



# ESMPRO

## Server Management Guide

November 5, 2018  
Rev 1.35e

# Trademarks

- NEC ESMPRO and EXPRERSSCOPE are registered trademarks of NEC Corporation
- Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.
- Intel, Intel® vPro is a trademark or registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.
- Linux is a trademark or registered trademark of Linus Torvalds in United States and other countries.
- Other Corporation name and trade name are trademarks or registered trademarks.

# Cautions

- Unauthorized copying of all or part of this manual is prohibited.
- The contents of this manual may change in the future without notice.
- It is not possible to make reproductions or alterations to this manual without the permission of our firm.
- Please note that we take no responsibility for any effects as a result of making use of this manual.

# Menu

<b>Chapter 1</b>	<b>Introduction.....</b>	<b>11</b>
<b>Chapter 2</b>	<b>NEC ESMPRO Manager Ver.5 Summary .....</b>	<b>13</b>
<b>2.1</b>	<b>About NEC ESMPRO Manager Ver.5 .....</b>	<b>13</b>
<b>2.2</b>	<b>Importance of the Server Management .....</b>	<b>13</b>
<b>2.3</b>	<b>Server Management in NEC Express5800 Series .....</b>	<b>14</b>
<b>2.4</b>	<b>Function Summary Achieved by NEC ESMPRO Manager.....</b>	<b>15</b>
2.4.1	Reporting Function.....	15
2.4.2	Configuration Management.....	15
2.4.3	NEC ExpressUpdate Functions.....	16
2.4.4	RAID Management.....	16
2.4.5	Remote Control.....	16
2.4.6	Management Target Server Setting.....	16
2.4.7	Power Management.....	16
2.4.8	Scheduled Running .....	16
<b>Chapter 3</b>	<b>Implementation and Initial Settings.....</b>	<b>17</b>
<b>3.1</b>	<b>Software which Requires the Installation and Settings. ....</b>	<b>17</b>
<b>3.2</b>	<b>Functional Differences between Windows Edition and Linux Edition .....</b>	<b>17</b>
<b>3.3</b>	<b>Installing the NEC ESMPRO Manager and Environment Settings .....</b>	<b>18</b>
3.3.1	Installing the NEC ESMPRO Manager .....	18
3.3.2	Logging in to the Web Console of the NEC ESMPRO Manager.....	23
3.3.3	Access Control.....	25
3.3.4	User Account Management.....	25
3.3.5	User Account Management (Using Directory Service).....	27
3.3.6	Network Setting, Option Setting.....	27
<b>3.4</b>	<b>NEC ESMPRO Agent Installation and Settings.....</b>	<b>29</b>
3.4.1	NEC ESMPRO Agent Installation and Initial Settings.....	29
<b>3.5</b>	<b>Installing the NEC ExpressUpdate Agent.....</b>	<b>31</b>
3.5.1	Installing the NEC ExpressUpdate Agent.....	31
<b>3.6</b>	<b>Installing and Setting up the NEC Universal RAID Utility.....</b>	<b>31</b>
3.6.1	Installing and Setting up NEC Universal RAID Utility.....	31
<b>3.7</b>	<b>Installing and Setting up the LSI SMI-S Provider .....</b>	<b>31</b>
3.7.1	Installing and Setting up the LSI SMI-S Provider .....	31
<b>3.8</b>	<b>Setting up the EXPRESSSCOPE Engine 3 .....</b>	<b>32</b>
3.8.1	Setting up from the Web console of the EXPRESSSCOPE Engine 3.....	32
3.8.2	Setting up from BMC Configuration Tool (Online version) .....	33
3.8.3	Setting up from BMC Configuration Tool (Offline version) .....	34
<b>Chapter 4</b>	<b>Server Management .....</b>	<b>35</b>
<b>4.1</b>	<b>About NEC ESMPRO Manager Web Console.....</b>	<b>35</b>
4.1.1	Header Menu (1) .....	36
4.1.2	Tree View (2) .....	36
4.1.3	Local Navigation (3) .....	37
4.1.4	Operation Area (4) .....	37
<b>4.2</b>	<b>Group.....</b>	<b>38</b>
4.2.1	Group.....	38

4.2.2	Chassis .....	39
4.2.3	Power Group .....	39
4.2.4	Edit Group Set .....	39
<b>4.3</b>	<b>Registering a Server.....</b>	<b>40</b>
4.3.1	Auto Registration .....	40
4.3.2	Manual Registration .....	42
<b>Chapter 5</b>	<b>Server Fault Detection and Notification .....</b>	<b>45</b>
<b>5.1</b>	<b>Referencing Server Fault Information (Web Console) .....</b>	<b>45</b>
<b>5.2</b>	<b>Referencing Server Fault Information (Alert Viewer) .....</b>	<b>45</b>
5.2.1	Starting Alert Viewer .....	45
5.2.2	Referencing Detailed Information for an Alert.....	47
5.2.3	Automatically Saving Received Alerts to a File .....	48
<b>5.3</b>	<b>Server Fault Notification (Linking with WebSAM AlertManager).....</b>	<b>49</b>
5.3.1	Expandable Notification Methods and Features.....	49
5.3.2	Convenient Notification Methods.....	50
5.3.3	Expanding Notification Methods.....	51
<b>5.4</b>	<b>Transferring Notifications from NEC ESMPRO Agent to Another Manufacturer's Console (Trap Transfers) .....</b>	<b>51</b>
5.4.1	Transferring Traps .....	52
5.4.2	Starting the ESMPRO/SM Trap Redirection Service.エラー! ブックマークが定義されていません。	
5.4.3	Format of the Transferred Trap.....	53
5.4.4	Settings on Other Manufacturers' Management Consoles .....	55
<b>5.5</b>	<b>Receiving Alerts from a Device on which NEC ESMPRO Agent Cannot be Installed.....</b>	<b>55</b>
<b>5.6</b>	<b>Lists of Notification Items.....</b>	<b>55</b>
<b>5.7</b>	<b>Express Notification Service .....</b>	<b>56</b>
<b>Chapter 6</b>	<b>Configuration Management .....</b>	<b>57</b>
<b>6.1</b>	<b>System Management (ServerAgent) .....</b>	<b>57</b>
6.1.1	CPU Monitoring.....	60
6.1.1.1	The CPU Monitoring Feature .....	60
6.1.1.2	Using CPU Monitoring .....	63
6.1.2	Memory Monitoring .....	66
6.1.2.1	The Memory Monitoring Feature .....	66
6.1.2.2	The Use of Memory Monitoring .....	67
6.1.3	Temperature Monitoring .....	70
6.1.3.1	The Temperature Monitoring Feature.....	70
6.1.3.2	Using Temperature Monitoring .....	70
6.1.4	Fan Monitoring .....	73
6.1.4.1	The Fan Monitoring Feature.....	73
6.1.4.2	Using Fan Monitoring .....	74
6.1.5	Monitoring Case Voltage .....	75
6.1.5.1	The Case Voltage Monitoring Feature .....	75
6.1.5.2	Using Case Voltage Monitoring .....	76
6.1.6	Power Supply Unit Monitoring.....	77
6.1.6.1	The Power Supply Unit Monitoring Feature .....	77
6.1.6.2	Using Power Supply Unit Monitoring.....	77
6.1.7	Cooling Unit Monitoring.....	79

6.1.7.1	The Cooling Unit Monitoring Feature .....	79
6.1.7.2	Using Cooling Unit Monitoring.....	79
6.1.8	Case Cover Monitoring .....	80
6.1.8.1	The Case Cover Monitoring Feature .....	80
6.1.8.2	Using Case Cover Monitoring .....	81
6.1.9	File System Monitoring .....	82
6.1.9.1	The File System Monitoring Feature .....	82
6.1.9.2	Using File System Monitoring.....	85
6.1.9.3	Changing the File System Available Capacity Monitoring Thresholds .....	88
6.1.9.4	Changing the Monitoring Interval .....	89
6.1.10	SCSI/IDE Device Monitoring.....	90
6.1.10.1	The SCSI/IDE Device Monitoring Feature .....	90
6.1.10.2	Using SCSI/IDE Device Monitoring.....	92
6.1.11	Disk Array Monitoring.....	94
6.1.12	LAN Network Monitoring .....	94
6.1.12.1	The LAN Monitoring Feature .....	95
6.1.12.2	Using LAN Monitoring .....	95
6.1.13	System Information Referencing.....	99
6.1.13.1	Referencing I/O Device Information .....	99
6.1.13.2	Referencing Software Information.....	100
6.1.13.3	Referencing BIOS Information .....	100
6.1.13.4	Referencing Device Information .....	101
6.1.14	Referencing Errors Detected at the Hardware Level .....	102
6.1.14.1	The ESRAS Utility Feature.....	102
6.1.15	Event Monitoring.....	104
6.1.15.1	The Event Monitoring Feature.....	104
6.1.15.2	Using Event Monitoring .....	104
6.1.16	Stall Monitoring .....	109
6.1.16.1	The Stall Monitoring Feature .....	109
6.1.16.2	Using Stall Monitoring .....	109
6.1.17	System Error (Panic) Detection .....	112
6.1.17.1	The System Error Detection Feature .....	112
6.1.17.2	Using System Error Detection.....	112
6.1.18	Shutdown Monitoring .....	113
6.1.18.1	The Shutdown Monitoring Feature .....	113
6.1.18.2	Using Shutdown Monitoring .....	113
6.1.19	Monitoring of PCI Hot-plugging.....	115
6.1.19.1	The PCI Hot-plugging Monitoring Feature .....	115
6.1.19.2	Using PCI Hot-plugging Monitoring.....	115
6.1.19.3	Operations when Detecting PCI Hot-plugging .....	115
6.1.20	Local Polling.....	116
6.1.21	Alive Monitoring .....	118
6.1.21.1	The Alive Monitoring Feature .....	118
6.1.21.2	Using Alive Monitoring.....	119
<b>6.2</b>	<b>System Management (VMware ESXi 5) .....</b>	<b>122</b>
6.2.1	VMware ESXi 5 Monitoring .....	122
6.2.1.1	Referencing CPU Information .....	123
6.2.1.2	Referencing Memory Information.....	124
6.2.1.3	Referencing Data Stores .....	124

6.2.1.4	Referencing Software Information.....	125
6.2.1.5	Referencing Storage Device Information .....	127
6.2.1.6	Referencing Network Information.....	127
<b>6.3</b>	<b>Management with the Management Controller.....</b>	<b>128</b>
6.3.1	Virtual LCD.....	128
6.3.2	LEDs .....	129
6.3.3	System Current Accumulated Time .....	129
6.3.4	System Monitoring .....	129
6.3.5	Configuration Information.....	129
<b>Chapter 7</b>	<b>NEC ExpressUpdate .....</b>	<b>131</b>
<b>7.1</b>	<b>NEC ExpressUpdate .....</b>	<b>131</b>
<b>7.2</b>	<b>Components Whose Versions Can Be Managed by NEC ExpressUpdate Functions.....</b>	<b>132</b>
7.2.1	With NEC ExpressUpdate Agent Installed .....	132
7.2.2	Without NEC ExpressUpdate Agent (Through EXPRESSSCOPE Engine 3) Installed ....	132
7.2.3	Components Other Than Automatic Application Target .....	133
<b>7.3</b>	<b>Types of Update Packages.....</b>	<b>133</b>
7.3.1	Availability of Automatic Update .....	133
7.3.2	Downgrade Availability .....	134
7.3.3	Reboot Requirement After Installation.....	134
<b>7.4</b>	<b>Repository Settings .....</b>	<b>135</b>
7.4.1	Location of Repository .....	135
7.4.2	Other Settings .....	136
<b>7.5</b>	<b>Repository Management Information .....</b>	<b>137</b>
7.5.1	Displaying Update Packages .....	138
7.5.2	Downloading Update Packages .....	138
7.5.3	Adding Update Packages .....	138
7.5.4	“Clean Removal History” for Update Packages.....	139
7.5.5	Removing Update Packages.....	139
7.5.6	Saving Update Packages.....	140
<b>7.6</b>	<b>Installing NEC ExpressUpdate Agent Remotely .....</b>	<b>140</b>
<b>7.7</b>	<b>Installing Update Packages on the Management Target Server .....</b>	<b>140</b>
7.7.1	Update/Installation (Other than NEC ExpressUpdate Agent) .....	141
7.7.2	Downgrade .....	141
7.7.3	Uninstallation.....	141
<b>7.8</b>	<b>Installing Update Packages at a Specified Time by Using the Remote Batch Functions .....</b>	<b>141</b>
<b>Chapter 8</b>	<b>RAID Management.....</b>	<b>143</b>
<b>8.1</b>	<b>RAID System Management Mode.....</b>	<b>143</b>
8.1.1	Using Standard Mode .....	143
8.1.2	Using Advanced Mode .....	143
<b>8.2</b>	<b>Descriptions of Management Items .....</b>	<b>144</b>
8.2.1	RAID System Information .....	144
8.2.2	RAID Log.....	144
8.2.3	RAID Controller.....	145
8.2.4	Battery .....	146
8.2.5	Disk Array .....	146
8.2.6	Logical Drive .....	147
8.2.7	Physical Device .....	148

<b>Chapter 9 Remote Control</b>	<b>149</b>
9.1 Remote Power Control	149
9.2 Power Management	150
9.3 Remote Console	150
9.4 IPMI Information	151
9.5 Logging in to the EXPRESSSCOPE Engine Series	152
<b>Chapter 10 Settings</b>	<b>153</b>
10.1 Connection Setting	153
10.2 NEC ExpressUpdate Agent Setting	153
10.3 Power Supply Option Setting	153
10.4 BMC Setting (EXPRESSSCOPE Engine 3)	155
10.4.1 Network	155
10.4.2 User Management	158
10.4.3 Alert Reporting	159
10.4.4 Miscellaneous	162
10.4.5 Reset	162
10.5 BIOS Setting	162
10.6 Backup/Restore	162
10.6.1 Backup	162
10.6.2 Restore	163
10.7 NEC ESMPRO Agent Extension Setting	163
10.8 Console Log Setting	163
10.9 NEC ESMPRO Agent	164
10.9.1 CPU	164
10.9.2 File System	165
10.9.3 Local Polling	166
10.10 Server Monitoring Setting	169
10.11 Remote Wake Up Setting	170
<b>Chapter 11 Power Management</b>	<b>172</b>
11.1 Power Measurement Function	172
11.1.1 Power Measurement Function Using NEC ESMPRO Manager	172
11.1.2 Power Measurement Function of EXPRESSSCOPE Engine 3 WebConsole	173
11.2 Power Capping	174
11.2.1 Non-Aggressive Mode (Non-Critical Power Capping)	174
11.2.2 Aggressive Mode (Critical Power Capping)	175
11.2.3 Safe Power Capping	175
11.2.4 Boot Time Configuration	175
11.2.5 Setting Power Capping Screen	175
11.3 Group Power Control	176
11.3.1 Balance Type Power Distribution Function	176
11.3.2 Priority Based Power Distribution Function	177
11.4 Suspend Periods Setting	177
<b>Chapter 12 Scheduled Operation/Remote Batch</b>	<b>179</b>
12.1 Scheduled Operation	179
12.2 Remote Batch	179

<b>Chapter 13</b>	<b>Command Line Interface.....</b>	<b>181</b>
<b>13.1</b>	<b>EXPRESSSCOPE Engine 3 .....</b>	<b>181</b>
13.1.1	Remote Control using SSH Client.....	181
13.1.2	Scripting.....	181
<b>13.2</b>	<b>NEC ESMPRO Manager.....</b>	<b>182</b>
<b>Appendix A</b>	<b>Log Collection.....</b>	<b>187</b>
1.	NEC ESMPRO Manager.....	187
2.	NEC ESMPRO Agent.....	189
3.	NEC ESMPRO Agent Extension.....	190
4.	NEC ExpressUpdate Agent.....	192
5.	Collection of IPMI Information.....	192
i.	NEC ESMPRO Manager.....	192
ii.	EXPRESSSCOPE Engine 3 .....	193
iii.	ESRAS Utility .....	194
<b>Appendix B</b>	<b>Comparison of EXPRESSSCOPE Engine Series Features .....</b>	<b>195</b>



# Terms

Table 1 Terms

用語	説明
Management Server	The computer on which ESMPRO/ServerManager is installed. Personal computer can be used for installation.
Management Target Server	The server which is managed by ESMPRO/ServerManager.
BMC	An abbreviation of Baseboard Management Controller. A management controller that monitors and makes reports about the system hardware, without relying on the state of the system or the OS. In NEC, BMC is called as EXPRESSSCOPE Engine.
IPMI	An abbreviation of Intelligent Platform Management Interface. This is a standard interface specification to manage servers, without relying on the system or the OS.
Intel vPro™ Technology	Hardware brand name of Intel's client computer. It enables remote management without relying on the state of the system power.
WBEM	An abbreviation of Web-Based Enterprise Management. Defined by DMTF.
PET Alert	Means Platform Event Trap, sent from BMC.
SA	Means NEC ESMPRO Agent
SAS	Means NEC ESMPRO ServerAgentService
URU	Means Universal RAID Utility
Server Conf.	Means Server Configuration Utility

# Associated Documents

**Table 2 Associated Documents**

Name	Storing Place
NEC ESMPRO ServerManager Installation Guide	<ul style="list-style-type: none"> <li>• Web(*1)</li> <li>• EXPRESSBUILDER</li> </ul>
NEC ESMPRO ServerAgent Installation Guide (Windows)	<ul style="list-style-type: none"> <li>• EXPRESSBUILDER</li> </ul>
NEC ESMPRO ServerAgentService Installation Guide (Windows)	<ul style="list-style-type: none"> <li>• Web(*1)</li> <li>• EXPRESSBUILDER</li> </ul>
NEC ESMPRO ServerAgent Installation Guide (Linux)	<ul style="list-style-type: none"> <li>• Web(*1)</li> <li>• EXPRESSBUILDER</li> </ul>
NEC ESMPRO ServerAgent Users Guide (Linux)	<ul style="list-style-type: none"> <li>• Web(*1)</li> <li>• EXPRESSBUILDER</li> </ul>
Universal RAID Utility Users Guide	<ul style="list-style-type: none"> <li>• Web(*1)</li> <li>• EXPRESSBUILDER</li> </ul>
NEC ESMPRO/ServerManager RAID System Management Guide for VMware ESXi 5	<ul style="list-style-type: none"> <li>• Web(*1)</li> </ul>
ESMPRO/ServerManager Ver.5 Command Line Interface	<ul style="list-style-type: none"> <li>• Web(*1)</li> <li>• EXPRESSBUILDER</li> </ul>
Command Line Interface User's Guide for NEC ExpressUpdate	<ul style="list-style-type: none"> <li>• Web(*1)</li> <li>• EXPRESSBUILDER</li> </ul>
ESMPRO Agent alert list	<ul style="list-style-type: none"> <li>• WEB(*1)</li> </ul>
BMC SNMPAlert List	<ul style="list-style-type: none"> <li>• WEB(*1)</li> </ul>
Server Configuration Utility User's Guide	<ul style="list-style-type: none"> <li>• Web(*1)</li> <li>• EXPRESSBUILDER</li> </ul>
EXPRESSSCOPE Engine User's Guide	<ul style="list-style-type: none"> <li>• Web(*1)</li> <li>• EXPRESSBUILDER</li> </ul>
(WhitePaper)NEC ExpressUpdateFunctions and Features	<ul style="list-style-type: none"> <li>• Web(*1)</li> </ul>
(WhitePaper)Introduction to the power monitoring and power control function	<ul style="list-style-type: none"> <li>• Web(*1)</li> </ul>
(WhitePaper)EXPRESSSCOPE Engine 3 Scripting Guide	<ul style="list-style-type: none"> <li>• Web(*1)</li> </ul>

(※1) Refer to <http://www.58support.nec.co.jp/global/download/>

# Chapter 1 Introduction

The purpose of this document is to provide customers who purchased NEC Express5800 series with the simpler server management by using NEC ESMPRO Manager, server management software of NEC Corporation.

As of November 2016, this document supports the following versions of devices and software.

**Table 3 Target device and software version**

Software	Condition	Version
NEC ESMPRO Manager	Windows	6.14
	(Linux *1)	-
NEC ESMPRO ServerAgentService	Windows	1.2
	Linux	1.1
NEC ESMPRO Agent	(Windows *2)	4.61
	(Linux *2)	4.5.XX
NEC ESMPRO Agent Extension	Windows	2.07
	Linux	2.08
Server Configuration Utility	Windows	1.06
	Linux	1.06
Universal RAID Utility	Windows	4.1
	Linux/VMware ESX	4.1
LSI SMI-S Provider	VMware ESXi 5.0-5.1	00.50.V0.13
	VMware ESXi 5.5, 6	00.57.V0.04
NEC ExpressUpdate Agent	Windows	3.14
	Linux	3.16

\*1 Linux Edition of NEC ESMPRO Manager does not support 6.05 or later.

\*2 The server which is not supported by NEC ESMPRO ServerAgentService is supported by NEC ESMPRO Agent.

## **Chapter 1 Introduction**

This chapter.

## **Chapter 2 NEC ESMPRO Manager Ver. 6 Overview**

Describes the overview of NEC ESMPRO Manager as the core of NEC server management software.

## **Chapter 3 Introduction and Initial Setting of NEC ESMPRO Manager**

Describes the introduction and the initial setting of NEC ESMPRO Manager and its related software.

## **Chapter 4 Server Management**

Describes how to register the management target servers to NEC ESMPRO Manager.

## **Chapter 5 Server Fault Detection and Report Service**

Describes how to confirm the server fault information and report service.

## **Chapter 6 Management Items**

Describes manageable items by NEC ESMPRO Manager.

## **Chapter 7 NEC ExpressUpdate**

NEC ExpressUpdate is a part of the functions of NEC ESMPRO Manager. It allows you to manage versions of firmware and software of the management target servers through an intuitive user interface. This chapter describes the outline and the use of NEC ExpressUpdate functions.

## **Chapter 8 RAID Management**

Once Universal RAID Utility is installed on the management target servers, RAID system reference and monitoring, and executing operation for RAID system can be performed by NEC ESMPRO Manager. This chapter explains about its management items

### **Chapter 9 Remote Control**

By using NEC ESMPRO Manager, Power control and Power management of the management target servers can be performed by remote control. This chapter describes how to operate remote control.

### **Chapter 10 Settings**

Describes how to perform backup and restore Power Option Setting, EXPRESSSCOPE Engine 3 Setting and BIOS Settings by remote control.

### **Chapter 11 Power Management**

Describes Power Control Function which implements Operational Continuity of Collecting the statistical information regarding power consumption (maximum power [W], minimum power [W], average power [W] and so on), Power Monitoring Function which periodically measures power consumption while controlling the total power consumption of the devices (the management target servers) below the set power consumption.

### **Chapter 12 Scheduled Operation/Remote batch**

Describes Scheduled operation/ Remote batch function which performs the power source operation at the specified time.

### **Chapter 13 Command Line Interface**

Describes Remote Server Management by using Command Line Interface.

### **Chapter 14 NEC ESMPRO ServerAgentService**

Describes NEC ESMPRO ServerAgentService, which is Agent for new hardware.

## Chapter 2 NEC ESMPRO Manager Ver.6 Summary

---

### 2.1 About NEC ESMPRO Manager Ver.6

NEC ESMPRO Manager Ver.6 is the server management software which enables the steady operation of the server system and more efficient system operation. It manages the configuration information/running status of the server resources and it sends alerts to the system administrator upon detecting the server failure in order to provide the prompt response to the issues.

NEC ESMPRO Manager Ver.6 is a web-based application. With the server and browser capable of communicating with the management target server on which the NEC ESMPRO Manager is installed, you can manage and monitor the server from any location.

### 2.2 Importance of the Server Management

Stable server operation is essential to ensure the stability of customers' computer system. The high load on the server management also needs to be reduced to ensure the stable operation.

- Stable operation of the server

Unplanned server stop leads immediately to the loss of customers' sales opportunities and profits. Therefore, the server is expected to run perfectly at any time. In the event of a server failure, quick acknowledgement of the incident and an investigation of the cause and troubleshooting are necessary. The sooner the damage recovery is achieved, the less cost will be incurred consequently.

- Reducing the cost of the server management

Server management requires a great deal of labor especially in the large-scale distribution system, or the server management in remote sites. Reducing the cost of the server management is the most certain way to the eventual cost down (benefit to customers).

## 2.3 Server Management in NEC Express5800 Series

NEC Express5800 series servers are managed by using the following NEC software and the EXPRESSSCOPE Engine series. EXPRESSSCOPE Engine is a dedicated controller installed on the motherboard of Express 5800 series and it provides the remote control functions, such as monitoring the condition of power supply, fan, temperature on the main device components, as well as the control over the keyboard, video, mouse (KVM) by the network for management, and remote access to CD/DVD-ROM/Floppy Disk Drives/ISO Image/USB Memory from the server.

**Table 4 Software used in server management**

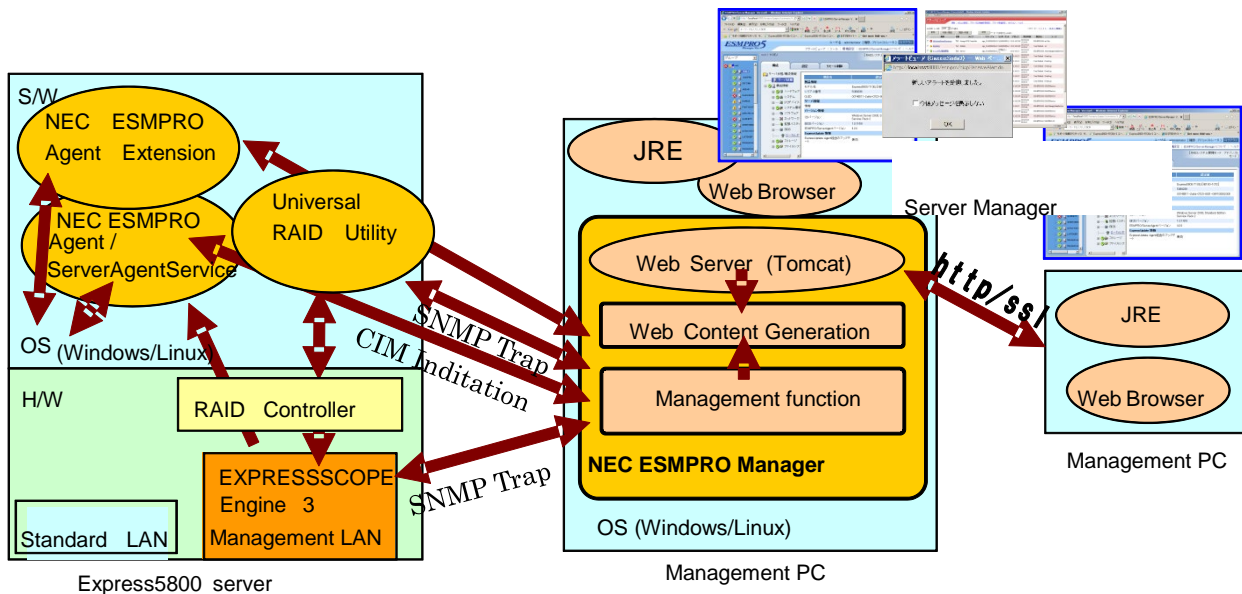
Name	Summary	Source of Supply
NEC ESMPRO Manager	Software installed on the management server to manage the multiple target servers. It supports Windows and Linux. *1	<ul style="list-style-type: none"> <li>• Web *2</li> <li>• EXPRESSBUILDER</li> </ul>
NEC ESMPRO Agent NEC ESMPRO ServerAgentService	Software to collect the detailed information of the management target server and to provide the alert function. It is installed on the OS of the management target server. It supports Windows and Linux.	<ul style="list-style-type: none"> <li>• Web (Linux only) *2</li> <li>• Pre-install *3</li> <li>• EXPRESSBUILDER</li> </ul>
NEC ESMPRO Agent Extension	Necessary software to realize the scheduled running function. Some settings are executed by this tool for EXPRESSSCOPE Engine 1/2.	<ul style="list-style-type: none"> <li>• Web *2</li> <li>• EXPRESSBUILDER</li> </ul>
NEC ExpressUpdate Agent	Necessary software to realize the NEC ExpressUpdate function which provides the batch updates of the SW or FW on the management target server from NEC ESMPRO Manager.	<ul style="list-style-type: none"> <li>• Web *2</li> <li>• Pre-install *3</li> <li>• EXPRESSBUILDER</li> </ul>
Universal RAID Utility	Necessary software to manage and monitor the RAID structure of the management target servers. It supports Windows, Linux and VMware ESX.	<ul style="list-style-type: none"> <li>• Web *2</li> <li>• Pre-install *3</li> <li>• EXPRESSBUILDER</li> </ul>
LSI SMI-S Provider	Necessary software to manage and monitor the RAID structure of the management target server. It supports VMware ESXi 5, 6.	<ul style="list-style-type: none"> <li>• Web *2</li> <li>• Pre-install *3</li> </ul>
Server Configuration Utility	Tool used for EXPRESSSCOPE Engine 3 configuration. This is a successor software of BMC Configuration Tool. The Offline version is booted up by pressing "F4" key after activating the power supply, and the Online version is installed on the OS of the management target server.	<ul style="list-style-type: none"> <li>• EXPRESSBUILDER (Online version)</li> <li>• Built in the server (Offline version)</li> </ul>

\*1 : In the case of installing NEC ESMPRO Manager on Linux, the management and monitoring by using the NEC ESMPRO Agent and the reception of an alert are not available.

\*2 : Refer to <http://www.58support.nec.co.jp/global/download/>

\*3 : In the case of pre-install model, the software is installed at the time of factory shipment.

The following is the software correlation diagram.



**Figure 1 Software correlation diagram**

\* If the OS of the management target server is VMware ESXi 5, “Universal RAID Utility” is replaced with “LSI SMI-S Provider” and “SNMP Trap” is replaced with “CIM Indication”. NEC ESMPRO ServerAgentService is also included in software on OS.

## 2.4 Function Summary Achieved by NEC ESMPRO Manager

The following operation can be realized by using NEC ESMPRO Manager and the related software.

### 2.4.1 Reporting Function

Reporting sent from the NEC ESMPRO Agent, NEC ESMPRO ServerAgentService or the EXPRESSSCOPE Engine installed on the management target servers to the NEC ESMPRO Manager is available in the event of a failure. The content of the report can be checked on the AlertViewer on the Web Console of NEC ESMPRO Manager.

There are two methods for report management. One is the self-management by the customer, and the other is by the Express Report Service which automatically reports to the maintenance center. Refer to the “Reporting Functions” described in the related documentation for the types and features of the report function.

### 2.4.2 Configuration Management

Various information about the server and the OS can be managed and monitored by the NEC ESMPRO Manager. If the EXPRESSSCOPE Engine 3 is installed, the hardware management and monitoring can be performed by registering the EXPRESSSCOPE Engine 3 to the NEC ESMPRO Manager as a management item, instead of using the Agent software. By installing the NEC ESMPRO Agent or NEC ESMPRO ServerAgentService on the management target servers, more information including the one on the OS can also be managed and monitored. In the case of the VMware ESXi5 on which NEC ESMPRO Agent cannot be installed, information managed by the VMware ESXi5 can be checked as a result of the direct communication between the NEC ESMPRO Manager and the VMware ESXi5.

### 2.4.3 NEC ExpressUpdate Functions

Version management of the System BIOS of the management target servers, the EXPRESSSCOPE Engine 2/3, some software/driver/firmware and batch applications of the update packages can be performed. When managing the software/driver/firmware, the NEC ExpressUpdate Agent needs to be installed on the OS of the management target servers.

In the case of the EXPRESSSCOPE Engine 3 installed server, update can be performed without installing System BIOS and the EXPRESSSCOPE Engine 3 on the NEC ExpressUpdate Agent. Refer to Chapter 7 for details.

### 2.4.4 RAID Management

Installing the Universal RAID Utility or the LSI SMI-S Provider on the management target server allows you to manage and monitor the RAID structure from the NEC ESMPRO Manager. Initialization and rebuild, etc. can also be performed. Refer to *Universal RAID Utility User's Guide*, or *NEC ESMPRO Manager RAID System Management Guide for VMware ESXi 5* stored in NEC EXPRESSBUILDER for details.

### 2.4.5 Remote Control

Batch control of the power supply and the power management of the management target servers within a group can be executed from NEC ESMPRO Manager.

### 2.4.6 Management Target Server Setting

Remote settings such as power supply option setting, EXPRESSSCOPE Engine 3 setting, BIOS setting and backup/ restore of the EXPRESSSCOPE Engine 3 setting can be remotely configured.

### 2.4.7 Power Management

Power management of the single management target server is available. NEC ESMPRO Manager enables the power allocation to the group which consolidates the multiple management target servers and power control over the group. EXPRESSSCOPE Engine 3 needs to be managed by the management target server. Refer to Chapter 11 for details.

### 2.4.8 Scheduled Running

Scheduled running which automatically controls the power supply of the management target server at a specified time and the remote batch function which executes the NEC ESMPRO Manager function at a specified time. NEC ESMPRO Agent Extension needs to be installed on the management target servers to perform the scheduled running.



## Chapter 3 Implementation and Initial Settings

This chapter describes the implementation and initial settings for the NEC ESMPRO Manager and the related software.

### 3.1 Software which Requires the Installation and Settings.

Software installation and settings are required according to the functions employed in order to manage the NEC Express5800 Series by using the NEC ESMPRO Manager. Be sure to perform the installation and settings necessary for the adopted functions.

**Table 5 Software which requires the installation and settings**

Function	Required Software
Management and Monitoring of the Multiple Servers	• NEC ESMPRO Manager
Report Function *2	• NEC ESMPRO Agent • EXPRESSSCOPE Engine 3
Structure Management	• NEC ESMPRO Agent *1 • NEC ESMPRO ServerAgentService • EXPRESSSCOPE Engine 3
NEC ExpressUpdate Functions(driver/software)	• NEC ExpressUpdate Agent • EXPRESSSCOPE Engine 3
RAID Management	• Universal RAID Utility • LSI SMI-S Provider
Remote Control	• EXPRESSSCOPE Engine 3 • NEC ESMPRO Agent
Power Management	• EXPRESSSCOPE Engine 3
Scheduled Operation	• NEC ESMPRO Agent Extension

\*1Not available in the case of managing with NEC ESMPRO Manager for Linux.

### 3.2 Functional Differences between Windows Edition and Linux Edition

NEC ESMPRO Manager has the following functional differences between Windows edition and the Linux edition.

**Table 6 Functional differences between Windows edition and Linux edition**

Destination OS	Functional difference
Windows	• System management using the NEC ESMPRO Agent is available.
Linux	• System management using the NEC ESMPRO Agent is not available. • Reception of report (alert) is not available. • Management of the VMware ESXi5 is not available

### 3.3 Installing the NEC ESMPRO Manager and Environment Settings

The followings are the descriptions of the installation and necessary environment settings of the NEC ESMPRO Manager which plays the core role in the server management.

#### 3.3.1 Installing the NEC ESMPRO Manager

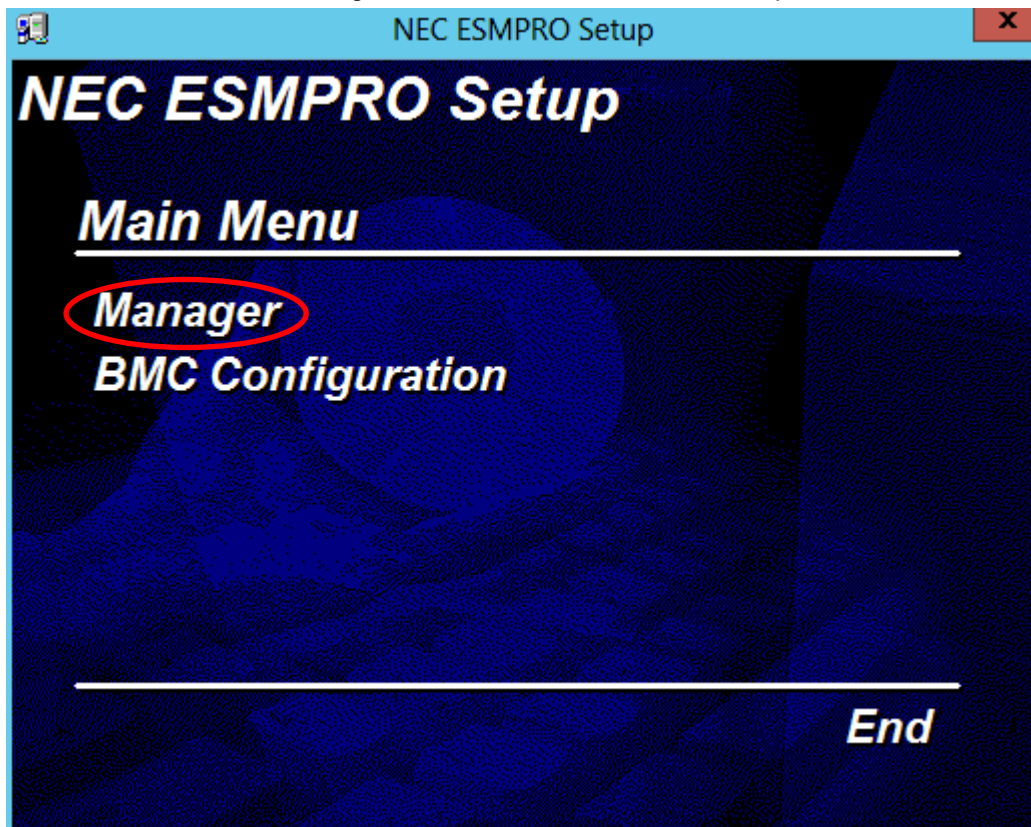
NEC ESMPRO Manager is stored in the NEC EXPRESSBUILDER attached to the NEC Express5800 Series. The latest version of the NEC ESMPRO Manager can be downloaded from NEC Corporate Website. (<http://www.58support.nec.co.jp/global/download/>).

Procedure for downloading the latest NEC ESMPRO Manager from NEC Corporate Website and installing it on the Windows OS is described below. Refer to *NEC ESMPRO Manager Ver.5.7 Installation Guide* for how to install, set up and the details about the environments for the installation and other precautions.



NEC ESMPRO Manager is available on neither Windows Server 2003 nor Windows Server 2003 R2.

1. Download the installation modules for NEC ESMPRO Manager for Windows OS.
2. Execute "SM<version>\_E\ESMMENU\SETUP.EXE" after decompressing the downloaded ZIP file.
3. Select "NEC ESMPRO Manager" from the main menu within setup.

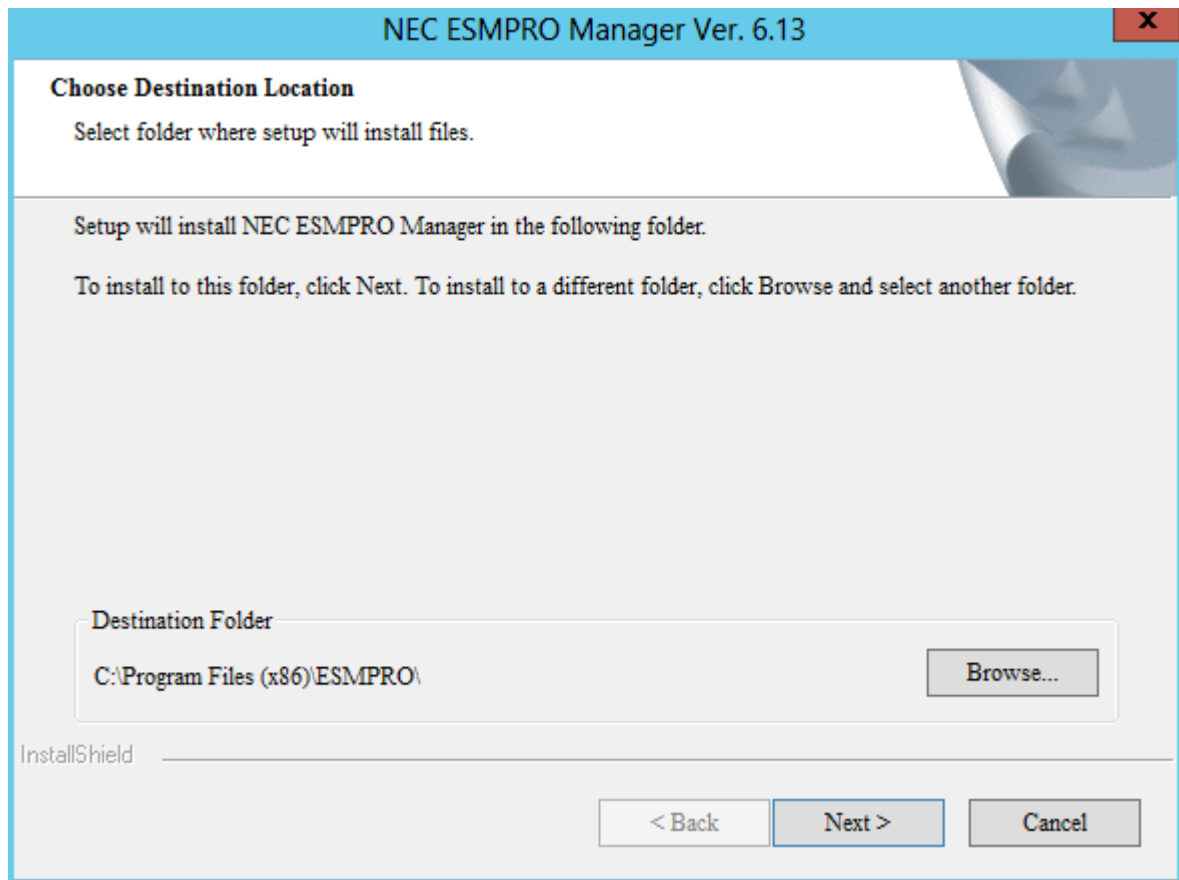


Decompressing the setup program may not be performed properly if the folder hierarchy is too deep.



If you double-click the menu, two identical dialog boxes appear. Click "End" to close one of the dialog boxes.

4. Perform the installation settings according to the Installer.
5. Specify target folder to install.



6. On the input screen of administrator name and password, specify the account information used for logging in the Web Console of NEC ESMPRO Manager.

NEC ESMPRO Manager Ver. 6.13

×

**Input of the administrator name and password**

Please enter the administrator name and password.

Administrator name

Password

Password(check)

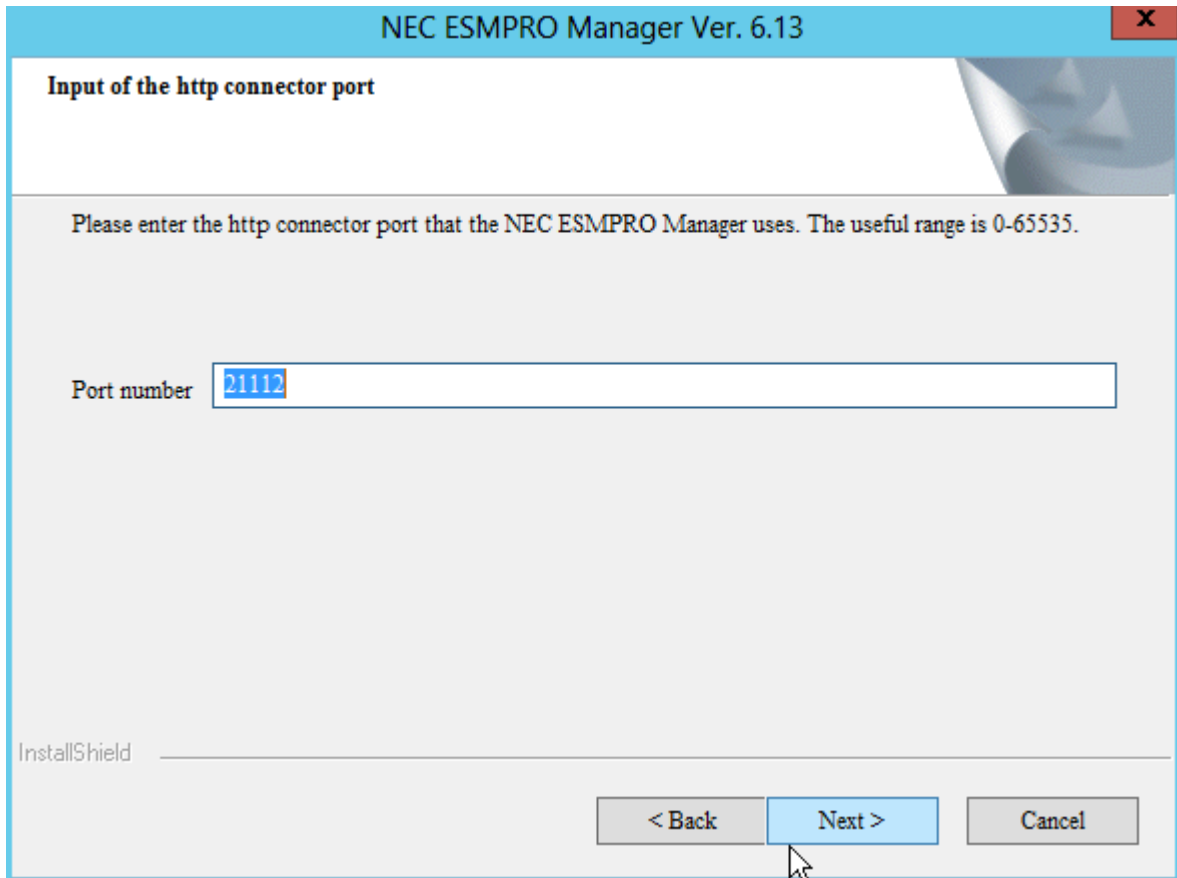
InstallShield

< Back

Next >

Cancel

7. Specify the port number used for Web Console of the NEC ESMPRO Manager.  
"21112" is set by default, but change it if used by other software.



NEC ESMPRO Manager Ver. 6.13

**Input of the http connector port**

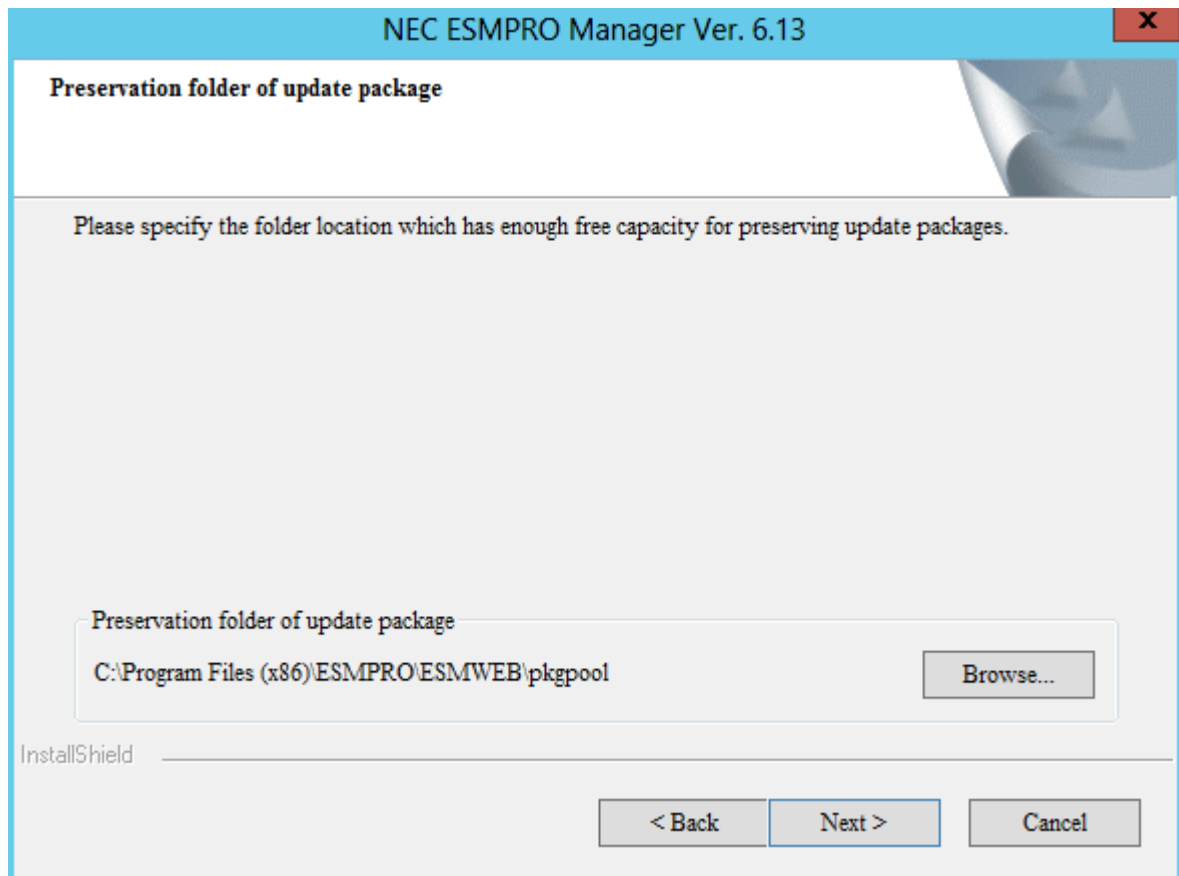
Please enter the http connector port that the NEC ESMPRO Manager uses. The useful range is 0-65535.

Port number

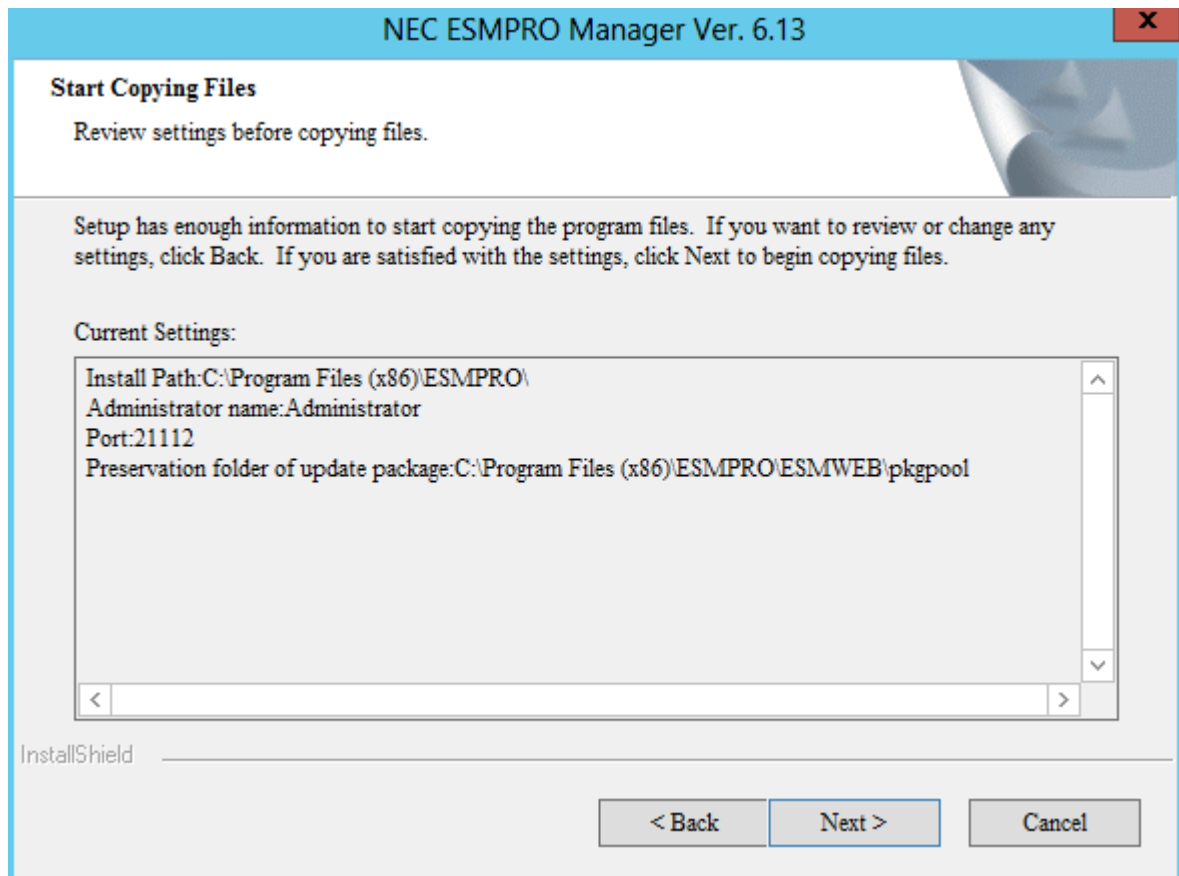
InstallShield

< Back Next > Cancel

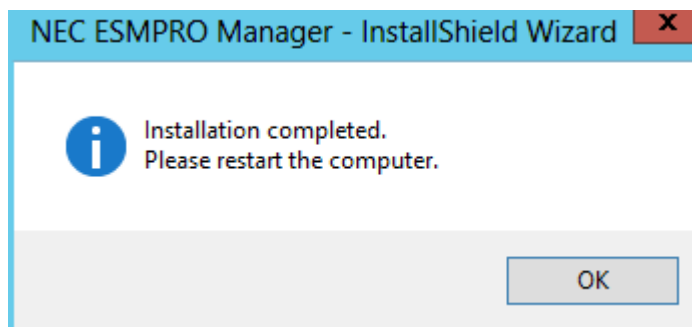
8. Select the directory for storing the update package downloaded by the NEC ExpressUpdate function.  
Specify the location where the sufficient disk capacity is left, as the saving may require a large capacity.



9. Confirm the installation settings.



10. Restart the OS after completing the installation.



### 3.3.2 Logging in to the Web Console of the NEC ESMPro Manager

The Web Console of the NEC ESMPro Manager has the access control by default and can be accessed only from the installed server. Log in to the Web Console with the user name and password specified at the time of the installation by clicking the ESMPro icon created on the desktop, or entering the following URL in the address bar on the browser.

`http://localhost:21112/esmpro`

- \* Replace the port number with the one specified at the time of the installation.
- \* HTTP is set by default, but the communication using the HTTPS is also available.  
Refer to *NEC ESMPro Manager Ver.5.7 Installation Guide* for how to set up.
- \* Reference to the "Online Help" is available from "Help" on the upper right of the screen after logging in.

