host.
2. Click "Edit" above the Host List.
3. Enter an appropriate value in each box on the Area for adding a new host.



4. Click "Add" on the Host List.

Editing Properties of Maps or Hosts

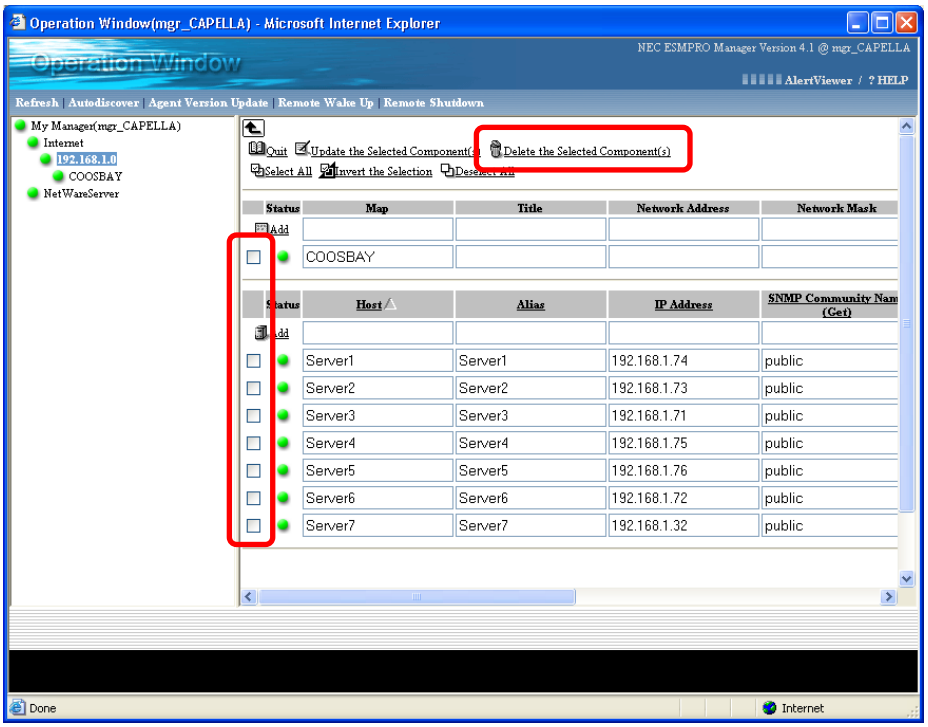
1. Select the map containing the map or host you want to edit.
2. Click "Edit" above the Map or Host List.
3. Change the value on the properties of the map or host you want to edit.
4. Click "Update the Selected Component(s)" above the Map or Host List.



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

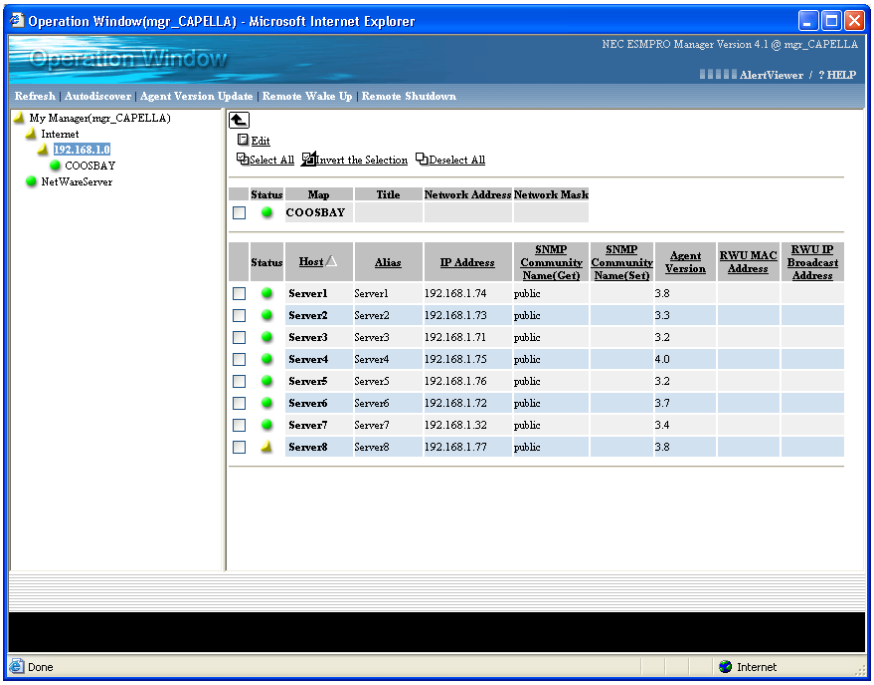
Deleting the Map or Host

1. Select the map containing the map or host you want to delete.
2. Click "Edit" above the Map or Host List.
3. Select the check box by the map or host you want to delete.
4. Click "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 icons are displayed to show the server status:

Status	Icon
Normal	
Warning	
Abnormal	
Unknown	

NOTE: The list of the managed servers and their status colors is updated at one minute intervals. However, each property information needs to be updated by clicking [Refresh].

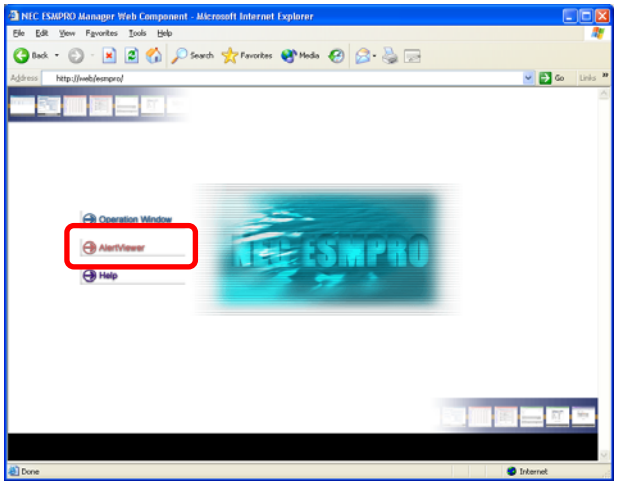
The status icon is displayed in gray (Unknown) when a target server is stopped or in sleep mode or when any problems occur on the network.