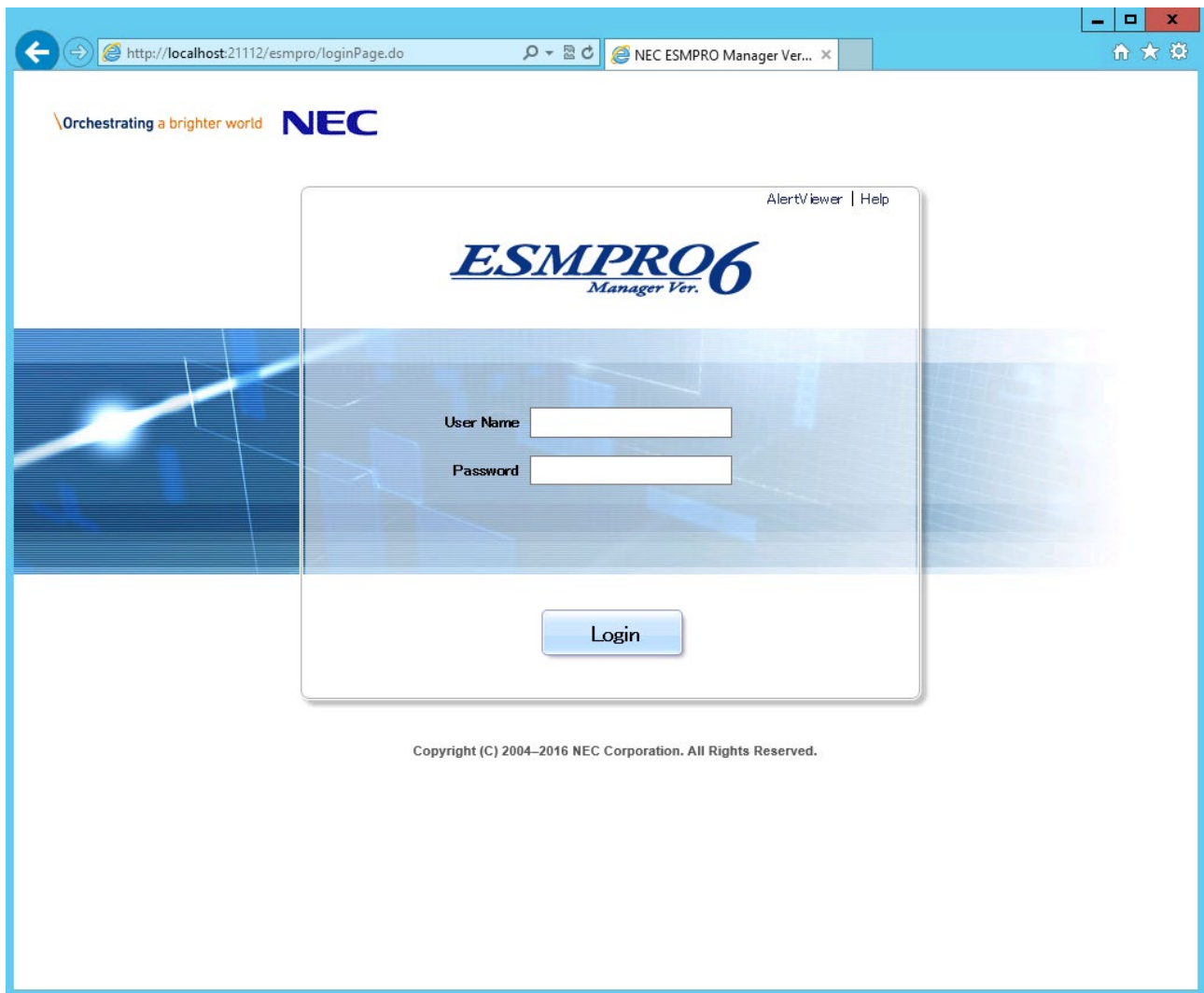
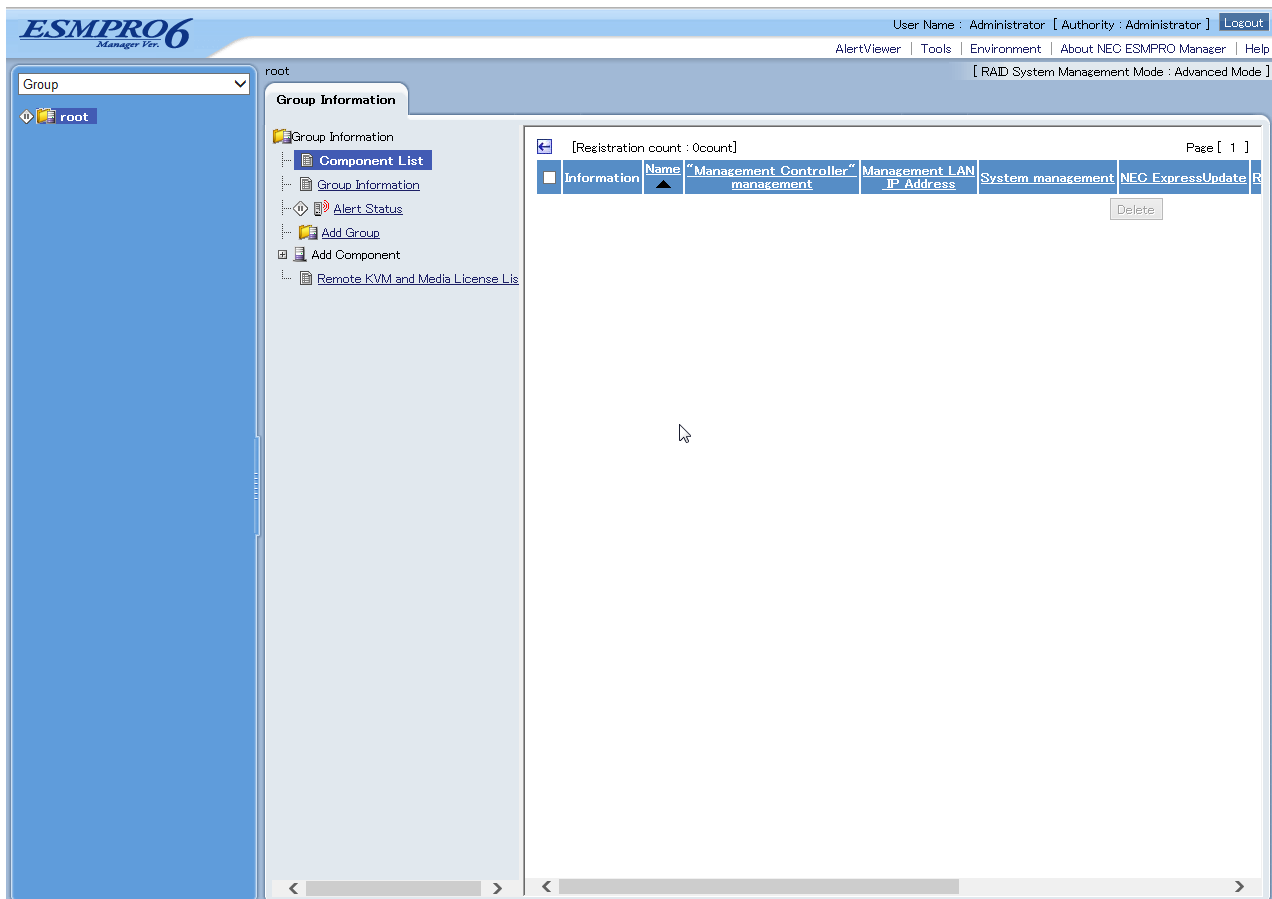


Figure 2 Login screen





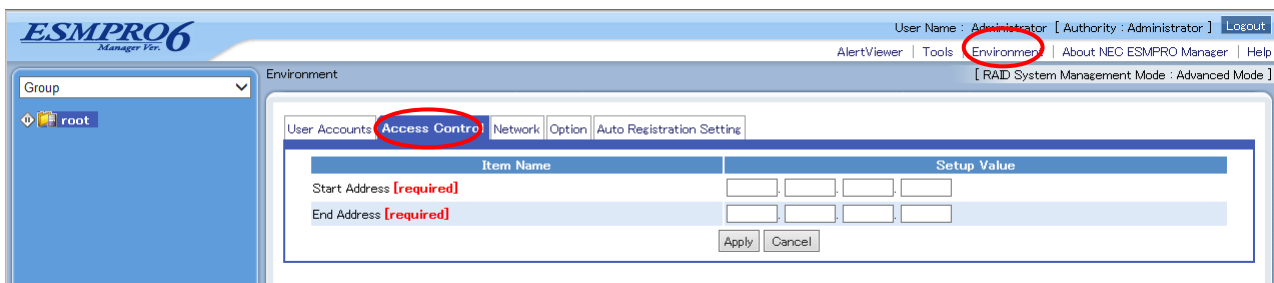
**Figure 3 Screen after logging in**

Refer to Chapter 4.1 for the Web Console screen of the NEC ESM PRO Manager.

### 3.3.3 Access Control

As explained in 3.3.2, the access control is set by default such that the only the server on which NEC ESM PRO Manager is installed can access to the Web Console of the NEC ESM PRO Manager.

After clicking “Environment” → “Access Control” → “Add Address”, the accesses from other servers’ browsers on the Network will be available by configuring the IP address which allows the communication.



**Figure 4 Access control setting screen**

### 3.3.4 User Account Management

It specifies the user account of the NEC ESM PRO Manager. Clicking “Environment” → “User Accounts” → “Users” displays the list of users set on the NEC ESM PRO Manager.

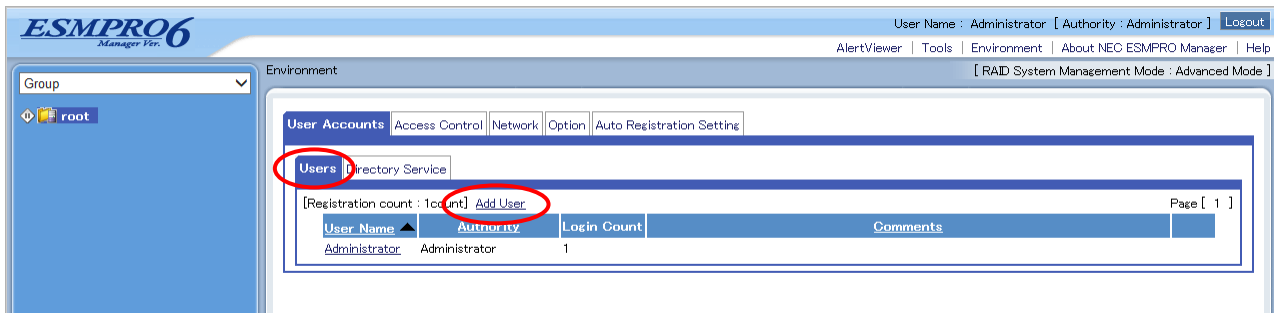


Figure 5 User list display

Users other than “Administrator” which is set by default at installation can be added, by selecting “Add Users”. When adding the user, the user right for each feature of the NEC ESMPro6 Manager can be defined in details. The method of using the Directory Service (LDAP or Active Directory) is explained in the next section.

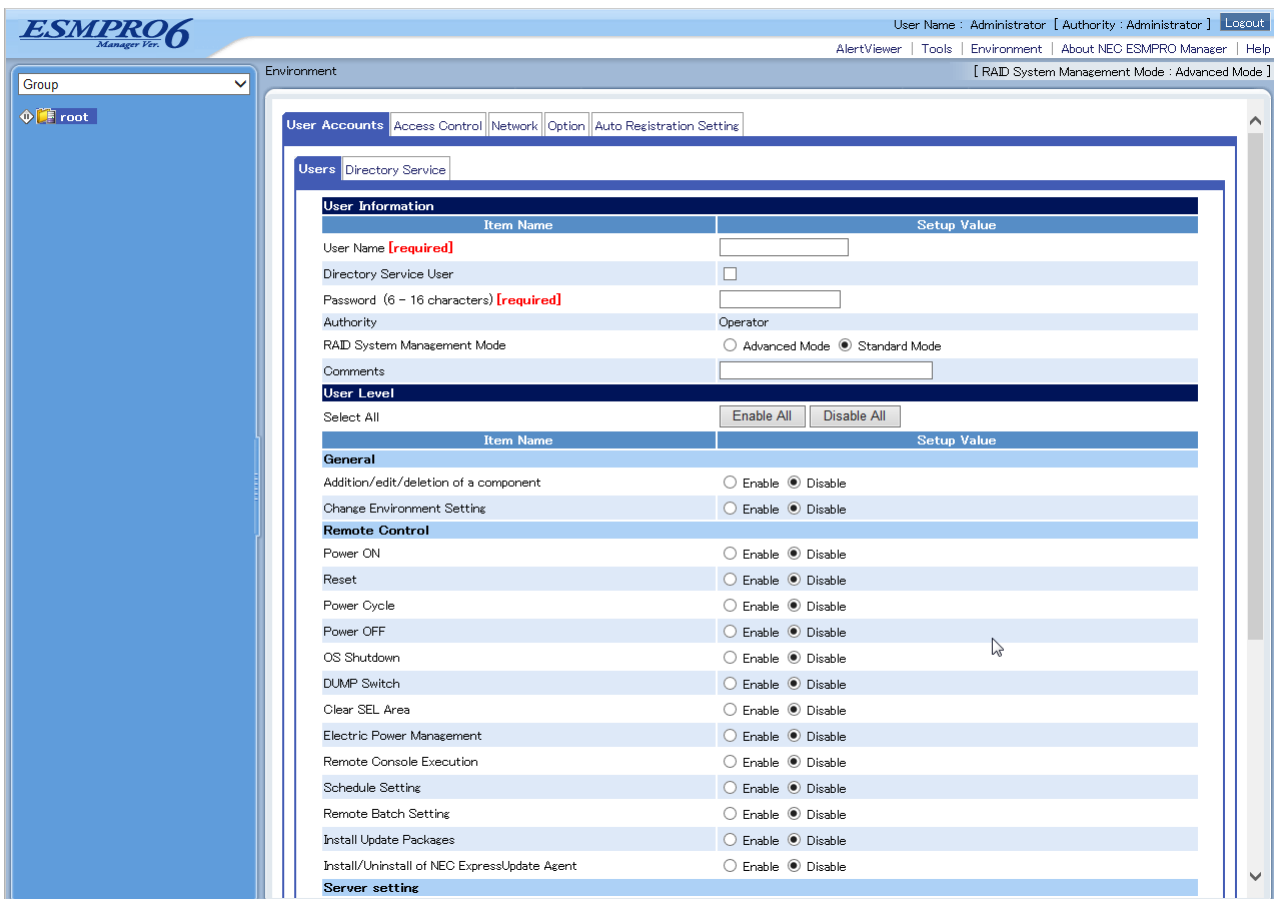


Figure 6 Add user

### 3.3.5 User Account Management (Using Directory Service)

Logging in by using Directory Service is available on the NEC ESMPRO Manager. Go to “Environment” → “User Account” → “Directory Service” and select the Directory Service (LDAP or Active Directory) and perform the necessary setting.

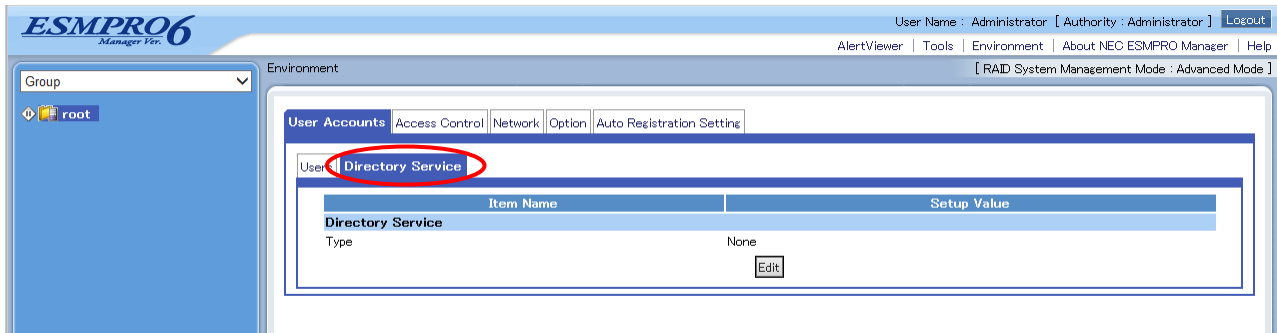


Figure 7 Directory Service setting

1. Set up the Directory Service on the NEC ESMPRO Manager.
2. Add the user who logs in by using the Directory Service from “Environment” → “User Accounts” → “Users” → “Add User”.  
In this case, the check box of the “Directory Service User” needs to be checked on.
3. Log out for once and try logging in as a Directory Service User.

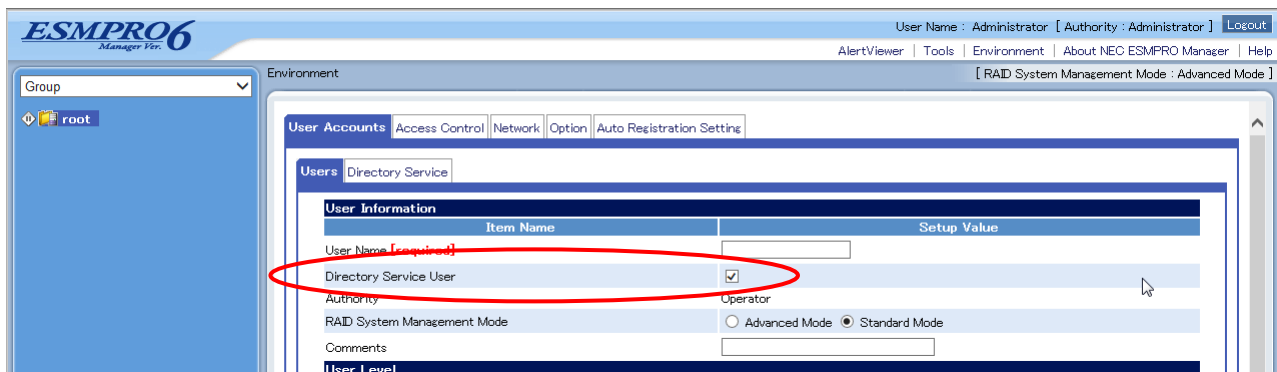


Figure 8 Add the user who uses Directory Service

When using “SSL-TLS” with binding algorithm of the Directory Service, a server certificate needs to be registered with JRE which the NEC ESMPRO Manager uses. For how to register, refer to *NEC ESMPRO Manager Ver.5.7 Installation Guide*.

### 3.3.6 Network Setting, Option Setting

Detailed settings for managing the management target serves on the NEC ESMPRO Manager are described below. The initial settings should be kept for normal operation.

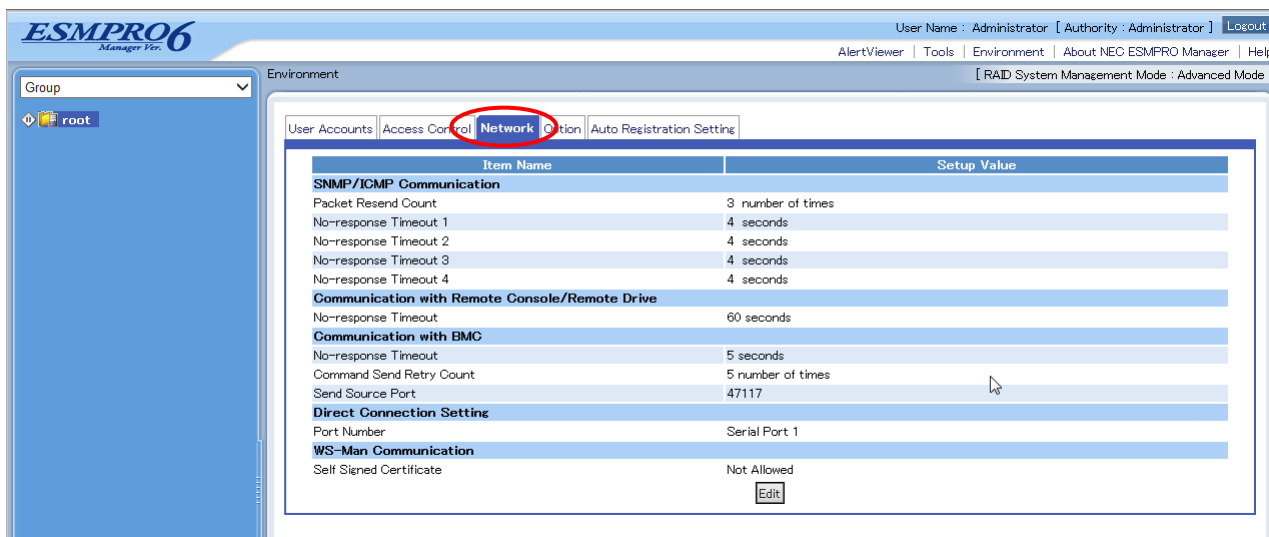


Figure 9 Network setting

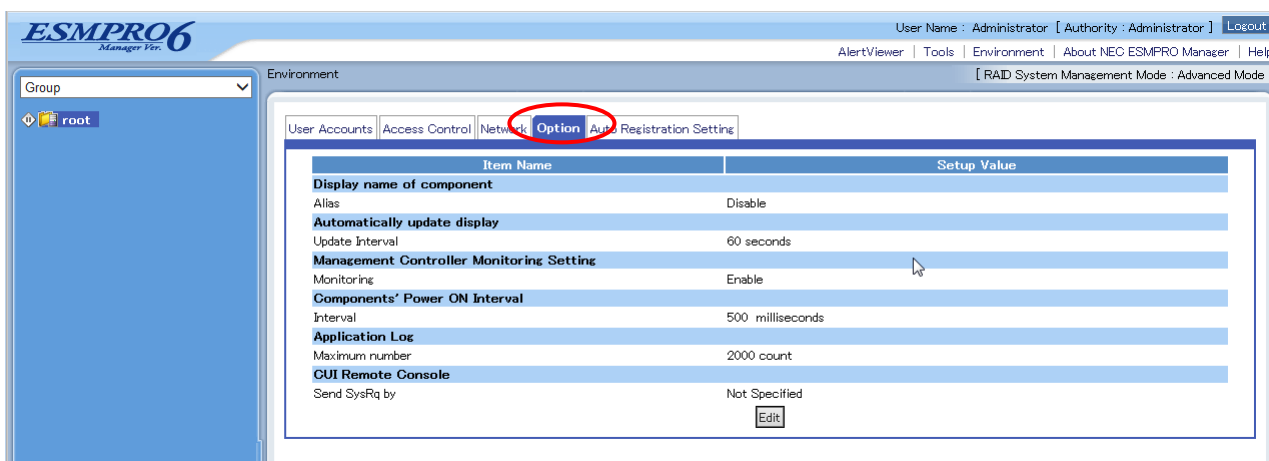


Figure 10 Option setting

## 3.4 NEC ESMPRO Agent, NEC ESMPRO ServerAgent Service

### Installation and Settings

This section describes the installation and initial settings of the NEC ESMPRO Agent or NEC ESMPRO ServerAgentService is required when using the reporting functions and system management functions.

#### 3.4.1 NEC ESMPRO Agent, NEC ESMPRO ServerAgentService Installation and Initial Settings

Modules to be installed on the NEC ESMPRO Agent, NEC ESMPRO ServerAgentService vary depending on the management target OS.

**Table 7 NEC ESMPRO Agent**

Monitoring Item	Module Storage Location	Web Release of the Latest Module
Windows	EXPRESSBUILDER	Released
Linux	EXPRESSBUILDER	Released
VMware( till ESX 4)	To be purchased	Released
VMware(ESXi 5 or later)	NA	NA
Virtual Machine	To be purchased	NA
Machines by other companies	To be purchased	NA

**Table 8 NEC ESMPRO ServerAgentService**

Monitoring Item	Module Storage Location	Web Release of the Latest Module
Windows	EXPRESSBUILDER	Released
Linux	EXPRESSBUILDER	Released
VMware( till ESX 4)	NA(Use NEC ESMPRO Agent)	NA
VMware(ESXi 5 or later)	NA	NA
Virtual Machine	NA(Use NEC ESMPRO Agent)	NA
Machines by other companies	NA(Use NEC ESMPRO Agent)	NA

When using Windows and Linux for NEC Express5800 series or NX7700x series, install the NEC ESMPRO Agent or NEC ESMPRO ServerAgentService from the NEC EXPRESSBUILDER attached to the server.

When using VMware ESX 4, be sure to purchase the NEC ESMPRO Agent for VMware separately.

VMware ESXi 5 does not have the service console capacity. So, the NEC ESMPRO Agent for VMware cannot be installed. Consequently, the monitoring must be performed directly from the NEC ESMPRO Manager.

When installing it on the virtual machine, purchase the NEC ESMPRO Agent for the Guest OS (Windows/Linux) separately. When installing it on the machine by other companies, purchase separately the NEC ESMPRO Agent (Windows/Linux) of the version supporting the applicable machine.



For the NEC Express5800 series or NX7700x series of the pre-install model, no installation is required as the installation should be completed at the time of factory shipment.



For downloading the update packages of NEC ESMPRO Agent for Windows, refer to the following URL for search by clicking on "ESMPRO".

<http://www.58support.nec.co.jp/global/download/>

Refer to the installation guides for how to install and perform the initial settings.

## 3.5 Installing the NEC ExpressUpdate Agent

How to install the NEC ExpressUpdate Agent required for using the NEC ExpressUpdate functions is described below. No setting items are specified for this software.

### 3.5.1 Installing the NEC ExpressUpdate Agent

NEC ExpressUpdate Agent is stored in the NEC EXPRESSBUILDER attached to the NEC Express5800 series. The latest version can be downloaded from the NEC Corporate Website.

(<http://www.58support.nec.co.jp/global/download/>).

Refer to the *NEC ExpressUpdate Agent Installation Guide* for how to install the NEC ExpressUpdate Agent. Remote batch installation from the NEC ESMPRO Manager is also available depending on the OS of the management target server. Refer to Chapter 7 for details.

## 3.6 Installing and Setting up the NEC Universal RAID Utility

Installation of the NEC Universal RAID Utility required for using the RAID management function is described below.

### 3.6.1 Installing and Setting up NEC Universal RAID Utility

If the OS of the management target server is either of Windows, Linux or VMware ESX, install the NEC Universal RAID Utility on the management target server.

NEC Universal RAID Utility is stored in the NEC EXPRESSBUILDER attached to the NEC Express5800 series. The latest version can be downloaded from the server information page on the NEC Corporate Website.

Refer to *Universal RAID Utility User's Guide Ver. 3.1* for how to install and set up. If the NEC ExpressUpdate Agent is installed on the management target server, remote batch installation from the NEC ESMPRO Manager is available. Refer to Chapter 7 or the White Paper "*ExpressUpdate Function and Features*" for details.

## 3.7 Installing and Setting up the LSI SMI-S Provider

Installation of the LSI SMI-S Provider required for using the RAID management functions is described below.

### 3.7.1 Installing and Setting up the LSI SMI-S Provider

If the OS of the management target server is VMware ESXi 5, install LSI SMI-S Provider on the management target server. LSI SMI-S Provider should be installed at the time of factory shipment if it is the pre-install model. The latest version of the LSI SMI-S Provider can be downloaded from the device information page on the NEC Corporate Website.

## 3.8 Setting up the EXPRESSSCOPE Engine 3

This section describes the EXPRESSSCOPE Engine 3 setting required for using the reporting function configuration management function and power management function via EXPRESSSCOPE Engine 3. In order to manage the EXPRESSSCOPE Engine 3 from the NEC ESMPRO Manager, the setup on the EXPRESSSCOPE Engine 3 is required.

Network setting of the EXPRESSSCOPE Engine 3 is required before performing the setup described below.

Setting change can be performed from the EXPRESSSCOPE Engine Web console or Server Configuration Utility. Refer to *EXPRESSSCOPE Engine 3 User's Guide*, *Server Configuration Utility User's Guide* or each Online

Help for the details about the setting method.

### 3.8.1 Setting up from the Web console of the EXPRESSSCOPE Engine 3

When setting up from the Web console of the EXPRESSSCOPE Engine 3, go to "Configuration" → "BMC" → "Miscellaneous" → "Management Software" and select "Enable" of the "ESMPRO Management". The information entered in "Authentication Key" field is required for the registration of the NEC EXPRESSSCOPE Engine 3 on the NEC ESMPRO Manager.

"Redirection (LAN)" should be set to "Enable" when using the remote console function of the NEC ESMPRO Manager. Refer to "9.3 Remote Console" for details.

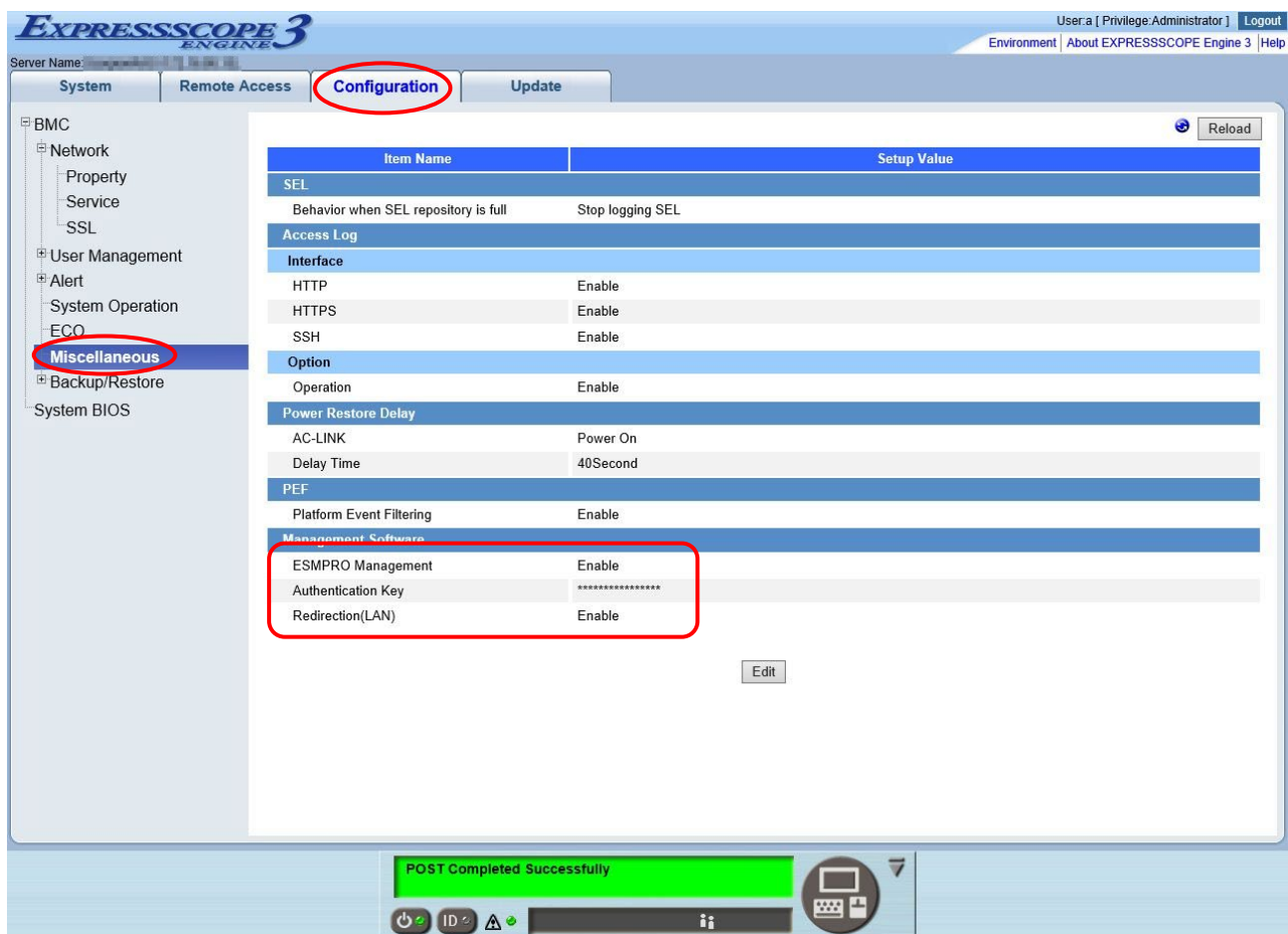


Figure 11 EXPRESSSCOPE Engine 3 Web console



### 3.8.2 Setting up from Server Configuration Utility (Online version)

Installing the Server Configuration Utility on the OS of the management target server allows you to change the setting of the EXPRESSSCOPE Engine 3. Start up the Server Configuration and go to “EXPRESSSCOPE Engine 3” → “Miscellaneous” → “Management Software” and select “Enable” of the “ESMPRO Management”. The information entered in “Authentication Key” field is required for the registration of the NEC EXPRESSSCOPE Engine 3 on the NEC ESMPRO Manager.



Server Configuration Utility is a successor software of BMC Configuration Tool.

“Redirection (LAN)” should be set to enable when using the remote console function of the NEC ESMPRO Manager. Refer to “9.3 Remote Console for details.

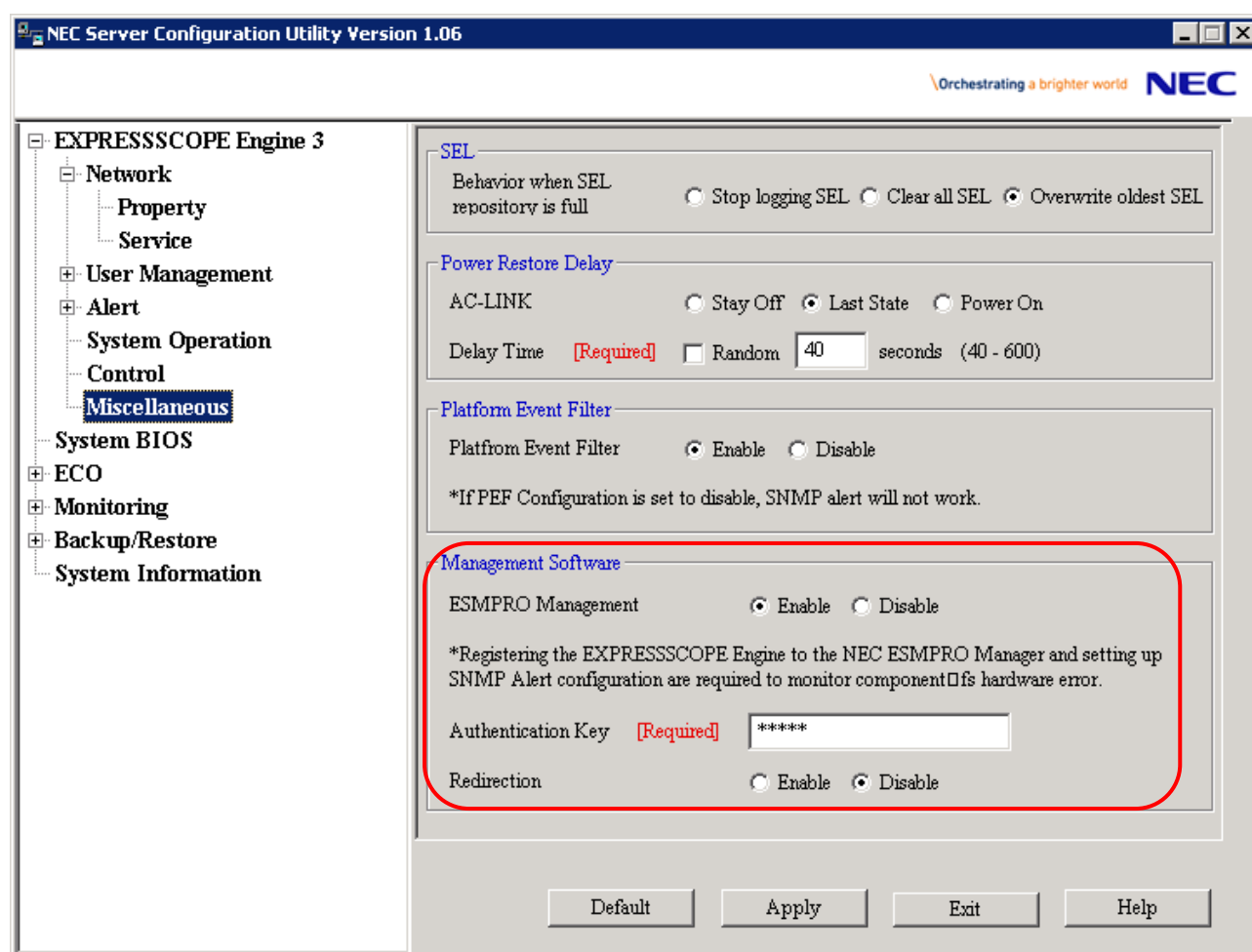


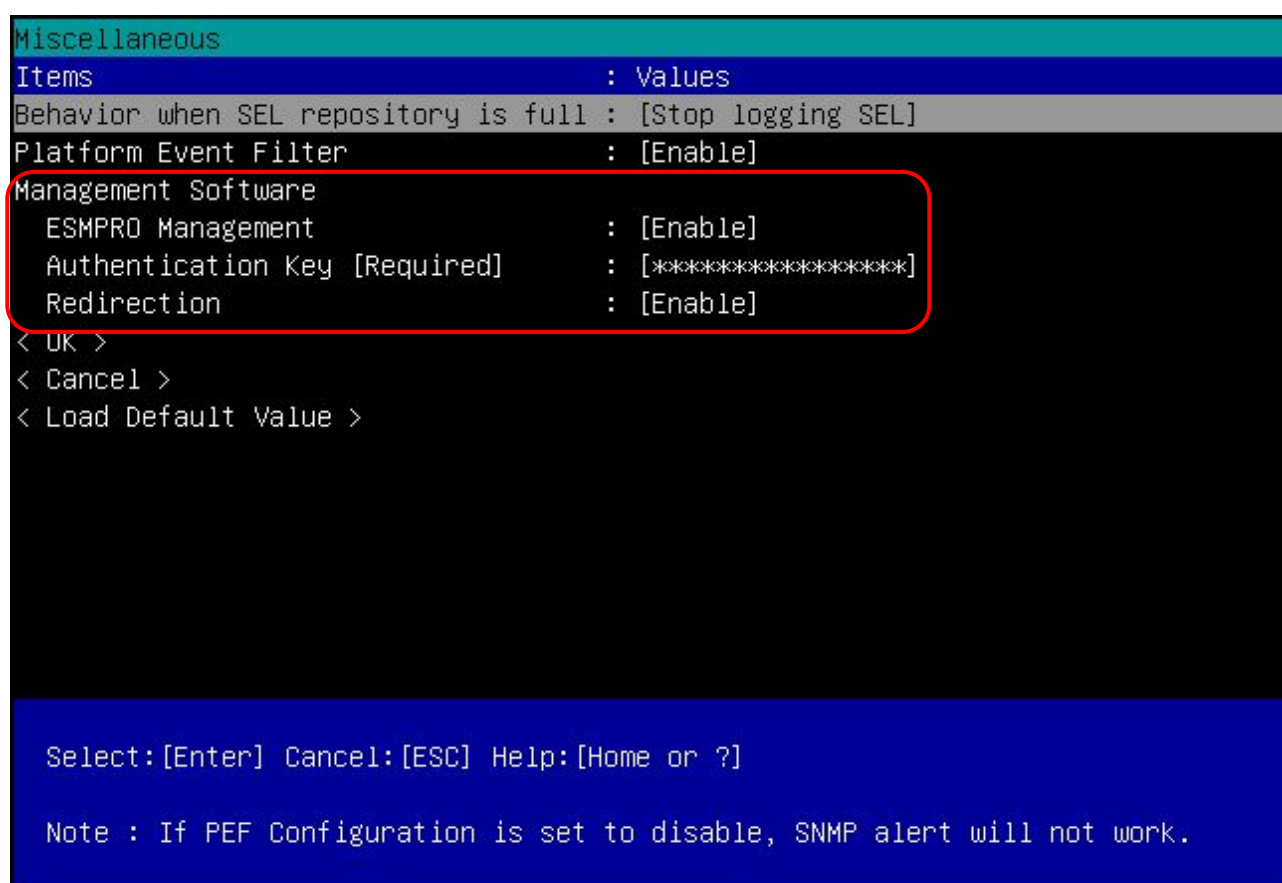
Figure 12 Server Configuration Utility (Online version)

### 3.8.3 Setting up from Server Configuration Utility (Offline version)

By pressing “F4” key while the NEC logo is displayed (POST) on the screen after turning on the power of the server, you can start up the BMC Configuration Tool.

“Keyboard type selection” → “Server Configuration Utility” → “EXPRESSSCOPE Engine 3” → “Miscellaneous” → “Management Software” and select “Enable” of the “ESMPRO Management”. The information entered in “Authentication Key” field is required for the registration of the NEC EXPRESSSCOPE Engine 3 on the NEC ESMPRO Manager.

“Redirection (LAN)” should be set to enable when using the remote console function of the NEC ESMPRO Manager. Refer to “9.3 Remote Consolefor details.



**Figure 13 Server Configuration Utility (Offline version)**

## Chapter 4 Server Management

Preparation for registering the management target servers to the NEC ESM PRO Manager should be done by the operations up to the previous chapter. This chapter describes the method of registering the management target server on the NEC ESM PRO Manager.

### 4.1 About NEC ESM PRO Manager Web Console

Web Console of the NEC ESM PRO Manager consists of the following four areas.

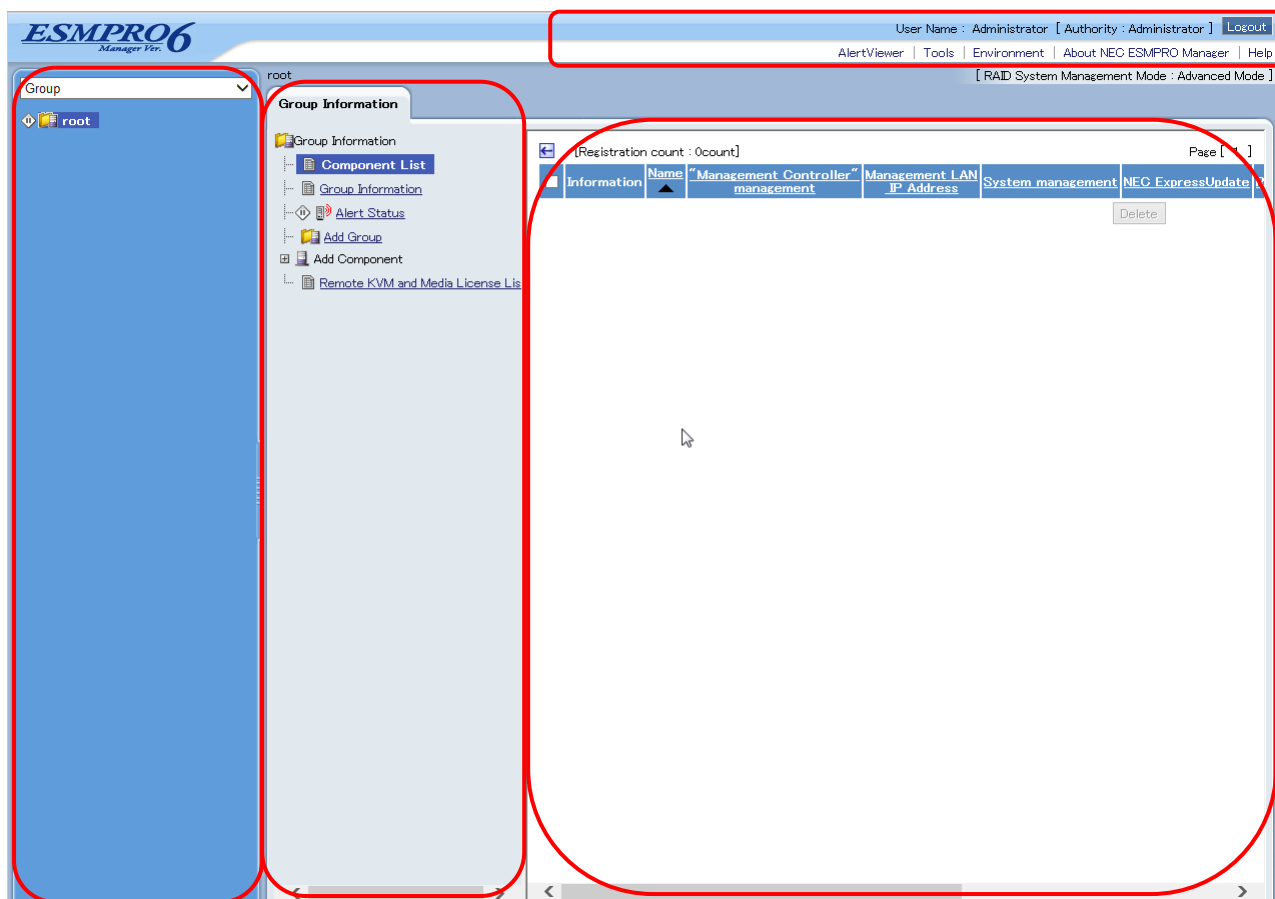


Figure 14 NEC ESM PRO Manager Web Console



Web Console of the NEC ESM PRO Manager logs out automatically if left for more than 30 minutes without being operated.



Update interval of the screen can be changed from “Environment” → “Option” → “Automatically update display” on the “Header Menu”.

### 4.1.1 Header Menu (1)

This is the menu for the functions that can be operated at any time. Startup of the AlertViewer or displaying and saving the logs of the NEC ESMPRO Manager and logging out of the NEC ESMPRO Manager can be performed.

**Table 9 Header Menu**

Menu Hierarchy1	Menu Hierarchy1	Descriptions
AlertViewer	—	It displays the alert received from the NEC ESMPRO Agent or the EXPRESSSCOPE Engine 3.
Tool	IPMI Information Backup File List	When backing up the IPMI information, the list of the backup files is displayed. Registering or deleting the file is also available.
	Searching Registered Components	It searches for the management target servers registered to the NEC ESMPRO Manager.
	Linkage Service	It is the screen concerning the liaison with PXE Service.
	NEC ExpressUpdate Management Information	It displays the related information or configures the options of the NEC ExpressUpdate. Refer to Chapter 7 for details.
Environment	User Accounts	It manages the users of the NEC ESMPRO Manager.
	Access Control	It configures the access control to the Web Console of the NEC ESMPRO Manager.
	Network	It configures the details required when managing the servers.
	Option	It configures the option of the NEC ESMPRO Manager.
About NEC ESMPRO Manager	—	It shows the version information of the NEC ESMPRO Manager and the logs can be displayed and downloaded.
Help	—	It shows the Online Help information of the NEC ESMPRO Manager.

### 4.1.2 Tree View (2)

It displays the management target servers managed by the NEC ESMPRO Manager in hierarchical view. Select the tree format from the pull-down menu of “Group”, “Chassis” and “Power group”. Editing the edit group can be performed from the “Edit group set”. Refer to 4.2 for details.

### 4.1.3 Local Navigation (3)

Information is displayed when a group or the management target server is selected. It shows a group/management target server information. It can also show the operations that can be executed to the group/management target server. It depends on the registration status of the management target server, but it shows generally the four tabs of “Constitution” “Setting” “Remote Control” and “Schedule”.

**Table 10 Local navigation when selecting the management target server**

Tab Name	Description
Constitution	It displays the constitutional information if the registration status is the management target server managing the NEC ESMPRO Agent, NEC ESMPRO ServeAgentService or the EXPRESSSCOPE Engine 3. Refer to Chapter 6.
Setting	Connection setting of the management target server, power supply option, the EXPRESSSCOPE Engine 3 setting and the SEL clear setting can be changed. Refer to 10.4.4 for details.
Remote Control	Power control, power management, remote console display, display and save of the IPMI information, login to the Web Console of the EXPRESSSCOPE Engine series can be executed from this tab. Refer to Chapter 9 for details.
Schedule	It configures the scheduled running which performs the power control at a specified time, and the remote batch function which performs the NEC ESMPRO Manager functions at a specified time. Refer to Chapter 12 for details.

When “Group” is selected, the three tabs, “Group Information”, “Server Control” and “Schedule” are displayed.

**Table 11 Local navigation when selecting “Group”**

Tab Name	Description
Group Information	It displays the list of the management target servers existing in the selected group. Addition of the subgroup to the group, addition and deletion of the management target servers can be executed from this tab. Refer to 4.2 Group for details.
Server Control	Select this tab when performing the batch operation on the management target servers in a group. Power measurement, ECO setting, System BIOS setting, power option, remote power control for a group and the menu of the NEC ExpressUpdate are displayed.
Schedule	Same as when selecting the management target server.

### 4.1.4 Operation Area (4)

Information selected from the menu and local navigation is displayed.

## 4.2 Group

NEC ESMPRO Manager allows you to manage the management target servers by dividing them into groups. By creating a group, you can execute the batch operation to the servers in a group. From the pull-down menu on the top right of the tree view, you can switch the group to be displayed.

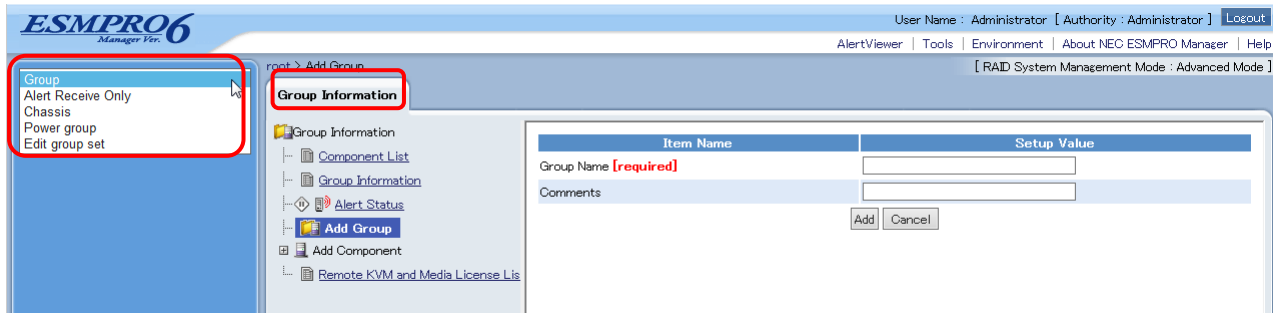


Figure 15 Switching the groups

### 4.2.1 Group

This is a group to manage the server. This menu is set by default after logging in to the NEC ESMPRO Manager. The structure of this group can be changed from the "Group Information".

- Adding a group  
Select the group to be added on the Tree View and select "Group Information" → "Add Group".
- Deleting a group  
On the Tree View, select the group to which the group to be deleted belongs and select "Group Information" → "Component List". Press "Delete" displayed on the right corner of the Operation Area.

### 4.2.2 Chassis

When managing the blade servers, etc. selecting this menu shows the information about each chassis.

### 4.2.3 Power Group

This is a dedicated group to use the group power control function. Edit the group by referring to 4.2.4 Edit group set. Refer to Chapter 11 for details.

### 4.2.4 Edit Group Set

This is the menu to edit the group structure. As of 2013, the edit operation of the power group is available. Refer to Chapter 11 for details.

## 4.3 Registering a Server

There are two methods of registering a management target server to the NEC ESMFRO Manager; the auto registration and manual registration.



One management target server can be managed by up to three NEC ESMFRO Managers. Note the following items.

- Be sure to use one NEC ESMFRO Manager for managing the management controller function.
- Be sure to use one NEC ESMFRO Manager for managing the RAID system function and the NEC ExpressUpdate function. When registering the same management target server to the multiple NEC ESMFRO Managers, specify the status of the RAID system function and the NEC ExpressUpdate function of the management target servers as “Not Registered”.
- Be sure to use one NEC ESMFRO Manager for managing the multiple EM cards and the blade servers on the same chassis.

### 4.3.1 Auto Registration

This is the method of automatically registering the management target servers identified after specifying the IP address range or the network address. Select “Group” from the pull-down menu of the tree view and select “Group Information” → “Add Component” → “Auto Registration”.

The screenshot displays the NEC ESMFRO Manager web interface. The top navigation bar shows the user is logged in as 'Administrator' with 'Authority: Administrator'. The breadcrumb trail indicates the path: 'root > Add Component > Auto Registration'. The left sidebar contains a tree view with the following structure:

- Group (selected)
  - root
    - Group Information (selected)
    - Component List
    - Group Information
    - Alert Status
    - Add Group
    - Add Component
      - Auto Registration (selected)
      - Manual Registration
      - Remote KVM and Media License List

The main content area is titled 'Group Information' and contains the following configuration sections:

Item Name	Setup Value
Destination Group	root
<b>Discovery Range</b>	
Discovery Mode	<input checked="" type="radio"/> IP Address Range Discovery <input type="radio"/> Network Address Discovery
Start Address [required]	<input type="text"/>
End Address [required]	<input type="text"/>
<b>SNMP (NEC ESMFRO Agent)</b>	
Discovery	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SNMP Community Name [required]	public
<b>WS-Man</b>	
Discovery	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
User Name/Password [required]	<input type="text"/> / <input type="text"/> <input type="button" value="Add"/>
<b>RAID system (Universal RAID Utility)</b>	
Discovery	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>NEC ExpressUpdate (ExpressUpdate Agent)</b>	
Discovery	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>BMC (EXPRESSSCOPE Engine)</b>	
Discovery	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Features NEC ExpressUpdate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Authentication Key [required]	<input type="text"/> <input type="button" value="Add"/>
<b>Intel(R) vPro(TM) Technology</b>	
Discovery	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
User Name/Password [required]	<input type="text"/> / <input type="text"/> <input type="button" value="Add"/>

At the bottom of the configuration panel, there is a  button.

Figure 16 Auto registration screen



**Table 12 Auto registration**

Item Name	Description
Registration Group	<ul style="list-style-type: none"> <li>• Select the group to which the management target server found by search should belong.</li> </ul>
Search Mode	<ul style="list-style-type: none"> <li>• Select either the search by the network address or by specifying the IP address range.</li> </ul>
SNMP(NEC ESMPRO Agent)	<ul style="list-style-type: none"> <li>• Set to “Enable” when managing and monitoring by using the NEC ESMPRO Agent. The community name specified by the SNMP setting on the OS is required.</li> <li>• Set to “Enable” when managing VMware ESXi 5.</li> </ul>
WS-Man	<ul style="list-style-type: none"> <li>• Set to “Enable” when managing and monitoring by using the NEC ESMPRO ServerAgentService. Enter the user/password of the Administrator of the target OS.</li> </ul>
RAID system management	<ul style="list-style-type: none"> <li>• Set to “Enable” when conducting the RAID management by using the Universal RAID Utility.</li> <li>• Set to “Enable” when conducting the RAID management using the LSI SMI-S Provider.</li> </ul>
NEC ExpressUpdate	<ul style="list-style-type: none"> <li>• Set to “Enable” when executing the NEC ExpressUpdate function through the NEC ExpressUpdate Agent. Refer to Chapter 7 for the details about the NEC ExpressUpdate.</li> </ul>
BMC(EXPRESSSCOPE Engine)	<ul style="list-style-type: none"> <li>• Set “Search” to “Enable” when managing and monitoring by using the NEC EXPRESSSCOPE Engine 3.</li> <li>• Set “NEC ExpressUpdate” to “Enable” when using the NEC ExpressUpdate function through NEC EXPRESSSCOPE Engine 3. Refer to Chapter 7 for the details about the NEC ExpressUpdate.</li> <li>• For the authentication key, enter the same information as the one in 3.8.</li> </ul>
Intel® vPro™ Technology	<ul style="list-style-type: none"> <li>• Set “Search” to “Enable” when managing and monitoring by using Intel® vPRO™ Technology.</li> </ul>

### 4.3.2 Manual Registration

Full Management: This is the method of manually registering all the items including the component name, the OS IP address and the IP address of the EXPRESSSCOPE Engine 3, etc. Each item should be configured as needed.

Item Name	Setup Value
Component Name <b>[required]</b>	<input type="text"/>
Alias	<input type="text"/>
Group	root
Connection Type	<input checked="" type="radio"/> LAN <input type="radio"/> Direct <input type="radio"/> Modem
<b>Common Setting</b>	
OS IP Address <b>[required]</b>	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
<b>SNMP (NEC ESM PRO Agent)/ WS-Man</b>	
Management	<input checked="" type="radio"/> Registration <input type="radio"/> Unregistration
Management Type	<input checked="" type="radio"/> SNMP <input type="radio"/> WS-Man
SNMP Community Name(Get)	public
SNMP Community Name(Set)	<input type="text"/>
<b>RAID system management</b>	
Management	<input checked="" type="radio"/> Registration <input type="radio"/> Unregistration
<b>NEC ExpressUpdate</b>	
Updates via NEC ExpressUpdate Agent	<input checked="" type="radio"/> Registration <input type="radio"/> Unregistration
Updates via Management Controller	<input checked="" type="radio"/> Registration <input type="radio"/> Unregistration
<b>BMC (EXPRESSSCOPE Engine)/ vPro (Common)</b>	
Management	<input checked="" type="radio"/> Registration <input type="radio"/> Unregistration
Management Type	<input checked="" type="radio"/> BMC <input type="radio"/> vPro
Authentication Key <b>[required]</b>	<input type="text"/>
<b>BMC (EXPRESSSCOPE Engine)/ vPro (LAN)</b>	
Current IP Address	<input checked="" type="radio"/> IP Address 1 <input type="radio"/> IP Address 2
Failover	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP Address1 <b>[required]</b>	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>
IP Address2	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>

Figure 17 Manual registration screen

**Table 13 Setting items for manual registration**

Item Name	Description
Component Name	<ul style="list-style-type: none"> <li>Name for displaying the management target servers on the NEC ESMPRO Manager.</li> </ul>
Group	<ul style="list-style-type: none"> <li>Select the group to which the management target servers belong when registered.</li> </ul>
Connection Type	<ul style="list-style-type: none"> <li>Connection type setting between the NEC ESMPRO Manager and the management target servers. Select "LAN" when connecting through Ethernet.</li> </ul>
Common Setting OS IP Address	<ul style="list-style-type: none"> <li>Enter the OS IP address. When the system management, RAID system management and the update via NEC ExpressUpdate Agent are all disabled, this item will be automatically deleted.</li> </ul>
SNMP/WS-Man Management/Management Type/ SNMP Community Name(Get/Set)	<ul style="list-style-type: none"> <li>Set to "Enable" when managing and monitoring by using via SNMP or WS-Man. The community name specified by the SNMP setting on the OS is required if SNMP is selected.</li> <li>Set to "Enable" when managing VMware ESXi 5.</li> </ul>
RAID system management	<ul style="list-style-type: none"> <li>Set to "Enable" when conducting the RAID management by using the Universal RAID Utility.</li> <li>Set to "Enable" when conducting the RAID management by using the LSI SMI-S Provider.</li> </ul>
NEC ExpressUpdate	<ul style="list-style-type: none"> <li>Set "Update via NEC ExpressUpdate Agent" to "Enable" when executing the NEC ExpressUpdate function via NEC ExpressUpdate Agent.</li> <li>When executing via NEC EXPRESSSCOPE Engine 3, set "Update via Management Controller" to "Enable". Refer to Chapter 6 for the details about the NEC ExpressUpdate.</li> </ul>
BMC/vPro (Common)	<ul style="list-style-type: none"> <li>When managing and monitoring by using the NEC EXPRESSSCOPE Engine 3 or Intel® vPro™, select the management item from "BMC" or "vPro" and select "Registration".</li> <li>When selecting "BMC", enter the same authentication key as the one in 3.8.</li> <li>When selecting "vPro", the user name and password fields necessary for communication with vPro™ will appear.</li> </ul>
BMC/vPro (LAN)	<ul style="list-style-type: none"> <li>Enter the IP address of the NEC EXPRESSSCOPE Engine series or the IP address of the Intel vPro™.</li> <li>Enter two IP addresses in the case of the server on which two management controllers are installed, such as ft server.</li> </ul>

For manual registration, it is necessary to press "Connection Check" on the screen after registration. By this operation, the communication with each Agent or the NEC EXPRESSSCOPE Engine 3 installed on the registered management target servers can be checked. The setting also can be changed at any time from "Setting" → "Connection Setting" 10.1 Connection Setting.

[Install NEC ExpressUpdate Agent](#)  
[Return to Connection Setting](#)

Check Connection Execution Result		
Management	Detected	Detail
NEC ExpressUpdate	Not Detected	Not Detected. Using the NEC ExpressUpdate Agent NEC ExpressUpdate function cannot be used.
RAID system management	Not Detected	Not Detected. RAID system management cannot be used.
"Management Controller" management	Detected	"Management Controller" management can be used. Using the "Management Controller" management NEC ExpressUpdate function can be used.
System management	Detected	System management can be used.

**Figure 18 Connection check result screen**

**Table 14 Connection check result**

Item Name	Description
NEC ExpressUpdate	The check result on using the NEC ExpressUpdate function is displayed.
RAID system management	The check result on using the Universal RAID Utility function is displayed. Alternatively, when the LSI SMI-S Provider is installed, RAID system management function can be used.
"Management Controller" management	The check result on using the "Management Controller" management function is displayed. NEC EXPRESSSCOPE Engine 3 or vPro™ setting is required.
System management	The check result on using the system management function is displayed. System management function by using the NEC ESMPRO Agent installed on the management target servers is available.
Install NEC ExpressUpdate Agent	The link for installation appears when the installation of the NEC ExpressUpdate Agent on the management target servers is available.

From "Setting" → "Server Setting" → "Conneciton Setting" connection check is available at any time.  
The registration work of the management target servers to the NEC ESMPRO Manager is now complete.

## Chapter 5 Server Fault Detection and Notification

This chapter describes confirmation method and notification when a fault occurs on a server managed by the NEC ESMPRO Manager. The features described are only available on the Windows version of NEC ESMPRO Manager.

### 5.1 Referencing Server Fault Information (Web Console)

Icons that display the operating state and status of each server are shown in the managed server list screen and the tree view in the Web Console in NEC ESMPRO Manager. Checking those icons will enable you to immediately identify the server where a fault is occurring.

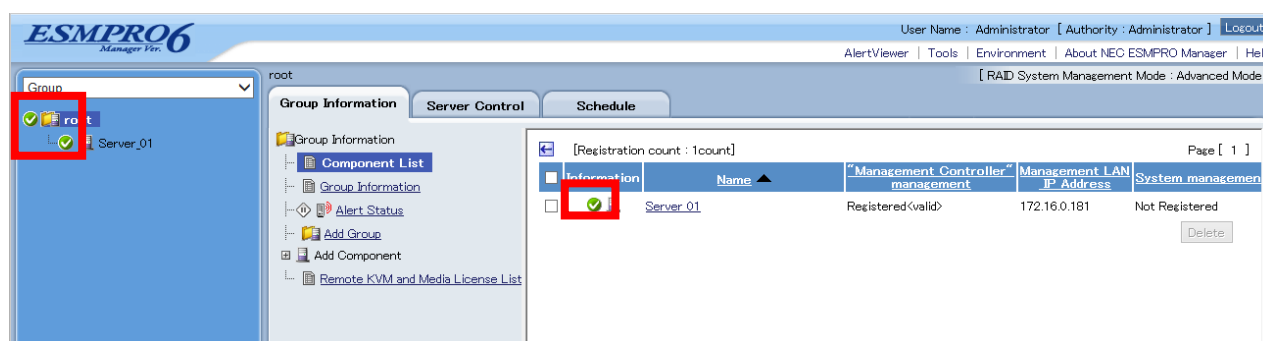









Figure 19 Managed Server List Screen in Web Console

The icons that are displayed for the state of each managed server have the following meanings.

Icon	State	Priority
	Unmonitored	Low ↓ High
	Currently Acquiring State	
	Normal	
	Unclear	
	DC-OFF, POST, OS Panic	
	Warning	
	Fault	

### 5.2 Referencing Server Fault Information (Alert Viewer)

Alerts sent to NEC ESMPRO Manager can be checked in Alert Viewer on a Web browser.

#### 5.2.1 Starting Alert Viewer

1. Log in to the NEC ESMPRO Manager Web Console and click on Alert Viewer.

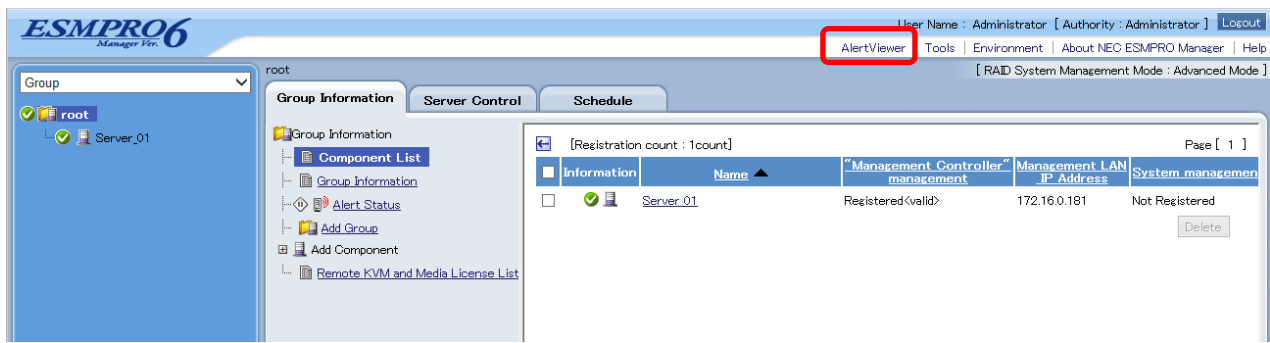
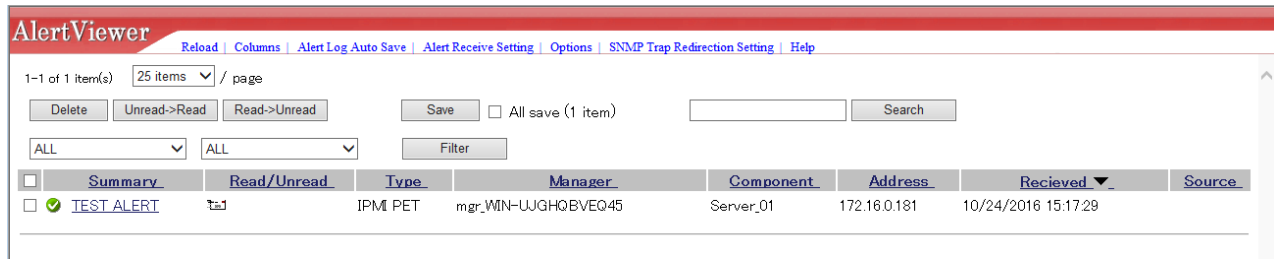


Figure 20 Web Console's Home Page

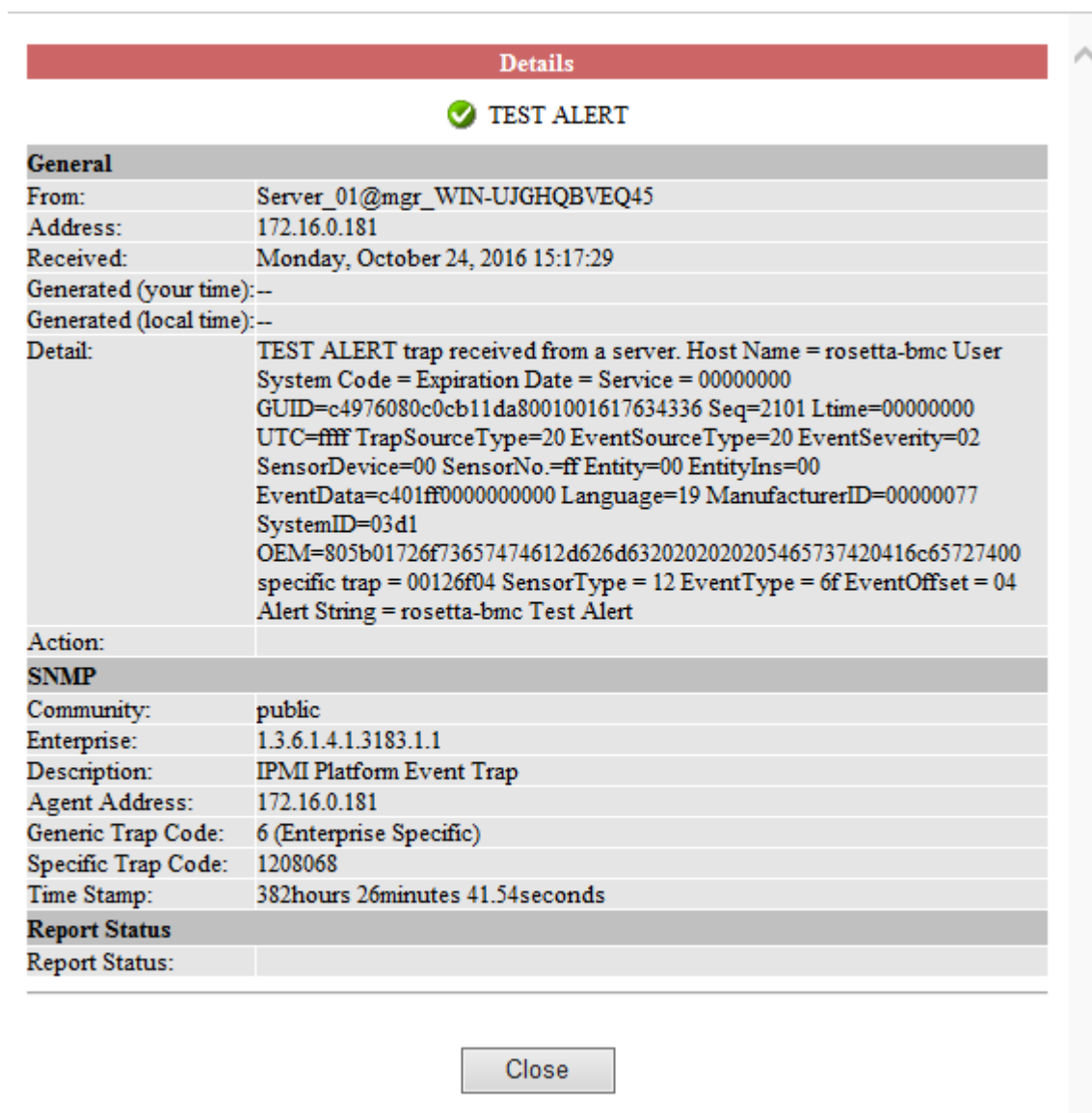
- Alert Viewer starts and a list of received alerts is displayed.



**Figure 21 Alert Viewer**

### 5.2.2 Referencing Detailed Information for an Alert

- Click "Overview" of the Alert for which you want to reference details.
- The Alert Details window will open, displaying detailed information for the alert.



**Figure 22 Alert Details Window**

### 5.2.3 Automatically Saving Received Alerts to a File

When you configure auto-save for the NEC ESMPRO Manager alert log, information for all received alerts will be saved to a file.



Since there is no limitation on the number of alerts that can be saved to the alert log, periodically back this file up and delete it, with consideration for your free disk space.



The save location of the relevant file cannot be changed. The default location is:  
<NEC ESMPRO Manager Installation Location>\ESMWEB\wbserver\webapps\esmpro  
\WEB-INF\service\alertlog

#### Configuring Auto-Save for the Alert Log

1. Log in to the NEC ESMPRO Manager Web Console and click on “Alert Viewer”.
2. Click “Alert Log Auto-Save Settings” from within “Alert Viewer”.

The image shows a web-based configuration window titled "Alert Log Auto Save". At the top, there is a checkbox labeled "Enable Alert Log Auto Save" which is checked. Below this, there are two tabs: "Destination" and "Output", with "Destination" currently selected. Under the "Destination" tab, there are two radio button options: "Use same file (ALLOG.txt or ALLOG.csv)." and "Create new file.", with the latter being selected. Below these, there is a section labeled "When" with four radio button options: "Daily" (selected), "Weekly", "Monthly", and "When file size reaches (1-999999999 MB)". Under the "When" section, there is a "File Size Options" section with two input fields: "File Size MB" containing the value "1" and "File Name" containing the value "ALEX". Below these fields is a checkbox labeled "Fix the current filename" which is unchecked. Further down, there is a label "Maximum number of files:" followed by an input field containing the value "10000". Below this, there is a label "Log file directory (Management computer) :" followed by a text area containing the path "C:\Program Files (x86)\ESMPRO\ESMWEB\wbserver\webapps\esmpro\WEB-INF\service\alertlog". At the bottom of the configuration area, there is a "Save as type" section with two radio button options: "TXT" and "CSV", with "CSV" being selected. At the very bottom of the window, there are two buttons: "OK" and "Cancel".

**Figure 23 Alert Log Auto-Save Settings Screen**

3. Check the “Perform alert log auto-saves” checkbox.
4. If you do not wish to overwrite the saved file, select “Do not overwrite the saved file”. To overwrite the saved file at the desired interval or file size, select “Overwrite the saved file”.
5. Select an extension (TXT or CSV) for the saved file.
6. Lastly, click the “OK” button.



See the NEC ESMPRO Manager Online Help for more information on the timing for the alert log's



auto-save overwrite feature, as well as each of the other items on the configuration screen.

## **5.3 Server Fault Notification (Linking with WebSAM AlertManager)**

The notification feature can be expanded by linking NEC ESMPRO Agent and NEC ESMPRO Manager with WebSAM AlertManager.

### **Expanding the Notification Feature of NEC ESMPRO Agent, NEC ESMPRO ServerAgentService**

The notification feature of NEC ESMPRO Agent and NEC ESMPRO ServerAgentService can be expanded to include the following new features: e-mailing of alert information, popup notifications to operators, output of alert information to printers and/or files, and the launching of specified applications when alerts occur.

### **Expanding the Notification Feature of NEC ESMPRO Manager**

Several of the Express Notification Services that can be performed as batch notifications from NEC ESMPRO Agent and NEC ESMPRO ServerAgentService are included in the expanded set of notification features: e-mailing of alert information, popup alerts, sending alert information to printers and/or files, and the launching of specified applications when alerts occur.

#### **5.3.1 Expandable Notification Methods and Features**

The expanded notification features are as follows.

##### **E-mail Notifications**

Notifications are made with e-mail via an e-mail server that supports the SMTP protocol.

The e-mail server can exist in either a LAN or a WAN environment.

##### **Command Execution**

Specified commands can be run when an alert occurs.

The computer on which the fault occurred, the time the fault occurred, and a description of the fault can all be passed as arguments to the commands.

##### **Signal Tower Notification**

A signal tower can be lit when an alert occurs.

##### **File Output**

Text can be written out to a file when an alert occurs.

##### **Printer Output**

Output can be sent to a printer when an alert occurs. Network printers are also supported.

##### **Popup Messages**

Display popup messages on screen.

A single popup message is continually displayed on screen. When there are multiple messages, pressing a button will cycle you through to the next ones.

### **Express Notification Service via Manager**

Transferring express notifications from multiple NEC ESMPRO Agents or NEC ESMPRO ServerAgentService to one administrative server can allow you to send express notifications via the administrative server (NEC ESMPRO Manager).



You will need to have installed WebSAM AlertManager on the administrative server.

Expansion with the following features is also possible.

### **Notification Suppression**

It is possible to suppress notifications for multiple occurrences of an identical event within a set period of time. You can also suppress notifications using a number of occurrences as a threshold value. It is also possible to combine these two options.

### **Saving and Restoring Notification Settings**

When managing multiple servers and clients with the same hardware and software configurations installed, it is possible to completely copy your notification settings from one server to another or from one client to another, without the need to repeat the same notification settings on each server.

## **5.3.2 Convenient Notification Methods**

You will find it convenient to use the expanded notification methods available through WebSAM AlertManager in situations such as the following.

### **To notify maintenance personnel in remote areas when a fault occurs**

- The use of e-mail enables maintenance personnel in remote areas to be notified.

### **To execute arbitrary commands such as those for recovery when a fault occurs**

- The use of command execution can allow for arbitrary commands to be executed.  
Output to event logs, etc. is enabled by using this feature.

### **To keep records of fault occurrence**

- The use of file and printer output can record and save a description of the fault, which is useful for analysis purposes.

### **To display the description of a fault on screen when a fault occurs**

- The use of popup messages displays a popup message on screen when a fault occurs, enabling real-time notification.

### **To trigger a visual or auditory response when a fault occurs**

- The use of signal tower notifications can light up a signal tower when a fault occurs, making it easier to identify when an occurrence has happened.

### **To use the administrative server to batch process express notifications**

- The use of the batch processing feature for express notifications allows you to receive express notification requests from multiple NEC ESMPRO Agents or NEC ESMPRO ServerAgentService all at once, then notify the maintenance center.

### 5.3.3 Expanding Notification Methods

The settings for the WebSAM AlertManager notification methods are described in the online documentation and product page FAQ for WebSAM AlertManager. See the following URL.

The WebSAM AlertManager website (Japanese):

[http://www.nec.co.jp/middle/WebSAM/products/p\\_am/index.html](http://www.nec.co.jp/middle/WebSAM/products/p_am/index.html)

See the Express Notification Service/Express Notification Service (HTTPS) installation guide stored in EXPRESSBUILDER for more on how to set Express Notification Service/Express Notification Service (HTTPS) via an administrative server.

The installation guide and modules can be downloaded from the NEC support portal. See the following URL.

The NEC support portal (Japanese):

<https://www.support.nec.co.jp/View.aspx?id=9010102124>

## 5.4 Transferring Notifications from NEC ESMPRO Agent, NEC ESMPRO ServerAgentService or BMC to Another Manufacturer's Console (Trap Transfers)

There is an extremely high number of notification types from NEC ESMPRO Agent, NEC ESMPRO ServerAgentService or BMC. Displaying these directly on another manufacturer's console requires the use of message definition files for each type of notification.

When you use the trap transfer feature, NEC ESMPRO Agent, NEC ESMPRO ServerAgentService or BMC notifications received by NEC ESMPRO Manager can be converted into a single format and sent to another manufacturer's management console. This significantly reduces the work needed to display notifications on those consoles.



You cannot transfer or display traps to/on NEC ESMPRO Manager.



See the Trap Transfer Destination Settings Help for more information on the trap transfer feature. SNMP Trap Transfer Destination Settings Help is available from the "NEC ESMPRO Manager Online Help. Select "Alert Viewer" → "SNMP Trap Redirection".

### 5.4.1 Transferring Traps

#### Setting the Transfer Destination

1. Start up the Alert Viewer from the NEC ESMPRO Manager screen.
2. Click SNMP Trap Transfer Destination Settings on The Alert Viewer to display the following screen.



The image shows a web-based configuration window titled "SNMP Trap Redirection Setting". The window has a red header bar with the title in white text. Below the header, there are two input fields: "Host Name/ IP Address" and "Community Name". Each field has a corresponding text box. To the right of the "Community Name" field is an "Add" button. Below the input fields is a "Close" button.

SNMP Trap Redirection Setting	
Host Name/ IP Address	Community Name
<input type="text"/>	<input type="text"/>
<input type="button" value="Add"/>	
<input type="button" value="Close"/>	

**Figure 24 SNMP Trap Transfer Destination Settings screen**

3. Enter either the transfer destination's host name or IP address in the "Host Name/IP Address" field. Enter the community name to use when transferring the SNMP trap in the "Community Name" field.
4. Click the "Add" button to save your settings and close the screen.

### 5.4.2 Format of the Transferred Trap

The specifications of the trap sent as a result of trap transfer are as shown below.

For more information, see the MIB definition files (ESMMNGR.MIB and ESMTPGEN.MIB) in the \ESMPRO\ESMWEB\mib folder in the directory in which NEC ESMPRO Manager was installed.

The SNMP version is SNMPv1.

ESMMNGR.MIB	Lists the managerTrap definitions.
ESMTPGEN.MIB	The import destination for the trap object used by managerTrap. There are also trap definitions within this file, but they are not sent with this feature.

**Table 15 List of Trap Fields**

Field	Value	Description
Enterprise	managerTrap (1.3.6.1.4.1.119.2.2.4.4.100.2)	—
Agent address	IP address of the server that sent the trap	—
Generic trap type	Enterprise Specific(6)	General trap code 6: vendor-defined trap
Specific trap type	managerTrapInformation(1) managerTrapWarning(2) managerTrapFatal(3)	Specific trap codes 1: information trap 2: warning trap 3: fault trap
Timestamp	Always '0'	—
Variable Bindings	managerName	The manager name affiliated with the server that sent the trap
	managerHostName	The name of the server that sent the trap Will be <i>unknown</i> when not registered in the operations window.
	managerIPAddress	IP address of the server that sent the trap
	trapGenName	Overview of the trap
	trapGenDetailInfo	Detailed trap information
	trapGenAction	Action required for the trap
	trapGenClassification	The trap's product name
	trapGenSourceName	The trap's service
	trapGenEventID	The trap's event ID Will be <i>ffffff(-1)</i> when there is no data.
	trapGenAlertType	The trap's alert type
	trapGenEventTimeStampWithOffsetFromUTC	Time the trap occurred Format : YYYYMMDDHHMMSS.UUUUUU±OOO YYYYMMDD                      year, month, day HHMMSS                         hour, minute, second UUUUUU                         microsecond ±OOO                             offset (in minutes) from UTC

### 5.4.3 Settings on Other Manufacturers' Management Consoles

Settings specific to the product will be necessary to display transferred traps on other manufacturers' management consoles.

For more information, either see the manuals for the specific console or inquire with its manufacturer.

## 5.5 Receiving Alerts from a Device on which NEC ESMPRO Agent Cannot be Installed

It is also possible to display notifications in NEC ESMPRO Manager's alert viewer from devices on which NEC ESMPRO Agent could not be installed.

**Table 16 List of NEC ESMPRO Manager's Support Status**

Managed Type	Required Work
EM Card	- Standard support with NEC ESMPRO Manager.
VMware ESXi 5 (RAID-specific information)	- Standard support with NEC ESMPRO Manager.
PET notifications from BMC	- Standard support with NEC ESMPRO Manager.
Other (notifications from unsupported devices)	- Standard support not offered, but display is possible when an alert definition file is created. See the following URL for more on the settings involved.  The NEC support portal (Japanese): <a href="http://www.support.nec.co.jp/View.aspx?id=3150102015">http://www.support.nec.co.jp/View.aspx?id=3150102015</a>



VMware ESXi 5 is supported with NEC ESMPRO Manager Version 5.6 or later. (Version 5.73 onwards is recommended.)

## 5.6 Lists of Notification Items

Each managed server sends a variety of alerts to NEC ESMPRO Manager when faults occur. See the following URLs for lists of the alerts sent by the servers.

**Table 17 Lists of Notification Items**

Component	URL	Overview
NEC ESMPRO ServerAgentService (Windows)	<a href="http://www.58support.nec.co.jp/global/download/esmpro/SAS_Ver1x_event_EN_Rev7.pdf">http://www.58support.nec.co.jp/global/download/esmpro/SAS_Ver1x_event_EN_Rev7.pdf</a>	A list of event items sent as notifications from NEC ESMPRO ServerAgentService (Windows).
NEC ESMPRO Agent (Windows)	<a href="http://www.58support.nec.co.jp/global/download/index.html">http://www.58support.nec.co.jp/global/download/index.html</a> - ESMPRO - ESMPRO alert list	A list of items sent as notifications from NEC ESMPRO Agent (Windows).
NEC ESMPRO Agent (Linux/VMware)	<a href="http://www.express.nec.co.jp/linux/download/esmpro/docs.html">http://www.express.nec.co.jp/linux/download/esmpro/docs.html</a> * Japanese	A list of event items sent as notifications from NEC ESMPRO Agent (Linux/VMware).
BMC	<a href="http://www.58support.nec.co.jp/global/download/index.html">http://www.58support.nec.co.jp/global/download/index.html</a> - ESMPRO - BMC SNMP Alert List	A list of event items sent as notifications from BMC. Used when not using a VMware ESXi environment or NEC ESMPRO Agent.
Universal RAID Utility	<a href="http://www.58support.nec.co.jp/global/download/index.html">http://www.58support.nec.co.jp/global/download/index.html</a>	A list of RAID-related event items sent

(Windows/Linux/VMware ESX)	<a href="#">al/download/index.html</a> - Utility - Universal RAID Utility	as notifications from the Universal RAID Utility.
LSI SMI-S provider (VMware ESXi 5 or later)	<a href="http://www.58support.nec.co.jp/global/download/index.html">http://www.58support.nec.co.jp/global/download/index.html</a> - ESMPRO - NEC ESMPRO Manager RAID system Management Guid for VMware ESXi5 or later	A list of RAID-related event items in the VMware ESXi 5 or later environment, sent as notifications from the SMI-S provider.



There are no SNMP notifications from BMC in a Windows or Linux environment in which NEC ESMPRO Agent exists.

## 5.7 Express Notification Service

Express Notification Service is a service wherein hardware faults are detected as early as possible, and notifications are sent immediately to the maintenance center. For more information, see the related documentation, *Introducing the Notification Feature*.

When in the VMware ESXi 5 or later environment, see the related documentation, *Module Installation Procedures for Express Notification Service (MG) for VMware ESXi-installed Equipment* and *The NEC ESMPRO Manager RAID System Administration Features Guide (VMware ESXi Edition)*.



## Chapter 6 Configuration Management

This is a description of items that can be managed using ESMPRO/ServerManager. They are broadly divided into three topics: items that can be managed using NEC ESMPRO Manager, NEC ESMPRO ServerAgent, and NEC ESMPRO ServerAgentService; items that can be managed through direct communication between NEC ESMPRO Manager and VMware ESXi 5 or later; and items that can be managed without ESMPRO/ServerAgent by connecting to the EXPRESSSCOPE Engine 3 and vPro™ (for management with the Management Controller).

### 6.1 System Management (NEC ServerAgent, NEC ServerAgentService)

The following is a list of items that can be managed using ESMPRO/ServerManager and ServerAgent.

**Table 18 Items that can be monitored with the System Management Feature**

Management Item	ServerAgent (Windows)	ServerAgent (Linux)	ServerAgent (VMware)	ServerAgent (Guest OS/Other Company's Version)
CPU Monitoring	Yes	Yes	Yes	Yes
Memory Monitoring	Yes	Yes	Yes	Yes (*4)
Temperature Monitoring	Yes	Yes	Yes	No
Fan Monitoring	Yes	Yes	Yes	No
Case Voltage Monitoring	Yes	Yes	Yes	No
Power Supply Unit Monitoring	Yes	Yes	Yes	No
Cooling Unit Monitoring	Yes	Yes	Yes	No
Case Cover Monitoring	Yes	Yes	Yes	No
File System Monitoring	Yes	Yes	Yes	Yes
SCSI/IDE Device Monitoring	Yes	Yes	Yes	Yes
Disk Array Monitoring	- (*1)	- (*1)	- (*1)	No
LAN Network Monitoring	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)
System Information Referencing	Yes	Yes	Yes	Yes (*4)
Referencing Errors Detected at the Hardware Level	Yes	Yes	Yes	No
Event Monitoring	Yes	Yes	Yes	Yes
Stall Monitoring	Yes	Yes	Yes (*2)	No
System Error (Panic) Monitoring	Yes	Yes	Yes	No
Shutdown Monitoring	Yes	Yes (*2)	Yes (*2)	No
Monitoring of PCI Hot-plugging	Yes	Yes	Yes	No
Local Polling	Yes	Yes	Yes	Yes
Alive Monitoring	Yes	Yes	Yes	Yes

\*1: Monitored using a Universal RAID Utility. See Chapter 8, RAID Management

\*2: Only supported when using a server management driver.

\*3: Changes to the settings are needed; the default is set to *No monitoring*.

\*4: Exclusive of items dependent on hardware.

The following are the items which can be managed by using NEC ESMPRO Manager and NEC ESMPRO ServerAgentService.

For more details, refer to Chapter 14 NEC ESMPRO ServerAgentService.

**Table 19 Items that can be monitored with the System Management Feature**

		Description	ServerManager Ver6		
			OS + BMC	SAS + BMC Non-Service Mode	SAS + BMC Service Mode
Hardware	Memory Bank	A feature to monitor garbled memory and to display physical information.	○	○	○
	Field Replaceable Unit	A feature to display device-specific information.	○	○	○
	CPU	A feature to monitor CPU failure and to display physical information and operational status.	○	○	○
System	CPU	A feature to display logical information of CPU and to monitor CPU utilization.	▲ (*1)(*2)	○ (*2)	○
	Memory	A feature to display logical information of memory and to monitor its status.	×	○ (*2)(*4)	○ (*4)
I/O Device		A feature to display information of I/O devices (serial port, parallel port, keyboard, mouse, video, etc.).	▲	▲	▲
Enclosure	Temperature	A feature to monitor temperature inside the chassis.	○	○	○
	Fan	A feature to monitor fans.	○	○	○
	Voltage	A feature to monitor voltage inside the chassis.	○	○	○
	Power Supply	A feature to monitor power supply units.	○	○	○
	Front Cover	A feature to detect open/close status of the chassis cover/door.	○	○	○
Software		A feature to display information of services, driver, and OS.	▲	▲	▲
Network		A feature to display information on network (LAN) and to monitor packets.	▲ (*1)(*2)	▲ (*1)(*2)	▲ (*1)(*2)
BIOS		A feature to display BIOS information.	○	○	○
Storage		A feature to monitor storage devices such as HDD and controllers and to display the configuration information.	×	○ (*2)	○
File System		A feature to display the file system configuration and to monitor its utilization.	▲ (*1)(*2)	○ (*2)	○

RAID System	A feature to monitor disk array controllers and to display their configuration information.	URU (*2)	URU (*2)	URU
Event log /Syslog Monitoring	A feature to monitor event logs on Windows OS and Syslog on Linux OS.	×	×	○
Server Monitoring	A feature to alive monitor the server with ping.	○	○	○
Monitor System Hangs	A feature to monitor OS stall by using Watch Dog Timer.	○(*3) Server Conf.	○(*3) Server Conf. (*5)	○(*3) Server Conf. (*5)
Monitor Shutdown Hangs	A feature to monitor shutdown by using Watch Dog Timer.	○(*3) Server Conf.	○(*3) Server Conf. (*6)	○(*3) Server Conf. (*6)
Electric Power Management	A feature to monitor power consumption of the server.	○	○	○
Local Polling	A feature to monitor arbitrary MIB of the server.	×	×	×

○ Supported

▲ Part of displayed items/features are supported.

×

Not supported.

\*1 Status information not displayed.

\*2 No report feature.

\*3 Conventionally, set from the control panel of NEC ESMPRO Agent.In NEC ESMPRO ServerAgentService, set by using Server Configuration Utility.

\*4 Supported by NEC ESMPRO Manager Ver6.05, NEC ESMPRO ServerAgentService (Windows) Ver1 2 or later, and NEC ESMPRO ServerAgentService (Linux) Ver1 0 or later.

\*5 For Linux, devices which use OpenIPMI driver are supported by using OpenIPMI.

\*6 For Linux, devices which use OpenIPMI driver are not supported.

SA : ESMPRO/ServerAgent

SAS : ESMPRO/ServerAgentService

URU : Unisersal RAID Utility

### 6.1.1 CPU Monitoring

A server's CPU can be monitored using ESMPRO/ServerManager and ServerAgent. CPU monitoring allows for early detection of CPU degradation and high CPU loads.

#### 6.1.1.1 The CPU Monitoring Feature

Once ESMPRO/ServerAgent detect an instance of CPU degradation or a high CPU load, an alert is sent to ESMPRO/ServerManager, which results in a change to the status color for the corresponding CPU on ESMPRO/ServerManager's web console. Access the web console to confirm if any CPUs are in an abnormal state.

CPU load monitoring can be performed at two levels: loads can be monitored at the CPU level, or at the level of the entire server. It is therefore possible to monitor the load for a server as a single unit without focusing on the individual CPU level.

To check CPU load monitoring, go to "Configuration Information" → "System" → "CPU".



The content that can be monitored with the CPU monitoring feature will vary by model.

### The Total Information Monitoring Feature

Displays CPU information at the server level.

Selecting "Total Information" allows a review of server-level CPU status information, including the number of logical CPUs, the number of physical CPUs, the total CPU monitoring status, the CPU load rate and load rate-specific status.

Item	Value
Number of logical CPUs	2
Number of physical CPUs	1
Threshold	Disabled
CPU load rate of the latest 1 minute	0 %
Status	Normal

**Figure 25 "Configuration Information" → "System" → "CPU" "Total Information" in the Web Console**

## CPU Information Monitoring Feature

Displays information at the CPU level.

Selecting “CPU Information” allows for a review of CPU-level CPU information, including the CPU name, version information, the CPU type, the internal and external clock rates, the user mode load rate, the privileged mode load rate, individual CPU monitoring status, individual CPU loads and status for the individual CPU.



- With devices that support hyper-threading, when this feature is enabled, the number of logical CPUs will be displayed as twice that of the physical CPUs.
- With multi-core devices, when this feature is enabled, the number of logical and physical CPUs will reflect the number of cores. For example, in a dual core device, there will be twice as many CPUs, and in a quad core device, four times as many.



Intel's hyper-threading technology allows for multiple threads (instruction streams) to run simultaneously on a single physical processor, which has the potential to increase throughput and improve performance.

Item	Value
CPU Name	Intel(R) Xeon(R) CPU E31220 @ 3.10GHz
Version	x86 Family 6 Model 42 Stepping 7
Type	Intel
Internal Speed	3.093 GHz
User Mode	0 %
Privileged Mode	0 %
Threshold	Disabled
CPU load rate of the latest 1 minute	0 %
Status	Normal

Figure 26 “Configuration Information” → “System” → “CPU” → “CPU [\*]” in the Web Console

## Status Colors

The icons for CPU information status display the state of CPU loads through the use of CPU load monitoring.



(Normal): The CPU load rate falls within the normal range,



(Warning): The CPU load rate exceeds the warning level.



(Error): The CPU load rate exceeds the abnormal level.

The screenshot shows the 'Constitution' tab in the Web Console. The left sidebar displays a tree view of server components. The 'Hardware' section is expanded, showing 'CPU Socket[1]' and 'CPU'. The 'CPU' item is selected, and the right pane displays a table of CPU information.

Item	Value
CPU Name	Intel(R) Xeon(R) processor
Version	x86 Family 6 Model 42 Stepping 7
Manufacturer	Intel Corporation
Internal Speed	3.1 GHz
External Speed	100 MHz
Status	✓ CPU is working properly.

**Figure 27 “Configuration Information” → “Hardware” → “CPU” in the Web Console**

Selecting “CPU Information” for each CPU under “Hardware” allows for a review of the CPU name, version information, CPU type and the internal and external clock rates. Select “Level 1 Cache”, “Level 2 Cache” or “Level 3 Cache” to review the individual CPU’s cache sizes, levels, types and formats.

### 6.1.1.2 Using CPU Monitoring

The following is a description of the use of CPU monitoring, including how to review faults during CPU monitoring, and how to change settings.

#### Reviewing CPU Faults

---

When a CPU-Related fault occurs, an alert is sent to the ESMPRO/ServerManager. Check whether an alert notice has come through related to a CPU in the Alert Viewer.

CPU subsystem is running in a reduced capacity.  
CPU Number: 1

#### Notification upon CPU Degradation

CPU xx load has exceeded the upper threshold(Error).

#### Notification upon High CPU Load

ESMPRO/ServerAgent detects CPU degradation at system launch. An alert is sent when CPU degradation is detected. Review CPU degradation by going to “Hardware” → “CPU” in the web console. You can also review the degradation with the following procedure, using the ESRAS utility.



In some instances, the sending of an alert immediately after a system launch may fail. When this happens, the alert notification will be delayed by the number of minutes set for the retry interval configured in the Alert Manager Settings Tool.



For models supporting IPMI, double-clicking on the relevant *processor fault* log record in the list (or selecting “View Related Information” from the “View” menu) will display the sensor information (CPU number) for the sensor that detected the event.



#### Intelligent Platform Management Interface (IPMI)

A standard interface specification that enables the monitoring of server hardware without any dependency on a specific hardware system or OS. Functions as a lower-level interface for management software like SNMP.

#### Setting the CPU Monitoring Feature

---

By default, CPU load rate monitoring is not performed. Settings need to be changed to perform CPU load rate monitoring.

The appropriate threshold value will vary depending on your specific system situation. For this reason, the default values are set on the high side, but the default values may not be the appropriate values for your threshold and monitoring interval values, so set them appropriately to suit your specific system.

Should you change any settings arbitrarily, however, there may be a higher frequency of alerts related to CPU loads depending on the new threshold value. Choose a threshold value that won't result in a greater frequency of alerts.

### 1) Changing the CPU Monitoring Threshold Value

The threshold value can be changed on either the web console of the ESMPRO/ServerManager or the Control Panel of the ESMPRO/ServerAgent.

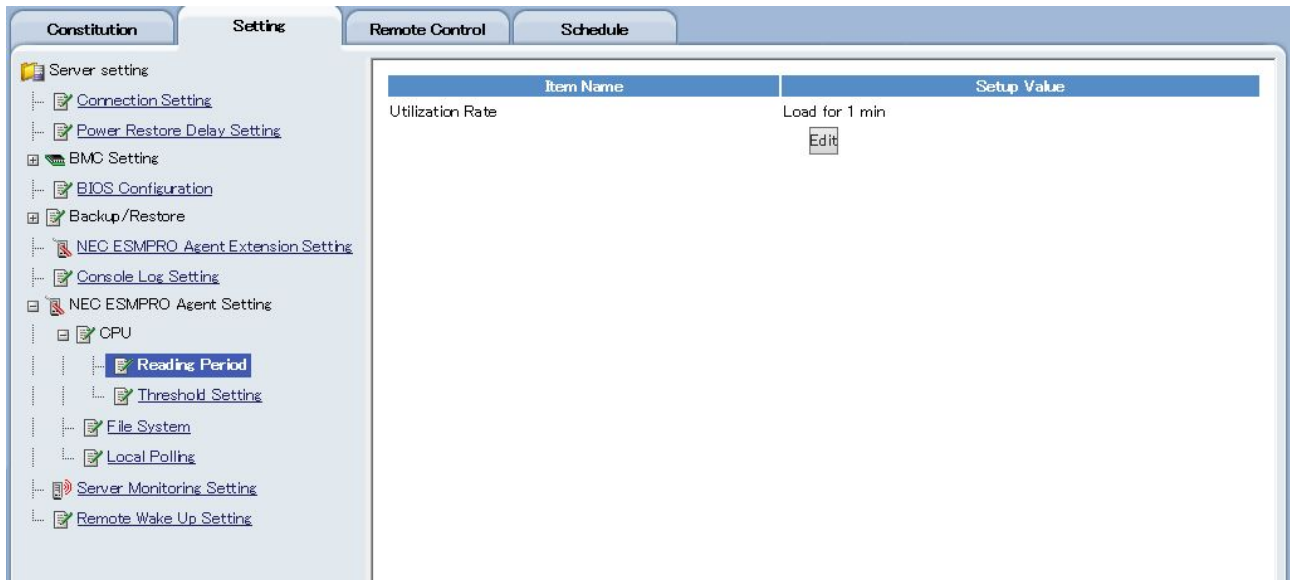


Figure 28 Monitoring Interval Settings Screen

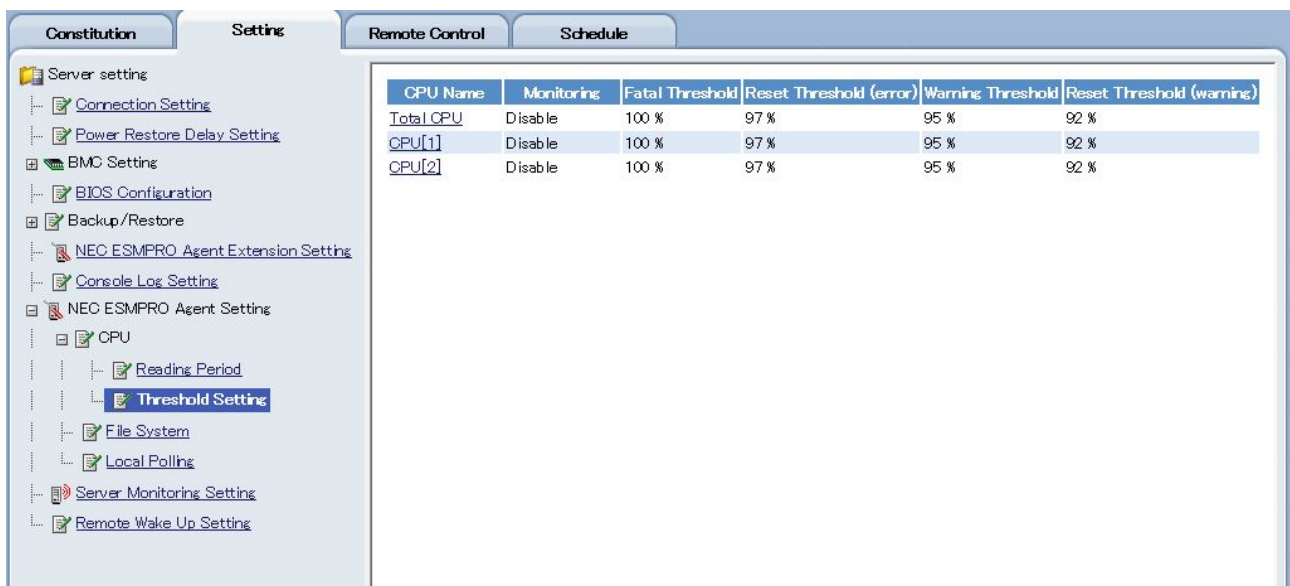


Figure 29 Threshold Value Settings Screen



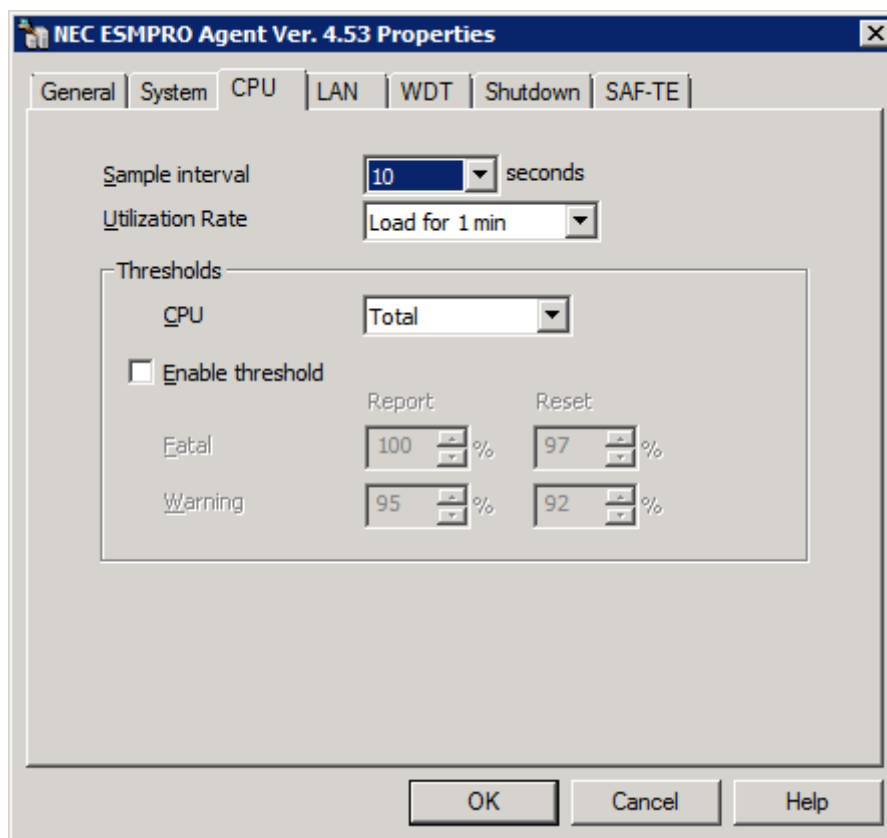


Figure 30 ESMPRO/ServerAgent Control Panel, CPU Load

#### Default Threshold Values

Monitoring Operations: Do not monitor  
 Target Monitoring Load Rate: Load rate per minute  
 CPU Load Rate Monitoring Information: See the table below (units: percent)

Monitored Item	Threshold (Abnormal)	Threshold (Abnormal Recovery)	Threshold (Warning)	Threshold (Warning Recovery)
CPU Load Rate	100	97	95	92

## 6.1.2 Memory Monitoring

Memory on the server can be monitored using ESMPRO/ServerManager and ServerAgent. The memory status monitoring feature can be used to detect faults related to the hardware, including memory degradation, the frequent occurrence of recoverable errors, and the occurrence of unrecoverable errors.

### 6.1.2.1 The Memory Monitoring Feature

The memory monitoring feature can be used to access information on the system's on-board memory (including the amount of memory implemented at the bank level, the total amount of memory there, the available volume there, the amount in use there and the use rate there, and the total amount of memory for page files, the available volume for them, the amount in use for them, and their use rate).

When ESMPRO/ServerAgent detects a fault specific to memory, an alert is sent to ESMPRO/ServerManager and a warning (in yellow) is displayed for the relevant memory bank's status color in the web console in ESMPRO/ServerManager. Access the web console to confirm the memory for which a fault has been detected.



The content that can be monitored with the memory monitoring feature will vary by model.

### More on the Memory Monitoring Feature

To reference memory information from ESMPRO/ServerManager select the desired memory bank by going to “Configuration Information” → “Hardware” → “Memory Banks” within the web console. Once selected, you can confirm memory status, redundancy status, and the amount of memory implemented at the bank level.

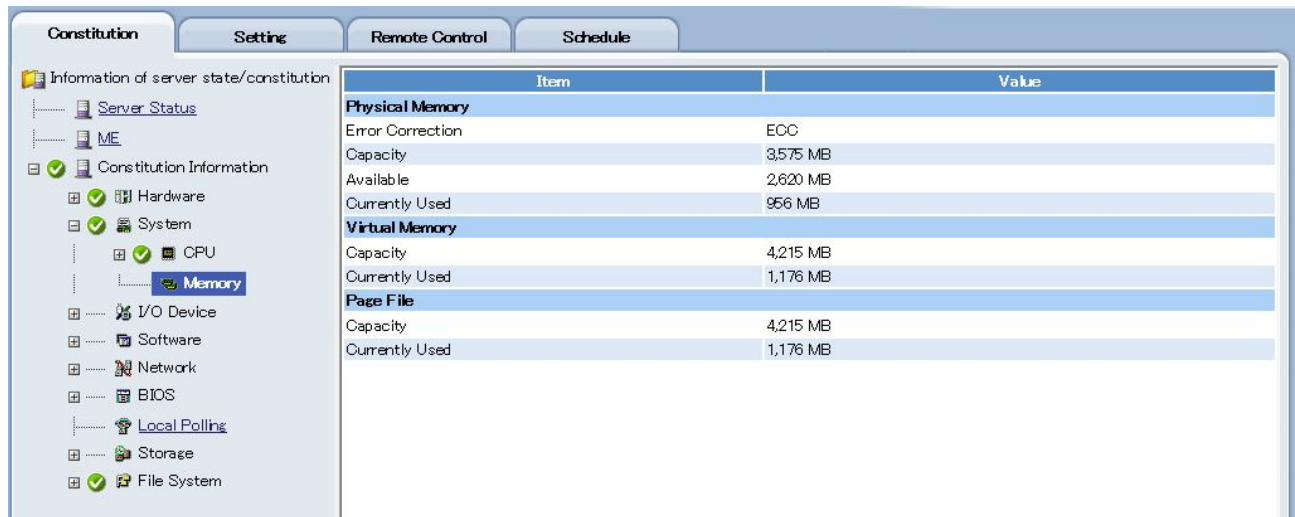


Figure 31 “Configuration Information” → “Hardware” → “Memory Banks” in the Web Console

The icons shown in the “Status” field of the desired memory bank display the state of the memory bank as detected with the memory monitoring feature.

- ✓ (Normal): The memory bank is functioning normally.
- ⚠ (Warning): A fault has occurred in the memory bank.

Select “System” → “Memory” to reference the total amount of memory, the available volume of it, the amount of it in use and its use rate, and the total amount of page files, the available volume for them, the amount in use for them and their use rate.



The screenshot shows the ESMPRO/ServerManager interface with the 'Constitution' tab selected. The left sidebar shows a tree view with 'System' expanded and 'Memory' selected. The main panel displays a table of memory information.

Item	Value
<b>Physical Memory</b>	
Error Correction	ECC
Capacity	3,575 MB
Available	2,620 MB
Currently Used	956 MB
<b>Virtual Memory</b>	
Capacity	4,215 MB
Currently Used	1,176 MB
<b>Page File</b>	
Capacity	4,215 MB
Currently Used	1,176 MB

**Figure 32 Memory Information**

### 6.1.2.2 The Use of Memory Monitoring

The following describes procedures specific to memory monitoring, including how to confirm faults and how to change settings.

#### Confirming Memory Faults

When a memory fault occurs, an alert is sent to ESMPRO/ServerManager. Check whether any alerts related to memory have arrived in the Alert Viewer. Memory degradation and unrecoverable errors are detected at system launch, so alerts are sent to ESMPRO/ServerManager after the system launches.

#### Sample Alert during Memory Degradation

A memory is a degenerate state.  
Date: 04/26/2012 17:45:12  
Memory ID: 1

#### Sample Alert during Recoverable Errors

Too many ECC Correctable Errors.

## Sample Alert during an Unrecoverable Error

ECC uncorrectable error occurred.



In some instances, the sending of an alert immediately after a system launch may fail. When this happens, the alert notification will be delayed by the number of minutes set for the retry interval configured in the Alert Manager Settings Tool.

When there is an alert for memory degradation, use the web console in ESMPRO/ServerManager to confirm which memory has degraded. To easily identify the memory in which the fault has occurred, under “Memory Banks” look for the status that is displaying a warning indicator. The memory level for which the warning indicator will appear will vary by server model: it will either occur for the entire memory bank or for two memory units at a time.

## Confirming Cache Faults

An alert is sent to the ESMPRO/ServerManager after system launch when cache degradation is detected. Check whether any alerts related to cache issues have arrived in the Alert Viewer.

## Sample Alert during Cache Degradation

A cache is a degenerate state.

Date: 04/26/2012 17:45:12

DIMM ID: 0x01

Site Original Size: 0x80

Site Current Size: 0x40



In some instances, the sending of an alert immediately after a system launch may fail. When this happens, the alert notification will be delayed by the number of minutes set for the retry interval configured in the Alert Manager Settings Tool.

ESMPRO/ServerAgent detects cache degradation at system launch. When cache degradation is detected ESMPRO/ServerAgent sends an alert to ESMPRO/ServerManager, but at that point you will be unable to confirm cache degradation in the ESMPRO/ServerManager web console because the system is already operating as if the cache in which the degradation occurred no longer exists. Upon receipt of a cache degradation alert, confirm that it occurred in the ESRAS utility log.

## Memory Monitoring Settings

The ESMPRO/ServerAgent will constantly monitor memory while the server is in operation. There is no way to disable memory monitoring.

## Memory Usage Threshold Monitoring

It is possible to perform memory usage threshold monitoring with the use of ESMPRO/ServerAgent's local polling feature. When you monitor memory usage thresholds, it is possible to send alerts to ESMPRO/ServerManager when memory usage exceeds a certain value.



See section 6.1.20 エラー! 参照元が見つかりません。 Local Polling, for more information on how to set the local polling feature.

### Sample Threshold Setting

In this example for a device with 5GB of physical memory, monitoring is set at an interval of one minute, a warning is sent when physical memory use exceeds 2GB, and a fault alert is sent when use exceeds 4GB.

Object ID	1.3.6.1.4.1.119.2.2.4.4.4.2.1.3.0
Monitoring	Enabled
Monitoring Period	Infinite
Monitoring Interval	60
Threshold Setting (maximum)	5242880
Threshold Setting (minimum)	0
Upper Threshold (send traps)	Enabled
Upper Threshold (fault threshold)	4194304
Upper Threshold (fault release)	3145728
Upper Threshold (warning threshold)	2097152
Upper Threshold (warning release)	1048576
Lower Threshold (send traps)	Disabled
Lower Threshold (warning release)	4
Lower Threshold (warning threshold)	3
Lower Threshold (fault release)	2
Lower Threshold (fault threshold)	1

### 6.1.3 Temperature Monitoring

Temperature within the server case can be monitored using ESMPRO/ServerManager and ServerAgent.

#### 6.1.3.1 The Temperature Monitoring Feature

When a fault specific related to temperature occurs, an alert is sent to ESMPRO/ServerManager. Check whether an alert related to temperature has arrived in the Alert Viewer.

Furthermore, depending on the severity of the fault, the server may shutdown when continued operations pose a risk.

#### Temperature Information

Selecting “Configuration Information” → “System Environment” → “Temperature” will enable the temperature of the various components within the case to be confirmed.

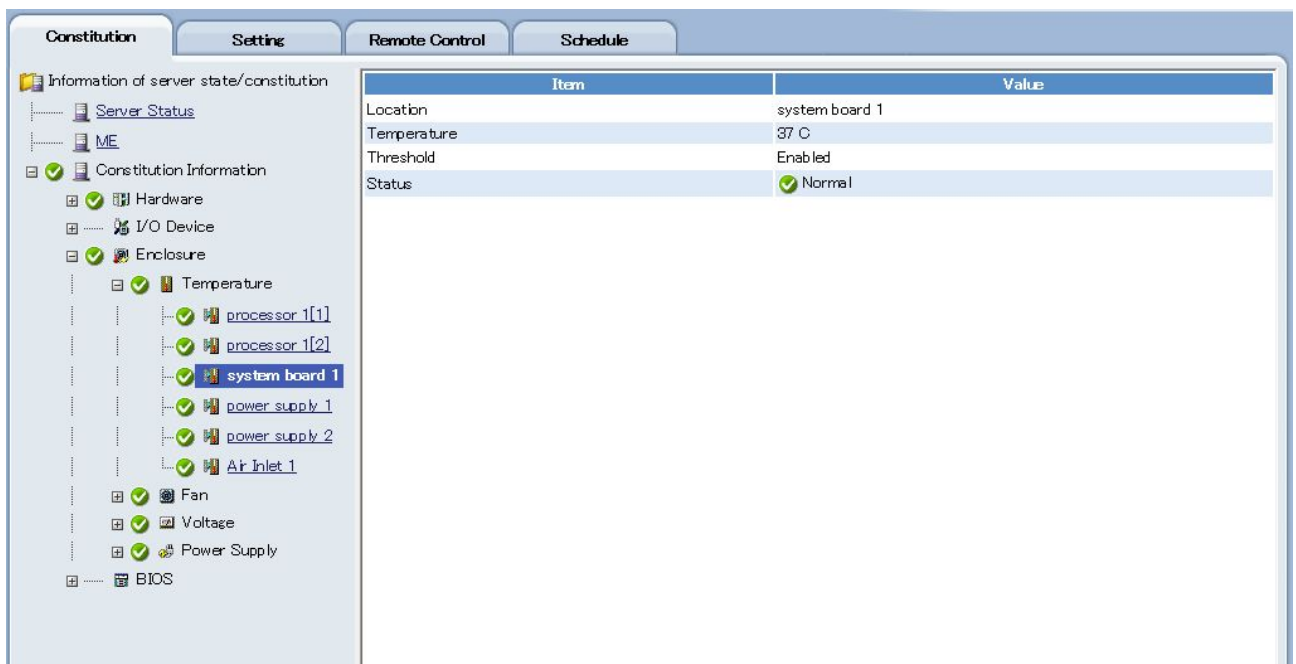


Figure 33 “Temperature” → “System Board” in the Web Console

The icons shown in the “Status” field of the desired temperature indicate the state of the temperature within the server case as detected with the temperature monitoring feature.

- (Normal): Temperatures are at a normal level.
- (Warning): Temperatures are at a warning level.
- (Error): Temperatures are at an abnormal level.

#### 6.1.3.2 Using Temperature Monitoring

The following describes the procedures specific to temperature monitoring, including how to check faults and change settings.

#### Checking Temperature Faults

When a fault specific to temperature occurs, an alert is sent to the ESMPRO/ServerManager. Check whether

an alert related to temperature has arrived in the Alert Viewer.