AlertViewer

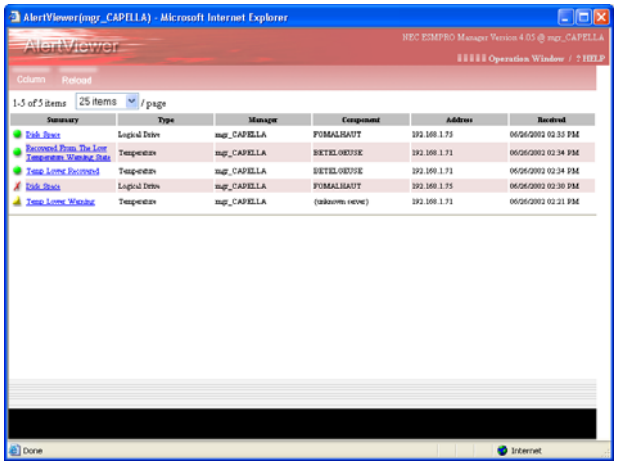
The AlertViewer displays the alert messages sent to the NEC ESMPRO Manager.

Starting the AlertViewer

Click "AlertViewer" on the Web Component title page.



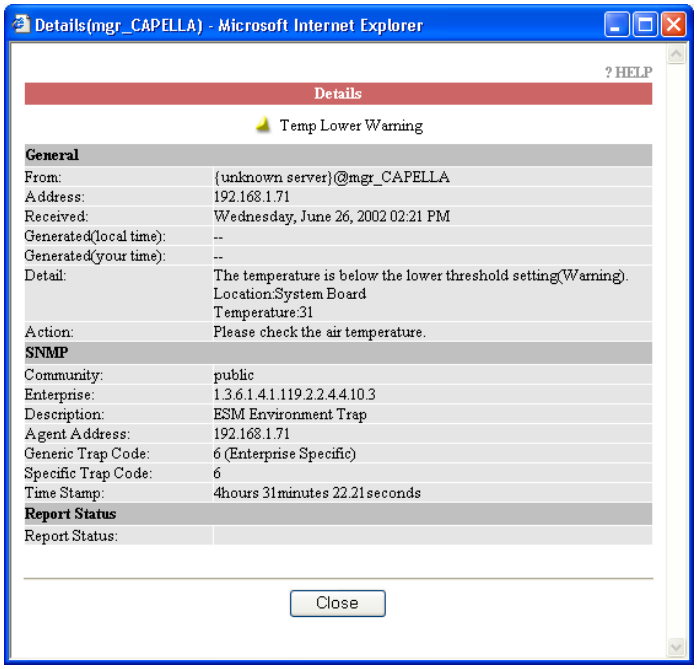
The AlertViewer starts, and a list of the received alert messages appears.



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

Viewing Detailed Alert Information

Click "Summary" to show the details of the alert. The detailed alert information is displayed in the Details window.

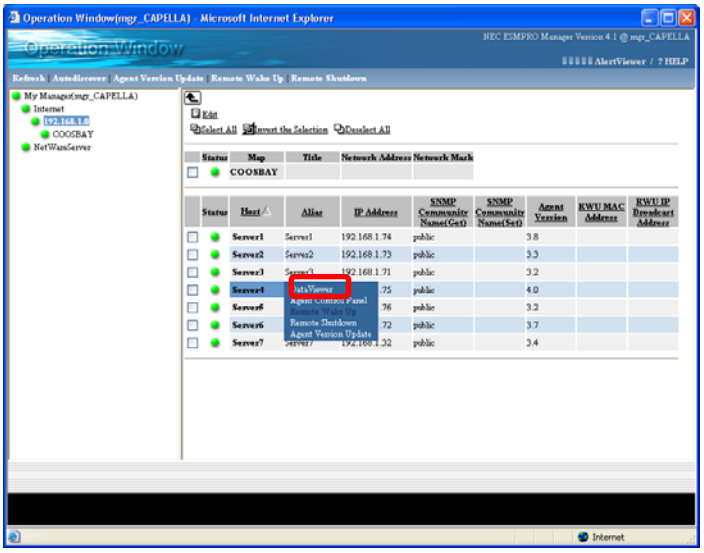


DataViewer

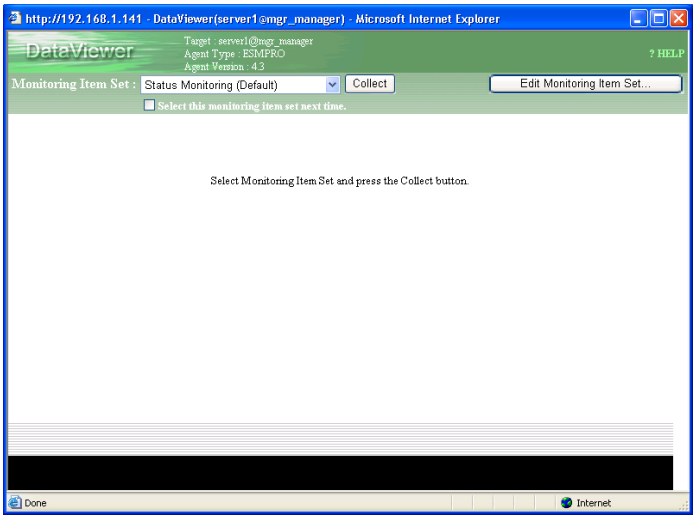
The DataViewer obtains the configuration information on the server in which the NEC ESMPRO Agent is installed and displays it in a tabular form.

Displaying Server Configuration Information

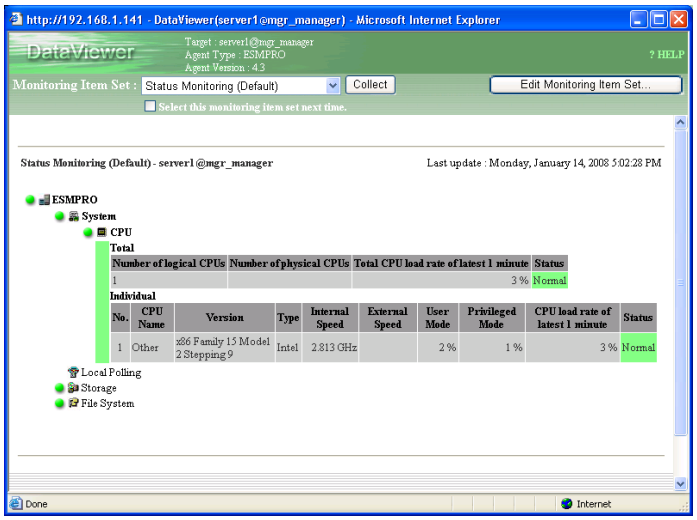
1. Position the cursor on a host name the Operation Window. Click DataViewer when the pop-up menu appears.



The DataViewer starts.



2. Select the monitoring item set to be managed from the Monitoring Item list, and click [Collect]. The information on the selected monitoring item set is displayed.