### Sample Alert for Abnormally High Temperatures

The temperature has exceeded the upper threshold setting(Error).  
Location: system board  
Temperature: 80 degrees C

### Settings for Temperature Monitoring

---

ESMPRO/ServerAgent constantly monitors server temperatures while the server is in operation. Threshold values for temperature monitoring are set to optimal levels for each device before being shipped and cannot, therefore, be changed. You can, however, change whether temperature monitoring is performed. The monitoring interval can also be changed for models that do not support IPMI. The default for temperature monitoring is for monitoring to be enabled, and the default monitoring interval for non-IPMI-compatible models is 60 seconds. Under normal circumstances, there is no need to change either of these settings, however.



## 6.1.4 Fan Monitoring

Fans installed in server cases can be monitored using ESM/PRO/ServerManager and ServerAgent. Fan monitoring can prevent temperature faults that result from fans stopping or slowing down.

### 6.1.4.1 The Fan Monitoring Feature

When ESM/PRO/ServerAgent detects a fan fault, it sends an alert to ESM/PRO/ServerManager, changing the status color for the relevant fan in ESM/PRO/ServerManager's web console. Access the web console to check which fan the fault is occurring on.

Furthermore, depending on the severity of the fault, the server may shutdown when continued operations pose a risk.

#### Fan Information

Select the desired fan under "Configuration Information" → "System Environment" → "Fans" to review the location and status of the fan installed within the case.

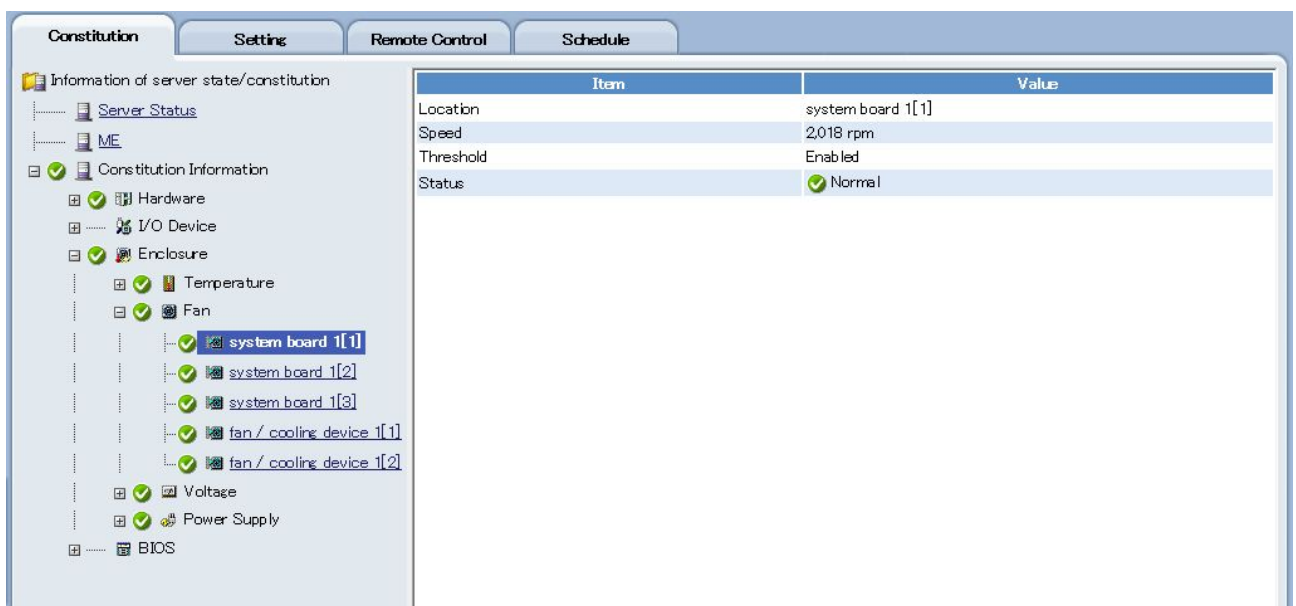





Figure 34 "Fans" → "System Board" in the Web Console

The icons shown in the "Status" field of the desired fan indicate the state of the fan as detected with the fan monitoring feature.

-  (Normal): Fan is operating normally.
-  (Warning): Fan is in a warning state.
-  (Error): Fan is in an abnormal state.

### 6.1.4.2 Using Fan Monitoring

The following describes the procedures specific to fan monitoring, including how to check faults and change settings.

#### Checking Fan Faults

---

When a fault specific to fans occurs, an alert is sent to the ESMPRO/ServerManager. Check whether an alert related to fans has arrived in the Alert Viewer.

#### Sample Alert for a Fan Warning

A sample alert message box with a light gray background and a thin black border. The text inside reads: "Processor 2 fan speed has fallen below the lower limit (Warning)." The box has rounded corners and a subtle drop shadow.

Processor 2 fan speed has fallen below the lower limit (Warning).

#### Settings for Fan Monitoring

---

ESMPRO/ServerAgent constantly monitors fans while the server is in operation.

Threshold values for fan monitoring are set to optimal levels for each device before being shipped and cannot, therefore, be changed.

Fan monitoring can be turned on and off for models supporting IPMI. Under normal circumstances, there is no need to change this setting, however.

## 6.1.5 Monitoring Case Voltage

Server voltage can be monitored using ESMPRO/ServerManager and ServerAgent. Use voltage monitoring to rapidly respond to server faults such as voltage fluctuations.

### 6.1.5.1 The Case Voltage Monitoring Feature

When ESMPRO/ServerAgent detects a voltage fault, it sends an alert to ESMPRO/ServerManager, changing the status color for the relevant voltage in ESMPRO/ServerManager's web console. Access the web console to check which voltage is faulty.

Furthermore, depending on the severity of the fault, the server may shutdown when continued operations pose a risk.

#### Displaying Voltage Information

Select items under “System Environment” → “Voltage” to review the voltage type, its value, the standard voltage value, the monitoring status, and the voltage status.

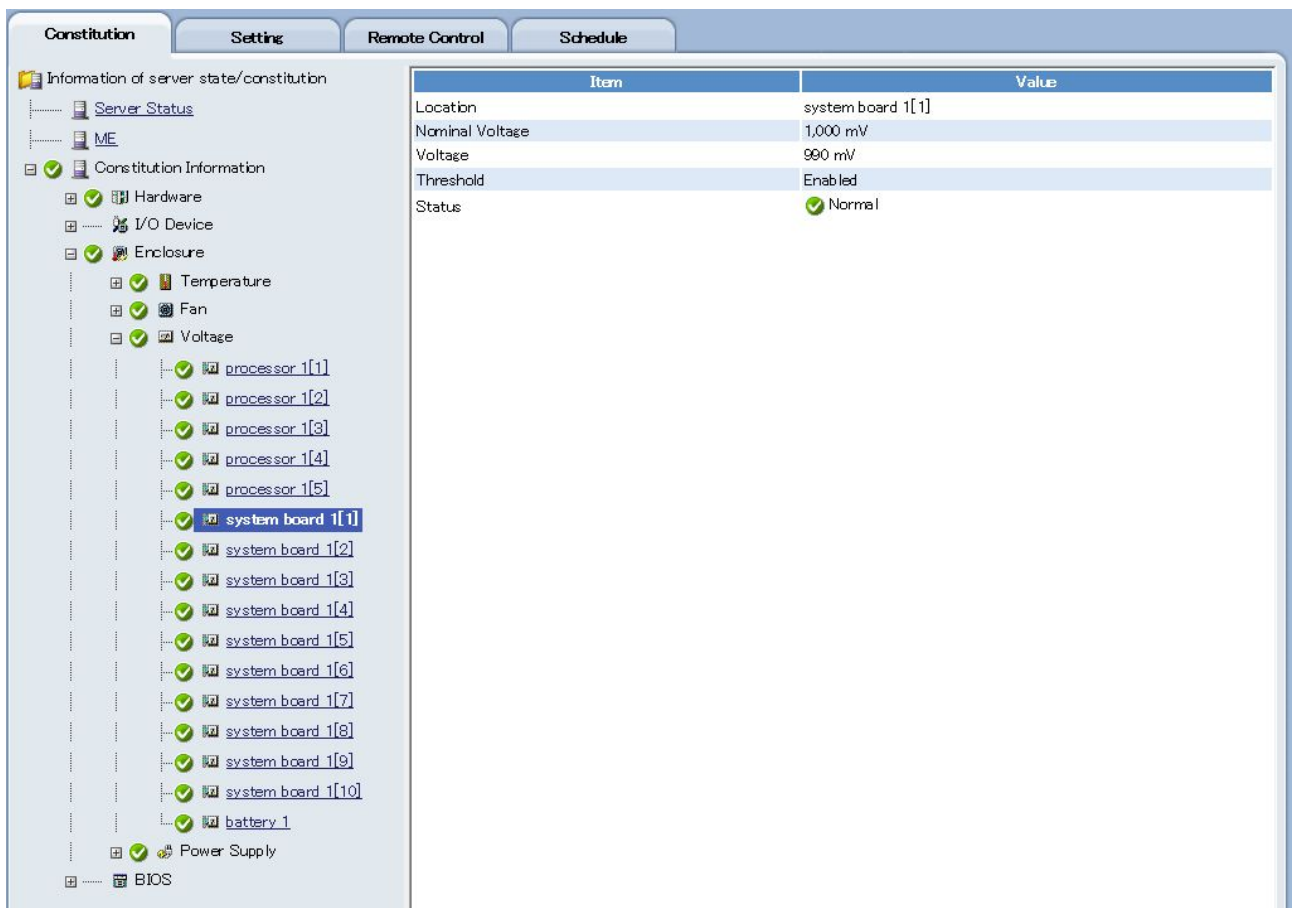





Figure 35 “Voltage” → “System Board” in the Web Console

The icons shown in the “Status” field of the desired voltage indicate the state of the case voltage as detected with case voltage monitoring.

-  (Normal): Voltage is normal.
-  (Warning): Voltage is in a warning state.
-  (Error): Voltage is in an abnormal state.

### 6.1.5.2 Using Case Voltage Monitoring

The following describes the procedures specific to case voltage monitoring, including how to check faults and change settings.

#### Checking Case Voltage Monitoring Faults

---

When a fault specific to voltage occurs, an alert is sent to the ESMPRO/ServerManager. Check whether an alert related to voltage has arrived in the Alert Viewer.

#### Sample Alert for Voltage above Threshold

The voltage has exceeded the upper limit (Error).  
Nominal Level: 1,245 mv  
Level: 2,240 mv

#### Settings for Case Voltage Monitoring

---

ESMPRO/ServerAgent constantly monitors case voltage while the server is in operation. Threshold values for case voltage monitoring are set to optimal levels for each device before being shipped and cannot, therefore, be changed. Voltage monitoring can be turned on and off, however, for models supporting IPMI. By default, monitoring is enabled and, under normal circumstances, there is no need to change this setting.

### 6.1.6 Power Supply Unit Monitoring

The following describes the procedures specific to power supply unit monitoring, including how to check faults and change settings.

#### 6.1.6.1 The Power Supply Unit Monitoring Feature

When a fault specific to the power supply unit occurs, an alert is sent to the ESMPRO/ServerManager. Check whether an alert related to the power supply unit has arrived in the Alert Viewer.

##### Power Supply Unit Information

Select “Configuration Information” → “Power Supplies” → “System Environment” to review the power supply unit status.

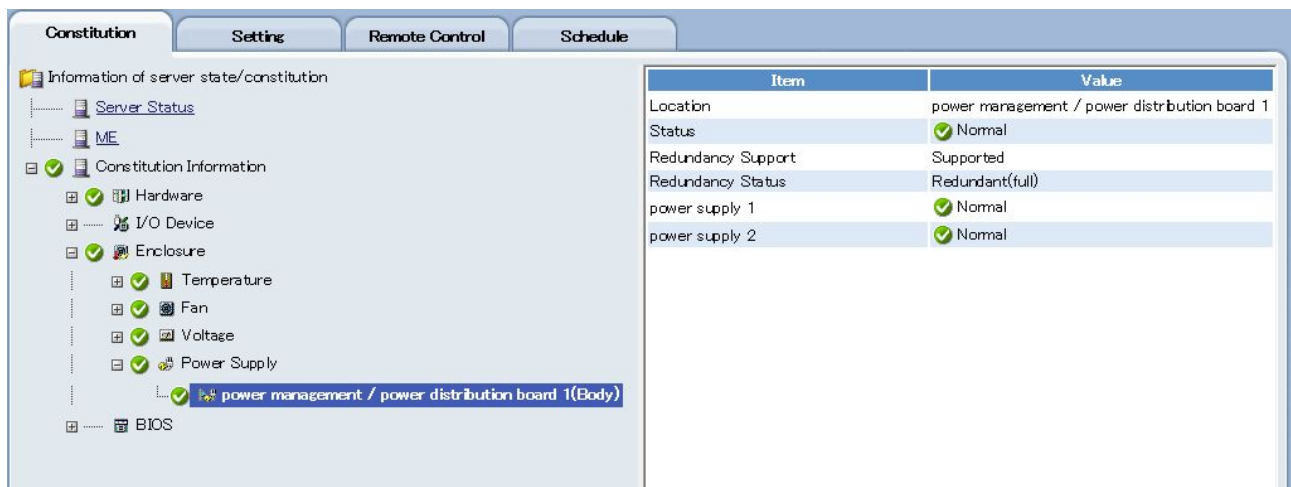


Figure 36 “Power Supplies” in the Web Console

#### 6.1.6.2 Using Power Supply Unit Monitoring

The following describes the procedures specific to power supply unit monitoring, including how to check faults and change settings.

##### Checking Power Supply Unit Faults

When a fault specific to the power supply unit occurs, an alert is sent to the ESMPRO/ServerManager. Check whether an alert related to the power supply unit has arrived in the Alert Viewer.

##### Sample Alerts when a Fault occurs in a Power Supply Unit

Power unit 1 is in fatal state.

The power unit is in reduced capacity state.

The power supply unit in which the fault has occurred can be confirmed by the power supply unit number in the alert or by referencing the individual power supply status under “System Environment” → “Power Supplies” → “Separate Power Supplies” in the web console.

## **Settings for Power Supply Unit Monitoring**

---

ESMPRO/ServerAgent constantly monitors power supply units while the server is in operation. Power supply unit monitoring cannot be turned off.

## 6.1.7 Cooling Unit Monitoring

The cooling units installed in server cases can be monitored using ESMPRO/ServerManager and ServerAgent. Cooling unit monitoring can prevent temperature faults within the case and equipment damage resulting from coolant leaks.

### 6.1.7.1 The Cooling Unit Monitoring Feature



When ESMPRO/ServerAgent detects a leak in the cooling unit, an alert is sent to the ESMPRO/ServerManager, changing the status color of the relevant cooling unit in ESMPRO/ServerManager's web console. Access the web console to review the cooling unit in which the fault is occurring.

Furthermore, depending on the severity of the fault, the server may shutdown when continued operations pose a risk.

#### Cooling Unit Information

Select the desired cooling unit under "System Environment" → "Cooling Units" to confirm the location and status of the cooling unit installed within the case.

The icons shown in the "Status" field of the desired cooling unit indicate the state of the cooling unit as detected with cooling unit monitoring.

-  (Normal): No leaks are occurring.
-  (Error): A leak is occurring.

### 6.1.7.2 Using Cooling Unit Monitoring

The following describes the procedures specific to cooling unit monitoring, including how to check faults and change settings.

#### Checking Cooling Unit Faults

---

When a fault specific to a cooling unit occurs, an alert is sent to the ESMPRO/ServerManager. Check whether an alert related to a cooling unit has arrived in the Alert Viewer.

#### Sample Alert during a Cooling Unit Leak

Liquid Leak has happened.

#### Settings for Cooling Unit Monitoring

---

ESMPRO/ServerAgent constantly monitors cooling units while the server is in operation. Cooling unit monitoring cannot be turned off.

## 6.1.8 Case Cover Monitoring

The case covers on a server can be monitored using ESMPRO/ServerManager and ServerAgent. Use case cover monitoring to prevent illegal access to servers.

### 6.1.8.1 The Case Cover Monitoring Feature

Case covers include front, side, top and PCI covers. When ESMPRO/ServerAgent detects that a case cover has been opened, an event is registered in the system's event log (or in syslog for Linux), changing the status color of the relevant case cover in ESMPRO/ServerManager's web console to that of a warning (yellow). Access the web console to review which case cover has been opened.

The icons shown in the "Status" field of the desired cover indicate the open state of the cover as detected with case cover monitoring.



(Normal): The case cover is closed.



(Warning): The case cover is open.



CAUTION

Some case covers may result in a loss of server power when the cover is open to ensure the system operates safely.



### 6.1.8.2 Using Case Cover Monitoring

The following describes the procedures specific to case cover monitoring, including how to check faults and change settings.

#### Checking Case Cover Faults

---

When a fault specific to a case cover occurs, the following event is registered to the *system* in the event viewer. Check the event viewer to see whether an event related to a case cover has been registered.

#### Event Log Content when the Front Cover is Open

The Front cover was opened.



Settings specific to alerts must be changed in order to receive alerts.

#### Settings for Case Cover Monitoring

---

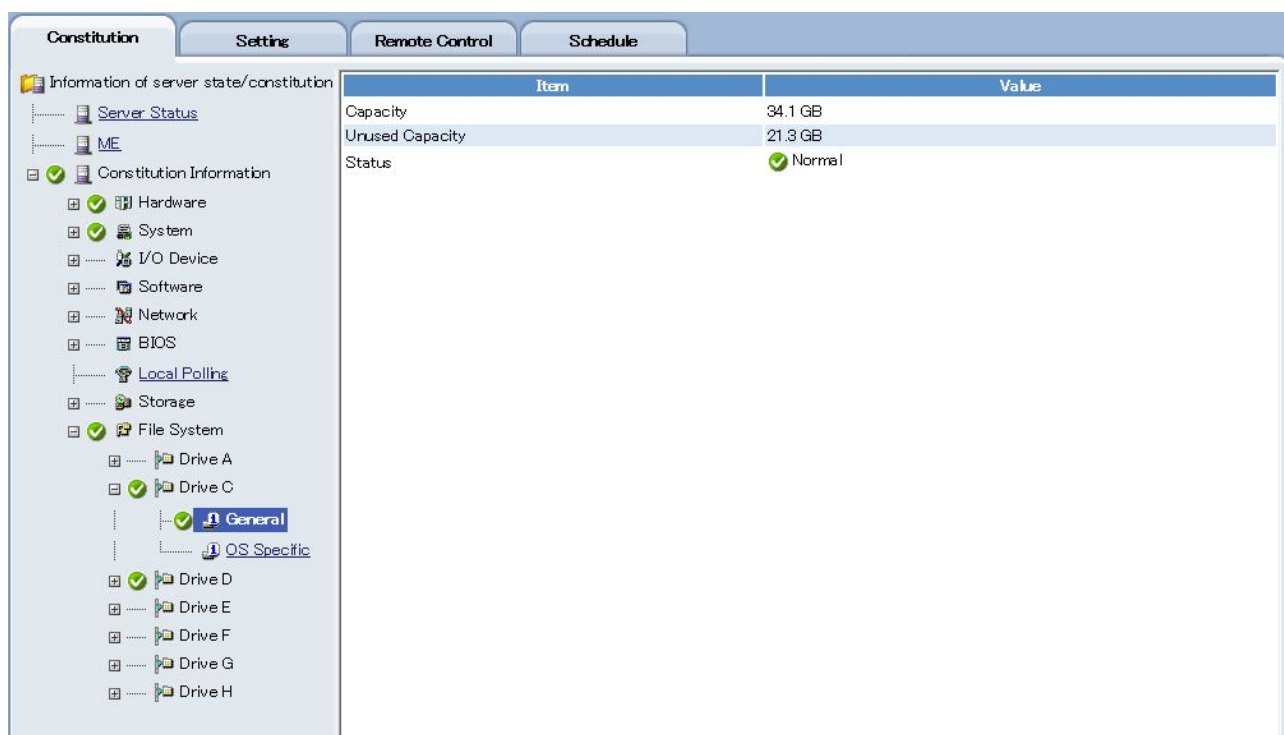
ESMPRO/ServerAgent constantly monitors case covers while the server is in operation. Case cover monitoring cannot be turned off.

## 6.1.9 File System Monitoring

The server's file system can be monitored using ESMPRO/ServerManager and ServerAgent.

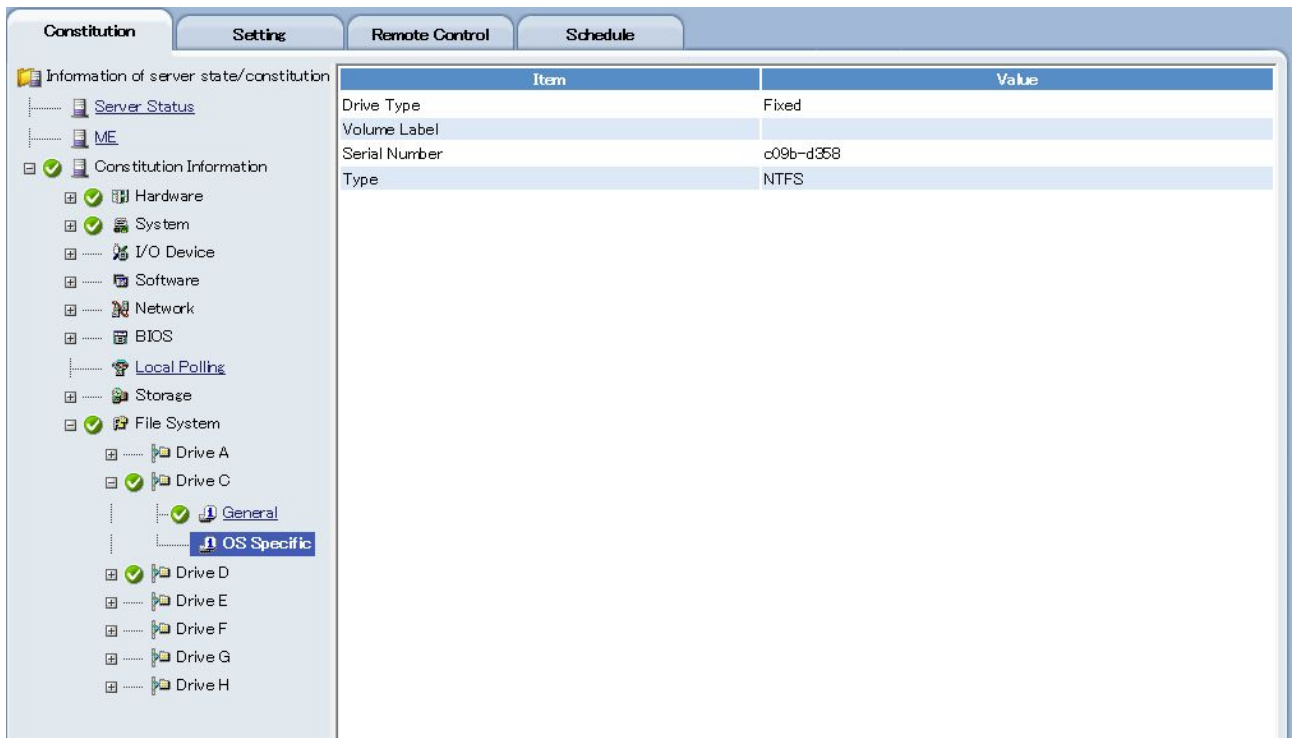
### 6.1.9.1 The File System Monitoring Feature

The file system monitoring feature manages the file systems assigned to the drive names that comprise the system. Access the web console in ESMPRO/ServerManager to review the configuration and information for the file systems. Managed information includes both general information such as capacity and available capacity, and additional information such as the drive type and the number of sectors per cluster.



Item	Value
Capacity	34.1 GB
Unused Capacity	21.3 GB
Status	Normal

**Figure 37 “File Systems” → “Drive [\*]” → “General Information” in the Web Console**



**Figure 38 “File Systems” → “Drive [\*]” → “Additional Information” in the Web Console**

### The Available Capacity Monitoring Feature

It is possible to detect a lack of available capacity early on when available capacity in a file system is monitored. When ESMPRO/ServerAgent detects a drive with insufficient available capacity, it sends an alert to ESMPRO/ServerManager, changing the status color of the relevant drive in the web console to abnormal (red). Access the web console to review which drive is lacking in available capacity. Since the threshold for a file system’s available capacity can be set to any value, monitoring can be performed with settings that suit the system environment. Available capacity monitoring only targets the file systems on a hard disk.



#### File Systems to be Managed

File system monitoring targets file systems to which drive names have been assigned. File systems to which drive names are not assigned to drive names are excluded.

Also excluded from available capacity monitoring are file systems for removable media such as floppy disks.



#### Configuration Information managed by File System Monitoring

The configuration information managed by file system monitoring varies depending on the file version on the monitoring service (ESMFSService). (The file version for EMFSService can be found by checking the properties of its executable file, *esmfs.exe*.)

- For file versions up to 4.1.0.2:  
Information specific to the file system cluster is managed.
- For file versions from 4.1.0.3 onward:  
Information specific to the file system cluster is not managed.  
The following are not displayed in the ESMPRO/ServerManager web console:  
*number of sectors/cluster, number of bytes/cluster, total number of clusters, number of clusters in use*



### **Remote Drive Monitoring**

File systems for *remote* drive types from Windows Server 2003 on are unable to be monitored.

### 6.1.9.2 Using File System Monitoring

The following describes the procedures specific to file system monitoring, including how to check faults (insufficient available capacity) and change settings.

#### Checking Insufficient Available Capacity in the File System

---

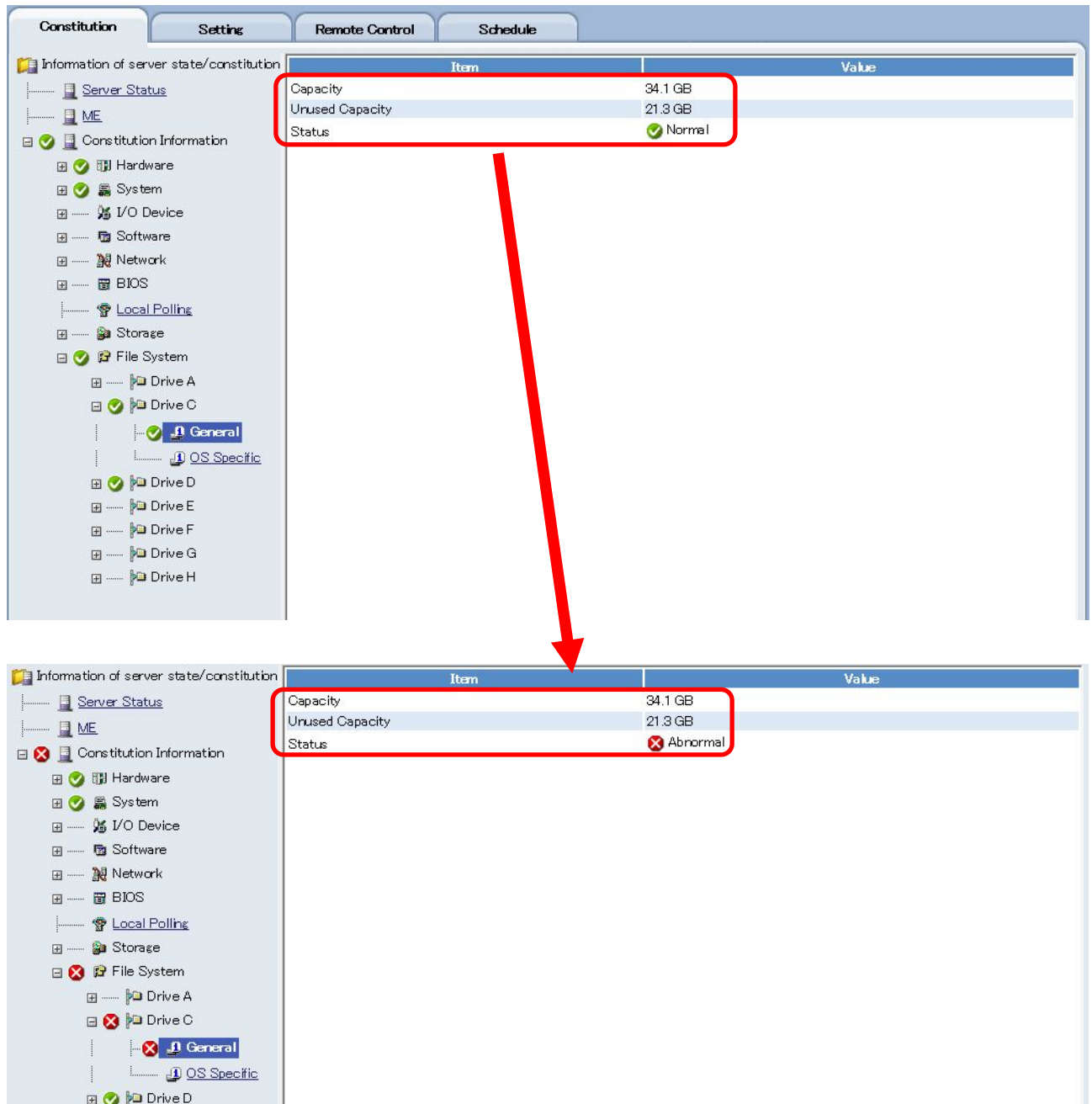
When there is insufficient available capacity in the file system, an alert is sent to the ESMPRO/ServerManager. Check whether an alert related to the file system has arrived in ESMPRO/ServerManager's Alert Viewer.

#### Sample Alert for Insufficient Available Capacity in the File System

The free capacity of this file system is less than "Fatal" level.  
File System : C (Index : 1)  
Free Space / Capacity : 328 / 4194 MB  
Threshold(Fatal) : 419 MB




Insufficient available capacity in file systems can be reviewed not only with alerts, but also with the web console.

When the available capacity of a file system falls below a threshold, the color of the icon in the “Status” field under “File Systems” → “General Information” of the desired drive will change to either an abnormal color (red) or a warning color (yellow).



**Figure 39 “File Systems” → “Drive [\*]” → “Additional Information” in the Web Console**

The icons shown in the “Status” field of the general information of the file system indicate the determination results for the thresholds for file system available capacity.

-  (Normal): Normal status.
-  (Warning): Below the warning threshold level.
-  (Error): Below the abnormal threshold level.

## Settings for File System Monitoring

The settings for file system monitoring can be changed in the ESM/ServerManager web console or in ESM/ServerAgent's control panel.

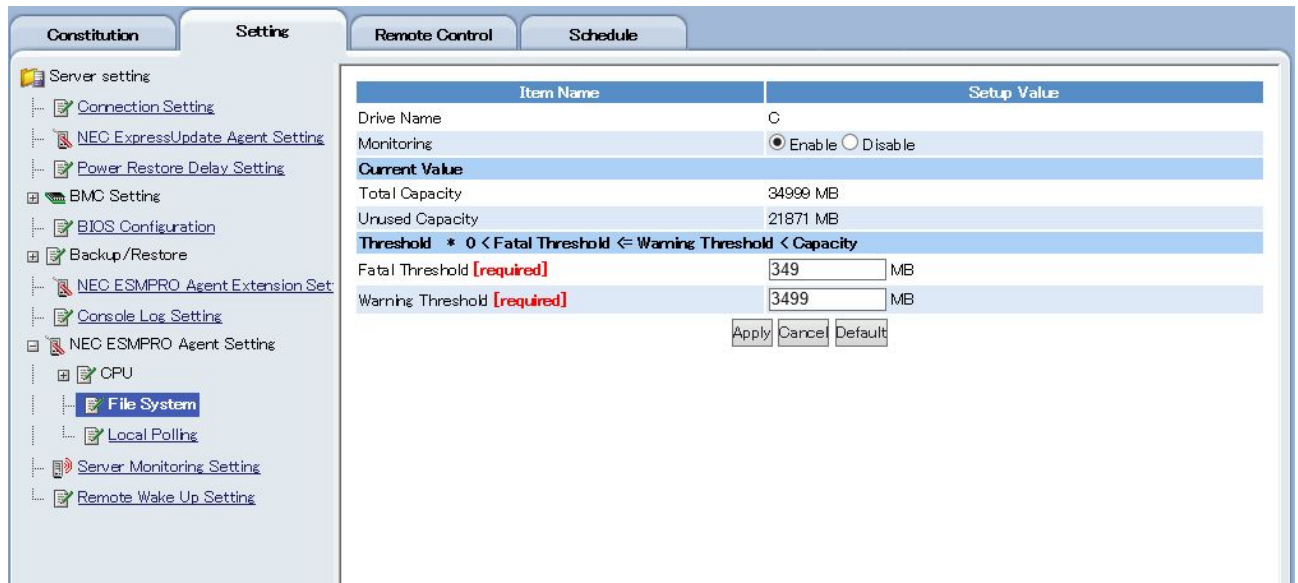


Figure 40 “File Systems” → “Settings” Tab → “Server Settings” → “ESM/ServerAgent Settings” in the Web Console

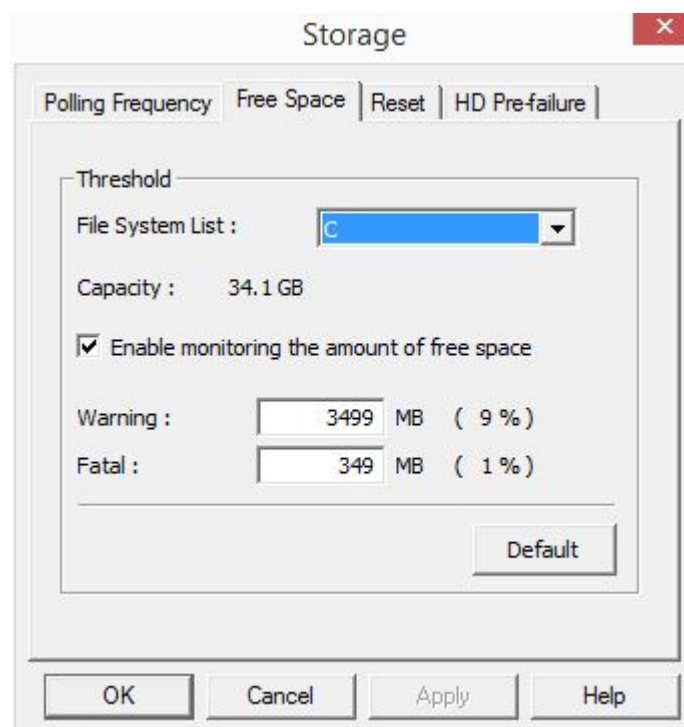


Figure 41 ESM/ServerAgent Control Panel



When it takes time to launch the **ESM/ServerAgent Storage Monitoring Properties** window, or when items within that window are grayed out, check that the properties settings for SNMP services, which are needed to run ESM/ServerAgent, are correct.

### 6.1.9.3 Changing the File System Available Capacity Monitoring Thresholds

The file system available capacity monitoring thresholds can be changed to any value in the ESMPRO/ServerManager threshold settings dialog box or in the ESMPRO/ServerAgent control panel.

By default, file system available capacity monitoring is enabled. Deselect the option to monitor available capacity to disable it.

The default values for the file system available capacity monitoring thresholds are as follows.

Monitored Item	Abnormal Threshold	Warning Threshold
Available Capacity (in MB)	Roughly 1% of total capacity	Roughly 10% of total capacity



In the event that alerts indicating insufficient file system available capacity are occurring frequently and you determine you actually have sufficient available capacity given your environment, change the thresholds such that the conditions of available capacity determination are stricter.



To set available capacity monitoring to only one level, for an abnormal level, instead of two, for warning and abnormal levels, set the threshold to be the same for abnormal and warning. (One level cannot be set for a warning level only.)



The following restrictions apply when using ESMPRO/ServerAgent in a cluster environment with CLUSTERPRO.

The thresholds and monitoring enabled status set for available capacity monitoring in operating servers are not passed on to standby servers in the event a failover occurs. Always set the thresholds and monitoring enabled status on the standby servers as well.



Changes to settings for capacity monitoring thresholds are not immediately applied. The new settings are effective after the next interval for the monitoring service, once the changes have been made.



Do not make configuration changes to a file system while the ESMPRO/ServerAgent control panel is open. Only do so after closing the “ESMPRO/ServerAgent Storage Monitoring Properties” window.

Should configuration changes to a file system be made while the “ESMPRO/ServerAgent Storage Monitoring Properties” window is open, close the properties window and re-launch it.



Available capacity monitoring is not supported for file systems with a total capacity of less than 100 MB.

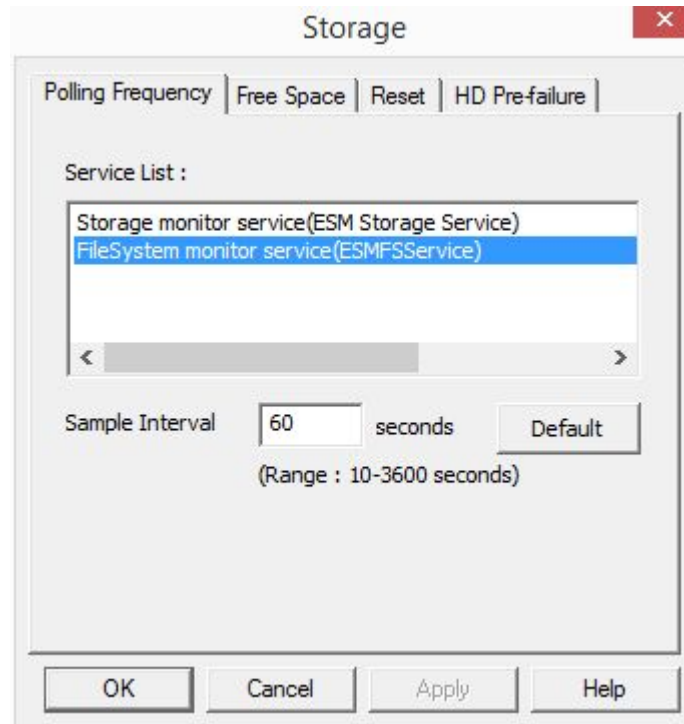
By default, the available capacity monitoring setting for such file systems is disabled.



#### 6.1.9.4 Changing the Monitoring Interval

The monitoring interval for file system available capacity monitoring can be changed to any value. Do so in the ESMPRO/ServerAgent control panel.

Item	Default	Available Setting Range
File System Monitoring Interval	60 sec.	10–3,600 sec.



**Figure 42 ESMPRO/ServerAgent Control Panel  
“Storage Monitoring” → “Monitoring Interval” Tab**



The Services List will not appear when services are halted.

## 6.1.10 SCSI/IDE Device Monitoring

Device configuration management and hard disk preventative maintenance can be performed on devices such as hard disks and CD-ROMs connected to the server using a SCSI or IDE interface, using ESMPRO/ServerManager and ServerAgent.

### 6.1.10.1 The SCSI/IDE Device Monitoring Feature

The SCSI/IDE device monitoring feature can perform configuration management of SCSI or IDE devices (including hard disks, CD-ROMs and tape backup devices) connected to the server. In addition, preventative maintenance can be performed to protect against faults with the hard disk preventative maintenance feature. SCSI and IDE device configurations and hard disk preventative maintenance diagnostic information can be referenced from the ESMPRO/ServerManager web console. Note that the condition of SCSI and IDE devices (their operating status) cannot be monitored.

**Table 19 Monitoring SCSI and IDE Devices**

Device Type	Configuration Management	Condition Monitoring	Preventative Maintenance
Hard Disk	Yes	No	Yes
CD-ROM (DVD-ROM)	Yes	No	No
Tape Device	Yes	No	No
Optical Memory Device	Yes	No	No
Other Devices	Yes	No	No



When it is a disk array, even if it is a SCSI or IDE device, the monitoring required is different than that offered by ESMPRO/ServerManager and ServerAgent for single unit devices. For disk arrays, see section 6.1.11 Disk Array Monitoring.



#### **Monitoring for Devices using Connections other than SCSI and IDE**

Storage monitoring is not performed on storage devices using connections other than SCSI and IDE, such as USB.



#### **DVD-ROM Monitoring**

DVD-ROM devices appear in the web console under the storage tree as CD-ROM devices.

## 1. Hard Disk Information

Detailed information specific to hard disks can be found in the hard disk preventative maintenance feature's diagnostic information.



### The Hard Disk Preventative Maintenance Feature

Hard disk preventative maintenance determines whether there are issues with the continued use of a hard disk. When a hard disk issue is detected with the hard disk preventative maintenance feature, ESMPRO/ServerAgent sends an alert to ESMPRO/ServerManager. Since it will be possible to identify a hard disk before it becomes unusable by a high frequency of errors as reported with hard disk preventative maintenance, it will be possible to implement workarounds such as the replacement of such hard disks before critical faults occur.

ESMPRO/ServerAgent confirms the error occurrence status for a hard disk using the hard disk's Self-monitoring, Analysis and Reporting Technology (SMART) feature. SMART manages data specific to hard disk faults on the respective hard disk, and when it determines that a critical fault is imminent, the hard disk itself issues an alarm. Respective hard disk vendors use thresholds appropriate to their own hard disks to determine preventative maintenance.

## 2. Interface-type Information (SCSI and IDE Information)

This is information displayed for all types of devices. The information displayed varies depending on the interface in use. Primarily, the following types of information can be referenced: connection status, including target ID, and the vendor, model, and serial number, etc.

Item	Value
Drive	Master
Controller Index	4
Vendor/Model	MATSHITADVD-RAM UJ8A0AS
Revision	1.00
Serial Number	

Figure 43 “Storage” → “CD-ROM” → “IDE Information” in the Web Console



The “Resource Information” found in “Storage” → “Controllers” → “SCSI Controller” in the ESMPRO/ServerManager web console, is displayed incorrectly for the x64 Edition. For “Resource Information”, check the system information and/or device manager for the target server.

### 6.1.10.2 Using SCSI/IDE Device Monitoring

The following describes the procedures specific to SCSI/IDE device monitoring, including how to check faults and change settings.

## 1. Checking Alerts

While the system is running, check whether alerts indicative of diagnostic errors from hard disk preventative maintenance have appeared in ESMPRO/ServerManager's Alert Viewer.

Sample Alert when a Hard Disk Preventative Maintenance Fault Occurs

S.M.A.R.T. predicts that your hard disk is going to fail.  
Address(Controller-Bus-ID-LUN):1-0-4-1  
HardDisk[2]:NEC HD0001 REV01

When diagnostic errors from hard disk preventative maintenance are detected, they can be confirmed not only with alerts, but also with the web console. When an error is detected, the status color of the icon in the hard disk's general information screen changes to that of a warning (yellow).

The icons for the hard disk general information indicate the diagnostic status of hard disk preventative maintenance.



(Normal): Normal status.

(Warning): Diagnostic fault detected for hard disk preventative maintenance.

## 2. SCSI/IDE Device Monitoring Settings

Settings for SCSI/IDE device monitoring can be changed either in the ESMPRO/ServerManager web console or in the ESMPRO/ServerAgent control panel.

### 2.1 Changing the Hard Disk Preventative Maintenance Threshold

By default, hard disk preventative maintenance is enabled. Since this feature is necessary to maintain the reliability of hard disks, do not disable it.

The threshold used for hard disk preventative maintenance (the SMART feature) is set to an appropriate value for each hard disk by the vendor, and, as such, cannot be changed.



When you enable or disable hard disk preventative maintenance, it is applicable to all hard disks. It is not possible to change the setting for individual hard disks.

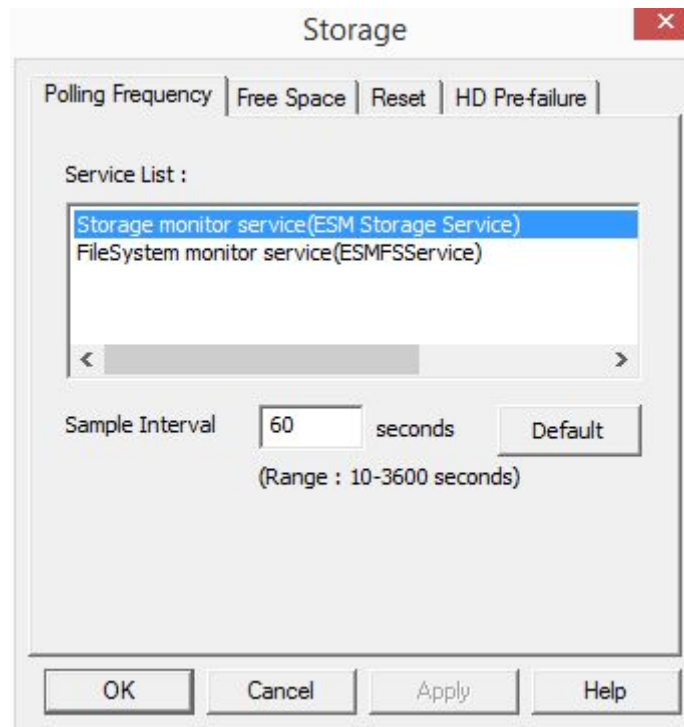
### 2.2 Changing the Monitoring Interval

The monitoring interval for SCSI/IDE device monitoring can be changed to any value. Change the

monitoring interval from the ESMPRO/ServerAgent control panel.

**Table 20 SCSI/IDE Device Monitoring Interval**

Item	Default	Available Setting Range
SCSI/IDE Device Monitoring	60 sec.	10 to 3,600 sec.



**Figure 44 “Storage Monitoring” → “Monitoring Interval” Tab in the ESMPRO/ServerAgent Control Panel**

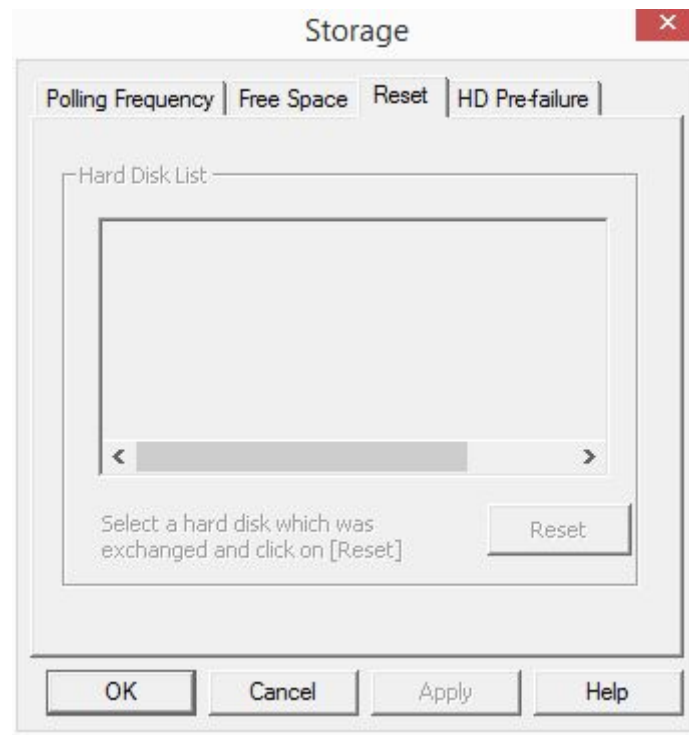


The Services List will not appear when services are halted.

### 3. Resetting SCSI/IDE Device Management Information

ESMPRO/ServerAgent manages the condition of the hard disk as it performs hard disk preventative maintenance. It is therefore necessary to manually reset hard disk management information upon hard disk replacement.

Reset management information using the ESMPRO/ServerAgent control panel.



**Figure 45 ESMPRO/ServerAgent Control Panel**



When the status color is that of a warning under “Storage” → “Hard Disks” → “General Information” → “Preventative Maintenance Information” in the ESMPRO/ServerManager web console, it will remain that way until a manual reset.

Always reset the management information upon hard disk replacement.

#### 6.1.11 Disk Array Monitoring

The condition of a disk array can be monitored with the installation of a Universal RAID Utility or a server that can be managed with an LSI SMI-S provider. For more information on disk array monitoring, see the topics on RAID management in Chapter 8.

#### 6.1.12 LAN Network Monitoring

The packets sent and received by a server can be monitored using ESMPRO/ServerManager and ServerAgent. Use packet monitoring to detect line faults, heavy line loads, and server resource insufficiencies.

### 6.1.12.1 The LAN Monitoring Feature

When ESMPRO/ServerAgent detects an issue specific to the LAN, an alert is sent to ESMPRO/ServerManager and at the same time an event is registered in the event log (or in syslog for Linux) for the system for the target server (that which ESMPRO/ServerAgent is operating).

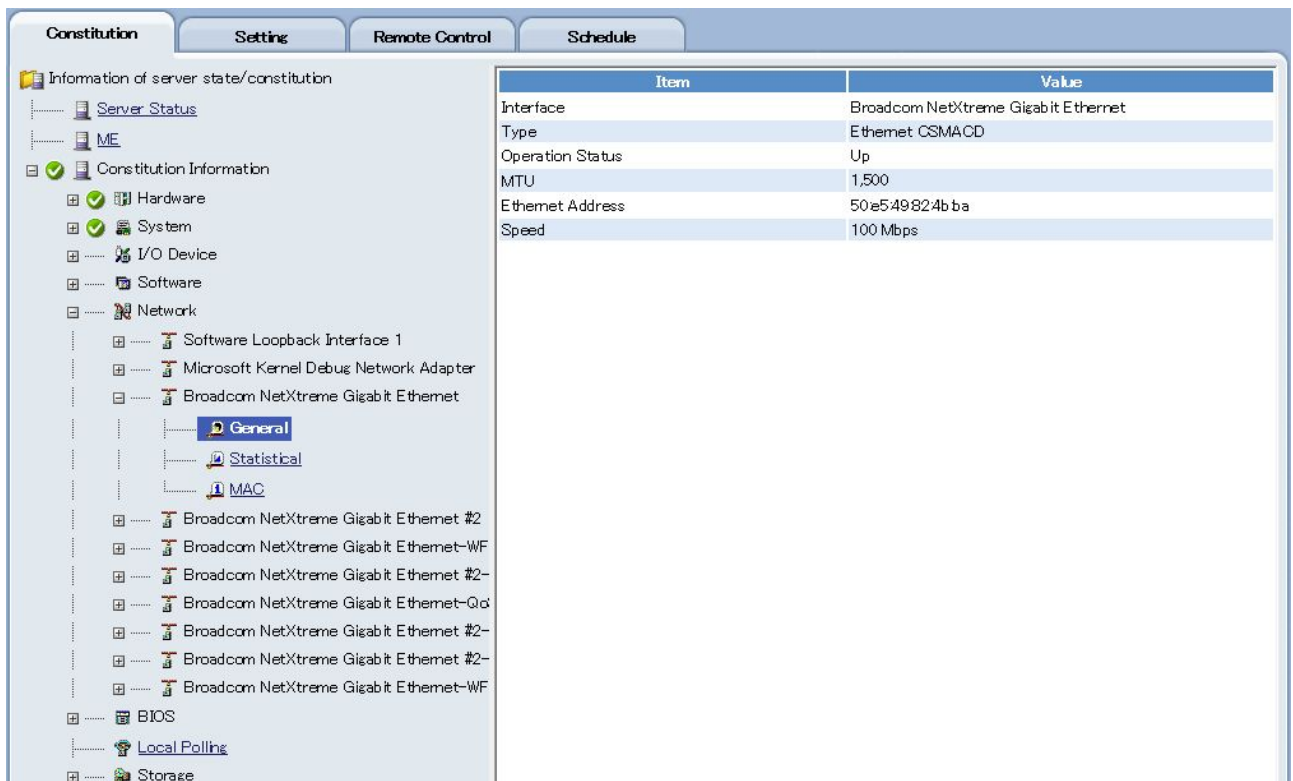


Figure 46 LAN Monitoring Feature



LAN monitoring cannot detect a link disconnection for a NIC.

### 6.1.12.2 Using LAN Monitoring

The following describes the procedures specific to LAN monitoring, including how to check faults and change settings.

#### Checking Network Faults

When a fault specific to the LAN occurs, ESMPRO/ServerAgent sends an alert to ESMPRO/ServerManager and an event is registered in the event log (or in syslog for Linux) for the system of the managed server. Check in the ESMPRO/ServerManager Alert Viewer or in the event log for the system of the managed server to see whether an event related to the LAN has been registered.

With LAN monitoring, when there are many corrupted packets and/or packet errors occurring per unit of time (the monitoring interval), it is determined that a fault has occurred on the network, and the following events are registered to the event log. Refer to the content of the event log to narrow down the cause.

It is a percentage of the number of packets sent and received during a monitoring interval that determine faults specific to the LAN, so there will be times when events are registered for temporary issues, such as short-term increases in the load. There is no issue when, after an event is registered, it is immediately

resolved. You will need to check the network environment (including the hardware) and/or consider re-distributing the load when recovery does not occur or when events occur frequently.

#### Sample Alerts when there is a Fault in the Line

A Network Hardware failure may have occurred. Device: \Device\E190x1 Error No.: 1  
Alignment Errors = 5 FCS Errors = 0 Carrier Sense Errors = 0

Alert when, of the received packets within the monitoring interval, the percentage of those with an alignment error (whose packet length is not a multiple of eight) exceeds a set value (the threshold: line fault).

A Network Hardware failure may have occurred. Device: \Device\E190x1 Error No.: 2  
Alignment Errors = 0 FCS Errors = 16 Carrier Sense Errors = 0

Alert when, of the received packets within the monitoring period, the percentage of those with an FCS error (where the error was detected with the checksum) exceeds a set value (the threshold: line fault).

A Network Hardware failure may have occurred. Device: \Device\E190x1 Error No.: 3  
Alignment Errors = 0 FCS Errors = 0 Carrier Sense Errors = 39

Alert when, of the sent packets within the monitoring interval, the percentage of those with a carrier sense error (the carrier sense could not be detected during the send) exceeds a set value (the threshold: line fault).

Network is under heavy load. Device: \Device\E190x1 Error No.: 1 Total Transmitted  
Packets = 57 Late Collisions = 9 Single-Collisions = 1 Multiple-Collisions = 6 Delayed  
Frames = 2 Excess Collisions = 0 MAC transmitted Errors = 0

Alert when, of the received packets within the monitoring period, the percentage of those for which either a collision or delay occurred (taking the sum of collision delays, unitary collisions, multiple collisions and delayed sends) exceeds a set value (the threshold: send retries).

Network is under heavy load. Device: \Device\E190x1 Error No.: 2 Total Transmitted  
Packets = 15 Late Collisions = 0 Single-Collisions = 0 Multiple-Collisions = 0 Delayed  
Frames = 0 Excess Collisions = 1 MAC transmitted Errors = 3

Alert when, of the received packets within the monitoring period, the percentage of those for which the packet was corrupt as a result of excessive collisions (taking the sum of the number of excessive collisions and the number of MAC send errors) exceeds a set value (the threshold: send aborts).



In addition, should the following be registered, it is possible that the network settings are incorrect. Review the manual again.

SNMP Service does not accept a request

This is registered when there is no response from the SNMP service during service initialization. Review the SNMP service settings.

## Settings for LAN Monitoring

By default, LAN monitoring is not enabled. Change the settings in the ESMPRO/ServerAgent control panel to enable LAN monitoring.

Once LAN monitoring is enabled, there should basically be no need to modify the thresholds for determining network status, but they can be set to any arbitrary value.

### Changing LAN Monitoring Thresholds

Change the thresholds from the ESMPRO/ServerAgent control panel.

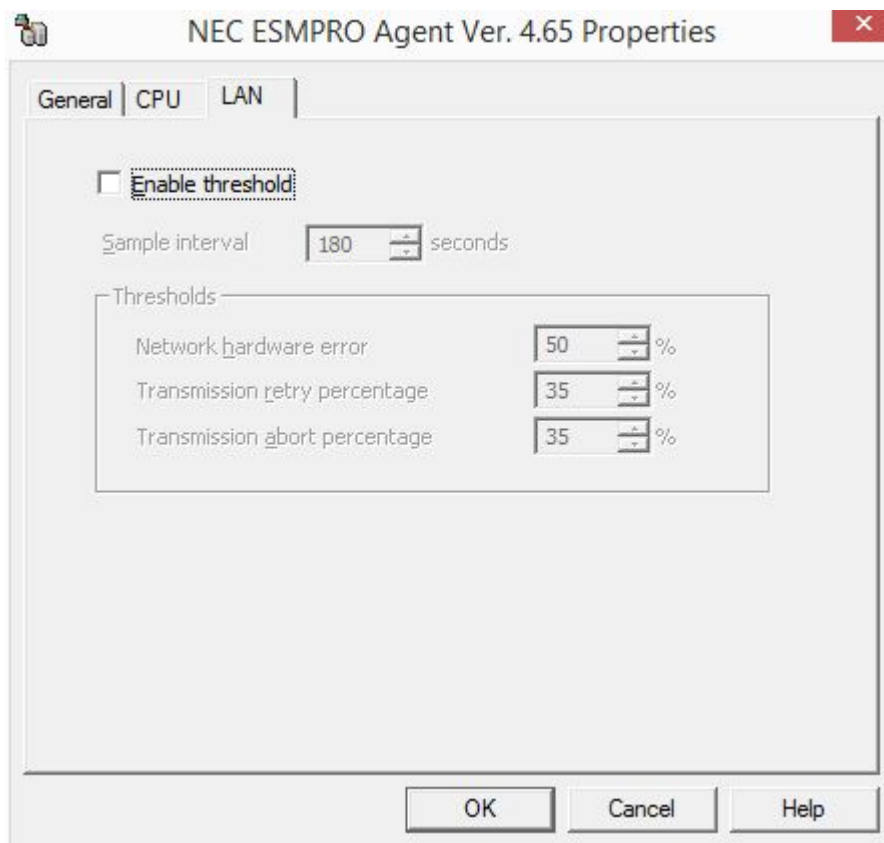


Figure 47 LAN Tab in the ESMPRO/ServerAgent Control Panel

### Threshold Defaults

Line Fault Occurrence Rate:	50% (0 to 100%) Set this to a larger value when line fault alerts occur frequently and they are ignorable.
Send Retry Occurrence Rate:	35% (10 to 50%) Set this to a larger value when, in either instance, heavy

Send Abort Occurrence  
Rate:

line load alerts occur frequently and they are ignorable.  
35% (10 to 50%)  
Set this to a larger value when, in either instance, heavy  
line load alerts occur frequently and they are ignorable.

### **Changing the LAN Monitoring Interval**

By default, the LAN monitoring interval is 180 seconds.

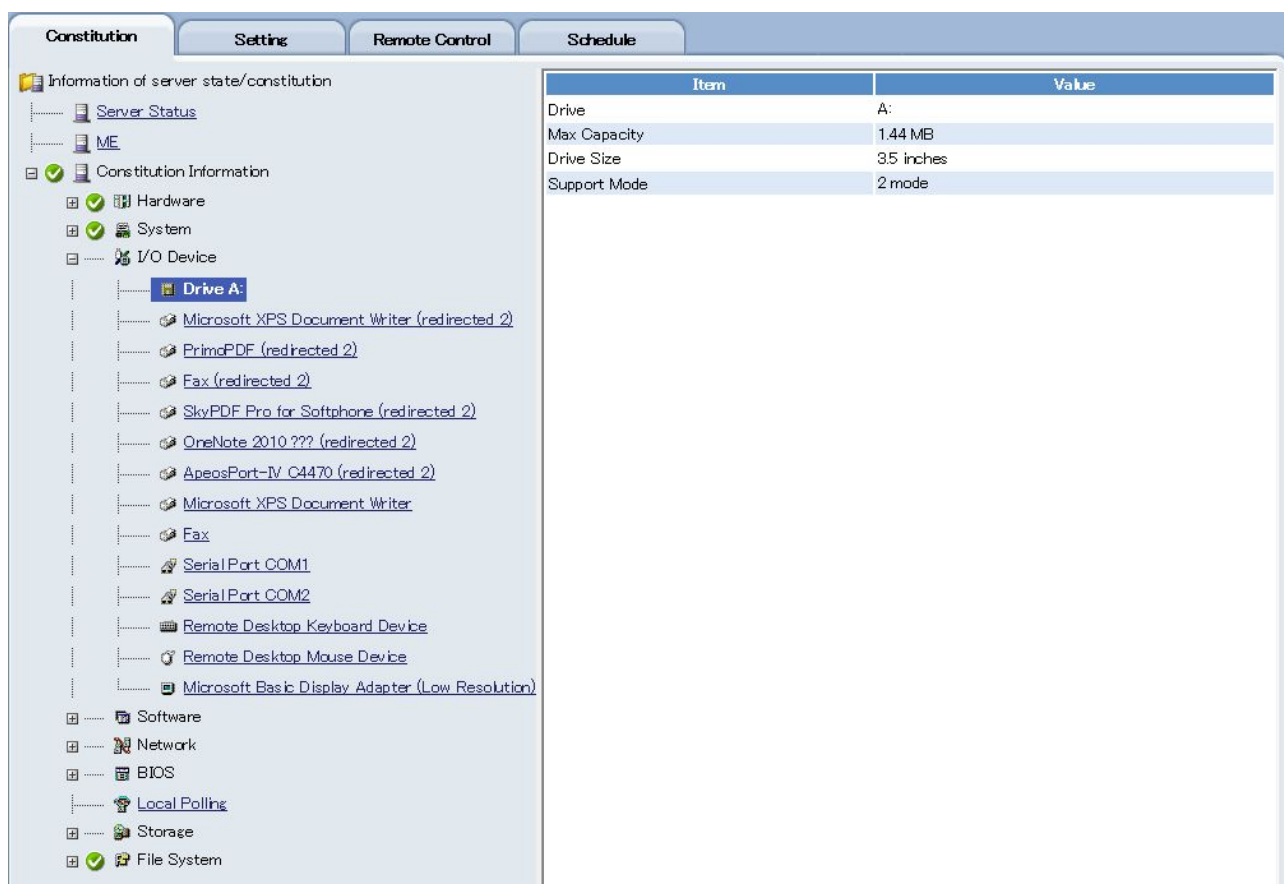
That setting can be changed to any value within the range of 1 to 3,600 seconds.

### 6.1.13 System Information Referencing

Information specific to the system environment, including information on I/O devices, software (services, drivers, operating systems), the BIOS (system, video and SCSI BIOS) and device information (including the CPU and system board) can be referenced using ESM/ServerManager and ServerAgent.

#### 6.1.13.1 Referencing I/O Device Information

Use the web console to select the desired I/O device under “I/O Devices” when referencing I/O device information from ESM/ServerManager. Information on I/O devices (floppy disk drives, serial ports, parallel ports, keyboards and mice) can be referenced.

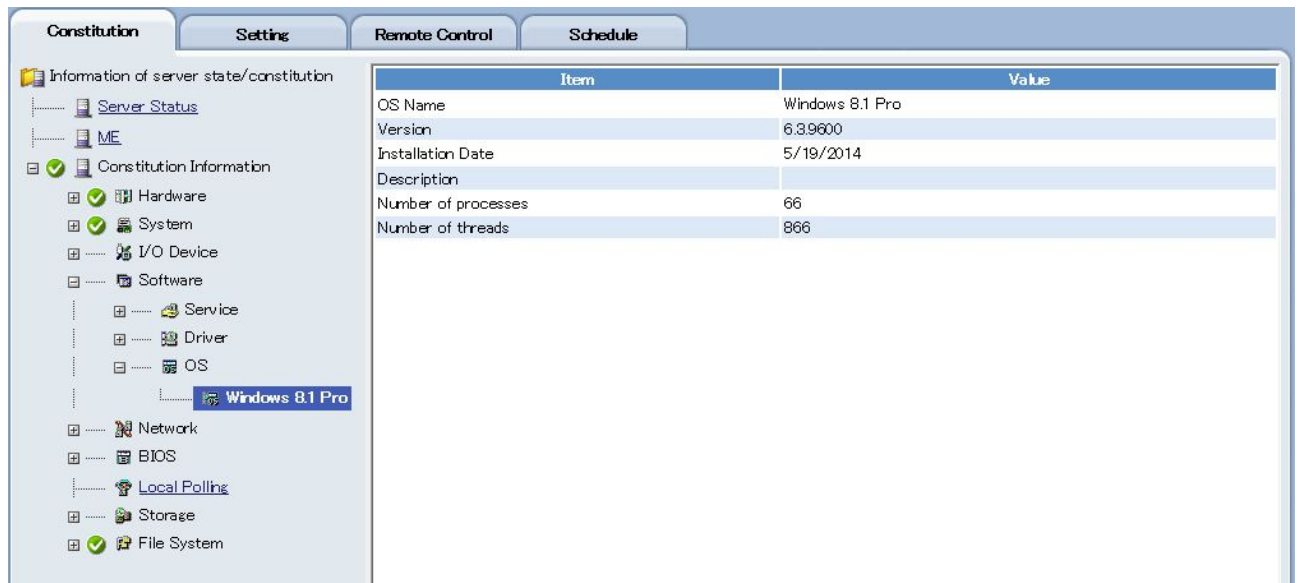


Item	Value
Drive	A:
Max Capacity	1.44 MB
Drive Size	3.5 inches
Support Mode	2 mode

Figure 48 “I/O Devices” → “Floppy Disk” in the Web Console

### 6.1.13.2 Referencing Software Information

Use the web console to make the desired selection under “Software” when referencing software information from ESM/ServerManager. The respective software information can be referenced.



The screenshot shows the 'Constitution' tab in the web console. Under 'Information of server state/constitution', the 'Software' item is expanded. The 'OS' item is selected, showing the following details:

Item	Value
OS Name	Windows 8.1 Pro
Version	6.3.9600
Installation Date	5/19/2014
Description	
Number of processes	66
Number of threads	866

**Figure 49 Software → OS, in the Web Console**

### 6.1.13.3 Referencing BIOS Information

Use the web console to select the desired BIOS under “BIOS” when referencing BIOS information from ESM/ServerManager. The respective BIOS information can be referenced.



The screenshot shows the 'Constitution' tab in the web console. Under 'Information of server state/constitution', the 'BIOS' item is expanded. The 'American Megatrends Inc.' item is selected, showing the following details:

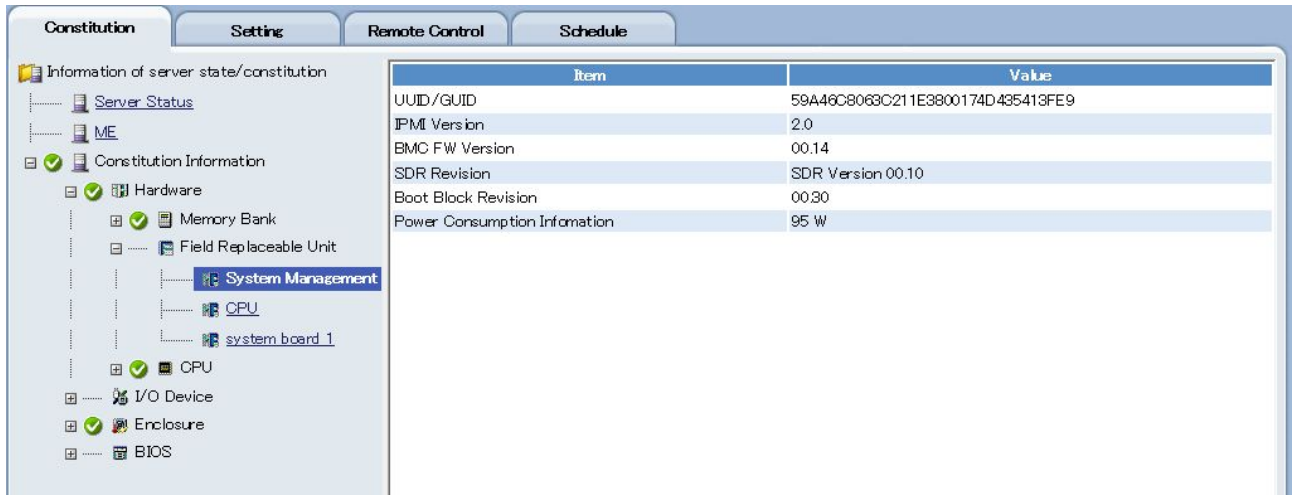
Item	Value
Type	Other
Manufacturer	American Megatrends Inc.
Version	4.6.0088
Release Date	11/04/2011
Size	16,384 KB
Start Address	f000h

**Figure 50 “BIOS” in the Web Console**

#### 6.1.13.4 Referencing Device Information

Use the web console to select the desired device information under “Hardware” → “Device Information”, when referencing device information from ESMPRO/ServerManager. The respective device information can be referenced.

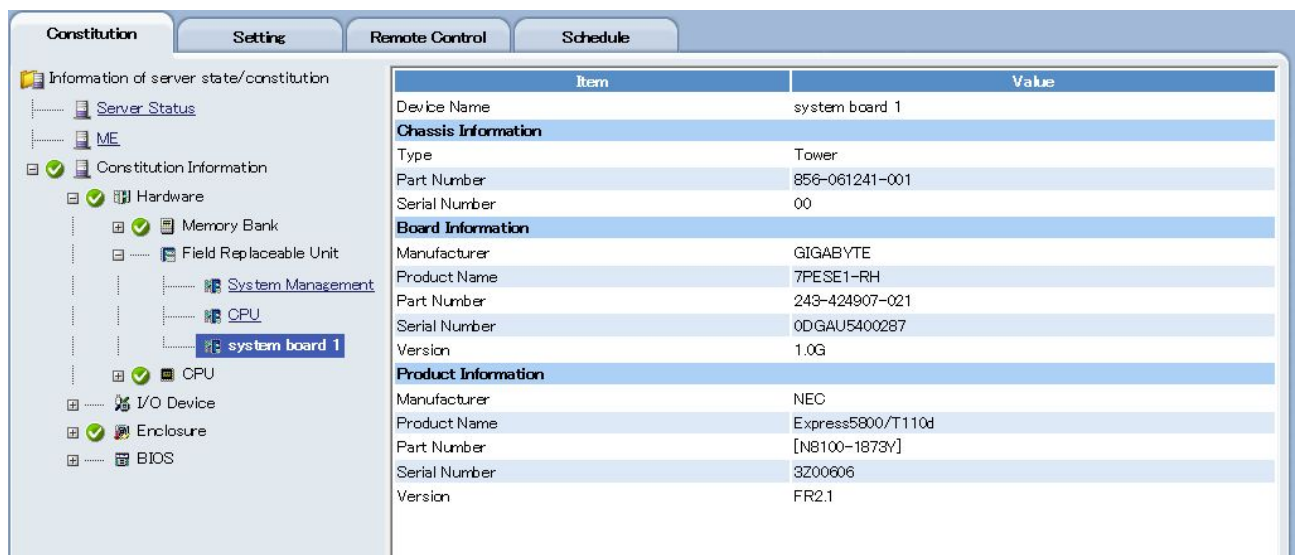
NOTE: The information that can be referenced for a device will vary by model.



The screenshot shows the 'Constitution' tab in the web console. The left sidebar displays a tree view with 'System Management' selected under 'Hardware'. The main panel shows a table of system information.

Item	Value
UUID/GUID	59A46C8063C211E3800174D435413FE9
IPMI Version	2.0
BMC FW Version	00.14
SDR Revision	SDR Version 00.10
Boot Block Revision	00.20
Power Consumption Information	95 W

Figure 51 “Device Information” → “System Management” in the Web Console



The screenshot shows the 'Constitution' tab in the web console. The left sidebar displays a tree view with 'system board 1' selected under 'System Management'. The main panel shows a table of device information.

Item	Value
Device Name	system board 1
<b>Chassis Information</b>	
Type	Tower
Part Number	856-061241-001
Serial Number	00
<b>Board Information</b>	
Manufacturer	GIGABYTE
Product Name	7PESE1-RH
Part Number	243-424907-021
Serial Number	0DGAU5400287
Version	1.0G
<b>Product Information</b>	
Manufacturer	NEC
Product Name	Express5800/T110d
Part Number	[N8100-1873Y]
Serial Number	3Z00606
Version	FR2.1

Figure 52 “Device Information” → “System Board” in the Web Console

### 6.1.14 Referencing Errors Detected at the Hardware Level

ESMPRO/ServerAgent and ServerManager offer the ESRAS utility, which can reference log information for events and errors detected at the hardware level, information specific to hardware system sensors, and information for field replaceable units.

With the use of the ESRAS utility, it is possible to detect faults related to general hardware issues and confirm the occurrence of hardware-level errors (such as power supply unit failures), enabling post-occurrence investigations and system diagnostics.

#### 6.1.14.1 The ESRAS Utility Feature

The ESRAS utility displays log information recorded in dedicated memory (NVRAM) on board the Express unit or the server management board. With models that support IPMI (Intelligent Platform Management Interface), the standard interface for hardware information, the recorded log information can be displayed via IPMI.

The ESRAS utility automatically recognizes and displays features specific to supported hardware information for target servers.



The ESRAS utility cannot display information for servers that support neither NVRAM nor IPMI.



The ESRAS utility is not provided in NEC ESMPRO ServerAgentService environment as the standard equipment.

## 1. NVRAM Information

### Displaying the Software Log

Displays log information for memory, critical and system errors.

Memory Error	Displays information for correctable errors detected/recorded during memory checks at, for example, the BIOS level (single-bit errors) and uncorrectable errors (multiple-bit errors).
Critical Error	Displays log information for critical errors (i.e., temperature or fan faults) that could lead to system errors.
System Error	Displays log information for OS system error messages (panic messages).

### Displaying the Hardware Log

Displays information on faults that occurred in the console device.

Register information is recorded when a system error (panic) occurs.

### Displaying the Server Management Extended Log

Greater detail for the hardware fault information and event log can be detected using a device with a server management board implemented.

### Managing NVRAM Log Information

Backs up and initializes log information recorded to the console device's NVRAM or the server sensing board or management board's NVRAM.

This backup data is effective when performing fault investigations.

## 2. IPMI Information

---

### Displaying IPMI Information

Displays system event logs (SEL) from local and networked computers, sensor data records (SDR), information for field replaceable units (FRU), management controller information (IPMI version information) and system current accumulation time.

SEL	Displays events and errors detected by the system and its sensors. This log is necessary for identifying causes after faults occur and for recovery work.
SDR	Displays information specific to hardware system sensors, the type of FRU information, and information on data storage positions. Information unique to sensors, such as thresholds, can be confirmed, depending on the information.
FRU Information	Displays replaceable modules that can be used by system maintenance personnel, or component information.
Management Controller Information (IPMI Version Information)	Displays the latest information for the connected target management machine, and the IPMI version information for backed up files.
System Current Accumulation Time	Displays the amount of current that has accumulated in the system until now. Only displays the latest information.

### Backing up IPMI Information

Backs up IPMI information to a file.

Backups can occur from either a local or a networked computer.

Backups encompass the SEL, the SDR, the FRU information, and management controller information (IPMI version information).

This backup data is effective when performing fault investigations.

### Displaying Backed Up IPMI Information

Loads and displays backed up IPMI information.

Displayed information encompasses the SEL, the SDR, the FRU information, and management controller information (IPMI version information).



The IPMI information backup file created with the ESRAS utility **is compatible with** backup files from the following software, and **can be referenced therein**.

- Offline Maintenance Utilities
- EzClct Viewer
- ESMPRO/ServerManager Ver.6

### 6.1.15 Event Monitoring

NEC ESMPRO Agent and NEC ESMPRO ServerAgentService can alert NEC ESMPRO Manager to the content of faults through the monitoring and detecting of various faults (events) that occur on the server. By default, NEC ESMPRO Agent is set to monitor and alert for events that lead to critical faults, but it is possible, depending on the system environment, to add or delete monitored events. Monitored events can be managed in the tree view of the Alert Manager Settings tool.

#### 6.1.15.1 The Event Monitoring Feature

##### 1. Types of Events that can be Monitored

---

The following two types of events can be monitored with NEC ESMPRO Agent and NEC ESMPRO ServerAgentService.

##### Event Log/Syslog

With Windows, the standard system event log is monitored.

Monitoring constantly tracks the registering of events based on the event's source name and event ID. When a target event is registered to the event log, that content is alerted to ESMPRO/ServerManager.

The default monitored events are set as the standard Windows service error events and the events registered to the ESMPRO products.

It is possible, depending on the system environment, to add or delete monitored events.



It is also possible to monitor events registered to applications other than NEC ESMPRO Agent and NEC ESMPRO ServerAgentService.

With Linux, the standard system syslog is monitored.

When a set keyword is recorded in the syslog, an alert is sent to ESMPRO/ServerManager. This monitored syslog cannot be changed from `/var/log/messages`.

##### NEC ESMPRO Agent, NEC ESMPRO ServerAgentService Events

Events that are monitored uniquely by NEC ESMPRO Agent, NEC ESMPRO ServerAgentService.

There are two types of NEC ESMPRO Agent or NEC ESMPRO ServerAgentService events: events that trigger an alert based on changes to server status resulting from a threshold determination, and events that trigger an alert based on some kind of fault.



It is only possible to turn the alerts for NEC ESMPRO Agent or NEC ESMPRO ServerAgentService events on and off. They cannot be added or deleted.

#### 6.1.15.2 Using Event Monitoring

##### 1. Adding and Deleting Monitored Events

---

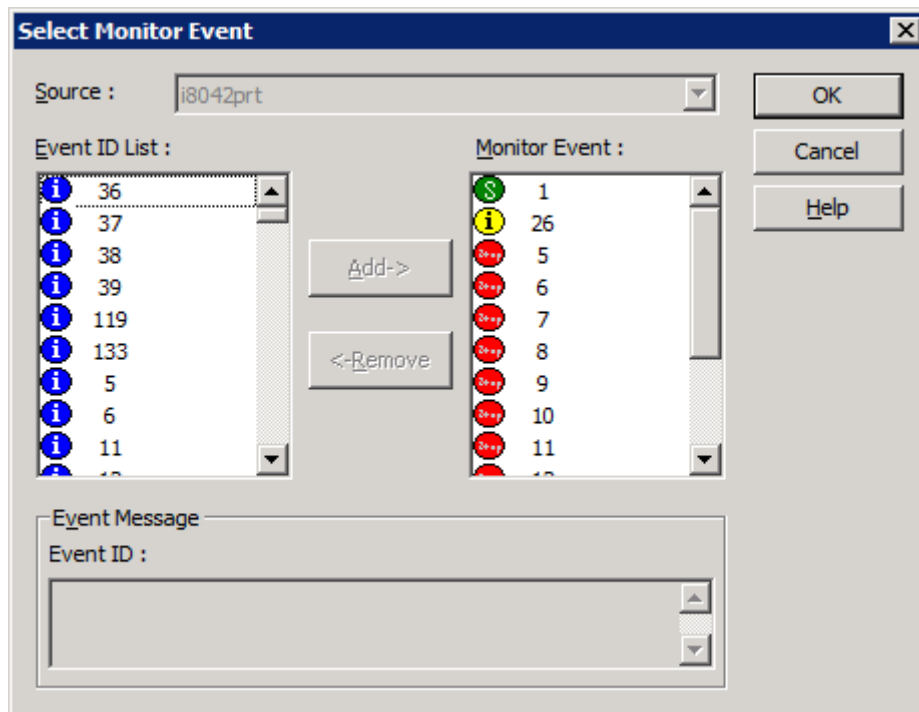
Once a monitored event is specified, other monitored events can be added or deleted.

##### Procedure

1. Launch the Alert Manager's setting tools.



2. Switch to the tree of the event to configure (event log, Agent event).
3. In the tree, select the source name you wish to monitor, and right-click.  
Select "Select Monitor Event" from the context menu.
4. The "Select Monitor Event" dialog box will appear. Activate the event you wish to monitor.



**Figure 53 Alert Manager Setting Tools and "Select Monitor Event" Dialog Box**

## 2. Configuring Alert Content for Monitored Events

---

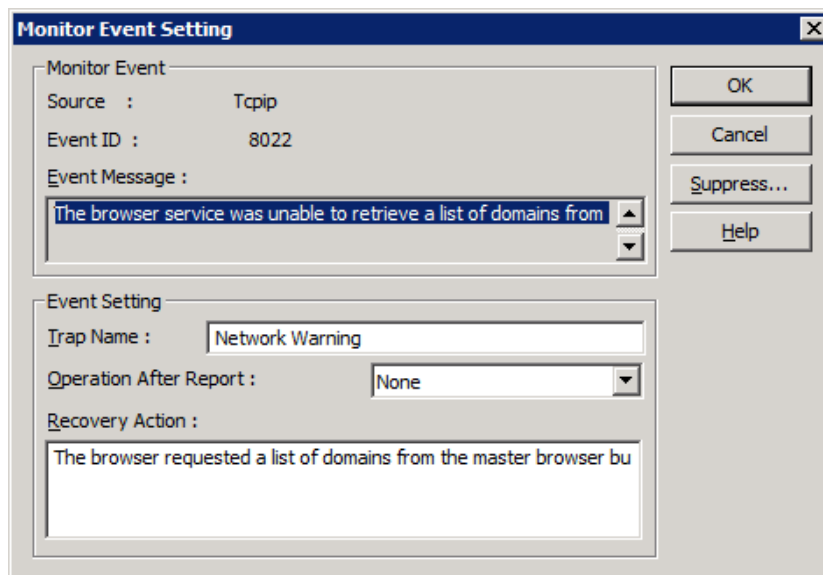
When monitored events are configured, alert content per event can be configured as well.



Configurable items include the drive name, post-alert action, and the recommendation. The information configured here will be displayed as the alert content in the Alert Viewer. The post-alert action indicates the operation that should occur after the event occurs; the three choices to select from are: *shutdown*, *reboot* and *do nothing*.

### Procedure

1. Launch the Alert Manager setting tools.
2. Switch to the tree view of the event you wish to configure (**Event Log, Agent Event**).
3. In the tree, select the source name you wish to monitor, and right-click.  
Select “Monitor Event Setting” from the context menu.
4. The “Monitor Event Setting” dialog box will appear. Set the alert content.



**Figure 54 Configure a Monitor Event Setting Dialog Box**

### 3. Configuring Monitored Event Alert Suppression

---

When ESMPRO/ServerAgent works in conjunction with WebSAM AlertManager it becomes possible to suppress alerts at the monitored event level.

There are two ways to suppress alerts: *time-based suppression* and *suppression based on number of occurrences*. Combining those two enables you to issue alerts only if specific conditions are met when identical events are detected, and to suppress identical alerts when they are unnecessary.



Time-based suppression suppresses alerts for the same events detected within a specified time. Suppression based on number of occurrences sends alerts for the same events when detected within a specified time. The two suppression methods can be set in combination.



Suppression of alerts cannot be limited to just ESMPRO/ServerAgent. Alerts are sent out for all detected monitored events.

#### Procedure

1. Launch the Alert Manager setting tools.
2. Switch to the tree view of the event you wish to configure ("Event Log", "Agent Event").
3. In the tree, select the source name you wish to monitor, and right-click.  
Select "Configure a Monitored Event" from the context menu.
4. The "Configure a Monitored Event" dialog box will appear. Click the "Suppress Alerts" button.
5. The "Suppress Alerts" dialog box will appear. Set the desired suppression methods.

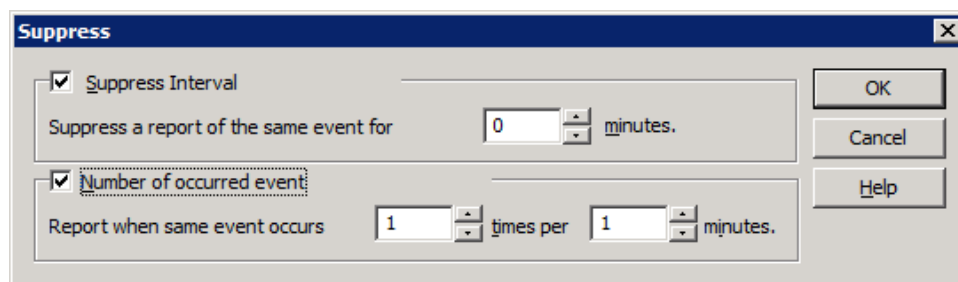
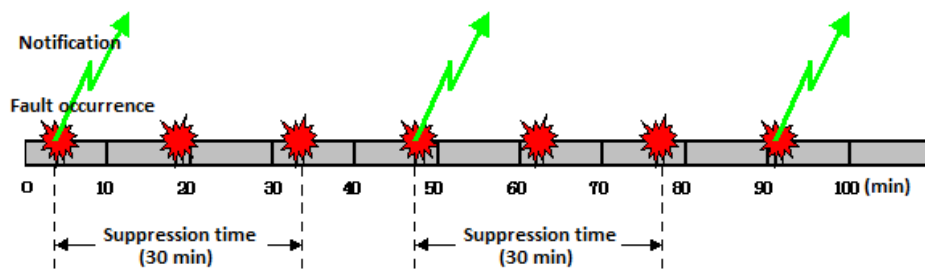


Figure 55 Suppress Alerts Dialog Box

## Sample Settings

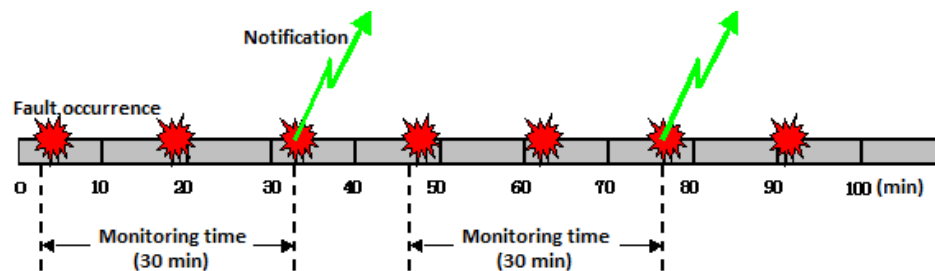
alerts event



Suppress for the same within a specified (30-minute) timeframe.

Once an alert occurs, no alert will occur if the same event is detected within the suppression timeframe (30 minutes). Alerts resume after the suppression timeframe has elapsed.

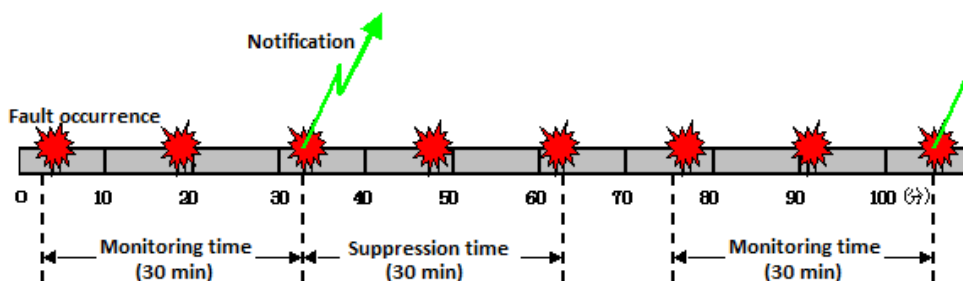
**Issue an alert if the same event occurs for the specified number of times (three times) within a specified (30-minute) timeframe.**



Issue an alert when the same event is detected for the specified number of times (three times) within the specified (30-minute) timeframe.

Subsequently, issue alerts for the same event for the specified number of times within the specified timeframe.

**Issue an alert if an event occurs for the specified number of times (three times) within a specified (30-minute) timeframe, and then suppress alerts for a specified (30-minute) timeframe.**



Issue an alert when the same event is detected for the specified number of times (three times) within the specified (30-minute) timeframe.

Once an alert occurs, no alert will occur if the same event is detected within the suppression timeframe (30 minutes). Once the suppression timeframe has elapsed, issue alerts for events detected for the specified number of times within the specified timeframe once more.

### 6.1.16 Stall Monitoring

System stall monitoring is possible using ESMPRO/ServerManager and ServerAgent (if the server is supported by NEC ESMPRO Agent) or Server Configuration Utility (if the server is supported by NEC ESMPRO ServerAgentService). Use stall monitoring to minimize server downtime when system stalls occur and impact on your business when running fully automated systems.

#### 6.1.16.1 The Stall Monitoring Feature

Stall monitoring monitors the operational status of the OS by regularly updating the watchdog timer (the timer for software stall monitoring) installed in the server with the server management driver.

When a timer update fails because there has been no response due to an OS stall, the timer times out, and the action that is pre-set to occur for a timeout is executed.



Stall monitoring is unsupported in environments using the VMware ESX 3.x / VMware ESX 4.x OpenIPMI driver.

#### 6.1.16.2 Using Stall Monitoring

The following describes the procedures specific to stall monitoring, including how to check faults and how to change settings.

##### 1. Checking System Stalls

---

While the system is running the watchdog time monitors the system for stalls. When a stall occurs, the stall occurrence is detected after the system launches, and an alert is sent to ESMPRO/ServerManager. Check whether an alert specific to stalls has arrived in ESMPRO/ServerManager's Alert Viewer.

##### Sample Alert when the Watchdog Timer Times Out

Time out of Watch Dog Timer has occurred.



In some instances, the sending of an alert immediately after a system launch may fail. When this happens, the alert notification will be delayed by the number of minutes set for the retry interval configured in the Alert Manager Settings Tool.

##### 2. Settings for Stall Monitoring

---

Stall monitoring is activated from the moment NEC ESMPRO Agent (if the server is supported by NEC ESMPRO Agent) is installed or Server Configuration Utility (if the server is supported by ESMPRO ServerAgentService) is installed; monitoring is set to be constant.

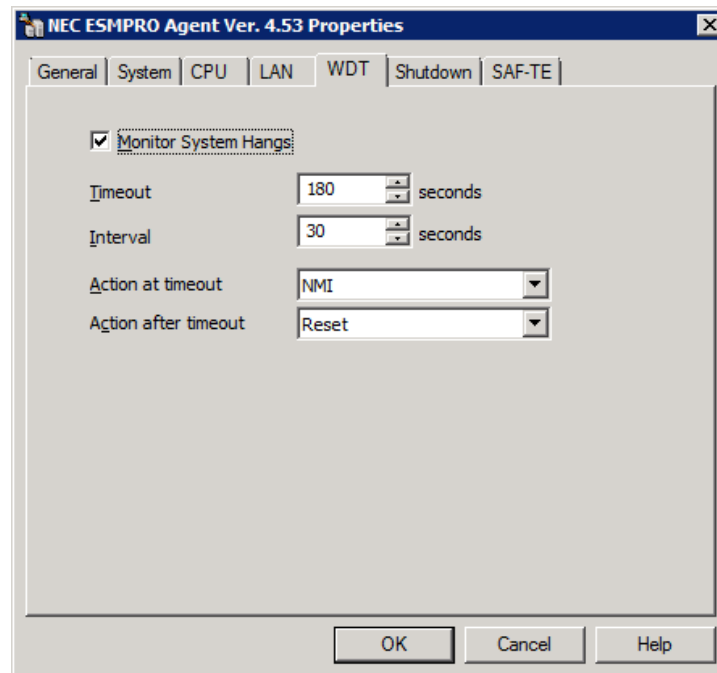
Under normal conditions, there is no need to modify the settings for the stall monitoring feature.

#### Activating/Deactivating Stall Monitoring

Use the ESMPRO/ServerAgent control panel or Server Configuration Utility to activate or deactivate stall monitoring.



When activating or deactivating stall monitoring on a model that does not support IPMI, the system will need to be restarted.



**Figure 56 ESMPRO/ServerAgent Control Panel's WDT Tab**

### Changing the Stall Monitor Action Settings

For servers that support IPMI, more advanced settings are possible, beyond simply activating and deactivating stall monitoring.

It is possible to configure the timeout time, the update interval, the action at timeout and the action after timeout in the ESMPRO/ServerAgent control panel or Server Configuration Utility.

### Default Threshold Values

Timeout Time	90 or 180 (a value appropriate to the model is set)
Update Interval	30
Action at Timeout	NMI
Action after Timeout	Reset



## Timeout Time

Specifies the time in seconds at which it is determined that the system has stalled.

## Update Interval

Specifies the interval in seconds at which the timeout timer is updated.

E.g., when the timeout time is 90 seconds and the update interval is 30 seconds, the time at which it will be determined that a stall has occurred will be between 60 and 90 seconds.

## Action at Timeout

Selects the action at timeout. Once the following action selection occurs, the action after timeout occurs.

None	Does nothing.
NMI	Triggers a STOP error.

## Action after Timeout

Selects the recovery method after timeout.

System	When the action at timeout is set to <i>NMI</i> , operated in conjunction with the content set in "Recovery" in the "Launch/Shutdown" tab of the "System" control panel. Should another timeout occur in conditions where it is impossible to perform memory dump collection, the memory dump will be collected when debug information is to be written out as specified in the "System" tab of the control panel, and the system will relaunch after a reset when it is specified to automatically relaunch.
Reset	When the action at timeout is set to <i>None</i> , no recovery action will occur. The system will remain in the stalled state, When the action at timeout is set to <i>NMI</i> , when a stall occurs, a STOP error is triggered, and the system resets and relauches after memory dump collection. Should another timeout occur in conditions where it is impossible to perform memory dump collection, the system will relaunch after a reset.
Power Cycle	When set to <i>None</i> , the system will reset and attempt to relaunch. When the action at timeout is set to <i>NMI</i> , when a stall occurs, a STOP error is triggered and the system resets and relauches after memory dump collection. Should another timeout occur in conditions where it is impossible to perform memory dump collection, the system will relaunch after a power cycle.
Power Cut	When set to <i>None</i> , the power will be turned off, and then immediately turned back on again. When the action at timeout is set to <i>NMI</i> , when a stall occurs, a STOP error is triggered and the system resets and relauches after memory dump collection. Should another timeout occur in conditions where it is impossible to perform memory dump collection, the power will be turned off. When set to <i>None</i> , system power will be turned off.

### 6.1.17 System Error (Panic) Detection

It is possible to detect when panics occur using ESMPRO/ServerManager and ServerAgent.

#### 6.1.17.1 The System Error Detection Feature

When a panic occurs in the system, ESMPRO/ServerAgent automatically detects the occurrence of a system error at the first system launch after the panic, and then sends an alert to ESMPRO/ServerManager.

#### 6.1.17.2 Using System Error Detection

The following describes the procedures specific to system error detection, including how to check faults and change settings.

## 1. Checking System Error Faults

---

ESMPRO/ServerAgent detects system errors at system launch. When a system error is detected, an alert is sent to ESMPRO/ServerManager. Check using the ESMPRO/ServerManager Alert Viewer whether any alerts specific to system errors have arrived.

### Sample Alert when a System Error Occurs

Alert generation time : Saturday, February 4, 2012 19:41 (+09:00)  
This is the event which occurred between this system start-up and the last system stop or system shutdown.

#### System Error Information

Time:02/04/2012 19:37:26

Dump Switch:OFF

Message:

\*\*\* STOP: 0x69696969

(0x00000000,0x00000000,0x00000000,0x00000000)



In some instances, the sending of an alert immediately after a system launch may fail. When this happens, the alert notification will be delayed by the number of minutes set for the retry interval configured in the Alert Manager Settings Tool.

## 2. Settings for System Error Monitoring

---

The system error monitoring feature constantly monitors for system errors. It cannot be turned off.



## 6.1.18 Shutdown Monitoring

It is possible to monitor whether shutdowns occurred normally using ESMPRO/ServerManager and ServerAgent (if the server is supported by NEC ESMPRO Agent) or Server Configuration utility (if the server is supported by NEC ESMPRO ServerAgentService).

### 6.1.18.1 The Shutdown Monitoring Feature

Shutdown monitoring monitors the time from the start of the shutdown process to the point the power turns off, using the updating by the server management driver of the watchdog timer (the timer used for monitoring software stalls) that comes with the server.

When the watchdog timer fails to be updated, the timer times out, and it is determined that the OS is stopped, at which point the action set in Action at Timeout is taken. Subsequently, the action set in Action after Timeout is taken.



Shutdown monitoring is not supported in environments using the OpenIPMI driver of Linux / VMware ESX 3.x / VMware ESX 4.x.

### 6.1.18.2 Using Shutdown Monitoring

The following describes the procedures specific to shutdown monitoring, including how to check faults and change settings.

#### 1. Checking Shutdown Faults

---

Shutdown stalls are monitored with the watchdog time during the execution of a shutdown. When a stall occurs during a shutdown process, the stall is detected after the system relaunches and an alert is sent to ESMPRO/ServerManager. Check using the ESMPRO/ServerManager Alert Viewer whether any alerts specific to shutdown stalls have arrived.

#### Sample Alert when the Watchdog Timer has Timed Out

Time out of Watch Dog Timer has occurred.



In some instances, the sending of an alert immediately after a system launch may fail. When this happens, the alert notification will be delayed by the number of minutes set for the retry interval configured in the Alert Manager Settings Tool.

## 2. Settings for Shutdown Monitoring

### Activating/Deactivating Shutdown Monitoring

Settings for shutdown monitoring can be changed in the NEC ESMPRO Agent control panel (if the server is supported by NEC ESMPRO Agent) or Server Configuration Utility (if the server is supported by NEC ESMPRO ServerAgentService).

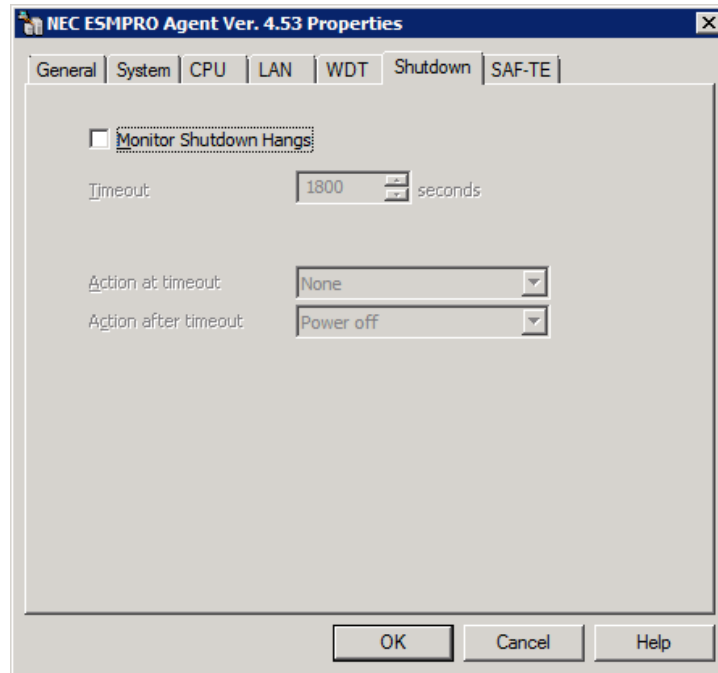


Figure 57 ESMPRO/ServerAgent Control Panel, Shutdown Tab

### Changing the Shutdown Monitoring Action Settings

Among the settings that can be changed in the ESMPRO/ServerAgent control panel or Server Configuration Utility are the timeout time, action at timeout, and action after timeout. The changes that can be made are that same as those that are indicated in section 3.16, Stall Monitoring.

#### Default Threshold Values

Timeout Time	1800
Action at Timeout	None
Action after Timeout	Power Cut



When performing shutdown monitoring, all shutdown processes will be monitored. When you have AP that use shutdowns that are not accompanied by OS relaunches or turning off of power, either extend the timeout time, or turn monitoring off.

### 6.1.19 Monitoring of PCI Hot-plugging

ESMPRO/ServerManager and ServerAgent support dynamic configuration changes to the system using PCI hot-plugging.

#### 6.1.19.1 The PCI Hot-plugging Monitoring Feature

ESMPRO/ServerAgent automatically detects a PCI hot-plugging event when one occurs on the system, and sends an alert to ESMPRO/ServerManager.

#### 6.1.19.2 Using PCI Hot-plugging Monitoring

The following is a description of how to check the detection of PCI hot-plugging events.

##### 1. Checking the Occurrence of PCI Hot-plugging Events

ESMPRO/ServerAgent automatically detects the occurrence of PCI hot-plugging events, and sends alerts to ESMPRO/ServerManager.

Review the content of alerts in the ESMPRO/ServerManager Alert Viewer.

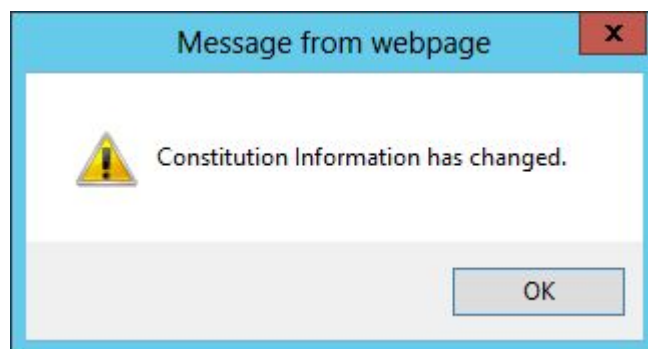
#### Sample Alert at the Occurrence of a PCI Hot-plugging Event

New device has been connected to the slot or the connector device.

Either the slot or connector power has been off, or device has been removed.

#### 6.1.19.3 Operations when Detecting PCI Hot-plugging

The following message is displayed in the ESMPRO/ServerManager web console when the occurrence of a PCI hot-plugging event is detected. The message prompts the user to rebuild the web console tree.



**Figure 58 Web Console Tree Rebuild Request**

Select "OK" to rebuild the web console tree, reflecting configuration changes to the system as a result of the PCI hot-plugging event.

## 6.1.20 Local Polling

Use of the local polling feature enables alerts from threshold settings and threshold monitoring even when there is no threshold setting button.



### Local Polling

Indicates a feature to monitor any item (only for integer values) not supported by the web console's GUI. It is called *local polling* because monitoring occurs within ESMPRO/ServerAgent (locally), based on the configured information. Configurations can be made to suit the system environment, setting thresholds and reflecting server status colors, and triggering alerts. Specific knowledge for configurations and MIB information for the monitored items will be necessary, however.

## 1. Using Local Polling

1. Open the web console.
2. From the tree view, select the server for which local polling is to be configured.
3. Select the "Settings" tab, select *Unregistered*, and click the "Edit" button.
4. Enter the MIB object ID under *Items* in the "Local Polling Settings" dialog box.  
If necessary, you can select an object ID from a preset list by clicking the "Object ID List" button.
5. Select *Enabled* for the monitoring option.
6. Configure values for "Monitoring Period", "Monitoring Interval", "(Threshold) Maximum", "(Threshold) Minimum", "Upper Threshold" and "Lower Threshold".
7. Click the "Apply" button to complete the settings process.

Item Name	Setup Value
<b>Monitoring Setting</b>	
Object ID [required]	1.3.6.1.4.1.119.2.2.4.4.16.2.2.2.1.0 Object ID List
Monitoring	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Monitoring Period	<input checked="" type="checkbox"/> Indefinite Period
Monitoring Duration [required]	1 seconds
<b>Threshold Setting</b>	
Max [required]	2147483647
Min [required]	-2147483648
<b>Upper Threshold</b> * Lower Threshold < Warning Reset Threshold < Warning Threshold < Fatal Reset Threshold < Fatal Threshold <= Max	
Trap Sending	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Fatal Threshold [required]	3
Reset Threshold (error) [required]	2
Warning Threshold [required]	1
Reset Threshold (warning) [required]	0
<b>Lower Threshold</b> * Min <= Fatal Threshold < Fatal Reset Threshold < Warning Threshold < Warning Reset Threshold < Upper Threshold	
Trap Sending	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Reset Threshold (warning) [required]	-1
Warning Threshold [required]	-2
Reset Threshold (error) [required]	-3
Fatal Threshold [required]	-4
Apply Cancel	

Figure 59 Local Polling in the Web Console

Upper and lower values can be set for monitored items with local polling. For example, since an appropriate range of values is needed for temperature monitoring, an upper and lower value would be set. But for CPU loads, for example, a fault would only be recognized when in excess of a certain load rate, so only an upper value would be set.

NOTE: Upper (and lower) values result in faults and warnings when they are exceeded (or fall below them), and the status is changed.

Upper (and lower) release values restore the fault or warning determination when they are exceeded (or fall below them).

8. The *Perform Polling* checkbox sets whether to perform polling for this MIB. When checked, the configured values are enabled at the polling interval.



When another SNMP-related product is installed on the server (e.g., an SNMP agent), MIBs defined by that product can be monitored using the same method as described above.

However, when specifying the object ID in the “Local Polling Settings” dialog box, it will be necessary to have identified in advance what MIBs are defined for that product. That is product-specific knowledge.

E.g., monitoring a database engine with SNMP agent features using ESMPRO/ServerManager.

### 6.1.21 Alive Monitoring

ESMPRO/ServerManager regularly communicates with managed servers (to the OS or SNMP service or BMC), and when a fault occurs on a managed server and communication ceases, ESMPRO/ServerManager changes the display of the managed server's status icon, and immediately alerts a manager of the fault. It is also possible to register an alert in the Alert Viewer when a fault occurs.



When ESMPRO/ServerAgent detects the fault as well, the display of the managed server's status icon will change, depending on the severity of the fault.

#### 6.1.21.1 The Alive Monitoring Feature

The following two methods are used for ESMPRO/ServerManager's Alive monitoring.

1. Regularly access the WS-Man service running on the OS for the managed server, and confirm whether the correct value is obtained. (Using Alive monitoring (WS-Man))
2. Regularly access the SNMP service running on the OS for the managed server, and confirm whether the correct value is obtained. (Using Alive monitoring (SNMP))
3. Regularly send an ICMP packet (ping) to the OS for the managed server, and confirm whether there was a response. (Using Alive monitoring (Ping))

When ESMPRO/ServerManager detects that communication with the managed server has ceased, the following alerts are registered to the alert viewer.

##### 1. Sample Alert Registered during Alive Monitoring (WS-Man)

The server doesn't respond to the WS-Management communication from Manager.  
There is the possibility that the service necessary to the WS-Management communication is down or the network doesn't operate normally between the manager and the server.

##### 2. Sample Alert Registered during Alive Monitoring (SNMP)

The SNMP service doesn't respond to SNMP request from Manager.  
There is the possibility that the SNMP service stopped, or the network doesn't operate normally between the manager and the server.

##### 3. Sample Alert Registered during Alive Monitoring (Ping)

The server doesn't respond to Ping request from Manager. There is the possibility that the server is down or the network doesn't operate normally between the manager and the server.



Alive monitoring (Ping) is disabled by default.



By default, the registration of alerts for Alive monitoring (WS-Man) and Alive monitoring (SNMP) and alive monitoring (Ping) are disabled.

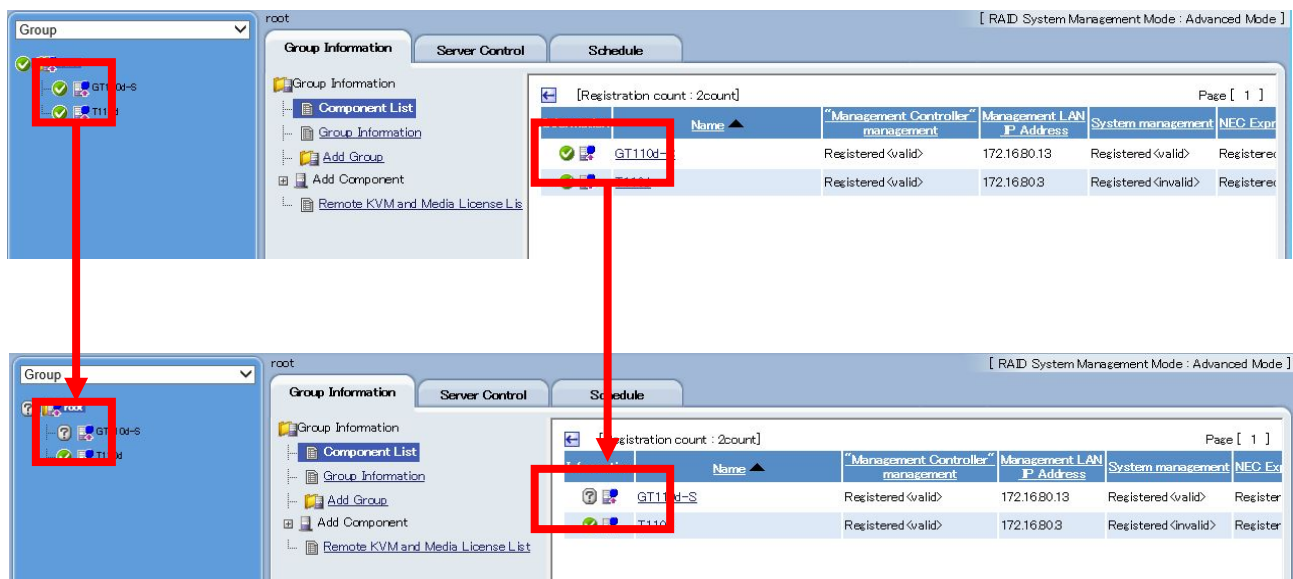
### 6.1.21.2 Using Alive Monitoring

The following describes the procedures specific to alive monitoring, including how to check faults and change settings.

#### Checking Faults

With alive monitoring, when communication between ESMPRO/ServerManager and the managed server ceases, display of the relevant icon in ESMPRO/ServerManager will change to that of a question mark (?), and an event will be registered in Alert View.

When a fault occurs, begin by checking that service connecting the SNMP service for the managed server and ESMPRO/ServerAgent is operating correctly if the target is managed via SNMP. In addition, confirm that there are no issues for the network connection linking ESMPRO/ServerManager and ESMPRO/ServerAgent.



**Figure 60 Status Display when Communication has ceased**

There are times when temporary environmental factors, such as increases in CPU load for the managed OS, excessive disk access, or network load, can cause an alert to be registered. In such cases, alert registration can be suppressed by adjusting the number of retries in the alive monitoring settings. In addition, alert registration can be suppressed by setting an alert registration schedule when you have systems where servers are halted and relaunched on a regular basis at set times.

## Alive Monitoring Settings

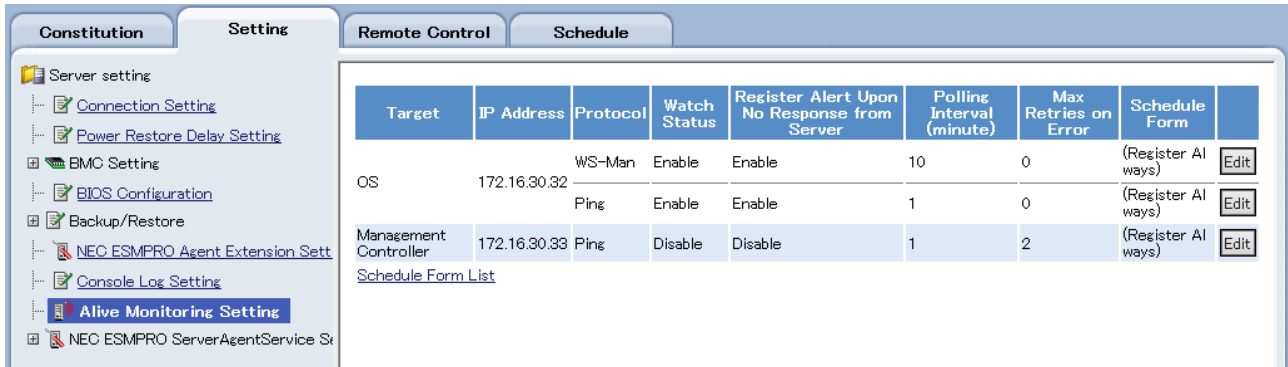


Figure 62 Alive Monitoring Settings(OS(WS-Man/Ping), Management Controller)

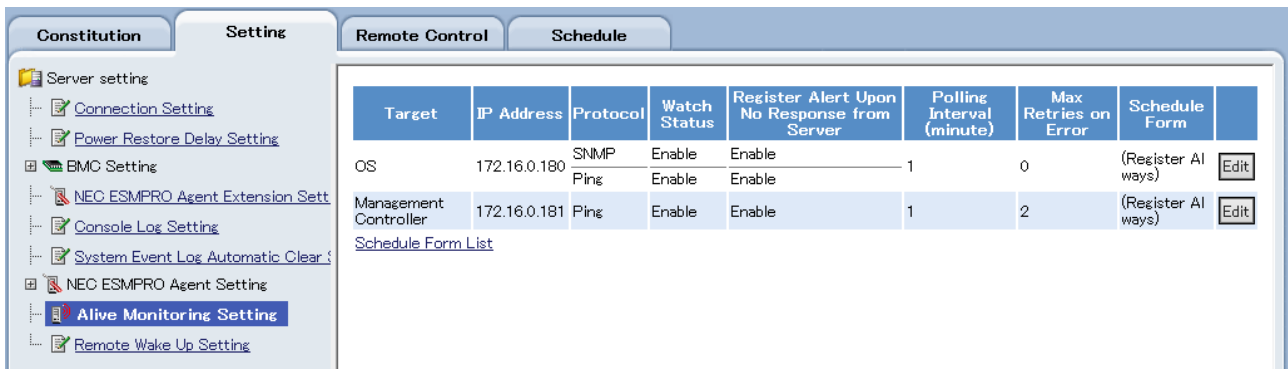


Figure 61 Alive Monitoring Settings(OS(SNMP/Ping), Management Controller)

By default, alive monitoring will not occur for managed servers. Separate settings are needed to enable alive monitoring. Those settings can be changed from the ESMPRO/ServerManager screen.

### 1) Enabling Alive Monitoring

Perform the settings from ESMPRO/ServerManager's server monitoring settings screen.

### Alive Monitoring (WS-Man)

When alive monitoring (WS-Man) is enabled, the status of monitored servers is regularly monitored with WS-Man. This is enabled by default.

### Alive Monitoring (SNMP)

When alive monitoring (SNMP) is enabled, the status of monitored servers is regularly monitored with SNMP. This is enabled by default.

### Registering Alerts for No Service Response

When this option is enabled, an event is registered in Alert Viewer when communication ceases between ESMPRO/ServerManager and ESMPRO/ServerAgent.

### Alive Monitoring (Ping)

When alive monitoring (ping) is enabled, the status of monitored servers is regularly monitored with pings. This is disabled by default.



## Registering Alerts for No Server Response

Enabling this option will register an event in Alert Viewer when there is no longer any ping response from a managed server.