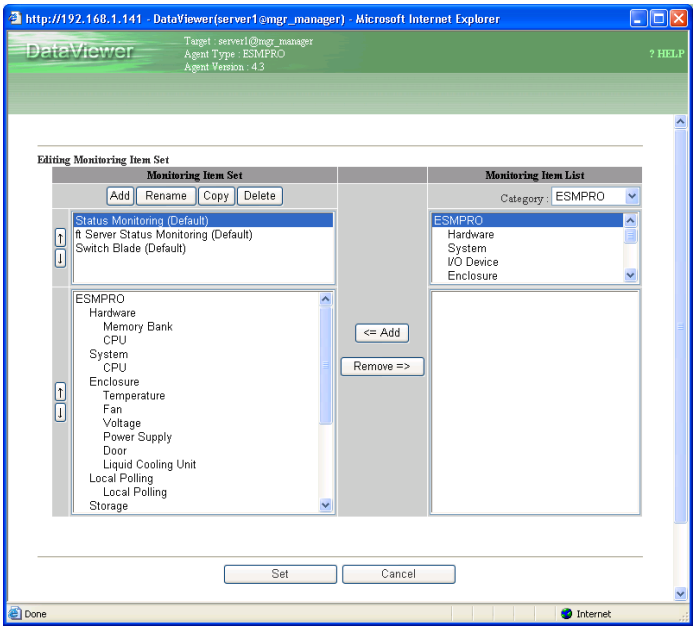
NOTE: The Agent Version of a target host must be properly set to start the DataViewer.

The information is not periodically updated. Click [Collect] to obtain the latest information.

Customizing the Monitoring Item Set

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

1. Click [Edit the Monitoring Item Set…] in the upper right corner of the DataViewer window. The Edit Monitoring Item Set window appears.



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

NOTE: Up to 100 monitoring item sets can be registered.

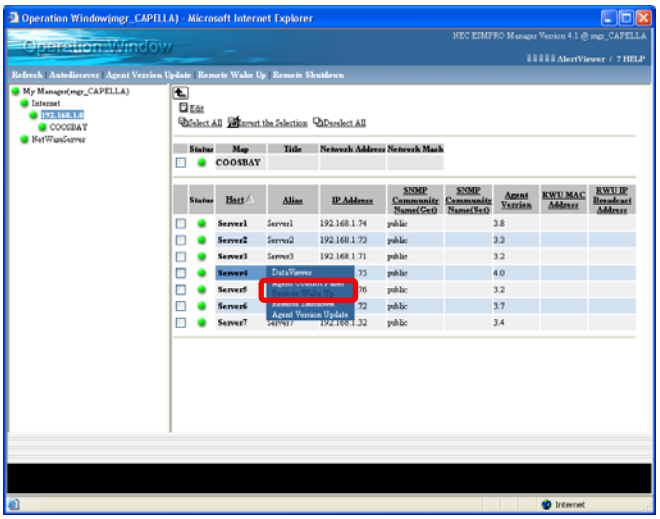
Clicking [Copy] enables you to create a new monitoring item set based on an existing monitoring item set.

AGENT CONTROL PANEL

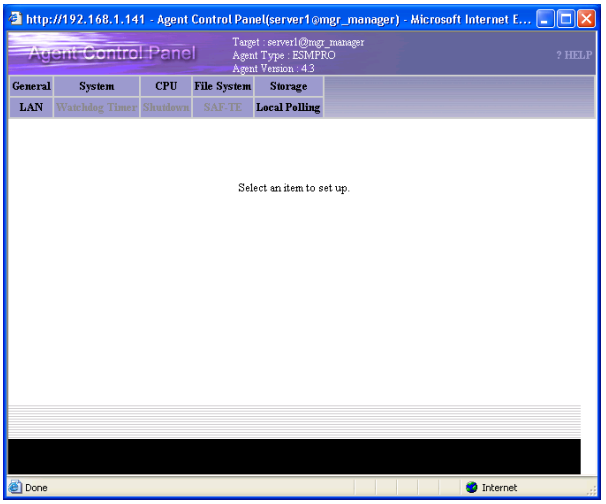
The Agent Control Panel allows you to change the operational settings of the NEC ESMPRO Agent.

Starting the Agent Control Panel

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



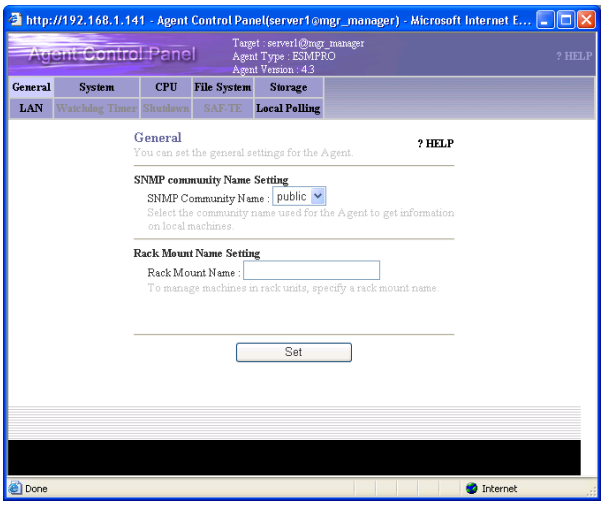
The Agent Control Panel appears.



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

Changing the Operational Settings

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



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

NOTE: The information is not periodically updated. Click 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 a pale color indicates that the NEC ESMPRO Agent did not return the information on that item for some reason, for example, the server does not support the item.

General

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

System

The System tab allows you to set the settings for monitoring 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.

If the setting is invalid, it is reported to the NEC ESMPRO Manager.

CPU

The CPU tab allows you to set the settings for monitoring CPU load. Monitoring CPU load can provide early detection of a high CPU load rate.

The CPU load status is displayed as the status color on the DataViewer. It is reported to the NEC ESMPRO Manager.

File System

The File System tab allows you to configure settings for monitoring the free capacity of the File System. Monitoring File System capacity can provide early detection of a potential shortage of free capacity.

Lack of free capacity is shown as the status color on the DataViewer. It is reported to the NEC ESMPRO Manager.

Storage

The Storage tab allows you to configure the settings for monitoring storage devices. The hard disk pre-failure prediction function monitors any potential 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 action to prevent it, for example, replacing the hard disk.

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

LAN

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

A failure of the LAN is reported 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 ESRAS 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 are reported 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 are reported 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.