### Default Settings

WS-Man Monitoring (Alive Monitoring)	Disabled
WS-Man Monitoring (Registering Alerts for No Server Response)	Disabled
SNMP Monitoring (Alive Monitoring)	Enabled
SNMP Monitoring (Registering Alerts for No Server Response)	Disabled
Ping Monitoring (Alive Monitoring)	Disabled
Ping Monitoring (Registering Alerts for No Server Response)	Disabled

### 2) Changing the Settings for Alive Monitoring

There is normally no need to change the following values, but the registration of alerts can be suppressed by adjusting the following parameters when environmental factors result in the intermittent registration of alerts.

### Changing the Number of Retries

Sets the number of retries that occur before an alert is registered for non-response from a service or server. The default is zero times, and an alert is registered as soon as response from a service or server fails. Setting this to two means that an alert will not be registered until two retries have occurred after a response from a service or server fails.



If the management target is BMC, the retry count is set to 2 by default..

### Changing the Monitoring Interval

The monitoring interval is set in minutes to confirm the status of devices that ESM/ServerManager is monitoring. The default is 10 minutes for WS-Man, and one minute for SNMP and Ping.

### Changing the Schedule

The use of schedule settings allows for the control of alert registrations when there is no response or a recovery detected from the device.

A schedule can be set in advance if, for example, servers are shutdown on a regular basis for operational purposes. This would suppress the registration of alerts.

### Default Settings

Number of Retries	2 times (When Alive Monitoring target is BMC) 0 time (Other than those above)
Monitoring Interval	10 minutes (WS-Man) 1 minute (SNMP and Ping)
Schedule	(Constant Registration)

## 6.2 System Management (VMware ESXi 5 or later)

By registering VMware ESXi 5 or later, which cannot use ESMPRO/ServerAgent, with ESMPRO/ServerManager, it becomes possible to display configuration information.

### 6.2.1 VMware ESXi 5 or later Monitoring

The following table compares items which can be monitored using ESMPRO/ServerAgent and using VMware ESXi 5 or later.

**Table 21 Items that can be monitored with VMware ESXi 5 or later**

Management Item	VMware ESXi 5 or later	(Reference) (*6) ServerAgent (VMware)
CPU Monitoring	Yes (*1)	Yes
Memory Monitoring	Yes (*1)	Yes
Temperature Monitoring	Yes (*2)	Yes
Fan Monitoring	Yes (*2)	Yes
Case Voltage Monitoring	Yes (*2)	Yes
Power Supply Unit Monitoring	Yes (*2)	Yes
Cooling Unit Monitoring	Yes (*2)	Yes
Case Cover Monitoring	Yes (*2)	Yes
File System Monitoring	Yes (*1) (*3)	Yes
SCSI/IDE Device Monitoring	Yes (*1)	Yes
Disk Array Monitoring	Yes (*5)	- (*7)
LAN Network Monitoring	No	Yes (*8)
Referencing System Information	No	Yes
Referencing Errors Detected at the Hardware Level	No	Yes
Event Monitoring	No	Yes
Stall Monitoring	No	Yes (*9)
System Error (Panic) Monitoring	No	Yes
Shutdown Monitoring	No	Yes (*9)
Monitoring of PCI Hot-plugging	No	Yes
Local Polling	No	Yes
Alive Monitoring	Yes (*4)	Yes

(\*1) No display of status information.

(\*2) Only for ESMPRO/ServerManager Version 5.73 and later, with devices with EXPRESSSCOPE Engine 3 installed, with the management controller feature enabled.

(\*3) Meant for data stores.

(\*4) Only ping monitoring is possible.

(\*5) The LSI SMI-S provider must be installed. See Chapter 8 RAID Management.

(\*6) See also Table 17 Items that can be monitored with the System Management Feature.

(\*7) Monitored using a Universal RAID Utility.

(\*8) Changes to the settings are needed; the default is set to *No monitoring*.

(\*9) Only supported when using a server management driver.



When VMware ESXi 5 or later is registered to ESM/ServerManager, the system management features are registered.



See the *ESM/ServerManager Version 6 Installation Guide* for more on how to register VMware ESXi 5 or later to ESM/ServerManager.

### 6.2.1.1 Referencing CPU Information

It is possible to confirm the VMware ESXi 5 or later CPU usage rate and name, etc., using ESM/ServerManager. It is possible to confirm the number of physical CPUs, the number of physical cores, whether hyperthreading is enabled, the CPU name and type, the clock cycles, and the usage rate for each logical CPU in the web console.



Threshold monitoring for CPU usage rates cannot be performed.



You can confirm the CPU usage rate for the host (VMware ESXi 5 or later). You cannot do so for any virtual machines.

Constitution		Setting	Remote Control	Schedule
Information of server state/constitution				
Server Status				
Constitution Information				
System				
CPU				
Memory				
Data Store				
Software Component				
Storage Device				
Network				
RAID System				
Item		Value		
Physical CPUs		1		
Physical Cores per CPU		6		
Hyper-Threading		Enable		
CPU Name		Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz		
Type		intel		
Speed		1.899 GHz		
CPU Usage (%)				
Total CPU		6.86 %		
CPU[1]		6.03 %		
CPU[2]		0.99 %		
CPU[3]		0.36 %		
CPU[4]		4.19 %		
CPU[5]		0.77 %		
CPU[6]		4.86 %		
CPU[7]		0.35 %		
CPU[8]		2.16 %		
CPU[9]		0.61 %		
CPU[10]		8.85 %		
CPU[11]		2.92 %		
CPU[12]		9.01 %		

Figure 63 “System” → “CPU” in the Web Console

### 6.2.1.2 Referencing Memory Information

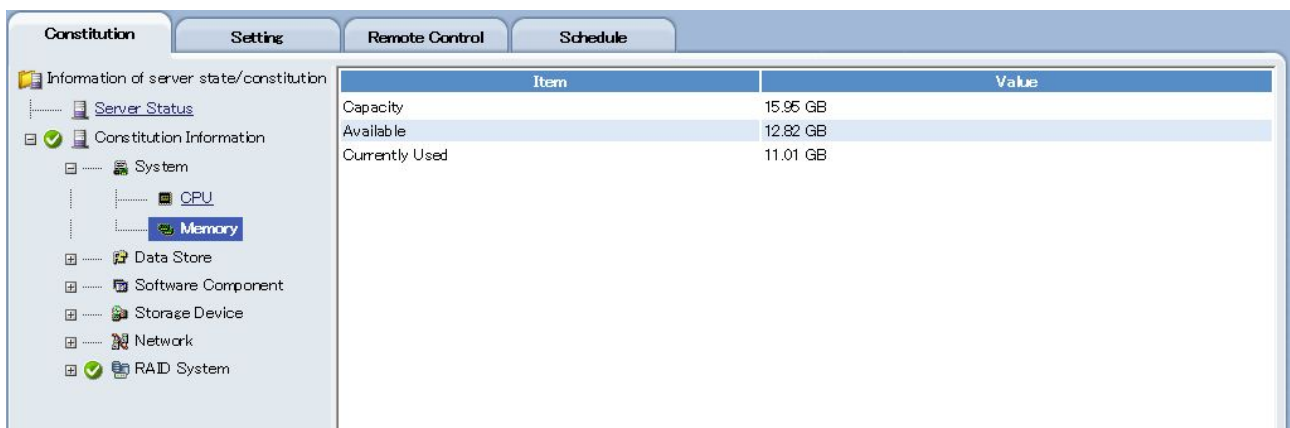
It is possible to confirm the amount of memory used for VMware ESXi 5 or later using ESM/PRO/ServerManager. It is possible to confirm the total amount of physical memory, the amount of available memory, and the amount in use, in the web console.



Threshold monitoring cannot be performed.



You can confirm memory information for the host (VMware ESXi 5 or later). You cannot confirm amounts of memory used by any virtual machines.



Item	Value
Capacity	15.95 GB
Available	12.82 GB
Currently Used	11.01 GB

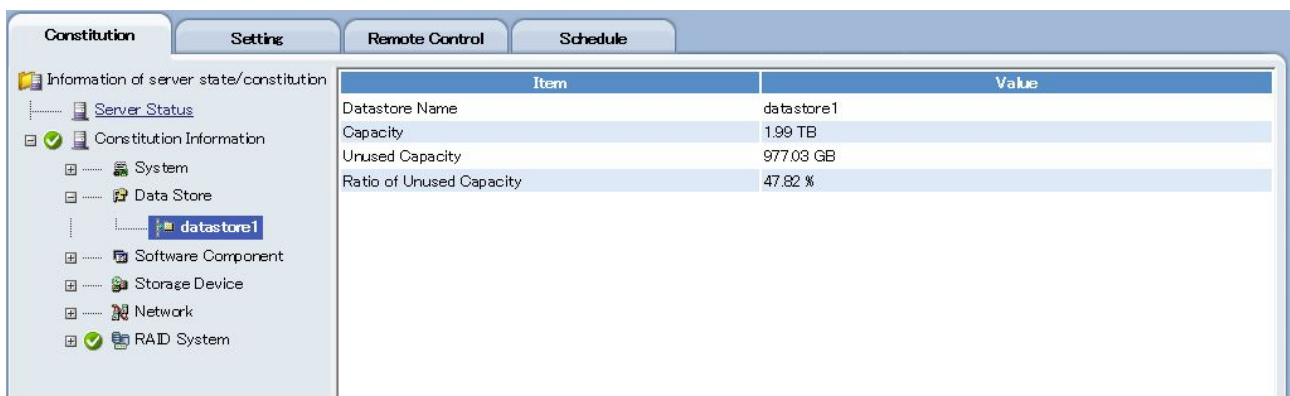
Figure 64 “System” → “Memory” in the Web Console

### 6.2.1.3 Referencing Data Stores

It is possible to confirm information for data stores managed by VMware ESXi 5 or later using ESM/PRO/ServerManager. It is possible to confirm the data store name, capacity, available capacity, and the ratio of available capacity, in the web console.



Threshold monitoring cannot be performed.



Item	Value
Datastore Name	datastore1
Capacity	1.99 TB
Unused Capacity	977.03 GB
Ratio of Unused Capacity	47.82 %

Figure 65 “Data Stores” in the Web Console

#### 6.2.1.4 Referencing Software Information

It is possible to reference information for software managed by VMware ESXi 5 or later using ESM/PRO/ServerManager. It is possible to reference the VMware ESXi 5 or later management information (description, manufacturer, and release date), the BIOS information and the driver information in the web console.



Figure 66 “Software Components” → “VMware ESXi” in the Web Console



Figure 67 “Software Components” → “System BIOS” in the Web Console

Constitution
Setting
Remote Control
Schedule

Information of server state/constitution

Server Status

Constitution Information

System
Data Store
Software Component

VMware ESXi
System BIOS
Driver

BMC Firmware (node 0) 4610000
Controller 500605B007282B80 (LSI MegaRAID SAS 9267-8i)
net-tx2
**esx-xserver**
scsi-megaraid-sas
sata-sata-promise
scsi-lps
net-e1000e
net-e1000
scsi-mptspi
ata-pata-hpt3x2n
net-s2b
esx-dvfilter-generic-fastpath
scsi-bfcB20

Item	Value
Description	X.Org Xserver and supporting libraries for OpenGL support.
Version	5.1.0-0.0.799733
Manufacturer	VMware
Release Date	2012-08-02 03:01:09(+00:00)
Install Date	2013-12-14 12:27:50(+00:00)

Figure 68 “Software Components” → “Drivers” in the Web Console

### 6.2.1.5 Referencing Storage Device Information

It is possible to confirm information for devices such as hard disks and CD-ROMs that connect to VMware ESXi 5 or later with a SCSI or IDE interface using ESM/ServerManager.

Item	Value
Driver Name	Local LSI Disk (naa.600605b007282b801a3e33d9156cab74)
Capacity	1.99 TB

Figure 69 “Storage Devices” in the Web Console

### 6.2.1.6 Referencing Network Information

It is possible to confirm information for networks managed with VMware ESXi 5 or later using ESM/ServerManager. It is possible to confirm the type, status, MTU, physical (MAC) address and speed (transfer speed) for NICs that connect to VMware ESXi 5 or later in the web console.

Item	Value
Type	Ethernet
Operation Status	OK
MTU	1500
Ethernet Address	74:D4:35:41:3F:DC
Speed	100.00 Mbps

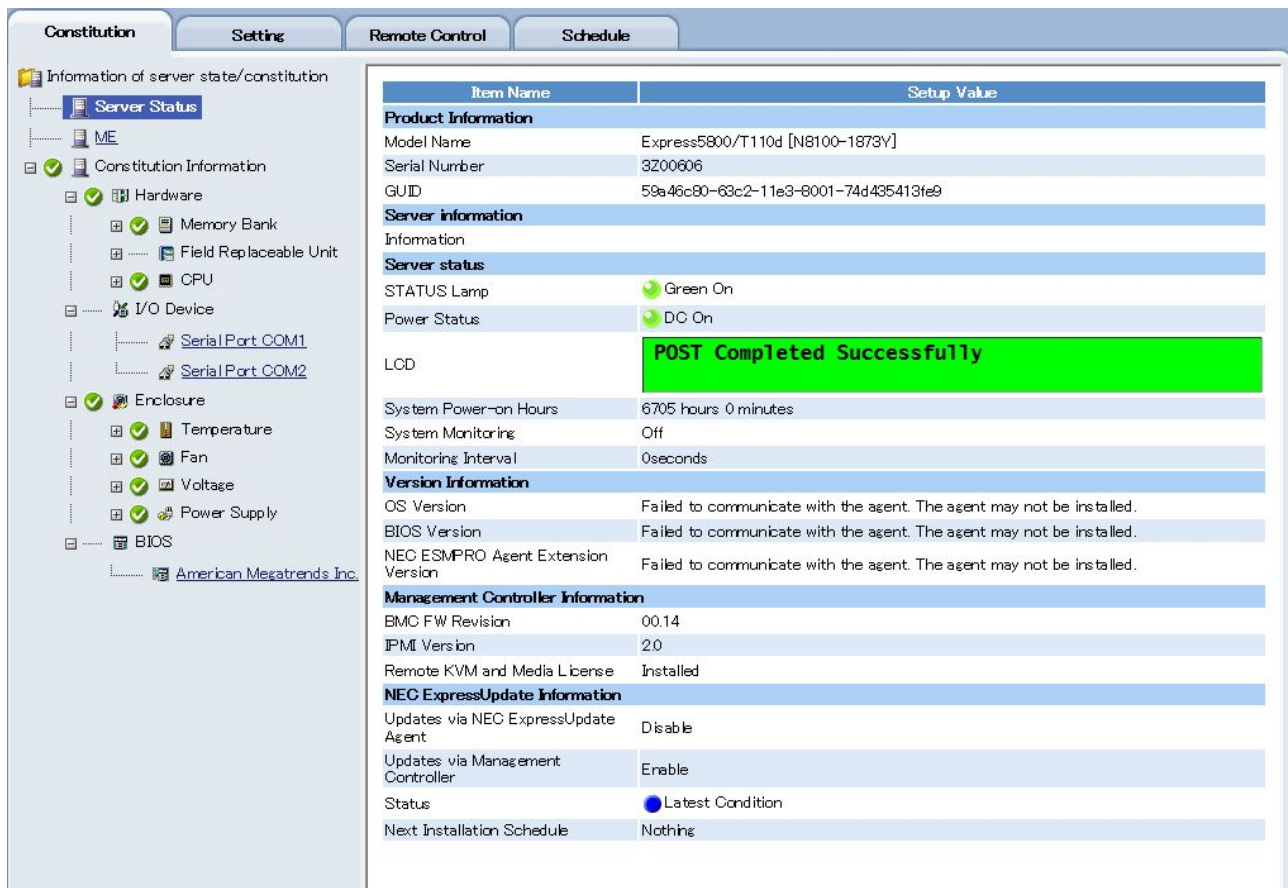
Figure 70 “Networks” in the Web Console

## 6.3 Management with the Management Controller

The following is a list of items that can be managed by connecting ESM/ServerManager with either EXPRESSSCOPE Engine 3 or vPro™, for devices on which ESM/ServerAgent is either not installed or is installed but not powered on.

**Table 22 Comparing EXPRESSSCOPE Engine 3 and vPro™**

Management Item	EXPRESSSCOPE Engine 3	vPro™
Virtual LCD	Yes	No
Status LED	Yes	No
Power Source Status	Yes	Yes
System Current Accumulation Time	Yes	No
System Monitoring	Yes	No
Configuration Information	Yes	Yes



**Figure 71 ESM/ServerManager Web Console**

### 6.3.1 Virtual LCD

Displays the messages from the LCD or the virtual LCD from the front of a managed server. Content such as POST codes and messages are displayed on the LCD. For more information on what is displayed on the LCD, see the maintenance guide of the device itself.



### 6.3.2 LEDs

#### 1. STATUS LEDs

Displays the condition of the STATUS LEDs for the managed server.

STATUS LEDs will be lit in green when a managed server is operating normally. See the user guide for the device itself for information on the conditions and meanings of the displays of the STATUS LEDs.

#### 2. Power Source Status

Displays the status of the power source for the managed server.

### 6.3.3 System Current Accumulated Time

Displays how long the managed server has been in a powered on (DC ON) state.

### 6.3.4 System Monitoring

Displays the running state of the watchdog timer that monitors stalls for the managed server.

### 6.3.5 Configuration Information

The screenshot displays the 'Configuration Information' screen within a server management application. The interface is divided into two main panels. The left panel, titled 'Information of server state/constitution', contains a hierarchical tree view with expandable nodes. The right panel displays a table of configuration items and their current values.

Item Name	Setup Value
<b>Product Information</b>	
Model Name	Express5800/T110d [N8100-1873Y]
Serial Number	3Z00606
GUID	59a46c80-63c2-11e3-8001-74d435413fe9
<b>Server information</b>	
Information	
<b>Server status</b>	
STATUS Lamp	Green On
Power Status	DC On
LCD	POST Completed Successfully
System Power-on Hours	6705 hours 0 minutes
System Monitoring	Off
Monitoring Interval	0seconds
<b>Version Information</b>	
OS Version	Failed to communicate with the agent. The agent may not be installed.
BIOS Version	Failed to communicate with the agent. The agent may not be installed.
NEC ESMPRO Agent Extension Version	Failed to communicate with the agent. The agent may not be installed.
<b>Management Controller Information</b>	
BMC FW Revision	00.14
IPMI Version	2.0
Remote KVM and Media License	Installed
<b>NEC ExpressUpdate Information</b>	
Updates via NEC ExpressUpdate Agent	Disable
Updates via Management Controller	Enable
Status	Latest Condition
Next Installation Schedule	Nothing

Figure 72 Configuration Information Screen

1. Hardware  
Displays detailed information (from the hardware perspective) specific to memory banks, device information and CPUs.
2. I/O Devices  
Displays detailed information specific to floppy disks, printers, serial ports, parallel ports, keyboards, mice and display adapters.
3. System Environment  
Displays detailed information specific to temperature, fans, voltage, power supplies, covers, cooling units and batteries.
4. BIOS  
Displays detailed information specific to system, video and SCSI BIOS.
5. PCIeSSD  
Displays detailed information specific to PCIeSSD.

## Chapter 7 NEC ExpressUpdate

This chapter provides the functional overview and the method for using NEC ExpressUpdate. Descriptions about NEC ExpressUpdate and the setting information are provided in 7.1 to 7.5. The actual method is explained from 7.6. For more convenient usage information, refer to “*NEC ExpressUpdate Functions and Features*” published on NEC corporate Web site.

### 7.1 NEC ExpressUpdate

NEC ExpressUpdate is the function to enable downloads and management of System BIOS, EXPRESSSCOPE Engine 2 and 3, software, drivers versions of the management target server, and batch application of the update files. NEC ExpressUpdate Agent needs to be installed on the OS of the management target server to manage software and drivers.

NEC ExpressUpdate functions download, from NEC corporate Web site, the update packages for the server registered with NEC ESMPRO Manager and retain them in the location called repository up to the past three generations.

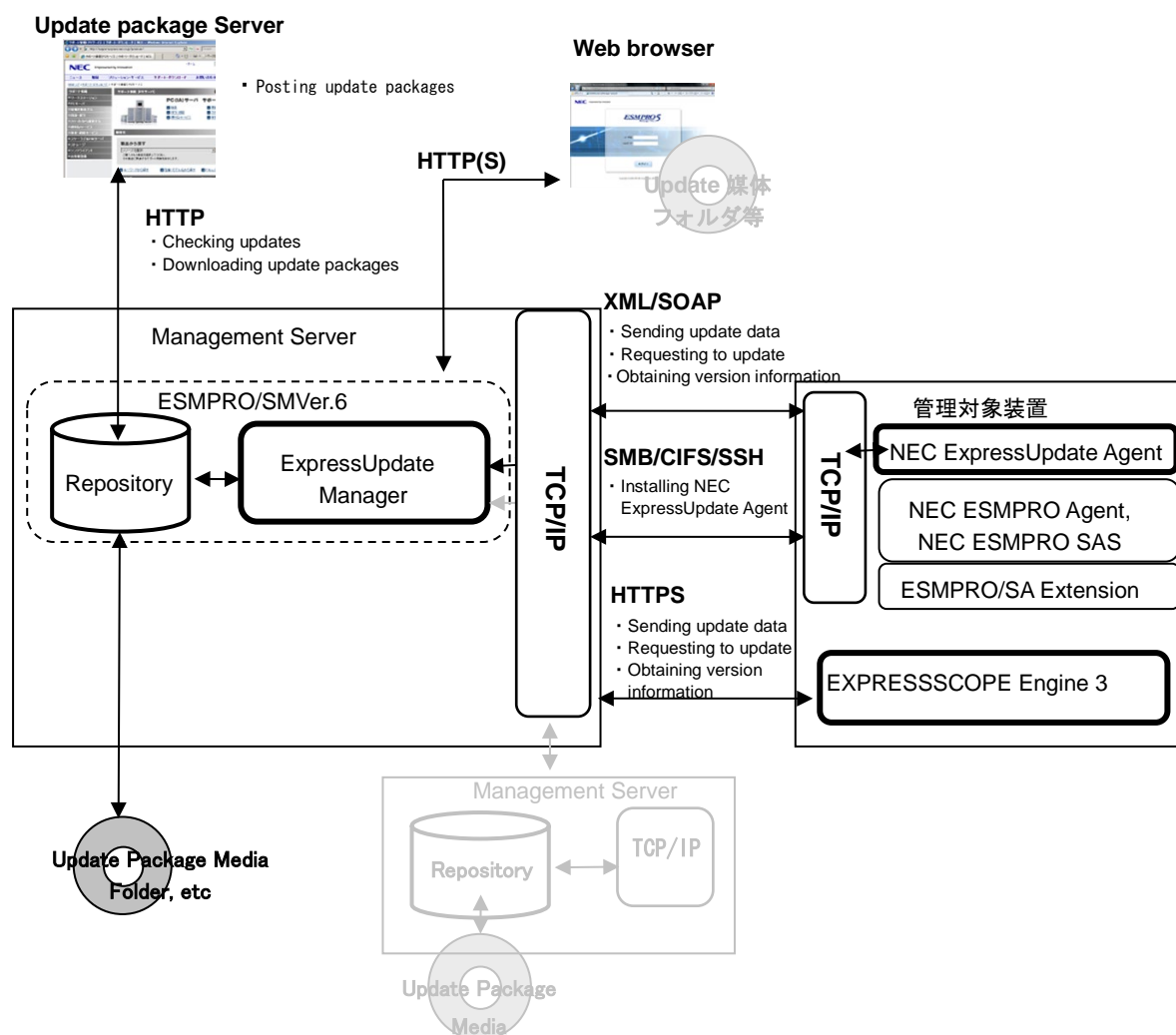


Figure 81 NEC ExpressUpdate conceptual diagram

NEC ExpressUpdate functions are realized by using the following components.

**Table 23 Components realizing NEC ExpressUpdate functions**

	Description
NEC ESMPRO Manager	It provides NEC ExpressUpdate functions.
Update Package	Update files of firmware and each software, such as System BIOS, EXPRESSSCOPE Engine 3, etc., which are published on the NEC corporate Web site or the update package server.
Update package server	It publishes the update packages for NEC ExpressUpdate functions. Repository communicates with it for downloading the update packages.
Repository	It downloads the update packages and manages the generations. Setting of download interval, addition and deletion of the update packages can be performed. Refer to 7.4 and 7.5 for details.
NEC ExpressUpdate Agent	It is installed on the management target server. It is necessary for managing software and drivers using NEC ExpressUpdate functions. It can be remotely installed from NEC ESMPRO Manager for some OSs. Refer to 7.6 for details.
EXPRESSSCOPE Engine 3	It is necessary for realizing NEC ExpressUpdate functions through EXPRESSSCOPE Engine 3. EXPRESSSCOPE Engine 3 of the management target server needs to be managed from NEC ESMPRO Manager. Refer to 3.8 for the setup method.

## **7.2 Components Whose Versions Can Be Managed by NEC**

### **ExpressUpdate Functions**

The components whose versions can be managed by NEC ExpressUpdate functions may vary depending on whether NEC ExpressUpdate Agent is installed on the management target server or not.

#### **7.2.1 With NEC ExpressUpdate Agent Installed**

With NEC ExpressUpdate Agent installed on the management target server, NEC ExpressUpdate functions are realized through NEC ExpressUpdate Agent. The following component versions can be managed and updated.

- System BIOS
- EXPRESSSCOPE Engine 3
- NEC ExpressUpdate Agent
- NEC ESMPRO Agent Extension
- NEC ESMPRO Agent
- NEC ESMPRO ServerAgentService
- Universal RAID Utility

#### **7.2.2 Without NEC ExpressUpdate Agent (Through EXPRESSSCOPE Engine 3) Installed**

With EXPRESSSCOPE Engine 3 installed on the management target server, despite NEC ExpressUpdate Agent not installed on the OS, NEC ExpressUpdate functions are realized through EXPRESSSCOPE Engine 3. The following component versions can be managed and updated.

- System BIOS

- EXPRESSSCOPE Engine 3

### 7.2.3 Components Other Than Automatic Application Target

Updating the components other than the ones described above requires a manual installation to each management target server after manually collecting and saving the update package from the repository. Refer to 7.5 “Repository Management Information” for details.

## 7.3 Types of Update Packages

There are various types of update packages.

### 7.3.1 Availability of Automatic Update

Update packages can be roughly divided in two types. One is available for batch installation to the management target server by using NEC ExpressUpdate functions, while the other requires manual collection and saving of them from the repository, and installation to each management target server. This information can be checked on “NEC ExpressUpdate Installation” screen and “Repository Management Information” screen. As for the method for collecting and saving the update package from the repository, refer to 7.5 “Repository Management Information”.

The screenshot shows the NEC ExpressUpdate interface. The top menu bar includes 'Constitution', 'Setting', 'Remote Control', and 'Schedule'. The sidebar on the left lists various management functions. The main content area is titled 'Update/Install' and shows a list of modules to be updated. The table below represents the data shown in the screenshot.

Status	Module Name	Current Version	Installation Version	Estimate(minute)	Reboot	Severity
Not Latest	System BIOS	4.6.3C19	4.6.8C25	10	Necessary	High
Not Latest	BMC Firmware	01.28	01.33	350	Necessary	Low
Latest Condition	SDR(Sensor Data Record)	00.08	00.08	10	Necessary	Medium
Latest Condition	NEC ExpressUpdate Agent	3.11	-	-	-	-
Latest Condition	NEC ESMPRO Agent Ver.4.5	Unknown	4.55	10	-	-
Not Latest	Universal RAID Utility	2.40 Rev 1582	4.02 Rev 2879	5	Necessary	-
-	System BIOS	4.6.3C19	4.6.8C25	-	-	High
-	BMC Firmware	01.28	01.33	-	-	Low
-	RAID Controller [N8103-149/150/151/160] FW/BIOS	-	3.140.125-3364	-	-	High
-	RAID Controller [N8103-152/167] FW/BIOS	-	3.152.155-2153	-	-	High
-	RAID Controller [N8103-161/169/172/173/174] FW/BIOS	-	3.230.115-3241	-	-	High
-	SAS Controller [N8103-142] FW/BIOS	-	19.00.00.00	-	-	High

Below the table, there are checkboxes for 'Automatic Reboot' and 'Install only latest version'. An 'Execute' button is present, along with the text 'Estimated Time Total 365 Minutes'. At the bottom, there are notes about installation version and status, and a link to 'How to apply the update package for manual update'.

Figure 82 NEC ExpressUpdate screen

IPMI Information Backup File List
Searching Registered Components
ExpressUpdate Management Information














Repository Settings
Repository Management Information
NEC ExpressUpdate Agent Install Status

Location of the repository: Local
Latest downloaded: None
Download Update Packages













Total size of update packages: 2432 MB
Free Space: 13.5 GB
Add Update Packages

(Package selection)
By Component

☐ NavyGem

	Module Name	Additional information	Version	Release Date	Size(MB)
<input type="checkbox"/>	RAID Controller [N810G-149/150/151/160] FW/BIOS	 	3.140.115-2999	04/10/2014	14.1
<input type="checkbox"/>	RAID Controller [N810G-149/150/151/160] FW/BIOS	 	3.140.125-3364	06/17/2014	14.1
<input type="checkbox"/>	RAID Controller [N810G-149/150/151/160] FW/BIOS	 	3.140.95-1967	04/05/2013	14.1
<input type="checkbox"/>	RAID Controller [N810G-152/167] FW/BIOS	 	3.152.155-2153	02/21/2013	19.2
<input type="checkbox"/>	RAID Controller [N810G-152/167] FW/BIOS	 	3.152.155-2153	04/05/2013	14.2
<input type="checkbox"/>	RAID Controller [N810G-161/168/172/173/174] FW/BIOS	 	3.230.115-3241	07/17/2014	14.5
<input type="checkbox"/>	Universal RAID Utility		4.00 Rev 2791	09/17/2014	35

☐ Scorpion

	Module Name	Additional information	Version	Release Date	Size(MB)
<input type="checkbox"/>	RAID Controller [N810G-149/150/151/160] FW/BIOS	 	3.140.115-2999	04/10/2014	14.1
<input type="checkbox"/>	RAID Controller [N810G-149/150/151/160] FW/BIOS	 	3.140.125-3364	06/17/2014	14.1
<input type="checkbox"/>	RAID Controller [N810G-149/150/151/160] FW/BIOS	 	3.140.95-1967	04/05/2013	14.1
<input type="checkbox"/>	RAID Controller [N810G-152/167] FW/BIOS	 	3.152.155-2153	02/21/2013	19.2
<input type="checkbox"/>	RAID Controller [N810G-152/167] FW/BIOS	 	3.152.155-2153	04/05/2013	14.2
<input type="checkbox"/>	RAID Controller [N810G-161/168/172/173/174] FW/BIOS	 	3.230.115-3241	07/17/2014	14.5

☐ R120b-1

? Note for update package

Clean Removal History

Enables you to download update packages which have been removed manually.

Clean Removal History

Remove Update Packages

Removes specified update packages.

☐ Please check it if you want to remove update packages even though other NEC ESMPRO Manager is in use.
Remove Update Packages

Save Update Packages

Saves specified update packages.

Save Update Packages

**Figure 83 Repository management information screen**

### 7.3.2 Downgrade Availability

Some update packages allow you to install older versions than the current version, while others not. Refer to 7.7.2 for details.

### 7.3.3 Reboot Requirement After Installation

Some update packages require re booting the management target server after installation, while others not. This information can be checked on NEC ExpressUpdate "Update package installation" screen. It is also possible to reboot automatically the management target server after completing the installation of the update packages which require rebooting.

## 7.4 Repository Settings

It sets the repository options.

### 7.4.1 Location of Repository

When NEC ESMPro Manager is installed, the repository which downloads the update packages and manages the generations is incorporated at the same time. NEC ExpressUpdate functions normally use the repository on the installed NEC ESMPro Manager. However, the remote repository on the NEC ESMPro Manager installed on another server is also available. This is a highly useful function in an environment where the number of servers connecting to the external network is limited.

Open “ExpressUpdate Management Information” tab in “Tool” on Management screen.

1. Enter the information for “Repository Password” in the “Repository Settings” of the server to be used.

The screenshot displays the "ExpressUpdate Management Information" tab within the NEC ESMPro Manager. The "Repository Settings" sub-tab is active, showing a table with two columns: "Item Name" and "Setup Value".

Item Name	Setup Value
<b>Common Setting</b>	
Location of the repository	<input checked="" type="radio"/> Local <input type="radio"/> Remote
<b>Repository Password Setting</b>	
Password [required]	.....
Password (for confirmation) [required]	.....
<b>Automatic Downloading Settings</b>	
Address of the Update Package Server	http://expressupdate.express.nec.co.jp/
Downloading Schedule	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Proxy Server Settings</b>	
Address	
Port Number (0 - 65535)	
User Name	
Password	
<b>Settings of update packages for manual update</b>	
Default status icon	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>

At the bottom of the form, there are "Apply" and "Cancel" buttons.

**Figure 84 Repository settings screen**

2. Set the following items on the “Repository Settings” of the server to be used by selecting “Remote” from “Location of the repository” under “Common Setting”.

IPMI Information Backup File List | Searching Registered Components | ExpressUpdate Management Information

Repository Settings | Repository Management Information | NEC ExpressUpdate Agent Install Status

Item Name	Setup Value
<b>Common Setting</b>	
Location of the repository	<input type="radio"/> Local <input checked="" type="radio"/> Remote
<b>Remote Repository Settings</b>	
Address <b>[required]</b>	<input type="text"/>
Port Number (0 - 65535) <b>[required]</b>	<input type="text" value="0"/>
Password <b>[required]</b>	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**Figure 85 Repository settings screen**

**Table 24 Remote repository settings**

Item	Description
Address	Enter IP address of the server whose repository is to be used remotely.
Port Number	Enter Port Number used by NEC ESMPRO Manager. It should be 8080, if not changed from the default.
Password	Enter the same character string as "Repository Password Setting" entered in the "Repository Settings" of the server to be used.

## 7.4.2 Other Settings

IPMI Information Backup File List | Searching Registered Components | ExpressUpdate Management Information

Repository Settings | Repository Management Information | NEC ExpressUpdate Agent Install Status

Item Name	Setup Value
<b>Common Setting</b>	
Location of the repository	<input checked="" type="radio"/> Local <input type="radio"/> Remote
<b>Repository Password Setting</b>	
Password <b>[required]</b>	<input type="password" value="....."/>
Password (for confirmation) <b>[required]</b>	<input type="password" value="....."/>
<b>Automatic Downloading Settings</b>	
Address of the Update Package Server	http://expressupdate.express.nec.co.jp/
Downloading Schedule	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
<b>Proxy Server Settings</b>	
Address	<input type="text"/>
Port Number (0 - 65535)	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>
<b>Settings of update packages for manual update</b>	
Default status icon	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

**Figure 86 Repository settings screen**

**Table 25 Repository settings**



Item	Description
Automatic Downloading Settings	Update settings of the repository. Repository accesses the update package server at a fixed interval and downloads the latest update package if released.
Proxy Server Settings	It sets the proxy server when the repository accesses the update package server.
Settings of update packages for manual update	It selects the initial status on NEC ExpressUpdate "Update package installation" screen when the update packages not supporting automatic update are downloaded

## 7.5 Repository Management Information

It manages the update packages in the repository.















IPMI Information Backup File List
Searching Registered Components
ExpressUpdate Management Information

Repository Settings
Repository Management Information
NEC ExpressUpdate Agent Install Status













Location of the repository: Local      Latest downloaded: None      [Download Update Packages](#)  
Total size of update packages: 243.2 MB      Free Space: 13.5 GB      [Add Update Packages](#)

(Package selection)      By Component

☐ NavyGem

Module Name	Additional information	Version	Release Date	Size(MB)
<input type="checkbox"/> RAID Controller [N810G-149/150/151/160] FW/BIOS	 	3.140.115-2999	04/10/2014	14.1
<input type="checkbox"/> RAID Controller [N810G-149/150/151/160] FW/BIOS	 	3.140.125-3364	06/17/2014	14.1
<input type="checkbox"/> RAID Controller [N810G-149/150/151/160] FW/BIOS	 	3.140.95-1967	04/05/2013	14.1
<input type="checkbox"/> RAID Controller [N810G-152/167] FW/BIOS	 	3.152.155-2153	02/21/2013	19.2
<input type="checkbox"/> RAID Controller [N810G-152/167] FW/BIOS	 	3.152.155-2153	04/05/2013	14.2
<input type="checkbox"/> RAID Controller [N810G-161/168/172/173/174] FW/BIOS	 	3.230.115-3241	07/17/2014	14.5
<input type="checkbox"/> Universal RAID Utility	 	4.00 Rev 2791	09/17/2014	35

☐ Scorpion

Module Name	Additional information	Version	Release Date	Size(MB)
<input type="checkbox"/> RAID Controller [N810G-149/150/151/160] FW/BIOS	 	3.140.115-2999	04/10/2014	14.1
<input type="checkbox"/> RAID Controller [N810G-149/150/151/160] FW/BIOS	 	3.140.125-3364	06/17/2014	14.1
<input type="checkbox"/> RAID Controller [N810G-149/150/151/160] FW/BIOS	 	3.140.95-1967	04/05/2013	14.1
<input type="checkbox"/> RAID Controller [N810G-152/167] FW/BIOS	 	3.152.155-2153	02/21/2013	19.2
<input type="checkbox"/> RAID Controller [N810G-152/167] FW/BIOS	 	3.152.155-2153	04/05/2013	14.2
<input type="checkbox"/> RAID Controller [N810G-161/168/172/173/174] FW/BIOS	 	3.230.115-3241	07/17/2014	14.5

☐ R120b-1

[Note for update package](#)

Clean Removal History  
Enables you to download update packages which have been removed manually.
[Clean Removal History](#)

Remove Update Packages  
Removes specified update packages.  
☐ Please check it if you want to remove update packages even though other NEC ESMPRO Manager is in use.
[Remove Update Packages](#)






Save Update Packages  
Saves specified update packages.
[Save Update Packages](#)

Figure 87 Repository management information screen

### 7.5.1 Displaying Update Packages

Update packages managed by the repository are displayed on a list. The items to be displayed are as follows.

**Table 26 Update package information**

Item	Icon	Description
Module Name	-	Name of the update package.
Automatic update Supported/Unsupported	 	It displays whether the batch installations to the management target server is possible by using NEC ExpressUpdate functions, or whether it is necessary to manually collect the update package from the repository and install it manually on each management target server.
Downgrade Available/Unavailable		The update package does not support downgrade.
Multiple models of server supported		The update package supports multiple models of server.
Remote Repository Available/Unavailable		Repository is remotely in use by another NEC ESMPRO Manager. This icon is displayed for the update package which the management target server of the remote NEC ESMPRO Manager needs. Be sure to pay attention when deleting this update package.
Version	-	It displays the version of the update module in the update package.
Release Date	-	It displays the released date of the update package.
Size	-	It displays the capacity of the updated package.

### 7.5.2 Downloading Update Packages

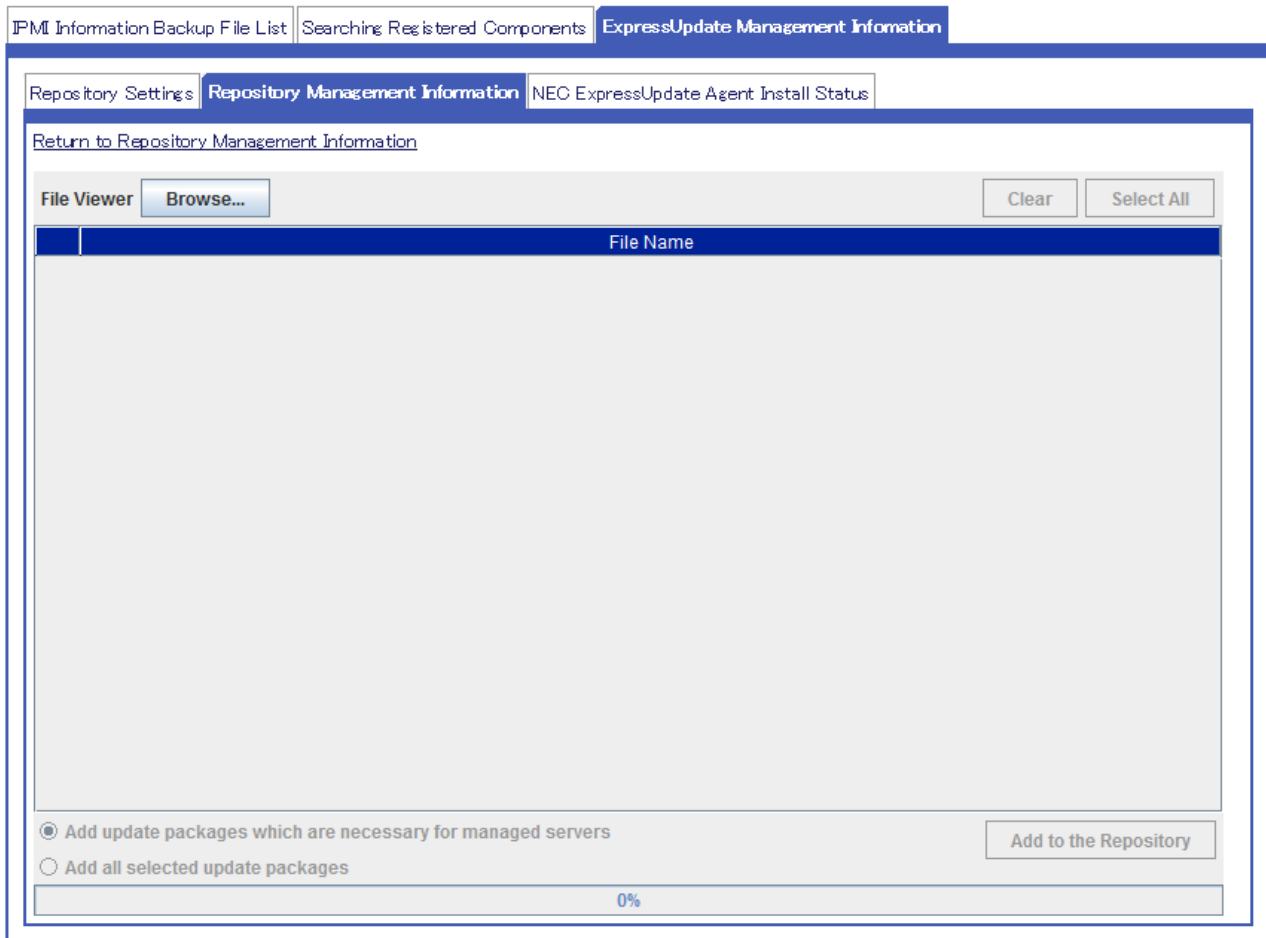
Repository accesses the update package server when “Download Update Packages” is pressed, then it downloads the latest update package for the server managed by NEC ESMPRO Manager if released. It may take some time for completing this operation.

### 7.5.3 Adding Update Packages

Update packages manually downloaded from NEC corporate Web site can be added to the repository. The method for adding the update packages can be selected from the following options.

**Table 27 Options for adding update packages**

Item	Description
Add update packages which are necessary for managed server	A mode for automatically discriminating and adding to the repository only necessary update packages among those selected from file viewer for the server managed by NEC ESMPRO Manager. Update packages added in this mode are targeted for generation management.
Add all selected update packages	A mode for adding all the selected update packages to the repository. Update packages added in this mode are exempt from generation management.



**Figure 88 Repository management information screen - Adding update packages**

#### 7.5.4 “Clean Removal History” for Update Packages

Update packages deleted on the “Repository Management Information” screen cannot be downloaded again even when you execute “Download Update Packages”. Press “Clean Removal History” button for downloading the update package again. However, if the update package removed is older than three versions, it cannot be downloaded again even “Clean Removal History” is pressed.

#### 7.5.5 Removing Update Packages

Selected updated package can be deleted from the repository. Be \*d that the update package necessary for the management target server of the remote repository will be deleted at the same time when you delete the update package whose icon indicates that it is used by the remote repository.

### 7.5.6 Saving Update Packages

The update package not supporting automatic update can be collected from the repository and installed on the management target server.

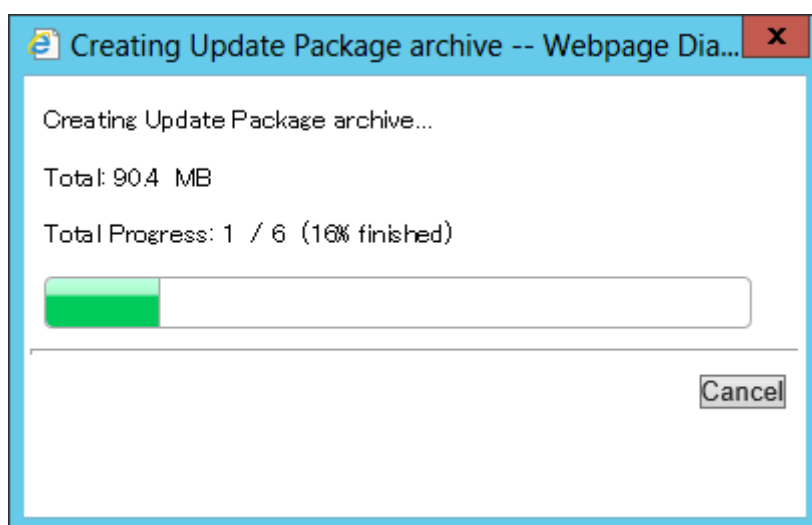


Figure 89 Dialog box showing the update package archive under construction

## 7.6 Installing NEC ExpressUpdate Agent Remotely

It is the function to install NEC ExpressUpdate Agent from NEC ESMPRO Manager if the OS of the management target server meets the conditions indicated below, and the settings of firewall, UAC Control, and port of the OS are properly configured. As for the necessary settings on each OS, refer to the “*NEC ESMPRO Manager Ver.5.7 Installation Guide (Windows)*”. As for the method for remotely installing NEC ExpressUpdate Agent, refer to “*NEC ExpressUpdate Functions and Features*”.

Table 28 Remote installation of NEC ExpressUpdate Agent

	OS type
Remote Installation Available	Microsoft Windows Server 2003, Microsoft Windows Server 2003 R2, Microsoft Windows Server 2008, Microsoft Windows Server 2008 R2, Microsoft Windows XP, Microsoft Windows Vista RedHat Enterprise Linux 5,6
Remote Installation Unavailable	Microsoft Windows Server 2012, Microsoft Windows Server 2012 R2, Microsoft Windows 7/8/8.1/10

## 7.7 Installing Update Packages on the Management Target Server

The status of NEC ExpressUpdate is reflected on the icon of tree view. In the case of using NEC ExpressUpdate functions on a single server, select the management target server to be updated, then select “Remote Control” tab and “NEC ExpressUpdate” for displaying the update package installation screen of NEC ExpressUpdate.

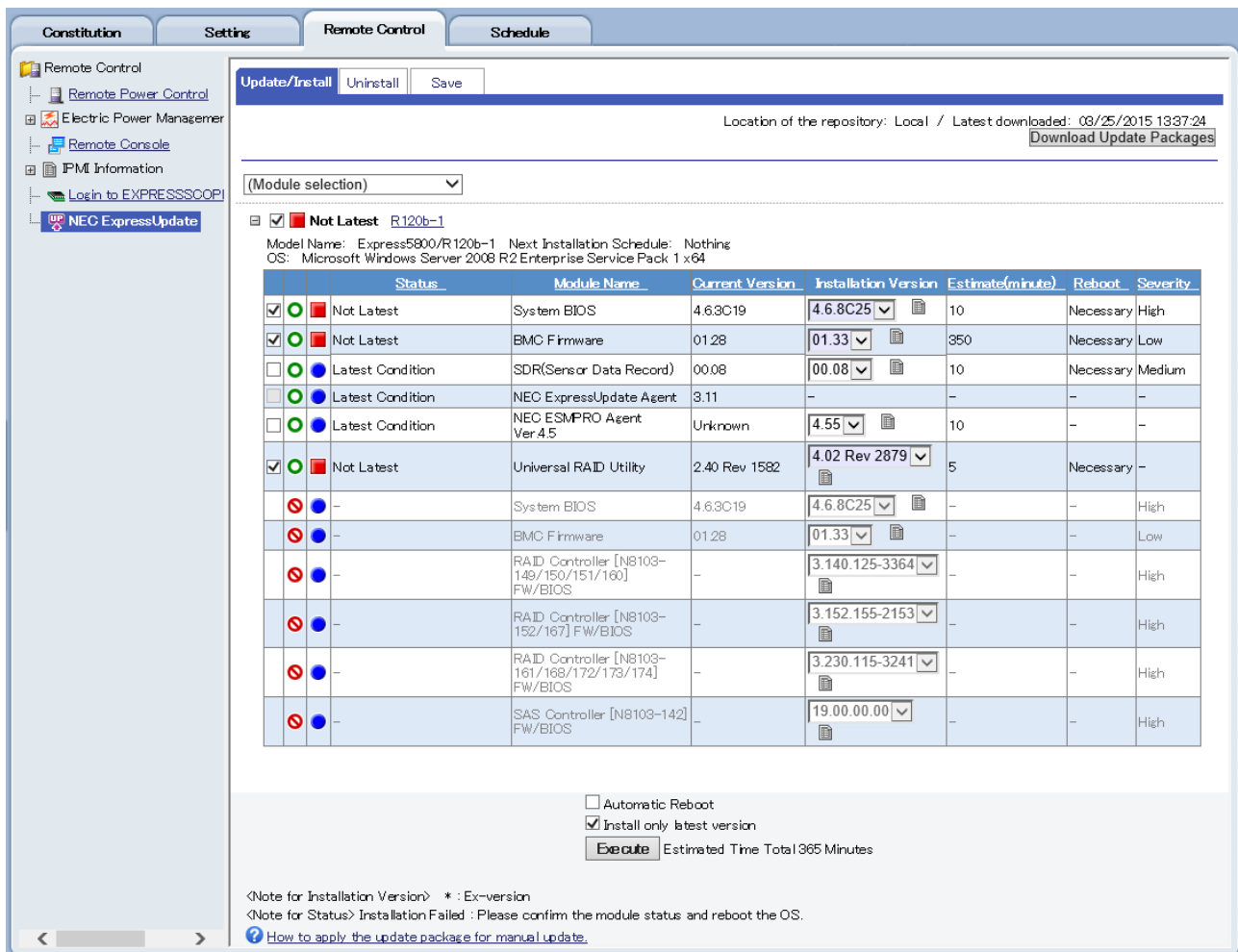



Figure 90 NEC ExpressUpdate screen

### 7.7.1 Update/Installation (Other than NEC ExpressUpdate Agent)

The icon  shows the update package available for update/installation. From the pull-down menu, select the version to be installed. The latest version is selected by default.

### 7.7.2 Downgrade

Selecting the older version than the current version from the pull-down menu enables the downgrade. Clear the "Install only latest version" check box. Only the package supporting downgrade are downgraded.

### 7.7.3 Uninstallation

Uninstalling update packages can be performed by selecting options from "Uninstall" tab. Only the package supporting uninstallation is uninstalled.

## 7.8 Installing Update Packages at a Specified Time by Using the Remote Batch Functions

From "Schedule" tab, select "Remote Batch" for displaying the remote batch settings screen. Select "Install Update Packages" from "Remote Batch Item" for specifying a date and time.

Constitution
Setting
Remote Control
Schedule

Schedule
Remote Batch
Scheduled Running

Select Remote Batch New

Item Name	Setup Value
Remote Batch Item	<span>Install Update Packages</span>
Remote Batch Type	<span>Specified Date</span>
Start Date/Time	<span>3/25/2015 (Wed)</span> <span>20</span> : <span>00</span>
Automatic Reboot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Download Update Packages	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply
Delete
Cancel

**Figure 91 Remote batch settings screen**

## Chapter 8 RAID Management

---

Registering a server on which Universal RAID Utility or LSI SMI-S Provider is installed as the management target of NEC ESMPRO Manager enables you to check and monitor RAID System, and execute operations, etc. for RAID System managed by Universal RAID Utility or LSI SMI-S Provider.

Refer to “*Universal RAID Utility User’s Guide*” or “*NEC ESMPRO Manager RAID System Management Guide for VMware ESXi 5*” for the detailed information of RAID System managed by Universal RAID Utility or LSI SMI-S Provider.

### 8.1 RAID System Management Mode

Changeable options or executable operations may vary depending on user’s RAID System Management Mode. The mode for each user can be set up when adding a new user.

#### 8.1.1 Using Standard Mode

User accounts other than the administrator of NEC ESMPRO Manager have the right to use the Standard Mode by default.

Change the information at “User Information” so that the Advanced Mode user can use only Standard Mode. Select “Standard Mode” from “RAID System Management Mode” of “User Information”.

As for the method of changing the information at “User Information”, refer to Chapter 3.

#### 8.1.2 Using Advanced Mode

Administrator user account of NEC ESMPRO Manager has the right to use Advanced Mode by default.

Change the information at “User Information” so that the user who is authorized to use only Standard Mode can also use Advanced Mode. Select “Advanced Mode” from “RAID System Management Mode” of “User Information”.

As for the method of changing information at “User Information”, refer to Chapter 3.

## 8.2 Descriptions of Management Items

NEC ESMPRO Manager shows the configuration of RAID System existing in the server targeted for management as a hierarchical structure. The type and status of each server targeted for management are displayed with icons.

### 8.2.1 RAID System Information

It displays RAID System Status, Operation, and Running Operation.

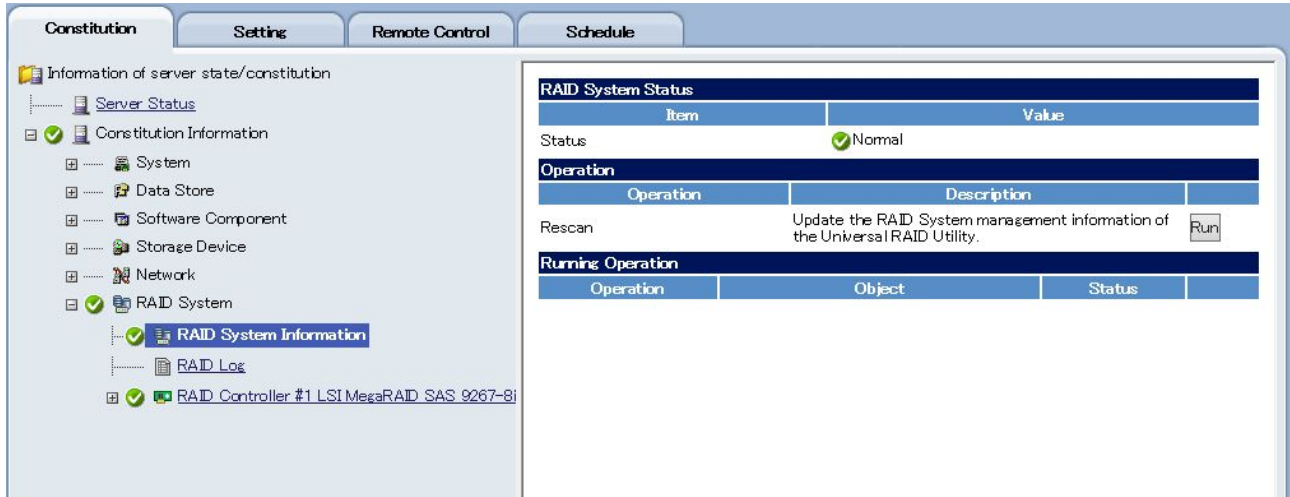


Figure 73 RAID System information screen

### 8.2.2 RAID Log

It displays RAID System operation log.



## 8.2.3 RAID Controller

It displays RAID controller information. The following operations can also be executed.

1. Edit  
Settings of RAID Controller can be changed.
2. Operation  
Operations for the displayed RAID Controller can be executed.

The screenshot displays a web-based interface for RAID controller management. The top navigation bar includes tabs for 'Constitution', 'Setting', 'Remote Control', and 'Schedule'. The left sidebar shows a tree view under 'Information of server state/constitution', with 'RAID Controller #1 LSI MegaRAID SAS 9267-8i' selected. The main content area is divided into two sections: 'Property/Setting' and 'Operation'.