Syslog

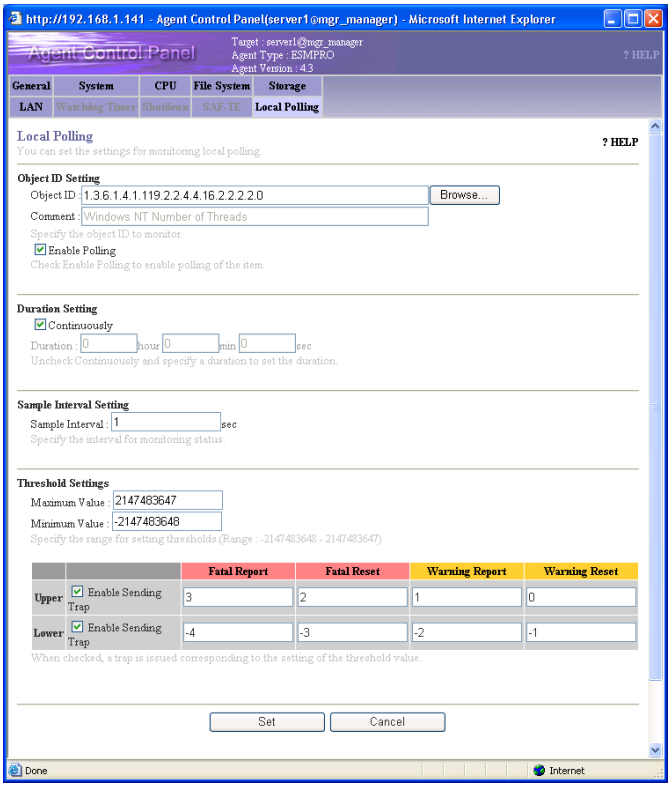
The Syslog tab allows you to configure the settings for monitoring Syslog.

Local Polling

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

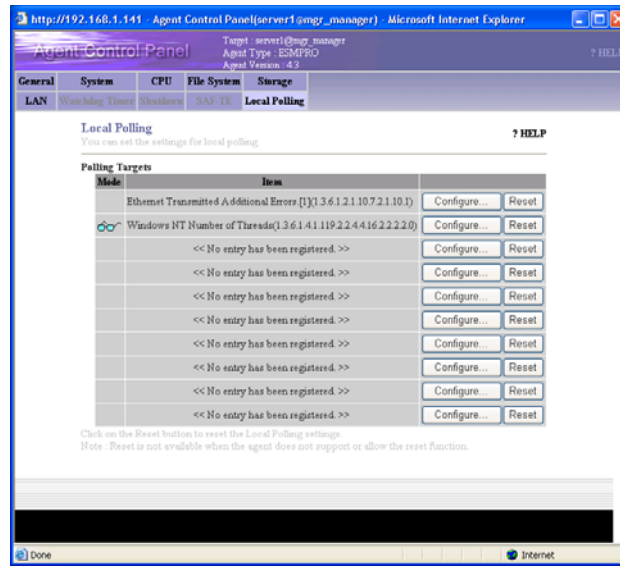
Using this function, you can monitor the items for which the threshold setting function is not supported (e.g., network traffic information and used physical memory). Thus, an alert for the items will be sent when the monitored values are outside of the threshold range.

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.

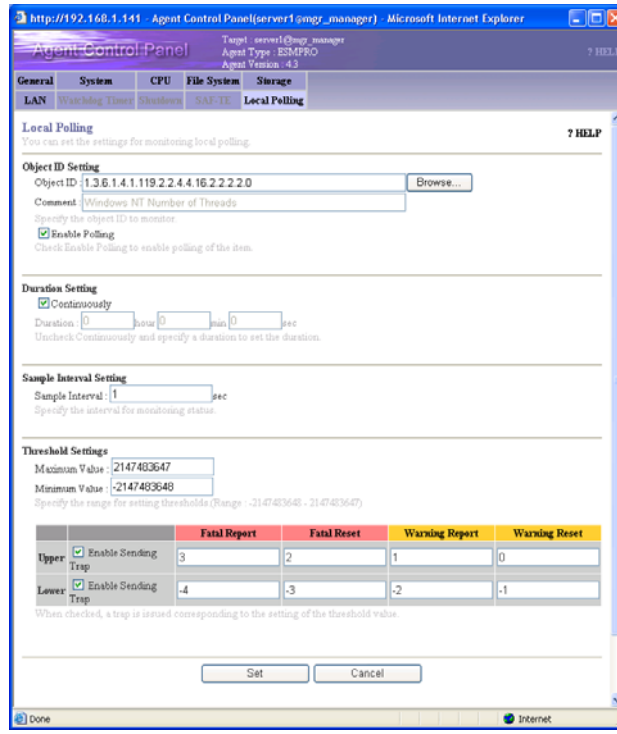


To use the Local Polling function, follow the instructions below.

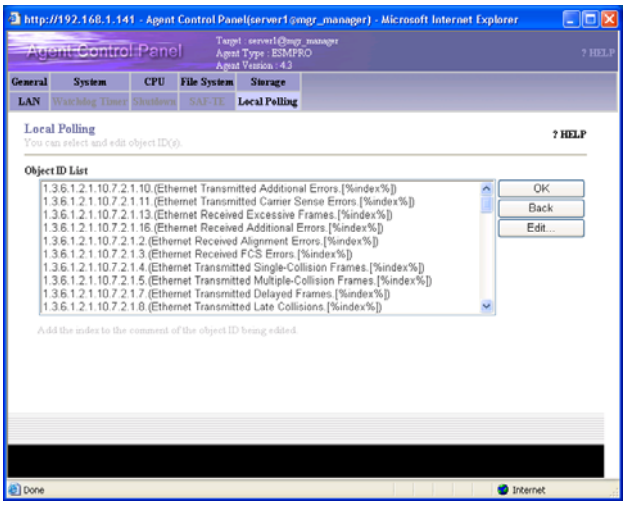
1. Click the Local Polling tab.



2. On the Polling Targets list, click [Configure…] for the target to be registered or changed.



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



4. Set Duration, Interval, Maximum Value and Minimum Value.

5. Set the 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 on 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 another SNMP agent is installed on the server to be managed, the MIB defined in that product can be monitored in the same way as above.

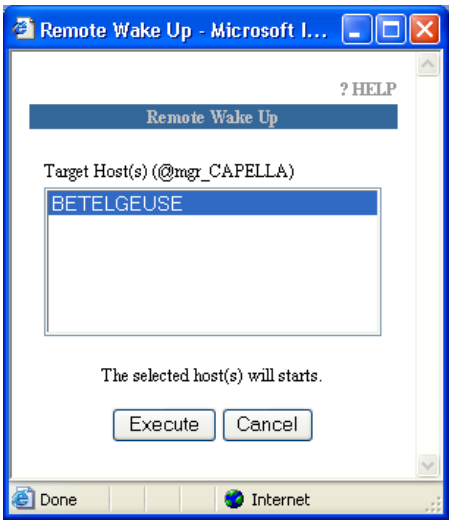
Note that an understanding of the managed server MIB information is required to determine appropriate local polling settings.

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. Select 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 the hosts you want to start from the Target Host(s) List, and click [Execute].

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 the manual for each component for how to set it up.

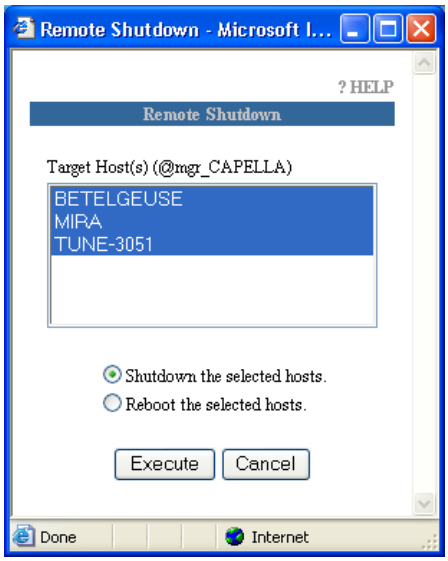
Additionally, the direct broadcast needs to be enabled in a router to use this function over the network via the router. See the router manual for details.

REMOTE SHUTDOWN

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

Remotely Shutting Down a Managed Server

1. Select 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.



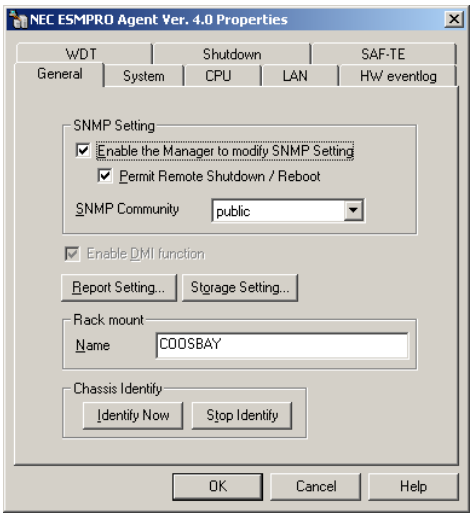
2. Select the hosts to be shut down from the Target Host(s) List, and click [Execute].

NOTE: To use the Remote Shutdown function, the NEC ESMPRO 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.

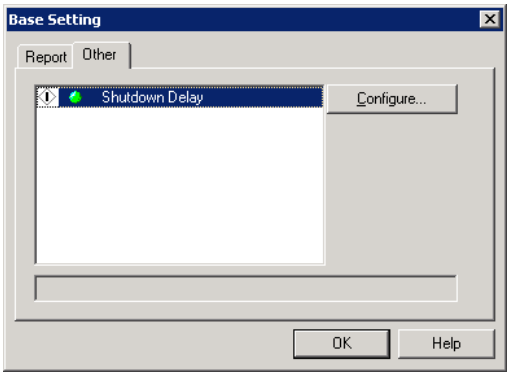
Setting the Agent Settings

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 [Report Setting] 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 the Other tab and check whether the icon displayed on the left of the "Shutdown Delay" item is green as shown below. If not, click the icon to change it to green.



5. Click [OK] to exit the menu.

Chapter 7

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 the HP OpenView Network Node Manager.

> **NOTE:** HP OpenView Integration does not support Windows Vista and Windows Server 2008.

HP OpenView Integration includes the following functions:

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

GETTING STARTED

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

Setting a Method for 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 the Operation Window and set the Method of receiving SNMP Trap to "Use SNMP Trap Service" on the My Manager dialog box.

Before Executing Auto-discovery of the NEC ESMPRO Agent

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

USING HP OPENVIEW INTEGRATION

Auto-discovering NEC ESMPRO Agent

To register an 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 among those registered on the HP OpenView Network Node Manager, and then discovers NEC ESMPRO Agent from among 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 reflects it in the color of 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 box.

First, the process for finding NEC ESMPRO Agent symbols from the selected network symbol is executed. Then component names are set in the NEC ESMPRO Agent Component Name field, and sub map names on which symbols are registered are listed.

Select the NEC ESMPRO Agent you want to delete from the list, and click [Delete] to delete it. If you click [Select All], all symbols in the list are selected.

Launching the DataViewer

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

Launching the Operation Window

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

Launching the AlertViewer

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

Displaying NEC ESMPRO Agent Traps

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

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

The setting for this forwarding function is always automatically done 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.
- Other 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 following items in Destination Setting:

Host name or IP address:	127.0.0.1
Community name:	The name of an SNMP community that HP OpenView accepts

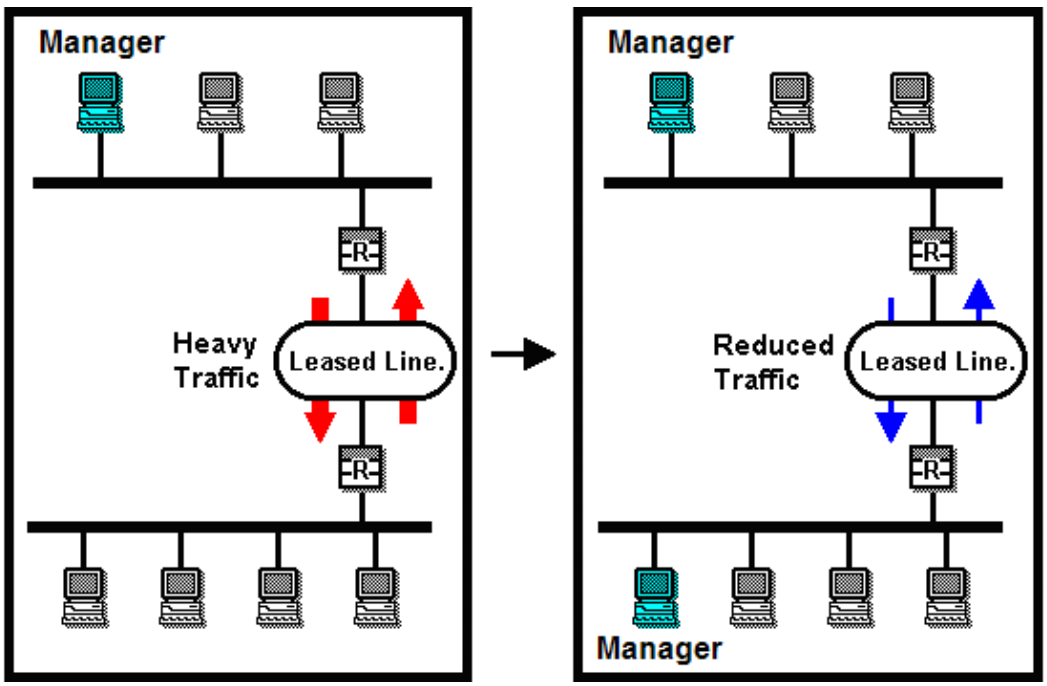
Appendix A

Inter-Manager Communication

NEC 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 NEC 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 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 the Customize menu in the Options menu.