**Property/Setting**

Item	Value
<b>General</b>	
Number	1
ID	0
Vendor	LSI Corporation
Model	LSI MegaRAID SAS 9267-8i
Firmware Version	3.140.95-1967
Cache Size	512MB
<b>Option</b>	
Rebuild Priority	Low
Consistency Check Priority	Low
Patrol Read	Enable
Patrol Read Priority	Low
Buzzer Setting	Disable
HDD Power Saving(Hot Spare)	Disable

[Edit](#)

**Operation**

Operation	Description	
Silence Buzzer	Stop the Buzzer sounding in the RAID Controller.	<a href="#">Run</a>

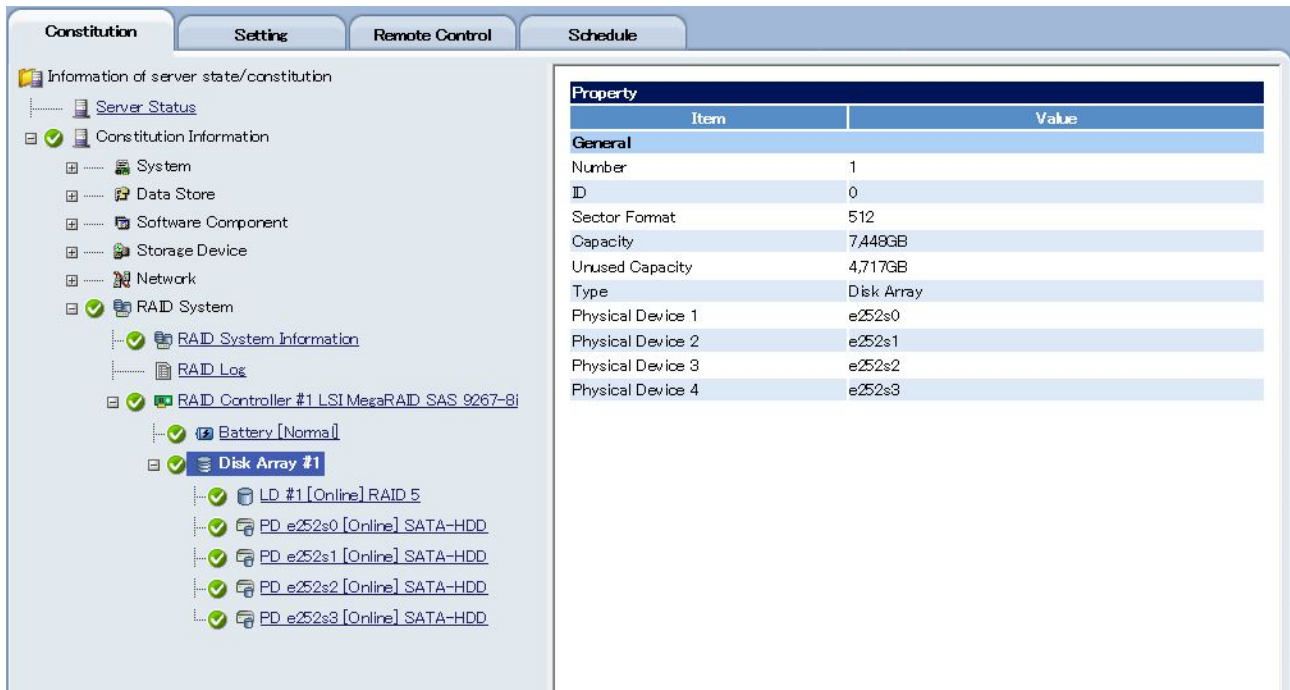
Figure 74 RAID controller screen

## 8.2.4 Battery

It displays Battery information.

## 8.2.5 Disk Array

It displays Disk Array information.



The screenshot displays the 'Disk Array' configuration screen. The left sidebar shows a tree view under 'Constitution' with 'Disk Array #1' selected. The right pane shows a table of properties for the selected disk array.

Property	
Item	Value
<b>General</b>	
Number	1
ID	0
Sector Format	512
Capacity	7,448GB
Unused Capacity	4,717GB
Type	Disk Array
Physical Device 1	e252s0
Physical Device 2	e252s1
Physical Device 3	e252s2
Physical Device 4	e252s3

Figure 75 Disk array screen

## 8.2.6 Logical Drive

It displays Logical Drive information. The following operations can also be executed.

1. Edit  
Settings of logical drives can be changed.
2. Operation  
Operations for displayed logical drives can be executed.

**Property/Setting**

Item	Value
<b>General</b>	
Number	1
ID	0
Disk Array Information	1
RAID Level	RAID 5
Sector Format	512
Capacity	2,047GB
Stripe Size	64KB
Cache Mode (Current)	Write Back
Type	Logical Drive
Status	Online

**Option**

Cache Mode (Setting) Auto Switch

**Operation**

Operation	Description	
Start Consistency Check (Automatic Stop enabled)	Start Consistency Check to the Logical Drive using automatic stop function. If Physical Device Medium Error are detected frequently, this function will stop automatically.	<input type="button" value="Run"/>
Start Consistency Check (Automatic Stop disabled)	Start Consistency Check to the Logical Drive without using automatic stop function. [Warning] If Physical Device Medium Error are detected frequently, access performance of the Physical Device may degrade.	<input type="button" value="Run"/>
Start Initialize(Full)	Start Initialize to the Logical Drive using Full mode. [Warning] The all data will be lost on Logical Drive if the partitions exist on it. Please make sure there is no important data before initializing Logical Drive.	<input type="button" value="Run"/>
Start Initialize(Quick)	Start Initialize to the Logical Drive using Quick mode. [Warning] The all data will be lost on Logical Drive if the partitions exist on it. Please make sure there is no important data before initializing Logical Drive.	<input type="button" value="Run"/>

Figure 76 Logical drive screen

## 8.2.7 Physical Device

It displays Physical Device information. The following operations can also be executed.

### 1. Operation

Operations for the displayed physical devices can be executed.

The screenshot displays the 'Physical Device' screen in a management console. The interface is divided into two main sections: a left-hand navigation pane and a right-hand content area.

**Left-hand navigation pane:** It shows a tree view of the server's state and constitution. The 'RAID System' is expanded, revealing the 'RAID Controller #1 LSI MegaRAID SAS 9267-8i'. Under this controller, the 'Disk Array #1' is expanded, showing four logical drives (LD #1, LD #2, LD #3, LD #4) all in an 'Online' state. The 'Physical Device' (PD) is highlighted, showing it is a 'SATA-HDD'.

**Right-hand content area:** It displays the 'Property' table for the selected physical device. The table has two columns: 'Item' and 'Value'. The properties listed are:

Item	Value
Enclosure	252
Enclosure Position	Internal
Slot	0
ID	10
Device Type	HDD
Interface	SATA
Vendor/Model	ATA Hitachi HUA723020ALA
Firmware Version	MK70AA10
Serial Number	MK0251YGKPNTUA
Sector Format	512
Capacity	1,862GB
Status	Online
S.M.A.R.T.	Normal
Power Status	On

Below the property table is an 'Operation' table with two columns: 'Operation' and 'Description'. The operations listed are:

Operation	Description
Make Offline	Make the Physical Device offline. [Warning] If this Physical Device is the member of Logical Drives, the redundancy of Logical Drives will be lost.
Locate ON	Turn on the DISK lamp on the computer or enclosure in which the Physical Device is installed.
Locate OFF	Turn off the DISK lamp on the computer or enclosure in which the Physical Device is installed.

Each operation has a 'Run' button next to it.

Figure 77 Physical device screen

## Chapter 9 Remote Control

By using the NEC ESMPRO Manager, the power control and power management of the management target servers can be remotely executed. Refer to Chapter 6 for the information about the NEC ExpressUpdate.

### 9.1 Remote Power Control

The following operation can be executed on the management target servers. When selecting a group from the tree view, the remote power control can be executed simultaneously on the management target servers under the group.

**Table 29 Remote power control**

Operation	Description
Power ON *	It executes the power ON of the management target server which is in the power OFF status. If the management target server is in sleep mode, the status can be recovered by performing this operation.
Reset *	It executes the forced reset.
Power Cycle *	It executes the forced power OFF and then power ON.
Power OFF	It executes the forced power OFF.
OS Shutdown	It shuts down the OS. Shutdown may not be properly executed as it does not wait for the running applications and services to stop. Selecting "OS Shutdown Reboot*" can perform rebooting after the shutdown.
DUMP Switch	It behaves in the same way as when the DUMP Switch is pressed.
Clear System Event Log	It clears the System Event Log (SEL) within the EXPRESSSCOPE Engine. The SEL record which has been registered will be deleted.
Chassis Identify	It executes the chassis identification. The ID LED of the server blinks in blue while the chassis identification is executed by the NEC ESMPRO Manager.

\* : Specifying the One-Time Boot Device allows you to change the Boot device for the next startup.

The operations above require the following component or software.

**Table 30 Component/Software related to the remote power control**

Operation	EXPRESSSCOPE Engine 3	ExpressUpdate Agent	NEC ESMPRO Agent	NEC ESMPRO Agent Extension	VMware ESXi 5
Power ON	○	—	○ (*1)	—	○ (*1)
Reset	○	—	—	—	—
Power Cycle	○	—	—	—	—
Power OFF	○	—	—	—	—
OS Shutdown	○	—	○ *2	○ *2	○
DUMP Switch	○	—	—	—	—
Clear System Event Log	○	—	—	—	—

Chassis Identify	○	—	—	—	
------------------	---	---	---	---	--

\*1 : Remote wake up setting is required. The setting of the NEC ESMPRO Agent is not mandatory.

\*2 : OS Shutdown should be attempted first via NEC ESMPRO Agent Extension, and then via NEC ESMPRO Agent. For this, even if the NEC ESMPRO Agent disables “Permit Remote Shutdown/Reboot”, the shutdown will be executed via NEC ESMPRO Agent Extension if the NEC ESMPRO Agent Extension exists.

## 9.2 Power Management

Power measurement or ECO (power control) setting of the management target servers can be performed. Refer to Chapter 11 for power management.

**Table 31 Power management**

Function	Description
Power Measurement	Power consumption, maximum power consumption, minimum power consumption and the average power consumption can be measured up to 7 days. The data after the measurement can be retrieved by selecting “Download of Reading Data”. The character code of the file is UTF-8. When reading the data using the Microsoft Excel, specify UTF-8 as the character code by using “Get External Data” function.
ECO Setting	Power control function. Refer to Chapter 11.

## 9.3 Remote Console

The POST screen after turning power ON of the management target server, or for the server on which the EXPRESSSCOPE Engine is installed, SAC (Special Administration Console) of Windows and CUI screen for Linux can be displayed. GUI Remote Console function can be used for the server with vPro™. \* that JRE needs to be installed on the server displaying the Web Console of the NEC ESMPRO Manager in order to use this function.

The setting change of the EXPRESSSCOPE Engine side is required for using this function. In the case of the EXPRESSSCOPE Engine 3, select “Configuration” tab → “Miscellaneous” → “Management Software Setting”, and enable “Redirection (LAN)” of the Server Configuration Utility or the EXPRESSSCOPE Engine 3 Web Console.

For the EXPRESSSCOPE Engine and the EXPRESSSCOPE Engine 2, be sure to enable the settings by using the NEC ESMPRO Agent Extension.

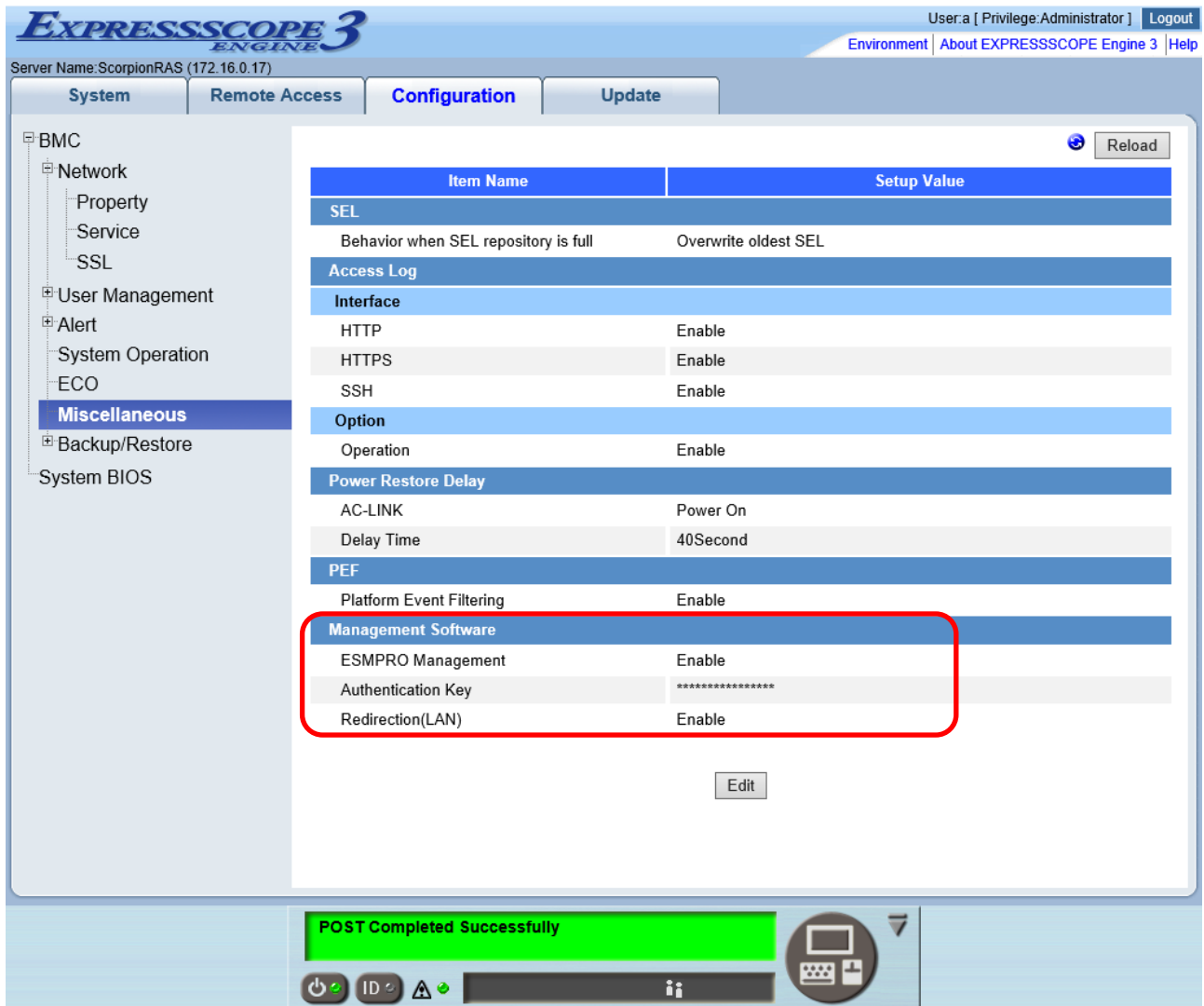


Figure 78 EXPRESSSCOPE Engine 3 Web Console management software setting

## 9.4 IPMI Information

When “Management Controller” is registered as “Enable” on the EXPRESSSCOPE Engine installed server at the time of registering the management target servers, the IPMI information of the management target server can be displayed and collected.

Table 32 IPMI information

Function			Description
System Event Log			It collects the System Event Log (SEL).
Sensor Information			It displays the sensor data record information.
Field Replaceable Unit Information	Replaceable	Unit	It displays the Field Replaceable Unit (FRU) information.
Controller Information			It displays the management controller information.
Backup			It stores the above data in the NEC ESMPRO Manager. Data can be downloaded from the screen after storing the data. The stored file can be checked and deleted from “Tools” → “IPMI Information Backup File List”.

## 9.5 Logging in to the EXPRESSSCOPE Engine Series

When “Management Controller” is registered as “Enable” at the time of registering the management target servers on the EXPRESSSCOPE Engine installed server, the single sign-on (entering the user name and password is not necessary when logging in) is available from the NEC ESMPRO Manager to the Web Console of EXPRESSSCOPE Engine series.

**Table 33 Logging in to EXPRESSSCOPE Engine Series**

Type	Description
EXPRESSSCOPE Engine, EXPRESSSCOPE Engine 2	The maximum number of the login sessions is 1. Single sign-on is not available when other users are logging in to the Web Console of EXPRESSSCOPE Engine/ EXPRESSSCOPE Engine 2.
EXPRESSSCOPE Engine 3	The maximum number of the login sessions is 3. When managed by the NEC ESMPRO Manager, it always consumes 1 session. From “Remote Access” tab → “Session Management” of Web Console of the EXPRESSSCOPE Engine 3, you can display and disconnect the logged in session.



## Chapter 10 Settings

Power supply option setting, EXPRESSSCOPE Engine 3 setting, BIOS setting, and the backup/restore of those settings, etc. can be remotely configured.

### 10.1 Connection Setting

The content of the connection setting to the management target servers can be changed. Press “Check Connection” button after making a change.

Refer to 4.3.2 Manual Registration for the details about each item.

Item Name	Setup Value
Component Name	T110d
Alias	
Group	root
Connection Type	LAN
<b>Common Setting</b>	
OS IP Address	172.16.80.2
<b>System management</b>	
Management	Registered<invalid>
SNMP Community Name(Get)	public
SNMP Community Name(Set)	
<b>RAID system management</b>	
Management	Registered<invalid>
<b>NEC ExpressUpdate</b>	
Updates via NEC ExpressUpdate Agent	Registered<invalid>
Updates via Management Controller	Registered<valid>
<b>"Management Controller" management (Common)</b>	
Management	Registered<valid>
Management Type	BMC
Authentication Key	*****
User Name	
Password	*****
<b>"Management Controller" management (LAN)</b>	
IP Address1	172.16.80.3
Subnet Mask1	255.255.0.0
<b>VMware Auth Information</b>	
User Name	
Password	

Edit Check Connection

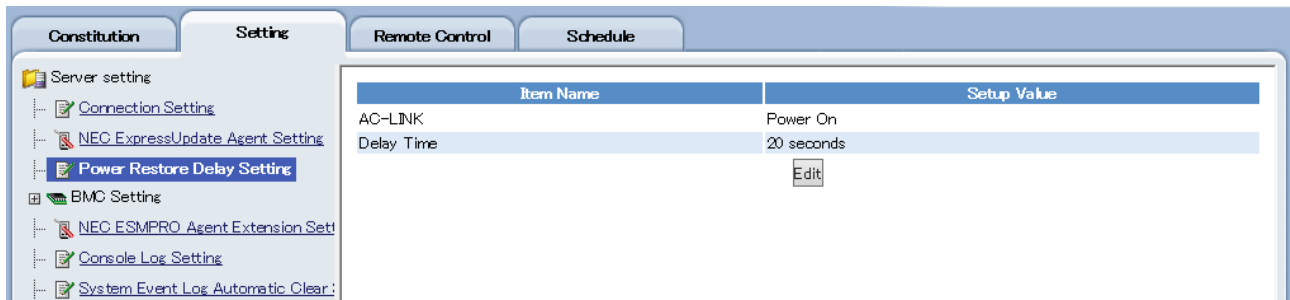
Figure 79 Connection setting screen

### 10.2 NEC ExpressUpdate Agent Setting

Logs of the NEC ExpressUpdate Agent on the specified management target servers can be retrieved.

### 10.3 Power Supply Option Setting

Displaying the power supply status and its configuration can be performed when the AC power supply status of the management target server changes from the OFF to ON. Rapid power consumption can be restrained by setting a variety of the Delay Time when simultaneously turning on the AC power supply of multiple servers.



**Figure 80 Power Restore Delay setting screen**

**Table 34 Power Restore Delay setting**

Item	Setup Value	Default Value
AC-LINK	It displays and configures the behavior when the AC power supply is ON. <ul style="list-style-type: none"> <li>● Stay Off : DC power supply is not turned on.</li> <li>● Last State : Same power supply as when the AC power supply is turned OFF.</li> <li>● Power On : DC is always ON.</li> </ul>	Last State
Delay Time	AAA -BBB *AAA is the available minimum setting value for each management target server. *BBB is 600, when the EXPRESSSCOPE Engine 3 is installed on the management target server. *BBB is 255, when the EXPRESSSCOPE Engine 3 is not installed on the management target server.	Available minimum setting value for each management target server.

## 10.4 BMC Setting (EXPRESSSCOPE Engine 3)

Setting change of EXPRESSSCOPE Engine 3 of the management target server can be performed. The items to be displayed vary depending on the functions which the management target servers support. Setting change is available only in the case where the “LAN” is the connection type between the NEC ESMPRO Manager and the management target servers.

In this document, description on the setting change on EXPRESSSCOPE Engine2 and earlier is omitted.

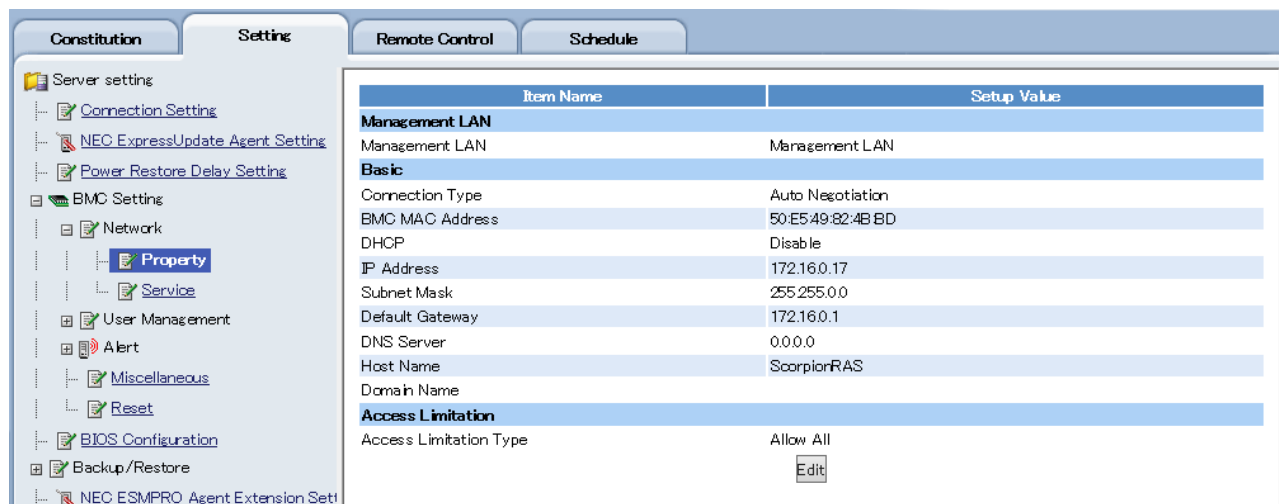


Figure 81 BMC setting screen

### 10.4.1 Network

Items related to Network are displayed within the BMC configuration information.

#### 1. Property

Setting of Network environment used in the BMC.

Table 35 Management LAN setting

Item	Setup Value	Default Value
Management LAN Setting	LAN port used for communication with the BMC is displayed. <ul style="list-style-type: none"> <li>● Management LAN : Dedicated Management LAN port is used for the BMC access.</li> <li>● Shared BMC LAN : Shared system LAN port is used for the BMC access.</li> </ul>	Management LAN

**Table 36 Basic setting**

Item	Setup Value	Default Value
Connection Type	When the LAN for management is Management LAN, it displays and configures the connection type. <ul style="list-style-type: none"> <li>● Auto Negotiation</li> <li>● 100Mbps Full Duplex</li> <li>● 100Mbps Half Duplex</li> <li>● 10Mbps Full Duplex</li> <li>● 10Mbps Half Duplex</li> </ul>	Auto Negotiation
BMC MAC Address	It displays the MAC address.	-
DHCP	It displays and configures DHCP. <ul style="list-style-type: none"> <li>● Enable</li> <li>● Disable</li> </ul>	Disable
IP address	It displays and configures the IP address.	192.168.1.1
Subnet Mask	It displays and configures the subnet mask.	255.255.255.0
Default Gateway	It displays and configures the default gateway.	0.0.0.0
Dynamic DNS	When DHCP is "Enable", it displays and configures the dynamic DNS. <ul style="list-style-type: none"> <li>● Enable</li> <li>● Disable</li> </ul>	Disable
DNS Server	It displays and configures the DNS Server.	0.0.0.0
Host Name	It displays and configures the host name. Host name can be configured with up to 63 characters. It is configured by rounding down if 64 or more characters are entered.	Blank
Domain Name	It displays and configures the domain name.	Blank

**Table 37 Basic setting**

Item	Setup Value	Default Value
-	The items in this table are not displayed in devices which do not support IPv6.	
IPv6	It displays and sets IPv6. <ul style="list-style-type: none"> <li>● Enable</li> <li>● Disable</li> </ul>	Disable
IPv6 Address Assignment Mode	It displays and configures IPv6 address allocation mode, when IPv6 is enabled. <ul style="list-style-type: none"> <li>● Static</li> <li>● Dynamic</li> </ul>	Dynamic
IPv6 Link Local Address	It displays IPv6 link-local address, if IPv6 is enabled.	-
IPv6 Global Address	It displays IPv6 global address, if IPv6 is enabled and IPv6 address allocation mode is "Dynamic".	-
IPv6 Static Address	It displays and configures IPv6 static address, if IPv6 is enabled and IPv6 allocation mode is "Static".	0::0
IPv6 Prefix Length	It displays and configures IPv6 prefix length, if IPv6 is enabled and IPv6 allocation mode is "Static".	64
IPv6 Gateway	It displays and configures IPv6 gateway address, if IPv6 is	0::0

Address	enabled and IPv6 allocation mode is "Static".	
IPv6 DNS Server Address	It displays and configures IPv6 DNS server address, if IPv6 is enabled and supports IPv6 DNS server address.	0::0

**Table 38 Access limitation setting**

Item	Setup Value	Default Value
Limitation Type	<p>It displays and configures the type of the access limitation.</p> <ul style="list-style-type: none"> <li>● Allow All</li> <li>● Allow Address</li> <li>● Deny address</li> </ul>	Allow All
IP address	<p>If the limitation type is either the Allow Address or Deny Address, it displays and configures the IP address whose access to the BMC should be allowed, or denied. The scope of the IP address is configured with comma-delimited.</p> <p>"*" can be used as a wildcard character.</p> <p>e.g., 192.168.1.*,192.168.2.1,192.168.2.254</p>	Blank

## 1. Service

The configurations for the service types used by the BMC are described below.

**Table 39 Web server configuration**

Item Name	Setup Value	Default Value
HTTPS	It displays and configures the HTTPS. <ul style="list-style-type: none"><li>● Enable</li><li>● Disable</li></ul>	Enable
HTTPS Port	It displays and configures the HTTPS port number when the HTTPS is "Enable". 1-65535	443
HTTP	It displays and configures the HTTP. <ul style="list-style-type: none"><li>● Enable</li><li>● Disable</li></ul>	Enable
HTTP Port	It displays and configures the HTTP port number when the HTTP "Enable". 1-65535	80

**Table 40 SSH configuration**

Item Name	Setup Value	Default Value
SSH	It displays and configures SSH. <ul style="list-style-type: none"><li>● Enable</li><li>● Disable</li></ul>	Enable
SSH Port	It displays and configures the SSH port number when SSH is "Enable". 1-65535	22

### 10.4.2 User Management

The items of the user management within the BMC configuration information are described below. Select "Add" or "Edit" to change.

**Table 41 User account setting**

Item Name	Setup Value	Default Value
No	It displays the user ID.	
User	It configures the user status. <ul style="list-style-type: none"><li>● Enable</li><li>● Disable</li></ul>	Enable
User Name	It displays and configures the user name.	Blank
Password	It configures the password.	Blank
Password Confirmation	It configures the password for confirmation.	Blank
Privilege	It displays and configures the access rights. <ul style="list-style-type: none"><li>● Administrator</li><li>● Operator</li><li>● User</li></ul>	Administrator

### 10.4.3 Alert Reporting

The items related to the alert reporting within the BMC configuration information are described below.

#### 1. E-mail Alert

How to configure the alert setting from the BMC via E-mail is described below.

**Table 42 Mail alert setting**

Item Name	Setup Value	Default Value
Alert	It displays and configures the alert. <ul style="list-style-type: none"><li>● Enable</li><li>● Disable</li></ul>	Disable
Waiting time for SMTP Server's Response	It displays and configures the timeout period from the e-mail sending to the successful connection to the SMTP server. 30-600(sec.)	30

**Table 43 E-mail setting**

Item Name	Setup Value	Default Value
To: 1	It displays and configures the address1. <ul style="list-style-type: none"><li>● Enable</li><li>● Disable</li></ul>	Enable
Address 1 e-mail address	It displays and configures an e-mail address of the address 1 when the address 1 (To) is "Enable".	Blank
To: 2	It displays and configures the address 2. <ul style="list-style-type: none"><li>● Enable</li><li>● Disable</li></ul>	Disable
Address 2 e-mail address	It displays and configures an e-mail address of the address 2 when the address 2 (To) is "Enable".	Blank
To: 3	It displays and configures the address 3. <ul style="list-style-type: none"><li>● Enable</li><li>● Disable</li></ul>	Disable
Address 3 e-mail address	It displays and configures an e-mail address of the address 3 when the address 3 (To) is "Enable".	Blank
From	It displays and configures the e-mail address of the sender.	Blank
Reply-To	It displays and configures the e-mail address of the reply destination.	Blank
Subject	It displays and configures the subject.	Blank

**Table 44 SMTP server setting**

Item Name	Setup Value	Default Value
Server	It displays and configures the SMTP server. Full domain name or the IP address can be configured.	0.0.0.0
Port	It displays and configures the SMTP port number. 1-65535	25
Authentication	It displays and configures the SMTP authentication. <ul style="list-style-type: none"> <li>● Enable</li> <li>● Disable</li> </ul>	Disable
Authentication Type	It displays and configures the SMTP authentication method when the SMTP authentication is "Enable". <ul style="list-style-type: none"> <li>● CRAM-MD5</li> <li>● LOGIN</li> <li>● PLAIN</li> </ul>	All checked
User Name	It displays and configures the SMTP user name when the SMTP authentication is "Enable".	Blank
Password	It displays and configures the SMTP password when the SMTP authentication is "Enable".	Blank

**Table 45 Alert level setting**

Item Name	Setup Value	Default Value
Alert Level	It displays and configures the event types to be reported. <ul style="list-style-type: none"> <li>● Error : When "Error" is detected by each sensor type, the checked address among the address 1 to 3 will receive the alert.</li> <li>● Error, Warning : When "Error" or "Warning" is detected by each sensor type, the checked address among the address 1 to 3 will receive the alert.</li> <li>● Error, Warning and Information : When "Error", "Warning" or "Information" is detected by each sensor type, the checked address among the address 1 to 3 will receive the alert.</li> <li>● Separate Settings : When "Error" is detected by each sensor type, the checked address among the address 1 to 3 will receive the alert.</li> </ul>	Error, Warning



## 1. SNMP Alert

It configures the alert settings by the SNMP sent from the BMC.

**Table 46 SNMP alert setting**

Item Name	Setup Value	Default Value
Alert	It displays and configures the alert status. <ul style="list-style-type: none"> <li>● Enable</li> <li>● Disable</li> </ul>	Disable
Computer Name	It displays and configures the host name.	Blank
Community Name	It displays and configures the community name.	public
Alert Progress	It displays and configures the alert progress when the alert response confirmation is "Enable". <ul style="list-style-type: none"> <li>● One Alert Receiver</li> <li>● All Alert Receiver</li> </ul>	One Alert Receiver
Alert Acknowledge	It displays and configures the alert acknowledge status. <ul style="list-style-type: none"> <li>● Enable</li> <li>● Disable</li> </ul>	Enable
Alert Retry Count	It displays and configures the report retry count when the alert response confirmation is "Enable". 0-7(time)	3
Alert Timeout	It displays and configures the alert timeout when the alert response confirmation is "Enable". 3-30(sec.)	6

**Table 47 Alert receiver setting**

Item Name	Setup Value	Default Value
Alert Receiver 1	It displays and configures the alert receiver 1 destination. <ul style="list-style-type: none"> <li>● Enable</li> <li>● Disable</li> </ul>	Enable
Alert Receiver IP address	It displays and configures the alert receiver 1 IP address when the alert receiver 1 is "Enable".	0.0.0.0
Alert Receiver 2	It displays and configures the alert receiver 2 destination. <ul style="list-style-type: none"> <li>● Enable</li> <li>● Disable</li> </ul>	Disable
Alert Receiver IP address	It displays and configures the alert receiver 2 IP address when the alert receiver 2 is "Enable".	0.0.0.0
Alert Receiver 3	It displays and configures the alert receiver 3 destination. <ul style="list-style-type: none"> <li>● Enable</li> <li>● Disable</li> </ul>	Disable
Alert Receiver IP address	It displays and configures the alert receiver 3 IP address when the alert receiver 3 is "Enable".	0.0.0.0

**Table 48 Alert level setting**

Item Name	Setup Value	Default Value
Alert Level	It displays and configures the event types to be reported. <ul style="list-style-type: none"> <li>● Error : When “Error” is detected by each sensor type, the alert will be sent.</li> <li>● Error, Warning : When “Error” or “Warning” is detected by each sensor type, the alert will be sent.</li> <li>● Error, Warning, Information : When “Error”, “Warning” or “Information” is detected by each sensor type, the alert will be sent.</li> <li>● Separate Settings : The event to be reported can be optionally set for each sensor type.</li> </ul>	Error, Warning

#### 10.4.4 Miscellaneous

The items of the various functions of BMC are described below.

**Table 49 SEL setting**

Item Name	Setup Value	Default Value
Behavior when SEL repository is full	It displays and configures the behavior when the SEL repository is full. <ul style="list-style-type: none"> <li>● Stop logging SEL : No other SEL will not be recorded.</li> <li>● Clear all SEL : Delete all the SELs and resumes the SEL recording.</li> <li>● Overwrite oldest SEL : Overwrite the old SEL with the new one.</li> </ul>	Stop logging SEL

**Table 50 PEF setting**

Item Name	Setup Value	Default Value
Platform Event Filter	It displays and configures the alert functions from BMC. <ul style="list-style-type: none"> <li>● Enable</li> <li>● Disable</li> </ul>	Enable

#### 10.4.5 Reset

It executes the BMC reset. Be sure to use only when the BMC functions are not behaving.

### 10.5 BIOS Setting

Some settings of the System BIOS on the EXPRESSSCOPE Engine 3 installed server can be changed from the NEC ESMPRO Manager. Refer to the User’s Guide of the server for the item details.

### 10.6 Backup/Restore

#### 10.6.1 Backup

For the EXPRESSSCOPE Engine 3 installed server, the Setup Value of the BMC or the battery controller can

be backed up.

### 10.6.2 Restore

For the EXPRESSSCOPE Engine 3 installed server, the Setup Value of the BMC or the battery controller can be restored.

## 10.7 NEC ESMPRO Agent Extension Setting

NEC ESMPRO Agent Extension setting on the management target server is retrieved for the display. Clicking the “Edit” button allows you to change the setting.

Clicking “Download Agent log” allows you to download “Application Log” of the NEC ESMPRO Agent Extension in a text format.

This function is available only in the case where the “LAN” is the connection type between the NEC ESMPRO Manager and the management target servers.

## 10.8 Console Log Setting

The displayed items are the retrieval setting of the console logs which store the screen data of the remote console and the failure message monitoring setting which monitors the screen data of the remote console.

## 10.9 NEC ESMPRO Agent



- This item is not supported by the NEC ESMPRO Manager installed on Linux.
- This item is not supported by the power supply bay and the VMware ESXi server.

### 10.9.1 CPU

It configures the threshold value of CPU utilization.

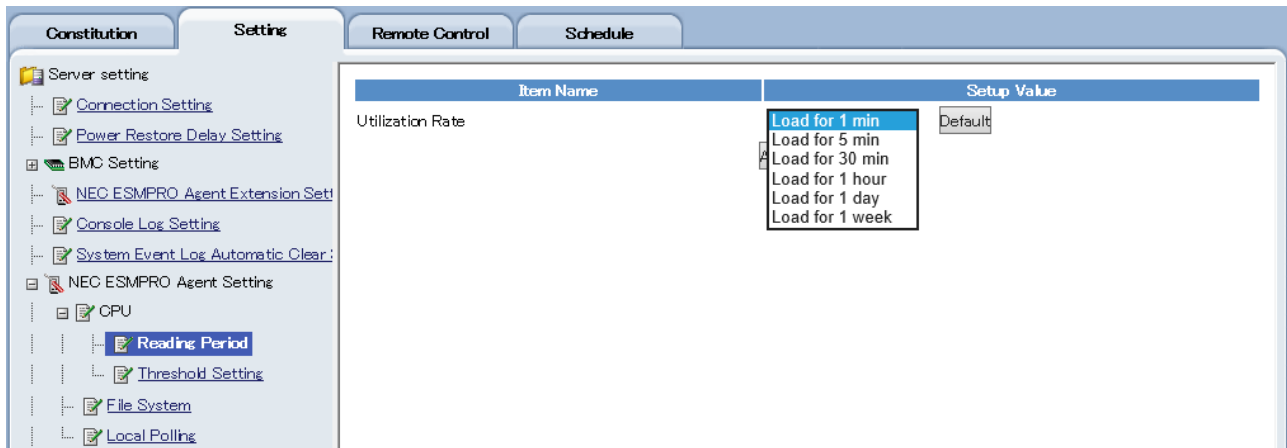


Figure 82 NEC ESMPRO Agent setting -CPU-

Table 51 NEC ESMPRO Agent setting –CPU-

Item Name		Descriptions
Monitoring Item	-	It specifies the type of CPU utilization (criterion time of CPU utilization) to be monitored.
Threshold Setting	Monitoring	It configures the “Enable” / “Disable” of CPU utilization monitoring.
	Fatal Threshold	It configures the upper limit to determine an error. If this value is exceeded, an error alert will be sent.
	Reset Threshold (Error)	It configures the value to reset the error determination. If the value falls below this, a warning alert will be sent to show the recovery from the error level to the warning level.
	Warning Threshold	It configures the upper limit to determine a warning. If this value is exceeded, a warning alert of the warning level will be sent.
	Reset Threshold (Warning)	It configures the value to reset the warning determination. If the value falls below this, a normal level alert will be sent to show the recovery from the warning level to the normal level.

## 10.9.2 File System

It configures the threshold value of the unused capacity monitoring of the file system.

File System List	Monitoring	Current Value	Fatal Threshold	Warning Threshold
C	Enable	Total Capacity 50007 MB Unused Capacity 11809 MB	500 MB	5000 MB
D	Enable	Total Capacity 20002 MB Unused Capacity 17891 MB	200 MB	2000 MB
E	Enable	Total Capacity 69131 MB Unused Capacity 47511 MB	691 MB	6913 MB
F	Enable	Total Capacity 139195 MB Unused Capacity 101356 MB	1392 MB	13919 MB
G	Enable	Total Capacity 139195 MB Unused Capacity 35962 MB	1391 MB	13919 MB
I	Enable	Total Capacity 953671 MB Unused Capacity 947082 MB	9536 MB	95367 MB
J	Enable	Total Capacity 2097149 MB Unused Capacity 1270936 MB	20971 MB	209714 MB
K	Enable	Total Capacity 764107 MB Unused Capacity 609636 MB	7641 MB	76410 MB

**Figure 83 NEC ESMPRO Agent setting – File System-**

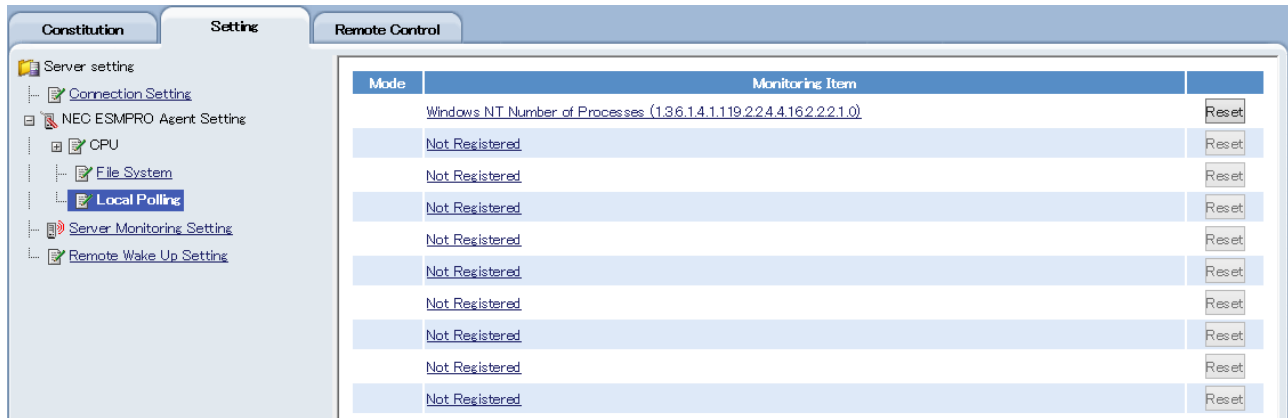
**Table 52 NEC ESMPRO Agent setting – File System-**

Item Name		Descriptions
Monitoring	-	It enables/disables monitoring for the unused capacity.
Current Value	Total Capacity	It displays the total capacity of the file system of the setting target.
	Unused Capacity	It displays the current unused capacity of the file system of the setting target.
Threshold	Fatal Threshold	It configures the unused capacity to determine an error level. If the capacity falls below this, an error alert will be sent.
	Reset Threshold (Error)	It configures the value to reset the error determination. If the value falls below this, a warning alert will be sent to show the recovery from the error level to the warning level. This item exists only on some devices of the Linux servers.
	Warning Threshold	It configures the unused capacity to determine a warning level. If the value falls below this, a warning alert will be sent.
	Reset Threshold (Warning)	It configures the value to reset the warning determination. If the value falls below this, a normal level alert will be sent to show the recovery from the warning level to the normal level. This item exists only on some devices of the Linux servers.

### 10.9.3 Local Polling

It configures the parameter for local polling.

By configuring the threshold value for the optional object ID, the reflection to the management target server status and the alert sending are enabled. However, the expert knowledge and the MIB of the monitoring item is required for configuration.



**Figure 84 NEC ESMPRO Agent setting – Local Polling-**

**Table 53 NEC ESMPRO Agent setting – Local Polling-**

Item Name		Descriptions
Monitoring Setting	Object ID	It selects the object ID. By clicking the object ID list button, you can select the one from the list already registered.
	Monitoring	It configures the enable/disable of the monitoring.
	Monitoring Period	Polling period is specified in seconds. If "Indefinite Period" is checked, the polling is executed continuously.
	Monitoring Duration	Polling duration is specified in seconds.
Threshold Setting	Max	It specifies the maximum value which the parameter can take.
	Min	It specifies the minimum value which the parameter can take.
Upper Threshold	Trap Sending	Traps are generated in response to the upper threshold if it is checked on.
	Fatal Threshold	It configures the upper value which determines an error. If this value is exceeded, an error alert will be sent.
	Reset Threshold (error)	It configures the value to reset the error determination. If the value falls below this, a warning alert will be sent to show the recovery from the error level to the warning level.
	Warning Threshold	It configures the upper value which determines a warning. If this value is exceeded, the warning alert will be sent.
	Reset Threshold (warning)	It configures the value to reset the error determination. If the value falls below this, a warning alert will be sent to show the recovery from the warning level to the normal level.
Lower Threshold	Trap Sending	Traps are generated in response to the lower threshold if it is checked on.
	Fatal Threshold	It configures the value to reset the warning determination. If this value is exceeded, a normal alert will be sent to show the recovery from the warning level to the normal level.
	Reset Threshold	It configures the lower value which determines a warning. If the

	(error)	value falls below this, a warning alert will be sent.
	Warning Threshold	It configures the value to reset the error determination. If this value is exceeded, a warning alert will be sent to show the recovery from the error level to the warning level.
	Reset Threshold (warning)	It configures the lower value which determines a warning. If the value falls below this, a warning alert will be sent.

## 10.10 NEC ESMPRO ServerAgentService Setting

This setting is available when using NEC ESMPRO ServerAgentService.

### 10.10.1 CPU

This setting enables to monitor utilization of each and whole CPU.

**表 54 NEC ESMPRO ServerAgentService Setting –CPU–**

Item Name		Descriptions
Reading Period	Utilization Rate	It specifies the type of CPU utilization (criterion time of CPU utilization) to be monitored.
	Sample Interval (Seconds)	It specifies monitoring intervals. Changing the interval resets the CPU utilization calculated until the time it is changed, and starts new calculation of the utilization.(NEC ESMPRO ServerAgentService Ver1.1 or later)
Threshold	Monitoring	It enables/disables the monitoring of CPU utilization rate.
	Fatal %	It sets the upper limit to determine errors.If this value is exceeded, an error alert will be sent.
	Reset (Error) %	It sets the value to reset the determination of abnormality.If falling below this value, a warning-level alert will be sent to notify it is recovered from error level to warning level.
	Warning %	It sets the upper limit to determine warnings.If this value is exceeded, a warning-level alert will be sent.
	Reset (Warning) %	It sets the value to reset the determination of warning.If falling below this value, a normal-level alert will be sent to notify it is recovered from abnormal level to normal level.

### 10.10.2 Memory

This setting enables to monitor memory usage amount of physical memory, virtual memory, and page file, respectively.

**表 55 ESMPRO/ServerAgentService Setting –Memory–**

Item Name		Descriptions
Reading Period	Sample Interval (Seconds)	It specifies monitoring intervals.
Threshold	Monitoring	It enables/disables each memory monitoring item.
	Fatal (MB)	It sets the upper limit to determine errors. If this value is exceeded, an error level alert will be sent.
	Reset (Error) (MB)	It sets the value to reset the determination of error.If falling below

		this value, a warning level alert will be sent to notify it is recovered from error level to warning level
	Warning (MB)	It sets the upper limit to determine warnings.If this value is exceeded, a warning-level alert will be sent.
	Reset (Warning) (MB)	It sets the value to reset the determination of warning.If falling below this value, a normal-level alert will be sent to notify it is recovered from warning level to normal level.

### 10.10.3 Storage

This setting is for preventive maintenance of hard disk.

**表 56 ESMPRO/ServerAgentService Setting –Storage-**

Item Name		Descriptions
Reading Period	Sample Interval (Seconds)	It specifies monitoring intervals.
HD-PreFailure		It enables/disables preventive maintenance of hard disk.

### 10.10.4 File System

This setting enables to monitor usage amount of each file system.

**表 57 ESMPRO/ServerAgentService Setting –File System-**

Item Name		Descriptions
Reading Periods	Sample Interval (Seconds)	It specifies monitoring intervals.
Threshold	Monitoring	It enables/disables the monitoring of each storage.
	Fatal (MB)	It sets the upper limit to determine errors.If falling below this value, an error level alert will be sent.
	Warning (MB)	It sets the upper limit to determine warnings.If falling below this value, a warning-level alert will be sent.



## 10.11 Server Monitoring Setting

Periodical monitoring and alert registration at the time of the non-response/recovery detection of the management target servers of the NEC ESMPro Manager are configured.

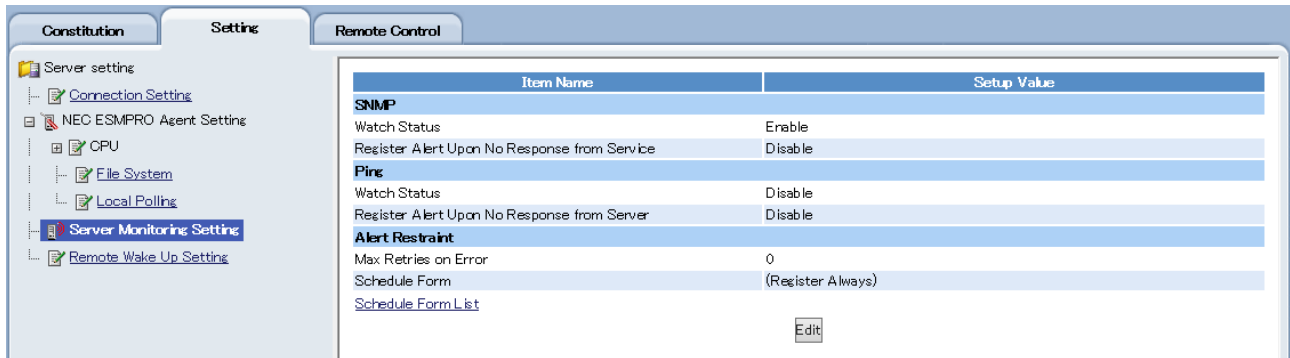


Figure 85 Server monitoring setting



CAUTION

- This item is not supported by the power supply bay.
- NEC ESMPro ServerAgentService does not support Server Monitoring with SNMP.

Table 58 Server monitoring setting

Item Name		Descriptions
SNMP	-	These items are displayed only when the target is NEC ESMPro Agent.
	Watch Status	It configures whether the the status of management target server should be periodically monitored by the SNMP. Management target servers registered automatically are set to "Enable" by default. "Disable" should be avoided normally. If set to "Disable", it will not be reflected on the status icon. (It is always excluded from the monitoring items except that the management method is other than system management and the status change is made due to alert reporting.)
	Register Alert Upon No Response from Service	This setting is enabled when "Watch Status" is enabled. It is set to "Disable" by default. If set to "Enable", an alert is registered to the AlertViewer when no response from the management server is detected and when it recovers from the status.
Ping	Watch Status	It configures whether to periodically monitor the operation status of the management target servers. It is set to "Disable" by default. If set to "Enable", it conducts the alive monitoring by Ping and if no response is sent from the management target server, the icon of the tree view will be displayed as "?".
	Register Alert Upon No Response from Server	It is enabled when the "Watch Status" is "Enable". It is set to "Disable" by default. If set to "Enable", it registers the alert to the AlertViewer when no response is sent from

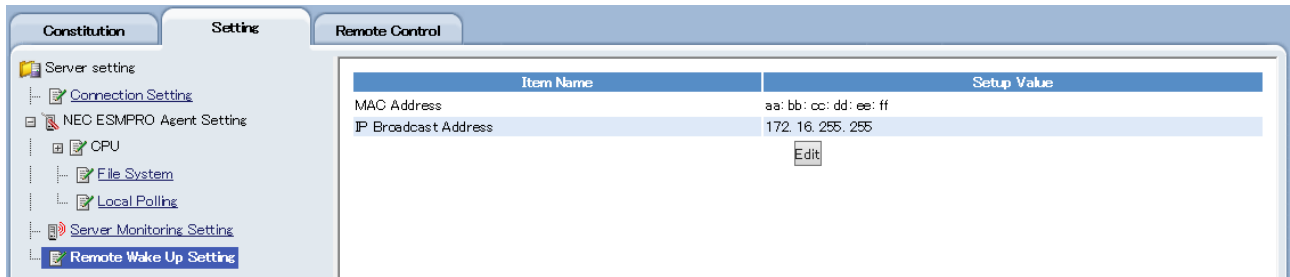
		the management target server and when it recovers from the status.
Polling Interval	Polling Interval	This setting is available when "Watch Status" or "Alive Monitoring" is enabled. This is set to 1 minute by default. Set the monitoring interval to check status of target devices.
Alert Restraint	-	This setting is enabled when "Watch Status" and "Register Alert Upon No Response from Server" is enabled, or "Alive Monitoring" or "Register Alert Upon No Response from Server" is enabled. When an alert detecting no response from the service or the management target server/an alert when detecting the recovery is registered intermittently, it can be restrained by appropriately setting the retry count value. Alternatively, by setting the schedule, the alert registration at detection of non-response/recovery can be restrained. If the periodical shutdown of the management target server is executed due to the operational reason for example, the alert sending can be restrained by the prior schedule setting.
	Max Retries on Error	It configures the retry count until the alert is registered when detecting the no response. It is set to "0" by default and registers an alert upon detecting non-response from the service or the management target server. If "2" is set, it will register an alert after detecting the non-response consecutively twice from the service or the management target server. The value can be set in a range from 0 to 100.
	Schedule Form	It configures the schedule form from the list registered in the Manager. "Register Always" is set by default. At the start-up, the name of the schedule form set to the management target server is displayed, but the following cases are regarded as "Send Always". <ul style="list-style-type: none"> <li>• When the Schedule Form is not configured.</li> <li>• When the Schedule Form configured does *xist.</li> </ul>



- If the Schedule Form configured on the multiple target servers is deleted, the management target servers on which the form is configured will be regarded as "Register Always".
- If the content of the Schedule Form configured on the multiple target servers is changed, the schedule setting of all the management target servers on which the form is configured will be changed.

## 10.12 Remote Wake Up Setting

Remote startup using the magic packet on the network can be performed. This menu is displayed only when "System Management Function" is enabled at the time of management target server registration.



**Figure 86 Remote wake up setting screen**



CAUTION

- This item is not supported by NEC ESMPRO Manager installed on Linux.
- This item is not supported by the power supply bay.
- Setting is not required if the Management Controller Management Function is enabled.

**Table 59 Remote Wake up setting**

Item Name	Descriptions
MAC Address	It configures MAC Address of the system where the Remote Wake Up function is set. When this item and "IP Broadcast Address" are configured, the "Power ON" can be executed.
IP Broadcast Address	It configures the IP Broadcast Address of the network to which the system where the Remote Wake Up function is set is connected. When this item and "MAC Address" are configured, the "Power ON" can be executed.

## Chapter 11 Power Management

This chapter describes about server power management. For more convenient usage information, refer to a whitepaper “Introduction to the Power Monitoring and Power Control Function”.

### 11.1 Power Measurement Function

This function can measure the power consumption of the server periodically.

#### 11.1.1 Power Measurement Function Using NEC ESMPRO Manager

NEC ESMPRO Manager can measure the power consumption of the managed server for a maximum of 1 week. Go to “Remote Control”, “Electric Power Management”, and “Power Measurement” and then click “Start Reading” button. During measurement, a real-time power graph can be drawn and the measurement result can be downloaded.

Selecting “Sum total of reading periods” enables to total the previous data such as maximum/ minimum/ average power, statistics of measurement counts, and inherit the detailed measurement data by measurement interval. When using a device equipped with EXPRESSSCOPE Engine 3, the value of capped power control set to the device is also included in the measurement result and graphs.

Also, in case EXPRESSSCOPE Engine 3 is installed, the setup values of the power capping are included in the measurement result and the graph.

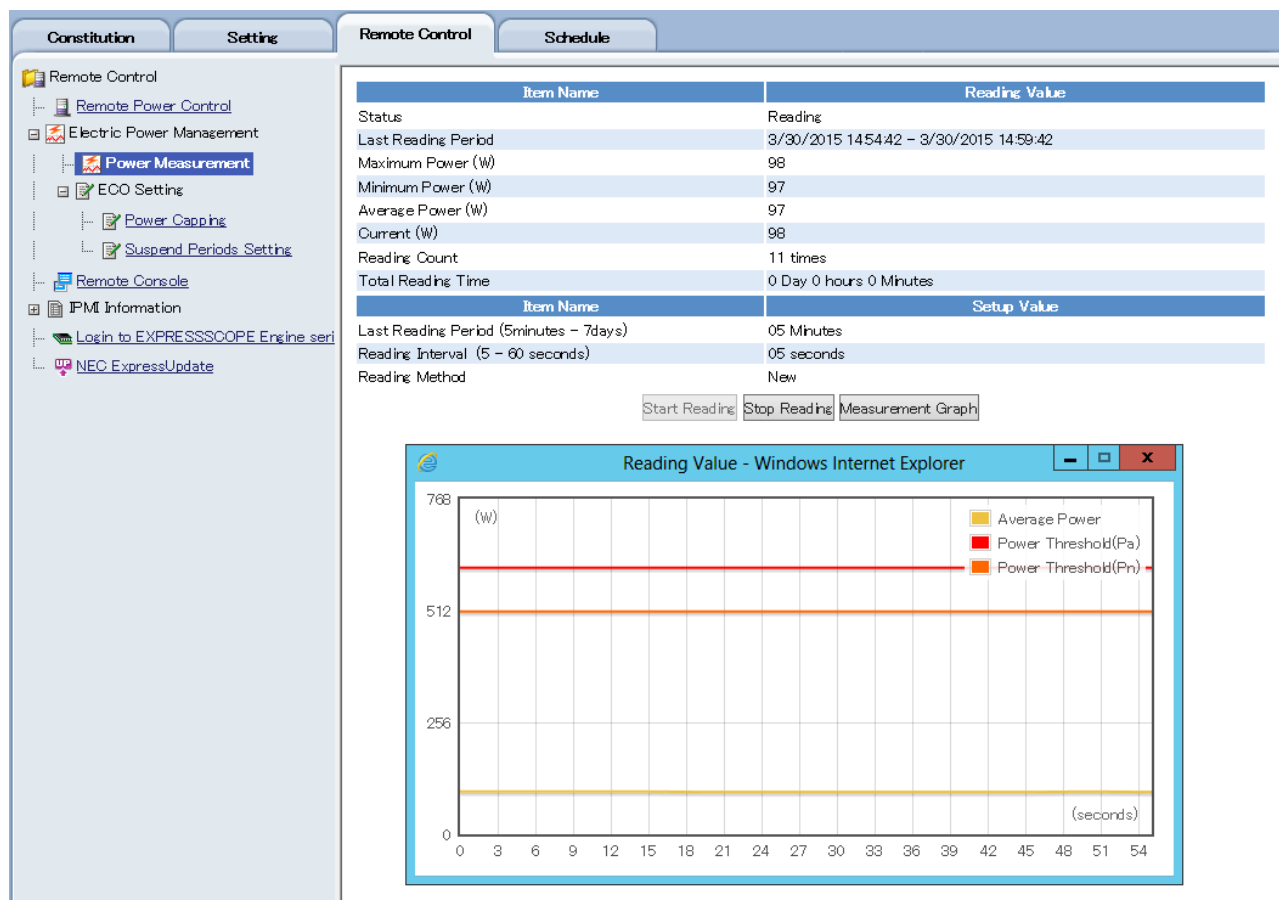


Figure 87 Electric power management – Power measurement -

### 11.1.2 Power Measurement Function of EXPRESSSCOPE Engine 3 WebConsole

When EXPRESSSCOPE Engine 3 is installed, it gives the function to measure the power constantly. The statistical information of the measurement can be confirmed on WebConsole. (\*Some servers are not supported).