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

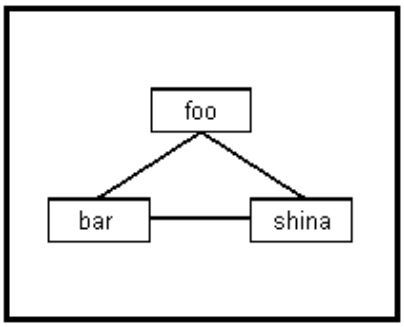


Figure A-2 Network Manager Group

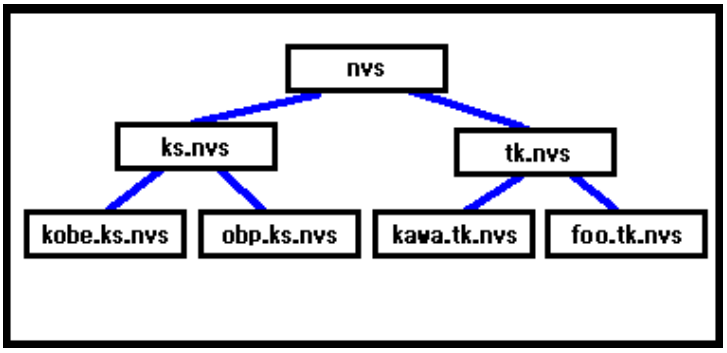


Figure A-3 Ladder Manager Group

In Figure A-3, the three communities, nvs, kawa.tk.nvs, and foo.tk.nvs, are directly connected to each other. ks.nvs and tk.nvs are adjacent communities. A 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 box.

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 NEC ESMPRO Manager.

Appendix B

Notes

MANAGER

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

If a version of NEC ESMPRO Manager is older than that of the 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 the NEC ESMPRO Agent.

2. About coexistence of NEC ESMPRO Manager with other vendor's SNMP management application

When another vendor's SNMP management application which receives an SNMP trap is used along with NEC ESMPRO Manager, one of them may fail to receive the SNMP trap due to a conflict between the two applications. Through the following procedures, the situation can be avoided.

<Work Around 1>

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

Select [Options] - [Customize] - [My Manager] on the Operation Window, and change the Method of receiving an SNMP Trap to "Use SNMP Trap Service".

< Work Around 2 >

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

TCP/IP report to Manager: Transfers an alert from a server to the NEC ESMPRO Manager using an original protocol on TCP/IP.

Note that the operability of the SNMP Trap reception function on the other vendor's SNMP management application cannot be guaranteed.

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

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

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

In case when other DMI management application 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.

5. 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.

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 a high load

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

  If you use the machine with an 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 operating with a 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 the 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 the system according to its IP Address, a DHCP which assigns IP address dynamically cannot be used.

9. About transmitting and receiving packets between NEC ESMPRO Manager and NEC ESMPRO Agent

Packets will be transmitted/received between NEC ESMPRO Manager and the Agent at the following times. We recommend reasonable care in operating in a system which charges you for things such as connection on a WAN.

- At autodiscovery of servers on the Operation Window.
- At a specified interval after specifying regular autodiscovery on the 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 the Operation Window.
- Irregularly, after specifying inter-manager communication on the Operation Window.
- At receipt of an 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 a specified interval for a specified server, after setting Automatic Data Collection.
- Regular polling about every one minute to monitor server status.*

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

10. Setting an 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 connected to the network. For more information, see "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, if the machine is not connected to the network, take the following steps to monitor the machine itself:

- Specify 127.0.0.1 for Start Address and End Address as a range for the Auto-discovering.
- 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 this group.

Note the following:

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 a global group member, it is necessary to start the Domain Controller before the Manager machine boots.

13. About the threshold dialog box for the temperature sensor

For some servers, only the Fatal status may be displayed on the dialog box for setting threshold values of the 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 the same version of the NEC ESMPRO Manager by performing an update installation if needed.

15. Operations as a user who does not have Administrators privilege

When you log on as a user who belongs to the NEC ESMPRO User Group but does not have Administrators privilege, there is the following problem (unless you specified the default Administrators as the NEC ESMPRO User Group during installation of NEC ESMPRO Manager):

[Problem]

When you select [Tools]- [Report Settings] on the AlertViewer to open the Alert Manager window, select [Setting] - [Base Setting] on that window to open the Receive tab of the Base Setting window and change the setting of Receive from Agent (TCP/IP), the following will occur:

- When you have changed from Receive valid (green) to Receive invalid (red):

  Even though the status of each item appears to be changed to "Receive invalid (red)", the service (Alert Manager Socket(R) Service) does not actually stop. In such a case, alert messages can never be received but an unnecessary service is running. This results in a waste of resources. In addition, whenever you change this status to Receive valid (green), the following error appears:

  "Failed to start the service. : Service name"

- When you have changed from Receive invalid (red) to Receive valid (green):

  Although the following message appears, the status of each item is changed to "Receive valid (green)".

  "Failed to start the service. : Service name"

  However, alert messages cannot be received because the service (Alert Manager Socket(R) Service) failed to start.

[Measure]

Log on as a user with Administrators privilege.

- If you have changed each item from Receive valid (green) to Receive invalid (red), restore it to "Receive valid (green)", and change it to "Receive invalid (red)" again.
- If you have changed each item from Receive invalid (red) to Receive valid (green), restore it to "Receive invalid (red)", and change it to "Receive valid (green)" again.

16. To upgrade your operating system

About an Upgrade Installation of Operating Systems Pay attention to performing an upgrade installation of operating systems in the environment where NEC ESMPRO Manager has been installed.
In the case of the following operating systems, NEC ESMRPRO Manager can continue to be used by upgrading your operating system:

Windows Server 2003, Windows Server 2003 R2
Windows Vista
Windows Server 2008

When you want to upgrade operating systems other than the above, uninstall NEC ESMPRO Manager before the upgrade.

[Procedure for upgrading operating systems]
Upgrade NEC ESMPRO Manager to this version, and then upgrade your operating system.

In addition, if the Web Component was added to NEC ESMPRO Manager, the Web Component might not be used because World Wide Web Publishing Service is disabled. In such a case, open the World Wide Web Publishing Service properties on the service window on the Web server, change [Startup type] to "Automatic" or "Manual", click [Apply] and then click [Start Service] to start up the service.

17. 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.

18. Maps to be specified at autodiscovery

After you execute Autodiscover on the 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 a map whose name is the same as its parent map was created at autodiscovery.
In such a case, delete the second mapA(*) (in this example) to resolve the situation..

19. AlertViewer shows "unknown server" in the Component column

If a managed server is not registered in the Operation Window, AlertViewer shows "unknown server" in the Component column.

To show the correct server name in any following alerts, autodiscover the managed server in the Operation Window.

To autodiscover the managed server, go to Operation Window, Tools, Autodiscover, Foreground, TCP/IP Hosts. Select the appropriate map (network) in the Autodiscover dialog box and click [Start].

20. About Setting a Windows Firewall

If the Windows Firewall is enabled, communication between NEC ESMPRO Manager and NEC ESMPRO Agent will be interrupted and the system will not work correctly.

To use NEC ESMPRO Manager with the Windows Firewall enabled, open the following ports:

[Target Ports]

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

For ports used by NEC ESMPRO Manager, see "26. Ports used by NEC ESMPRO Manager and Agent" described in the MANAGER section of this appendix.

■ About autodiscovery on Windows Vista

[Problem]

If the Windows Firewall is enabled on Windows Vista, the ICMP4_ECHO_REPLY response to the ICMP4_ECHO_REQUEST request issued by an application cannot be received by default. Therefore, the autodiscovery function that uses the ICMP request does not work properly.

[Steps to avoid this issue]

Perform the following procedure to create new Inbound Rule:

1) Select [System and Maintenance] - [Administrative Tools] - [Windows Firewall with Advanced Security] in [Control Panel].
2) Select "Inbound Rules" from the Tree, and select [Actions] - [New Rule...]. New Inbound Rule Wizard appears.
3) Leave the default values on pages other than the following, and finish the wizard.
   The Rule Type page: select "Custom".
   The Program page: select "All programs".
   The Protocol and Ports page: select "ICMPv4" as Protocol type.
   The Name page: specify an arbitrary name (ex. "ICMPv4")

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

[Problem]

If a monitored server has multiple IP addresses for a single network card, the IP address of the SNMP Response packet from NEC ESMPRO Agent may differ from the destination 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 the Operation Window, open [Properties] on the server icon, change the IP address to another one that is set on the monitored server, and reboot the Manager computer.

21. 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
2) map icon, and select [Properties] from the pop-up menu.
3) Double-click [Background], and select an appropriate background image.
4) Double-click [Maximum Number of Blade Slot in Chassis], and set an appropriate maximum number of slots.
5) Click [OK] to complete the settings.

22. About autodiscovery of SIGMABLADE

- When CPU blades are autodiscovered before EM Cards are done, the autodiscovered CPU blades will be registered directly under the network map that you specified at autodiscovery, not under a blade map.

  In such a case, delete the registered CPU blades, and autodiscover them again as follows:

  <When EM Cards and CPU blades are in the same segment>
  Register EM Cards first, and then autodiscover corresponding CPU blades, or specify the range of the addresses to include the EM Cards and the CPU blades that are in the same Blade Enclosure and autodiscover them.

  <When EM Cards and CPU blades are in different segments>
  Register EM Cards first, and then autodiscover the corresponding CPU blades.

- When you autodiscover SIGMABLADE, some icons named IP address may be registered outside of Blade Enclosure. These are, for example, the floating IP of EM card, and the IP used for out of band management. You can delete these icons manually as they are not used for the management function provided by Manager.

23. 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".

24. Display of network speed on DataViewer

When you monitor Linux servers, Speed will not be displayed on the Network General window of DataViewer. In such a case, check it on target servers.

25. About display of the network status on the DataViewer

When you monitor a server with Windows Vista installed, the message "Dormant" appears for Status on the Network General window of the DataViewer even if the network properly works. In such a case, check the network status from the monitored server.

26. About display of the teamed network interfaces on the DataViewer

If network interfaces are teamed on a server with Windows Vista or Windows Server 2008 installed, the network information may not be properly displayed. Check it on the monitored server.

27. About a message that appears after clearing the MTBF information

When you execute MTBF Clear on the Maintenance dialog for CPU Module, PCI Module, or Ethernet Board on the DataViewer that is monitoring a ft server, the following message appears which says you are updating firmware.

"Updating Firmware started, but it may take some time. ...."

This message is incorrect. Clearing the MTBF information has started actually.

28. Ports used by NEC ESMPRO Manager and Agent

NEC ESMPRO Manager and Agent use the following ports. If a firewall is placed between Manager and Agent, or if Windows Firewall is enabled, open the following ports.

■ Between Manager and Agent

Function	Manager (Port)	Direction	Agent (Port)	Protocol	Remarks
Operation Window (Autodiscovery)	-	-> <-	-	icmp	icmp
Operation Window (Server Status Polling) DataViewer Server Down Detection	Undeter-mined	-> <-	161	UDP	snmp
Report to Manager (SNMP)	162	-> <-	Undeter-mined	UDP	snmp-trap
Report to Manager (TCP/IP In-Band) Report to Manager (TCP/IP Out-of-Band)	31134	-> <-	Undeter-mined	TCP	-
Remote Wake Up	Undeter-mined	->	10101	UDP	magic packet

- The upper direction shows the direction at start-up, and the lower shows the return.
- Change both Agent and Manager settings when you change the port number for the Report to Manager (TCP/IP In-Band).

  The setting method is as follows.

  <Agent>

  1) Click the "Setting" - "Destination Setting" menu on Alert Manager and the Destination Setting dialog box displays.

2) Select the "TCP/IP In-Band" and click [Modify ID] on Destination Setting dialog box. The ID Setting dialog box displays.
3) Click [Address] on ID Setting dialog and the Manager (TCP/IP In-Band) Setting dialog box displays.
4) Set the port number to "Port Number" on Manager (TCP/IP In-Band) Setting dialog box.

<Manager>

1) Click the "Setting" - "Base Setting" menu on Alert Manager and the Base Setting dialog box displays.
2) Select the "Receive from Agent (TCP/IP)" and click [Configure] on Base Setting dialog box. The Receive from Agent (TCP/IP) setting dialog box displays.
3) Set the port number to "Port Number" on Receive from Agent (TCP/IP) Setting dialog box.

- Change both Agent and Manager settings when you change the port number for the Report to Manager (TCP/IP Out-of-Band).

<Agent>

1) Click the "Setting" - "Destination Setting" menu on Alert Manager, and the Destination Setting dialog box displays.
2) Select the "TCP/IP Out-of-Band" and click [Modify ID] on Destination Setting dialog box. The ID Setting dialog box displays.
3) Click [Address] on ID Setting dialog and the Manager (TCP/IP Out-of-Band) Setting dialog box displays.
4) Set the port number to "Port Number" on Manager (TCP/IP Out-of-Band) Setting dialog box.

<Manager>

1) Click the "Setting" - "Base Setting" menu on Alert Manager, and the Base Setting dialog box displays.
2) Select the "Receive from Agent (TCP/IP)" and click [Configure] on Base Setting dialog box. The Receive from Agent (TCP/IP) setting dialog box displays.
3) Set the port number to "Port Number" on Receive from Agent (TCP/IP) Setting dialog box.

- "Undetermined" means that the unoccupied port at the communication start-up will be selected.

■ Between Manager and Manager

Function	Manager (Port)	Direction	Manager (Port)	Protocol	Remarks
Inter-Manager Communication	Undetermined	-> <-	8806	TCP	-

- The port number can be changed in the Remote Manager dialog box by selecting Operation Window menu [Option] - [Customize] - [Remote Manager].
- "Undetermined" means that the unoccupied port at the communication start-up will be selected.

■ Between Manager or Agent and Mail Server

Function	Manager (Port) or Agent (Port)	Direction	Mail Server (Port)	Protocol	Remarks
Internet Mail	Undetermined	-> <-	25	TCP	smtp

- The port number for the Internet Mail can be changed by following.
  1) Click the "Setting" - "Base Setting" menu on Alert Manager, and the Base Setting dialog box displays.
  2) Select the "Internet Mail" and click [Configure] on Base Setting dialog box. The Internet Mail setting dialog box displays.
  3) Set the port number to "SMTP Port number" on Internet Mail Setting dialog box.
- "Undetermined" means that the unoccupied port at the communication start-up will be selected.

29. About Power Saving Mode of the operating system

- When a computer on which NEC ESMPRO Manager is installed goes into a power saving mode, all features of NEC ESMPRO Manager (such as alert reception, server status monitoring and automatic statistical data collection) stop. It is recommended that you disable the power saving mode.
- When a monitored server with the Wake On Directed Packet option enabled for the network adapter setting goes into the power saving mode, the server is powered on immediately by the server status monitoring feature of NEC ESMPRO Manager which regularly sends packets to the server. In such a case, disable the Wake On Directed Packet option.

30. About system event log when installing NEC ESMPRO Manager on Windows Vista

When installing NEC ESMPRO Manager on Windows Vista, the following event may be reported on Windows Logs (System). This event is reported by the installing service and is not a problem.

Source: Windows Defender
Event ID: 3004
Type: Warning
Description: Windows Defender Real-Time Protection agent has detected changes. Microsoft recommends you analyze the software that made these changes for potential risks. You can use information about how these programs operate to choose whether to allow them to run or remove them from your computer. Allow changes only if you trust the program or the software publisher. Windows Defender can't undo changes that you allow.

31. About application event log when installing NEC ESMPRO Manager

When installing NEC ESMPRO Manager, the following event will be reported on Application event log. This does not cause a problem with security, so you do not need to do anything for it.

Source:	WinMgmt
Event ID:	5603
Type:	Warning
Description:	A provider, ServerManager WMI Support eXtension, has been registered in the WMI namespace, Root\NEC\ESMPRO\SM\WSX, but did not specify the HostingModel property. This provider will be run using the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests. Ensure that provider has been reviewed for security behavior and update the HostingModel property of the provider registration to an account with the least privileges possible for the required functionality.

In addition to the above, there is ESMPROProvider as a provider name.
Source and Description might somewhat vary depending on operating systems.

WEB COMPONENT

1. About Windows Authentication for IIS

If you access to the Web Component from a browser on the Web server (local access) when using Integration Windows Authentication, a CGI window (Command Prompt) that originally runs in the background might appear. This is only a surface issue and does not have any negative influence on the operation.

If you access to the Web Component from a browser on a remote machine (remote access), this window never appears.

In addition, if you are using Windows authentication on Windows Vista or Windows Server 2008, the Web Component can be used only under the following conditions:

- When Administrators has been specified as the NEC ESMPRO User Group to install NEC ESMPRO Manager

<Local access/remote access>

  - Administrator

- When a group other than Administrators has been specified as the NEC ESMPRO User Group to install NEC ESMPRO Manager

<Local access>

  - Administrator

<Remote access>

  - Administrator
  - Any user that belongs to the NEC ESMPRO User Group

Note that the error messages shown below appear and the Web Component does not correctly work under any conditions other than the above.

Failed to collect information. (System error (OpenFileMapping(15))

Failed to collect information. (NVBASE System Service is not active.(15))

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 the information displayed in the window.

5. 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.

6. About autodiscovery of SIGMABLADE

When you autodiscover SIGMABLADE, some hosts named IP address may be registered. These are, for example, the floating IP of EM card, and the IP used for out of band management. You can delete these hosts manually as they are not used for the management function provided by Manager.

7. Display of network speed on DataViewer

When you monitor Linux servers, Speed will not be displayed on the Network General window of DataViewer. In such a case, check it on target servers.

8. About display of the network status on the DataViewer

When you monitor a server with Windows Vista installed, the message "Dormant" appears for Status on the Network General window of the DataViewer even if the network properly works. In such a case, check the network status from the monitored server.

9. About display of the teamed network interfaces on the DataViewer

If network interfaces are teamed on a server with Windows Vista or Windows Server 2008 installed, the network information is not properly displayed. Check it on the monitored server.

10. About Setting a Windows Firewall

If a Windows Firewall is enabled, communication between NEC ESMPRO Manager and NEC ESMPRO Agent will be disconnected and the system will not work correctly. In such a case, the Windows Firewall must be set on the NEC ESMPRO Manager machine.

For how to set the firewall, see "20. About Setting a Windows Firewall" described in the MANAGER section of this appendix.