Two types of graphs are displayed; one is past 24 hours base and the other is 10 minutes base. Also, each data is downloadable.

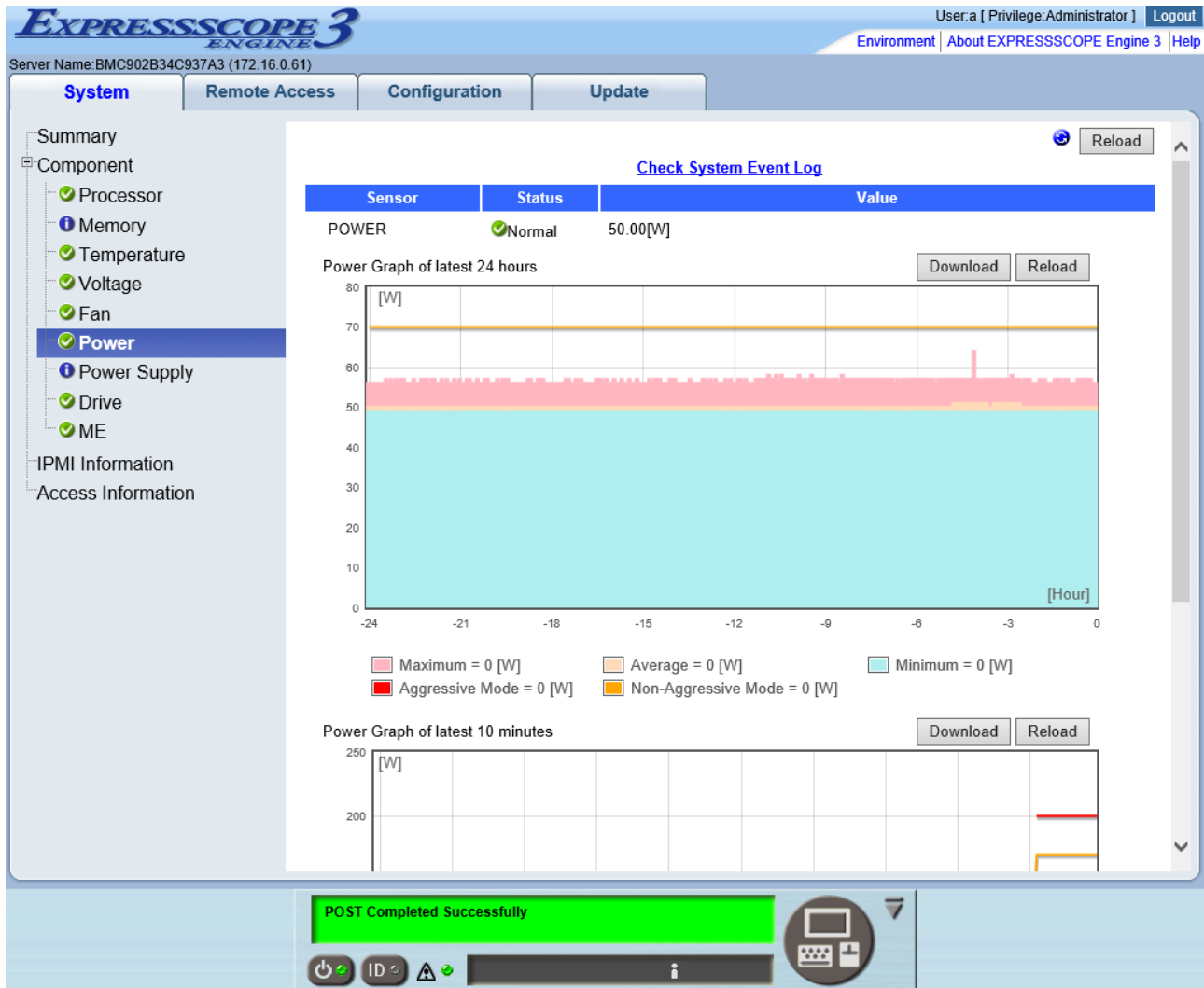


Figure 88 Power screen

## 11.2 Power Capping

The Power Capping provides operation continuity while controlling the total power consumption below the specified power consumption. (\* Some functions are limited depending on the server.)

The Power Capping can be set up by NEC ESMPRO Manager, Server Configuration Utility, WebConsole of EXPRESSSCOPE Engine 3 or Command Line Interface.

### 11.2.1 Non-Aggressive Mode (Non-Critical Power Capping)

When the power consumption exceeds Power Threshold (Pn) which is set up in Non-Aggressive Mode, the Power Capping controls the power consumption to the degree of not lowering the system efficiency excessively. Also, when the power consumption exceeds Pn, and the time limit which is set up in Correction time limit passes, reports are performed. To enable this alert, Non-Critical (Warning) report level of the sensor type "Power Capping" is needed to be enabled.

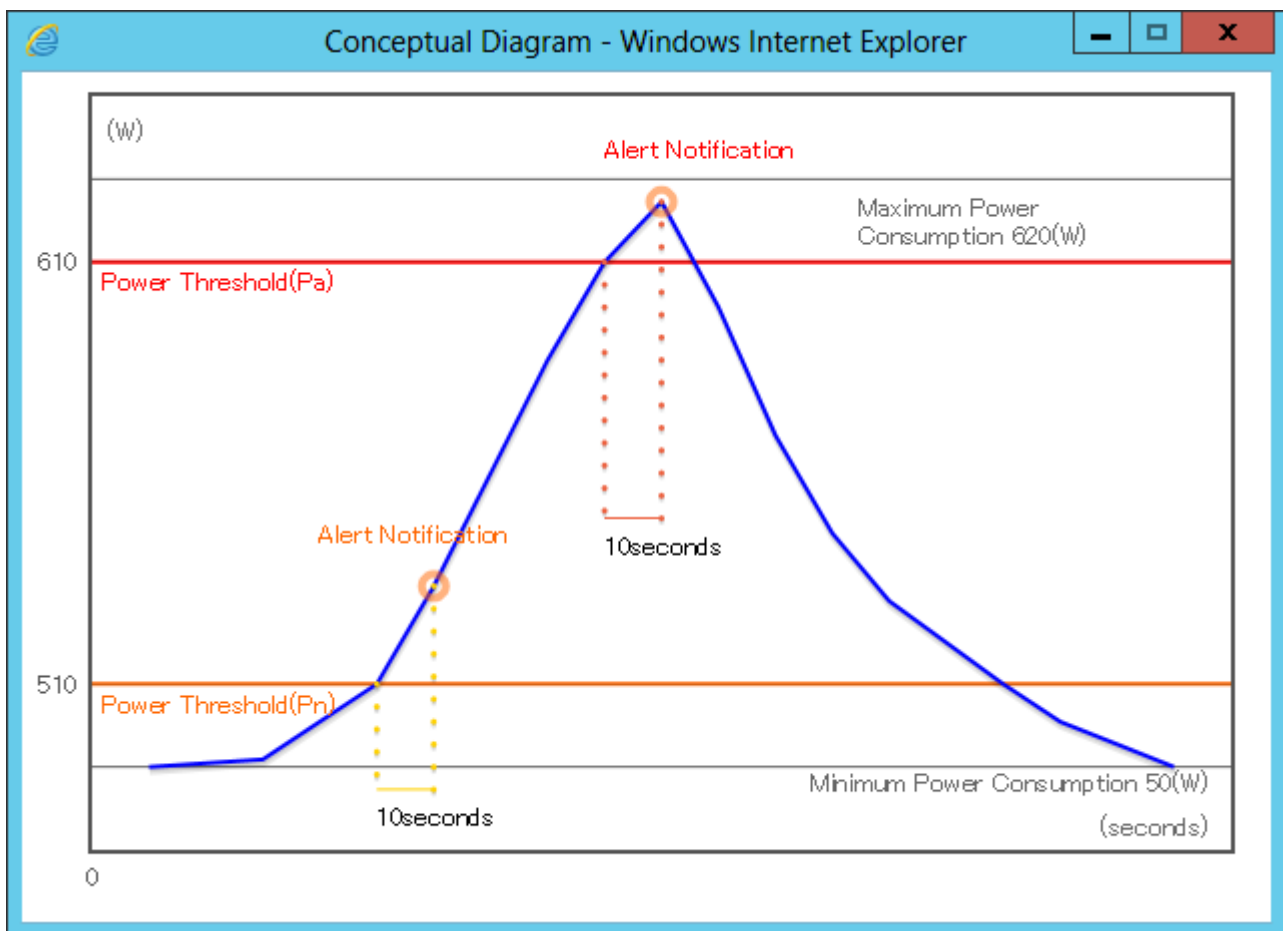


Figure 89 Power capping conceptual diagram

### 11.2.2 Aggressive Mode (Critical Power Capping)

When the power consumption exceeds Power Threshold (Pa) which is set up in Aggressive Mode, the Power Capping proactively controls the power consumption. Also, when the power consumption exceeds Pa, and the time limit which is set up in Correction time limit passes, reports are performed. To enable reporting, the report level Critical (Error) of the sensor type “Power Capping” is needed to be enabled. When “Shutdown System” is enabled, the power consumption exceeds Pa, and the time limit which is set up in the “Correction time limit” passes, shutdown is performed.

### 11.2.3 Safe Power Capping

The power consumption is forcibly reduced when the power consumption information can not be collected from the power unit.

### 11.2.4 Boot Time Configuration

It enables or disables the power control and sets up the number of CPU cores when starting the server. In Performance Mode, either “Performance Optimized” or “Power Optimized” can be chosen. Some servers may not support this function.

### 11.2.5 Setting Power Capping Screen

#### 1. NEC ESMPRO Manager

The screenshot displays the NEC ESMPRO Manager's 'Setting' tab. The left sidebar shows a tree view with 'Power Capping' selected. The main area contains several sections:

- Reference Table:** Shows power consumption limits for Maximum and Minimum configurations during operation and idle states.
- Statistics Tables:** Three tables showing current, maximum, minimum, and average power consumption, CPU throttling, and memory throttling.
- Aggressive Mode:** Includes checkboxes for 'Aggressive Mode', 'Shutdown System', and 'Correction time limit' (set to 10 seconds). The 'Power Threshold (Pa)' is set to 610 W.
- Non-Aggressive Mode:** Similar settings to Aggressive Mode, with 'Power Threshold (Pn)' set to 510 W.
- Safe Power Capping:** Includes a checkbox for 'Power Reading Timeout'.
- Boot Time Configuration:** Includes a checkbox for 'Boot Time Configuration'.

At the bottom, there are buttons for 'Apply', 'Cancel', 'Default', and 'Diagram'.

Figure 90 NEC ESMPRO Manager setting power capping screen

#### 2. EXPRESSSCOPE Engine 3 Command Line Interface

```

-> cd /admin1/system1
-> show
    Command Status: COMMAND COMPLETED

    ufip=/admin1/system1
    Targets:
        ~Abridged~
        oemnec_SafePowerCapping=disabled
        oemnec_Non-AggressiveMode=disabled
        oemnec_AggressiveMode=disabled

```

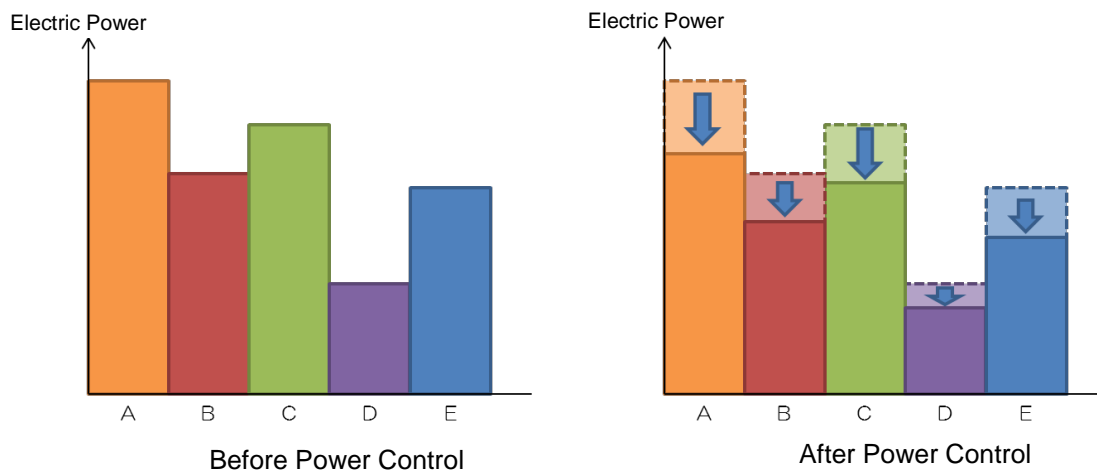
## 11.3 Group Power Control

NEC ESMPRO Manager (Version 5.54 or later) can automatically distribute power to the servers in the group. To use this function, use groupset for power management.

### 11.3.1 Balance Type Power Distribution Function

Balance Type Power Distribution Function can be selected by using NEC ESMPRO Manager (Version 5.7 or later). Power is distributed to all the managed servers in well balance, and the power consumption is regulated at a fixed rate.

For example, there is a group with 5 servers, A-E. When this function is enabled, if power runs short, the total amount of the power consumption of the group is controlled below the specified value by regulating the power distributed to all the servers at a fixed rate.



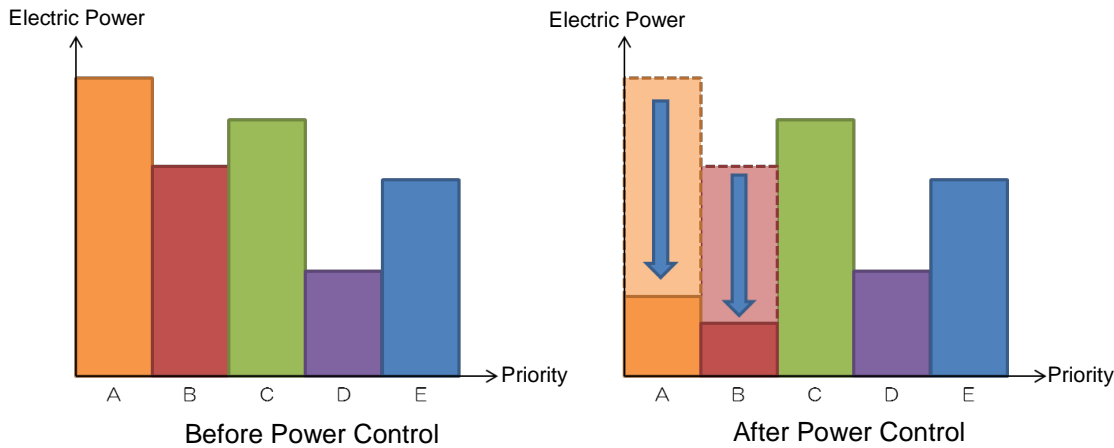
**Figure 91 Balance type power distribution function**



### 11.3.2 Priority Based Power Distribution Function

Power is preferentially distributed to the prioritized managed servers. The power consumption is controlled to the lower limit from lower priority managed servers in series.

For example, there is a group with 5 servers, A-E. When the order E,D,C,B and A is in the order of descending priorities to distribute power, if power runs short, the total amount of the power consumption of the group is controlled below the specified value by controlling from A. In case the power regulation to A does not cover the shortage as a group, power control is performed from B,C,D to E in the order.



## 11.4 Suspend Periods Setting

Setting and display of the schedule of time period to suspend the power consumption control are executed for each managed server or each power group. The power consumption control is disabled only during a certain period of time to improve the server performance. Suspend Periods Setting can be set up only by NEC ESMPro Manager. Up to 5 schedules can be registered for Suspend Periods.

The screenshot shows the 'Suspend Periods Setting' screen in the NEC ESMPro Manager. The left sidebar contains a tree view with the following items: Remote Control, Remote Power Control, Electric Power Management, Power Measurement, ECO Setting, Power Capping, Suspend Periods Setting (highlighted), Remote Console, IPMI Information, Login to EXPRESSSCOPE Engine seri, and NEC ExpressUpdate. The main panel has tabs for 'Constitution', 'Setting', 'Remote Control', and 'Schedule'. The 'Schedule' tab is active, showing a 'Select Schedule' dropdown set to 'New'. Below this is a table with two columns: 'Item Name' and 'Setup Value'. The 'Start Time' is set to 03:00 and the 'End Time' is set to 19:00. Below the table, there is a section for 'A day of the week [required]' with checkboxes for Mon., Tue., Wed., Thu., Fri., Sat., and Sun. The 'Sun.' checkbox is checked. At the bottom of this section are 'Add' and 'Cancel' buttons.

Item Name	Setup Value
Start Time	03 : 00
End Time	19 : 00

A day of the week [required] Mon. ☐ Tue. ☐ Wed. ☐ Thu. ☐ Fri. ☐ Sat. ☐ Sun. ☒

Add Cancel

Figure 92 Suspend periods setting screen

Constitution
Setting
Remote Control
Schedule

Remote Control
Remote Power Control
Electric Power Management
Power Measurement
ECO Setting
Power Capping
Suspend Periods Setting
Remote Console
IPM Information
Login to EXPRESSSCOPE Engine seri
NEC ExpressUpdate

### Addition of schedules

A day of the week	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon.																								
Tue.																								
Wed.																								
Thu.																								
Fri.																								
Sat.																								
Sun.																								

For additional information on schedule  
You can register up to five schedules.  
Click 'Addition of schedules' link or select Suspend Periods by drag-and-drop operation.

**Figure 93 Suspend periods setting screen**

## Chapter 12 Scheduled Operation/Remote Batch

### 12.1 Scheduled Operation

Scheduled operation is a function to set the execution of Shutdown OS and Power ON at the start time and at the end time of the suspension period respectively, in accordance with the set schedule of the suspension period (the period during which DC is OFF) on the management target server.

Installation of NEC ESMPRO Agent Extension is mandatory in order to use the scheduled operation. The schedule which is configured on the management target server as a result of a communication with NEC ESMPRO Agent Extension can be executed even when NEC ESMPRO Manager is not behaving.

This function can be executed per management target server or per group only in the case where LAN is the connection topology between NEC ESMPRO Manager and the management target server.

If the configuration is duplicated in both a group and the management target server, the configuration of a group will be prioritized.

### 12.2 Remote Batch

Remote batch is a function to execute the remote control operation from NEC ESMPRO Manager at a specified time.

Remote batch, unlike the scheduled operation, is executed only during the period in which NEC ESMPRO Manager behaves.

If the configuration is duplicated in both a group and the management target server, the configuration of a group will be prioritized. Note that some of the conditions differ from those in Chapter9.1 Remote Power Control..

**Table 60 Remote Batch Configuration**

Remote Batch Item	Description
Power ON *1	It executes Power ON by remote control.
Power OFF *1	It executes Power OFF by remote control.
Shutdown OS *2	It executes Shutdown OS by remote control.
Clear System Event Log *1	It clears the System Event Log (SEL) of the management target server.
Collect System Event Log, Sensor Information, Field Replaceable Unit Information *1	It collects all the IPMI information of the management target server and save them under the name of the specified output file.
Install Update Packages *3	Installation of the update packages of the management target server, etc. is executed by NEC ExpressUpdate.
Consistency Check of RAID System *4	It checks the consistency of logical drives.
Power Measurement *5	It measures the power of the management target server.

\*1: When BMC management of the managed server is enabled.

\*2: In the case where NEC ESMPRO Agent Extension is installed in the managed server and BMC management is enabled, where NEC ExpressUpdate Agent is installed and an update through NEC ExpressUpdate Agent is enabled, or where the system management (WS-Man) is enabled.

\*3: In the case where the managed server is equipped with EXPRESSSCOPE Engine 3, BMC management is enabled, and an update through the management controller is enabled, or where NEC ExpressUpdate Agent is installed and an update through NEC ExpressUpdate Agent is enabled.

\*4: In the case where Universal RAID Utility is installed in the managed server and the RAID system

management function is enabled.

\*5: In the case where the managed server is equipped with EXPRESSSCOPE Engine 3, and BMC management is enabled.

## Chapter 13 Command Line Interface

---

### 13.1 EXPRESSSCOPE Engine 3

#### 13.1.1 Remote Control using SSH Client

EXPRESSSCOPE Engine 3 can perform remote control of the main server from a SSH client. SSH (Version 2) protocol is supported. Remote control is executed by using the concept of command (Verb) and the target (Managed Element) proposed by DMTF (Distributed Management Task Force).

Refer to *EXPRESSSCOPE Engine 3 User's Guide* for details. The following is one of the examples.

1. Login  
User account is common between the command prompt for remote control and the remote management function which uses a Web browser. A command prompt will be displayed after a successful login.
2. Remote Control Command
  - i. Power ON  
Enter the following command at the command prompt.  
`start /admin1/system1`
  - ii. Forced Power OFF  
Enter the following command at the command prompt.  
`stop -force /admin1/system1`
  - iii. Shutdown OS  
Enter the following command at the command prompt.  
`stop /admin1/system1`
  - iv. System Reset  
Enter the following command at the command prompt.  
`reset /admin1/system1`
3. Logout  
Enter the “exit” command at the command prompt. The connection to EXPRESSSCOPE Engine 3 will be disconnected after logout.

#### 13.1.2 Scripting

EXPRESSSCOPE Engine 3 can be configured from the management server via network by using the script language. Configuration change can be done by downloading a JSON format file on which various configurations are described from EXPRESSSCOPE Engine 3, and saving it on the management server. Then the described content of the JSON format file can be changed according to the purpose, and uploaded on EXPRESSSCOPE Engine 3.

Refer to *EXPRESSSCOPE Engine 3 User's Guide* for details. The following is one of the examples.

Perl script which invokes BmcConfig.pm module reads the module as indicated below.

```
use BmcConfig;
```

Execute then the constructor in order to collect an instance (In the case of no verification of certificate)

```
$bmc = BmcConfig->new( host      => '192.168.2.33',  
                        username  => 'Administrator' ,  
                        password  => 'Administrator' ,  
                        ssl       => 1 ,
```

```
skipcertcheck => 1 );
```

Collecting a configuration or creating a new configuration can be done by using the collected instance.

```
( $ret , $json ) = $bmc->getConfig('basic');  
$ret = $bmc->setConfig('basic' , 'basic.json');
```

## 13.2 NEC ESMPRO Manager

NEC ESMPRO Manager Command Line Interface provides a command set which allows you to control the management target server from the server on which NEC ESMPRO Manager behaves by using the command line. The command set covers a part of the function which is executable by using a Web browser.

Refer to *NEC ESMPRO Manager Ver.5 Command Line Interface* for details.

Regarding the command line interface of NEC ExpressUpdate function, refer to *Command Line Interface for User's Guide for NEC ExpressUpdate*.

The following is an example which illustrates the procedure for issuing commands with a view to managing one management target server via LAN.

1. Create a group by using the “createGroup” command.

```
dscli createGroup GroupA
```

2. Register a management target server by using the “createServer” command.

```
dscli createServer ServerA GroupA guest 192.168.2.33
```

3. Execute a connection check of the management target server by using the “checkConnection” command.

```
dscli checkConnection ServerA
```

4. Confirm the information of the management target server by using the “esmcli” command.

```
esmcli -u Administrator -p Administrator 'show /cmps/ServerA'
```

# Chapter 14      **NEC ESMPRO ServerAgentService**

---

This chapter explains NEC ESMPRO ServerAgentService.

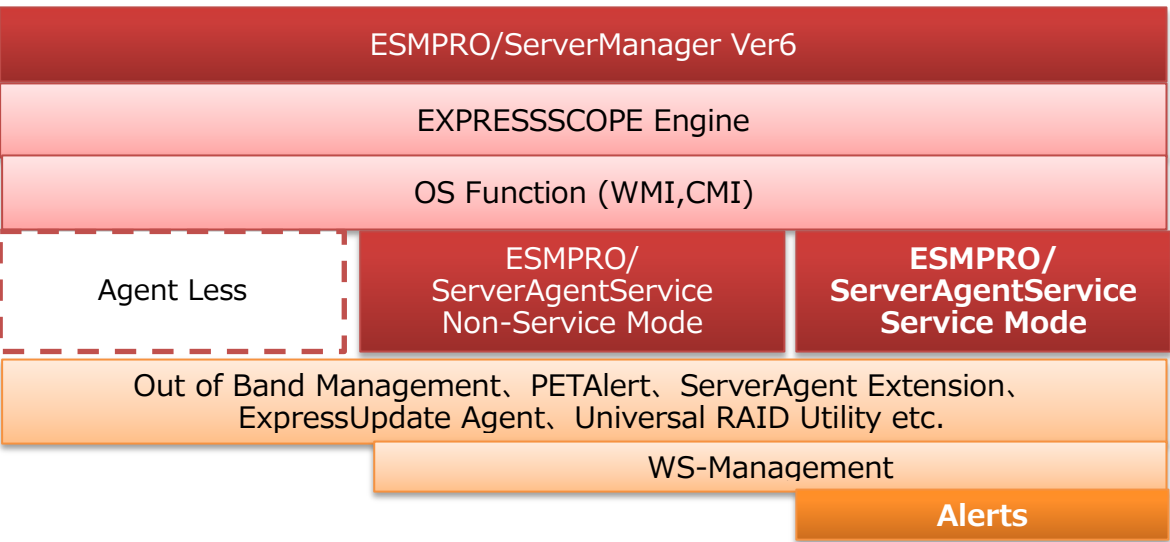
NEC ESMPRO ServerAgentService is a program to provide various information available via OS by using “WS-Management (WS-Man)”, an OS standard protocol and to control servers. The operation styles including NEC ESMPRO ServerAgentService are selectable according to the needs of customers.  
**(NEC ESMPRO ServerAgentService is available with NEC ESMPRO Manager Ver6 or later.)**

## 14.1 About NEC ESMPRO ServerAgentService

ESMPRO collects various information within the server products from Out Of Band (OOB: firmware attached to the server, such as BMC, etc.) or from In Band (IB: operating system installed in the server). NEC ESMPRO ServerAgentService has greatly advanced to "Agentless" by minimizing information collected from IB, compared to the conventional NEC ESMPRO Agent, and by collecting OOB information by NEC ESMPRO Manager. However, when it becomes agentless, a function of ESMPRO to report failure within OS will be unavailable. Therefore, the report function is provided by NEC ESMPRO ServerAgentService.

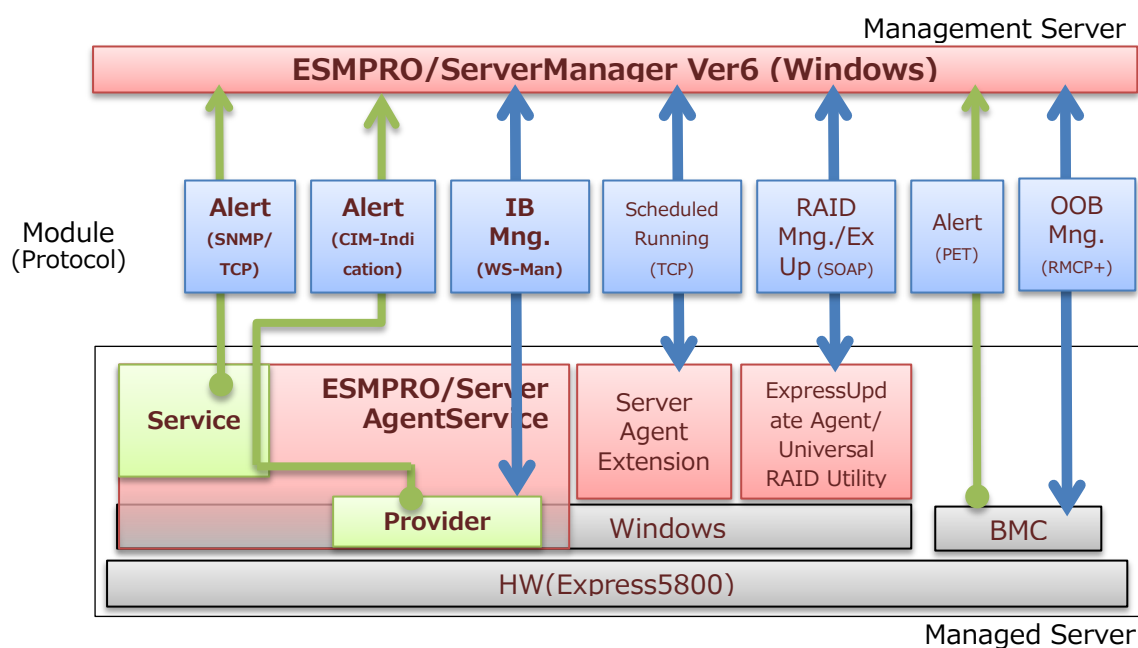
## 14.2 Service Mode and Non-Service Mode

In NEC ESMPRO ServerAgentService, “Service Mode” and “Non-Service Mode” are selectable at the installation. In “Non-Service Mode”, various information can be acquired by using WS-Man. In “Service Mode”, where the software is resident, alert to NEC ESMPRO Manager by CIM Indication, trap notification via SNMP, and report to the maintenance center are available in addition to the feature of Non-Service Mode. It is recommended to select Service Mode for management and monitoring of the system.

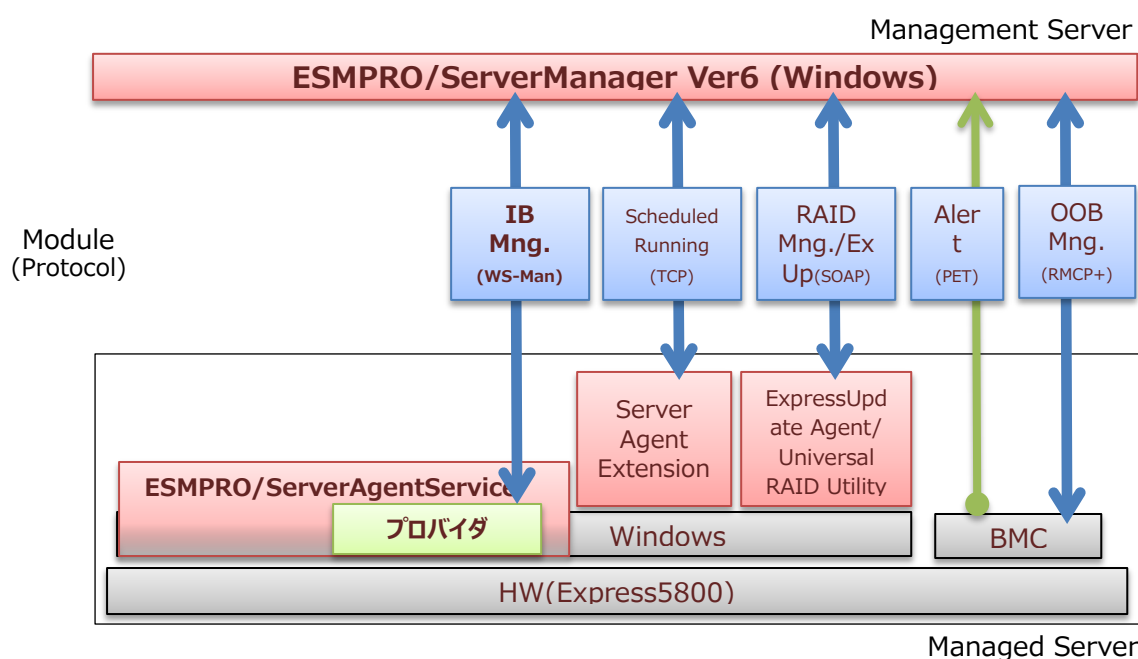


**Figure 94 Configuration Diagram of Operation Management**

The following diagram indicates the relations of NEC ESMPRO Manager, NEC ESMPRO ServerAgentService, and relating components.



**Figure 95 Configuration Diagram of Operation Management (Service Mode)**



**Figure 96 Configuration Diagram of Operation Management (Non Service Mode)**

The following sections explain four items (CPU, memory, storage, file system) which can be monitored by IB.

### 14.3 CPU Monitoring

CPU of the server can be monitored by using NEC ESMPRO Manager and NEC ESMPRO ServerAgentService.



### 14.3.1 Setting Item for CPU Monitoring

NEC ESMPRO ServerAgentService reports to NEC ESMPRO Manager when it detected the CPU load state exceeding the preset threshold. The state fluctuation of each CPU can be confirmed from Web Console of NEC ESMPRO Manager.

CPU Name	Each CPU, sum of CPU (CPU TOTAL)
Set Value	Abnormal threshold value, abnormal release value, warning threshold value, warning release value

By default, the above items are disabled in all CPU. Enable the monitoring targets and change the respective set values. The default value of each set value is 100%, 97%, 95%, and 92% from left.

Abnormality release value and warning release value are to reset abnormal state and warning state caused by exceeding abnormal and warning threshold value, when values fall below these release values. For example, in the case of default set value, CPU state turns warning when CPU utilization exceeds 95%, and warning state is released and turns normal when it falls below 92%.

### 14.3.2 How to Monitor CPU

By monitoring CPU load state, CPU utilization of each preset monitoring interval can be acquired. And the set value for the collected data can be selected from the table below.

Monitoring Target (Utilization)	1 minute, 5 minutes, 30 minutes, 1 hour, 1 day, 1 week
Monitoring Interval (second)	1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60

By default, "Utilization for 1 minute" and "10 seconds" are set, which means, CPU utilization rate is monitored for a minute with the interval of 10 seconds.

## 14.4 Memory Monitoring

Memory usage of the server can be monitored by using NEC ESMPRO Manager and NEC ESMPRO ServerAgentService.

### 14.4.1 Set Item for Memory Monitoring

NEC ESMPRO ServerAgentService reports to NEC ESMPRO Manager when it detected the memory usage exceeding the preset threshold. The state fluctuation of each memory can be confirmed from Web Console of NEC ESMPRO Manager.

Monitoring Target	Physical memory, virtual memory, page file
Set Value	Error threshold value, Error reset value, warning threshold value, warning reset value

By default, all the items are disabled. Enable the monitoring targets and change the set values upon necessity. Each default set value is calculated based on the total capacity of Physical memory, Virtual memory and page file. For example, Error value is 95 % of total capacity, Error reset value is 90% of total capacity, Warning value is 85% of total capacity and Warning reset value is 80% of total capacity. For details of each set value, refer to documents on NEC ESMPRO ServerAgentService.

### 14.4.2 How to Monitor Memory

Memory monitoring acquires the target memory usage by monitoring interval, and reports when it exceeds the above described set value. Settable value for the monitoring interval ranges from 1 to 32767.

By default, it is set to “60 seconds”.

## 14.5 Storage Monitoring

Preventive maintenance state of HDD (or SSD) in single configuration (on-board SATA) can be monitored by using NEC ESMPRO Manager and NEC ESMPRO ServerAgentService.

Settable items are "enable/disable HD preventive maintenance" and "monitoring interval (in seconds)". By default, they are set to "HD preventive maintenance - enabled, monitoring interval - 60 seconds".

## 14.6 File System Monitoring

File system (in Windows, drive) usage of the server can be monitored by using NEC ESMPRO Manager and NEC ESMPRO ServerAgentService.

### 14.6.1 Set Items for File System Monitoring

NEC ESMPRO ServerAgentService reports to NEC ESMPRO Manager when it detected the file system usage exceeding the preset threshold. The state fluctuation of each file system can be confirmed from Web Console of NEC ESMPRO Manager. Each default set value is calculated based on the size of each drive. For example, Error value is about 1% of total capacity and Warning value is about 10% of total capacity.

Monitoring Target	Each file system (drive)
Set Value	Error, Warning

### 14.6.2 How to Monitor File System

File system monitoring acquires the target file system capacity by preset monitoring interval, and reports when it exceeds the above described set value. Settable value for the monitoring interval ranges from 10 to 3600 (seconds).

By default, File system monitoring is enabled and monitoring interval is set to “60 seconds”.

# Appendix A Log Collection

This appendix describes how to collect logs in an event of an issue occurred when NEC ESMPRO Manager, NEC ESMPRO Agent, NEC ESMPRO ServerAgentService or EXPRESSSCOPE Engine 3 are running.

## 1. NEC ESMPRO Manager

The following two types of logs need to be collected.

- Log collected by logging in the management server (collectm)
- Application log collected on WebConsole.

The methods of how to collect logs are described below.

### Log collected by logging in the management server (collectm)

1. Log in to a management server as a user with administrative privilege.
2. Execute collectm.exe located in the following folder.  
\**<Installation path of NEC ESMPRO Manager>\esmsm\collectm\collectm.exe*
3. smlog folder is created. The log is stored under the folder.



Logs do not need to be collected when a Linux version of NEC ESMPRO Manager is used.

### A method of application log collection

Go to “About NEC ESMPRO Manager” and select “Application Log” tab to collect the log. The application log is a log that records communication with the management target servers and events triggered by operations or tasks performed by the operator, and is sorted by the date/time. Clicking the item name allows you to sort out the list by the item. Clicking the “Download” allows you to download the application log and the other information on NEC ESMPRO Manager. The maximum number of application logs can be modified by selecting “Environment Setting” and “Option Setting”. When the number of logs collected surpasses the maximum number, it deletes from oldest log and records a new log.



Follow the steps below when log-in to the WebConsole is failed, and the application logs cannot be collected.

### <Windows>

1. Log in to the management server as a user with administrative privilege.
2. Click “Control Panel”, “Administrative Tools” and “Services” to stop the services by the following order.
  - 1) ESMPRO/SM Web Container
  - 2) ESMPRO/SM Event Manager
  - 3) ESMPRO/SM Base AlertListener
  - 4) ESMPRO/SM Common Component
3. *<Installation path of NEC ESMPRO Manager>*¥  
ESMWEB\wbserver\webapps\esmp\WEB-INF\service  
Collect the file stored under the “service” folder.
4. Click “Control Panel”, “Administrative Tools” and “Services” to start the services by the following order.
  - 1) ESMPRO/SM Common Component
  - 2) ESMPRO/SM Base AlertListener
  - 3) ESMPRO/SM Event Manager

#### 4) ESM/PRO/SM Web Container

##### <Linux >

1. Log in to the management server as a root user.
2. Run the following commands to stop the services
  - 1) /etc/rc.d/init.d/esmsm stop
  - 2) /etc/rc.d/init.d/esmweb stop
3. /opt/nec/es\_manager/wbserver/webapps/esmp/WEB-INF/service  
Collect a file stored under the "service" directory.
4. Execute the following commands to restart the services.
  - 1) /etc/rc.d/init.d/esmsm start
  - 2) /etc/rc.d/init.d/esmweb start

Version Information		Application Log				
[Registration count : 194count]		Download		Page [ 1 2 3 4 5 6 7 8 9 10 ]		
Type	Component Name	IP Address	Management LAN IP Address	Date/Time	User Name	Contents
Information				4/2/2015 13:56:28	Administrator	Login was successful IP Address:0:0:0:0:0:1
Information				4/2/2015 13:06:08	Administrator	Login was successful IP Address:0:0:0:0:0:1
Information				3/31/2015 16:50:08	Administrator	Login was successful IP Address:0:0:0:0:0:1
Information	Rosetta	192.168.0.74		3/31/2015 15:43:35	Administrator	Check Connection was executed.
Information				3/31/2015 15:43:19	Administrator	The component was added.
Information				3/31/2015 15:41:30	Administrator	Login was successful IP Address:0:0:0:0:0:1
Information	T110d	172.16.80.2	172.16.80.3	3/30/2015 15:37:52	Administrator	Completed to get management engine information.
Information	T110d	172.16.80.2	172.16.80.3	3/30/2015 15:37:47	Administrator	Completed to set management engine information.
Information	T110d	172.16.80.2	172.16.80.3	3/30/2015 15:37:23	Administrator	Completed to get management engine information.
Information				3/30/2015 15:37:04	Administrator	Login was successful IP Address:0:0:0:0:0:1
Information	T110d	172.16.80.2	172.16.80.3	3/30/2015 15:04:49	Administrator	Completed to get management engine information.
Information	T110d	172.16.80.2	172.16.80.3	3/30/2015 14:57:28	Administrator	The Power Consumption information was obtained.
Information	T110d	172.16.80.2	172.16.80.3	3/30/2015 14:57:23	Administrator	The Power Consumption information was set.
Information	T110d	172.16.80.2	172.16.80.3	3/30/2015 14:57:04	Administrator	The Power Consumption information was obtained.
Information	T110d	172.16.80.2	172.16.80.3	3/30/2015 14:56:58		The power reading stopped.
Information	T110d	172.16.80.2	172.16.80.3	3/30/2015 14:54:42		The power reading started.
Information	T110d	172.16.80.2	172.16.80.3	3/30/2015 14:54:41		The power reading stopped.
Information	T110d	172.16.80.2	172.16.80.3	3/30/2015 14:54:38	Administrator	The Power Consumption information was obtained.
Information	T110d	172.16.80.2	172.16.80.3	3/30/2015 14:54:33	Administrator	The Power Consumption information was set.
Information	T110d	172.16.80.2	172.16.80.3	3/30/2015 14:54:15	Administrator	The Power Consumption information was obtained.

Figure 97 Application Log

## 2. NEC ESMPRO Agent, NEC ESMPRO ServerAgentService

<Managed machines (Windows)>

1. Log in as a user with administrator privilege.
2. Execute collect.exe stored in %esmdir%\tool.

The log folder is created, and the data is stored under the folder. For details, refer to readme.txt stored under %esmdir%\tool. When a log folder is already placed in the current folder in which collect.exe exists, the folder needs to be either deleted or renamed.

3. Zip the created log folder and collect the zipped file.



### In the case a failure occurs on execution of collect.exe (Windows)

Refer to the following phenomena and workarounds.

**Table 62 Workaround in the case a failure occurs during log collection (Windows)**

Phenomenon	Workaround
A message, "Cannot access xxx.txt." (e.g., Applicat.txt, Security.txt, or System.txt) is output to command prompt during COLLECT Log collection.	This occurs when event log size is big. COLLECT collects event logs also in text format, and when the size is too big, a creation of xxx.txt takes longer time. In such a case, an error message, "Cannot access xxx.txt." may be output.
An application error occurs when running eventlog.exe during COLLECT Log collection.	A known issue of COLLECT. The correction modules for known issues are available in currently published COLLECT. Obtain the latest COLLECT (*) and collect information.
The file size of registry information keeps on increasing during COLLECT Log collection.	A known issue of COLLECT. The correction modules for known issues are available in currently published COLLECT. Obtain the latest COLLECT (*) and collect information.
The following appears during COLLECT Log collection and the process stops.  =====Error Contents===== Command : logfile.exe collect.inf log\collect.inf Command : cmd.exe /C move Errorinf.log log\Errorinf.log The process cannot access the file. It is being used by other process.	This is the waiting state for the completion of collection due to reasons such as the log file size is big. Wait until the collection completes.  COLLECT Log collects various logs to utilize them for various inspections. It may be taking time for collection of logs not directly relevant to the failure inspection you are performing. When it took too long for log collection and the process was halted, even COLLECT Logs in the middle of collection may be inspectable. In such a case, contact NEC customer support center with the following attachments: Error message contents Collected COLLECT Logs errorinf.log stored in the same folder as the executed Collect.exe
The screen remains COLLECT END and does not proceed to the next during COLLECT Log collection.	This is the waiting state for the completion of collection due to reasons such as the log file size is big. Wait until the collection completes.  COLLECT Log collects various logs to be utilized for various inspections. It may be taking time for collection of logs not directly relevant to the failure inspection you are performing. When it took too long for log collection and the process was halted, even COLLECT Logs in the middle of collection may be inspectable. In such a

	case, contact NEC customer support center with the following attachments: Error message contents Collected COLLECT Logs errorinf.log stored in the same folder as the executed Collect.exe
--	---

(\*)<http://www.support.nec.co.jp/View.aspx?id=3140100402>

<Managed machine (Linux)>

1. Log in as a root user.
2. Navigate to any directory.
3. Execute the following command.  

```
# tar czvf ntagent.log.tgz /opt/nec/esmpro_sa/log/ntgaent.*
```

 If NEC ESM PRO Agent earlier than 4.4.48-1 is used on VMware ESX server, execute the following command as well.  

```
# tar czvf vmkernel.tgz /var/log/vmkernel*
```
4. Execute collectsa.sh.  

```
# /opt/nec/esmpro_sa/tools/collectsa.sh
```

 Collect collectsa.tgz and tagent.log.tgz files which are created in the current directory.  
 If NEC ESM PRO Agent earlier than 4.4.48-1 is used on VMware ESX server, collect vmkernel.tgz as well.



#### **In the case issues occur during operation of collectsa.sh (Linux)**

If fault information collection tool (collectsa.sh) does not operate (terminate) correctly, attach the collected information and contact NEC customer support center.

1. Close the fault information collection tool (collectsa.sh).
  - ① Press <Ctrl>+<C> keys on the terminal on which the fault information collection tool (collectsa.sh) is operating.
  - ② Confirm that the fault information collection tool (collectsa.sh) is closed.  

```
# ps aux | grep collectsa.sh |grep -v grep
```

 If the following is displayed, collectsa.sh runs in the background.  

```
#root 9913 0.0 0.4 4196 1124 pts/0 T 9:46 0:00 /bin/bash ./collectsa.sh
```
  - ③ In this case, terminate the process.  

```
# kill -9 {pid}
```

 (例) # kill -9 9913
2. Compress “collectsa” directory created in the current directory in tgz format.  

```
# tar czvf collect_dir.tgz collectsa/
```
3. Collect the compressed file.

### **3. NEC ESM PRO Agent Extension**

Click “Setting” tab, “NEC ESM PRO Agent Extension Setting” and “Download Agent Log.” to download application log of NEC ESM PRO Agent Extension in a text format.

This feature is enabled when NEC ESM PRO Manager and managed servers are connected via LAN.

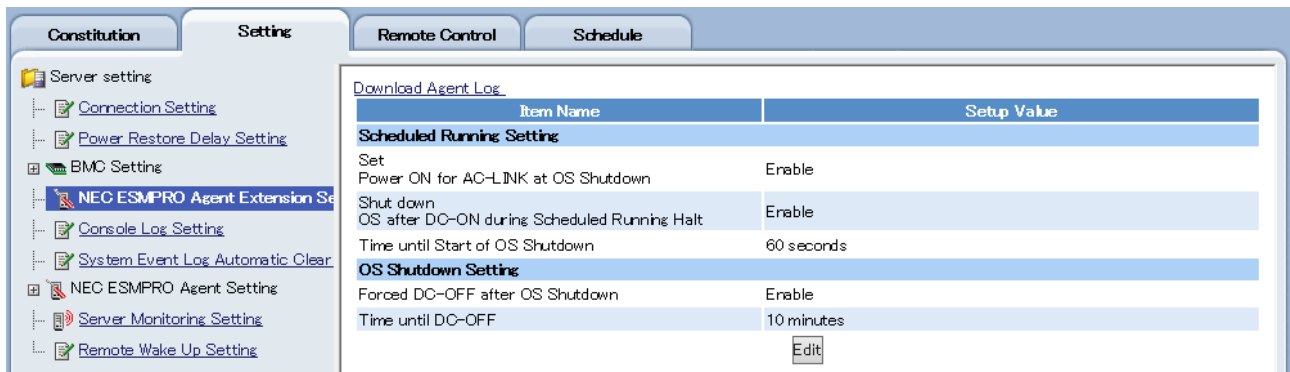


Figure 98 NEC ESMPRO Agent Extension setting screen

## 4. NEC ExpressUpdate Agent

Click “Setting” tab, “NEC ExpressUpdate Agent Setting” and “Download Agent Log.” to collect logs of NEC ExpressUpdate Agent.

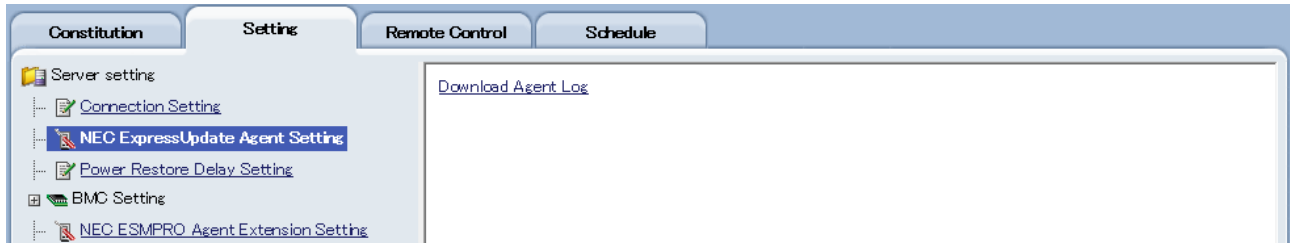


Figure 99 NEC ExpressUpdate Agent setting screen

## 5. Collection of IPMI Information

### i. NEC ESMPRO Manager

IPMI information displayed in the IPMI information screen is saved in the backup file. The saved files are displayed on the “IPMI Information Backup File List” screen in the “Tool” of the “Header Menu”. On the “IPMI Information Backup File List” screen, files can be displayed or downloaded. The IPMI information file in a binary format can be uploaded again to be read.

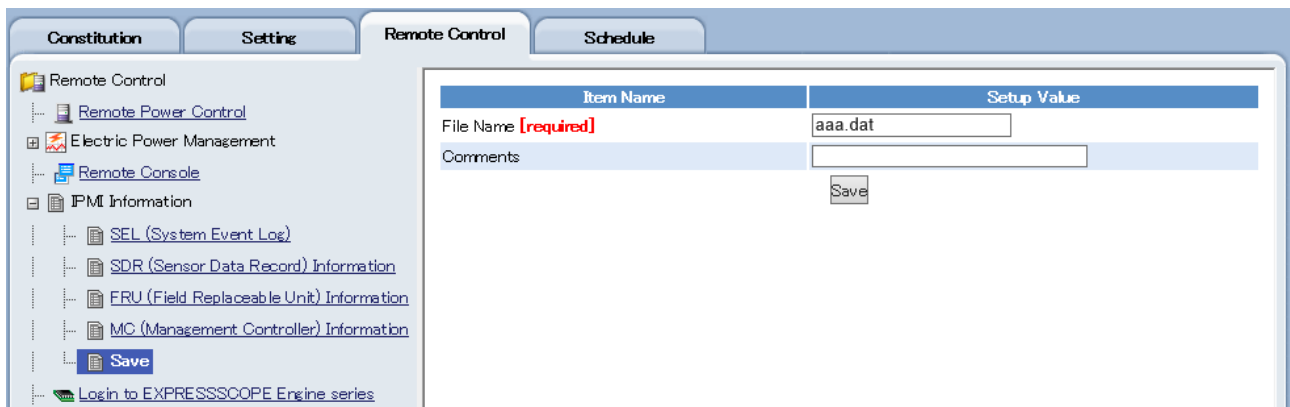


Figure 100 Saving IPMI information

IPMI Information Backup File List		Searching Registered Components		ExpressUpdate Management Information	
Upload File		Browse...	Upload		
File Name	Size	File Attribute	Backup Date/Time	Comments	
<a href="#">aaa.dat</a>	12465 byte (s)	Writable	2/26/2015 08:56:10	bbb	
<a href="#">bbb.dat</a>	16885 byte (s)	Writable	5/7/2013 14:44:14		
<a href="#">foo.dat</a>	9198 byte (s)	Writable	7/25/2013 20:54:27		
<a href="#">bmiddat</a>	27044 byte (s)	Writable	9/25/2013 16:09:21		

Figure 101 IPMI Information Backup File List



## ii. EXPRESSSCOPE Engine 3

On the WebConsole, select “System” tab and “IPMI information” and click “Backup”. Specify a destination which has a write privilege, and click “Save”. The file is saved as "ipmi.dat" by default.

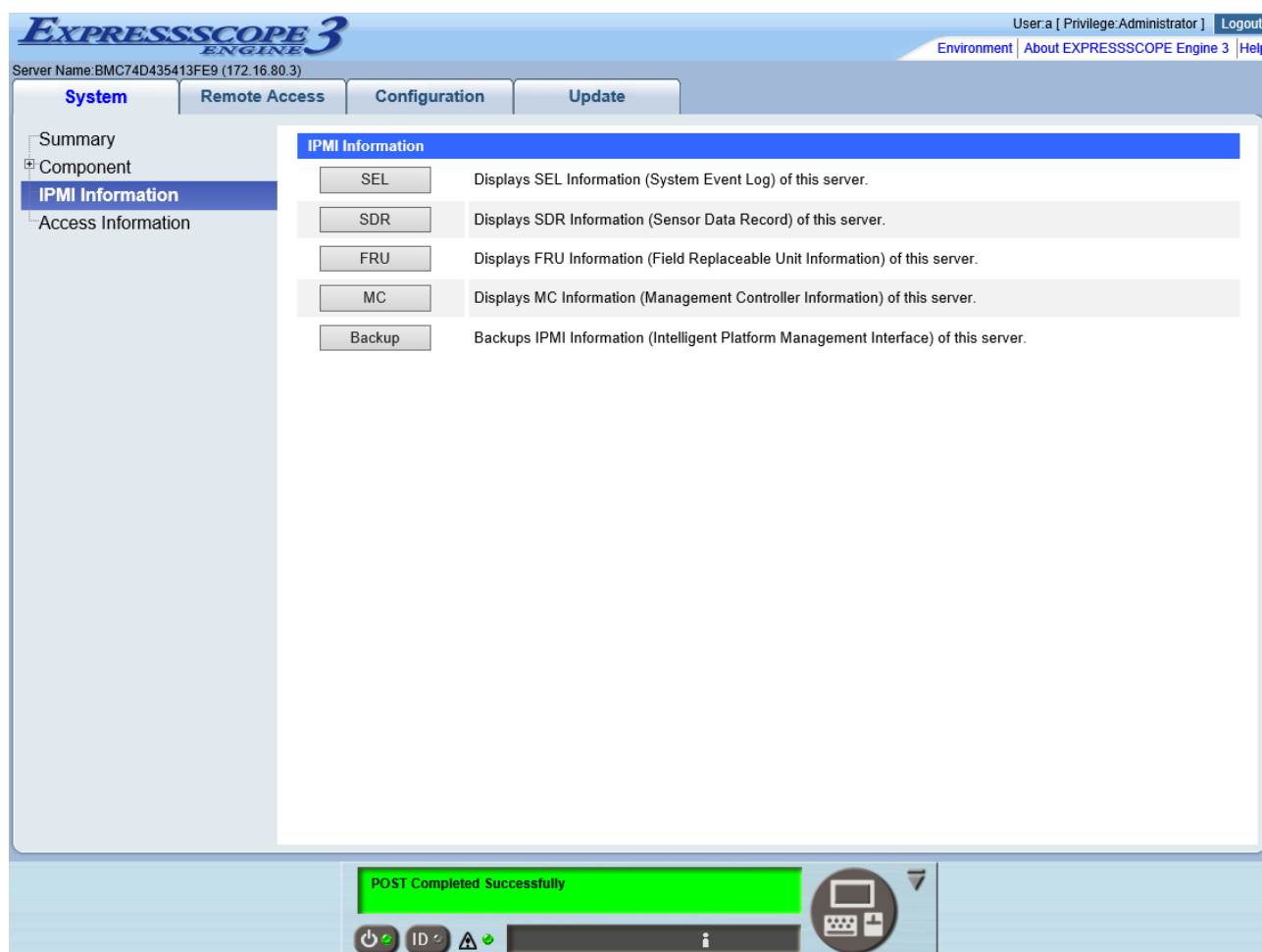


Figure 102 EXPRESSSCOPE Engine 3 WebConsole

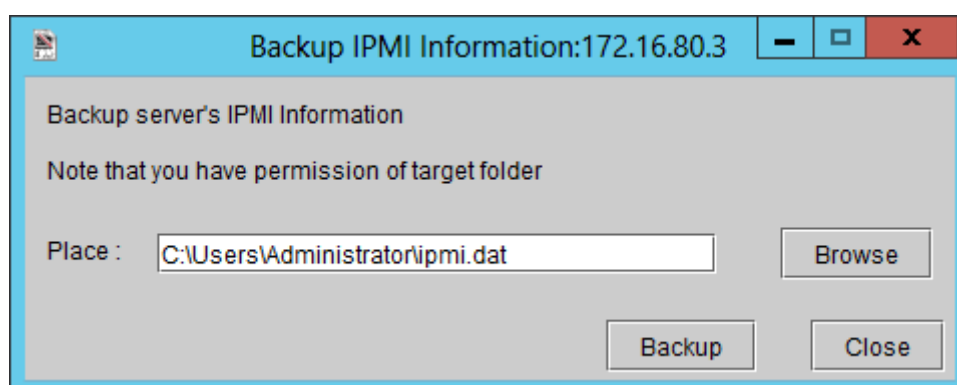
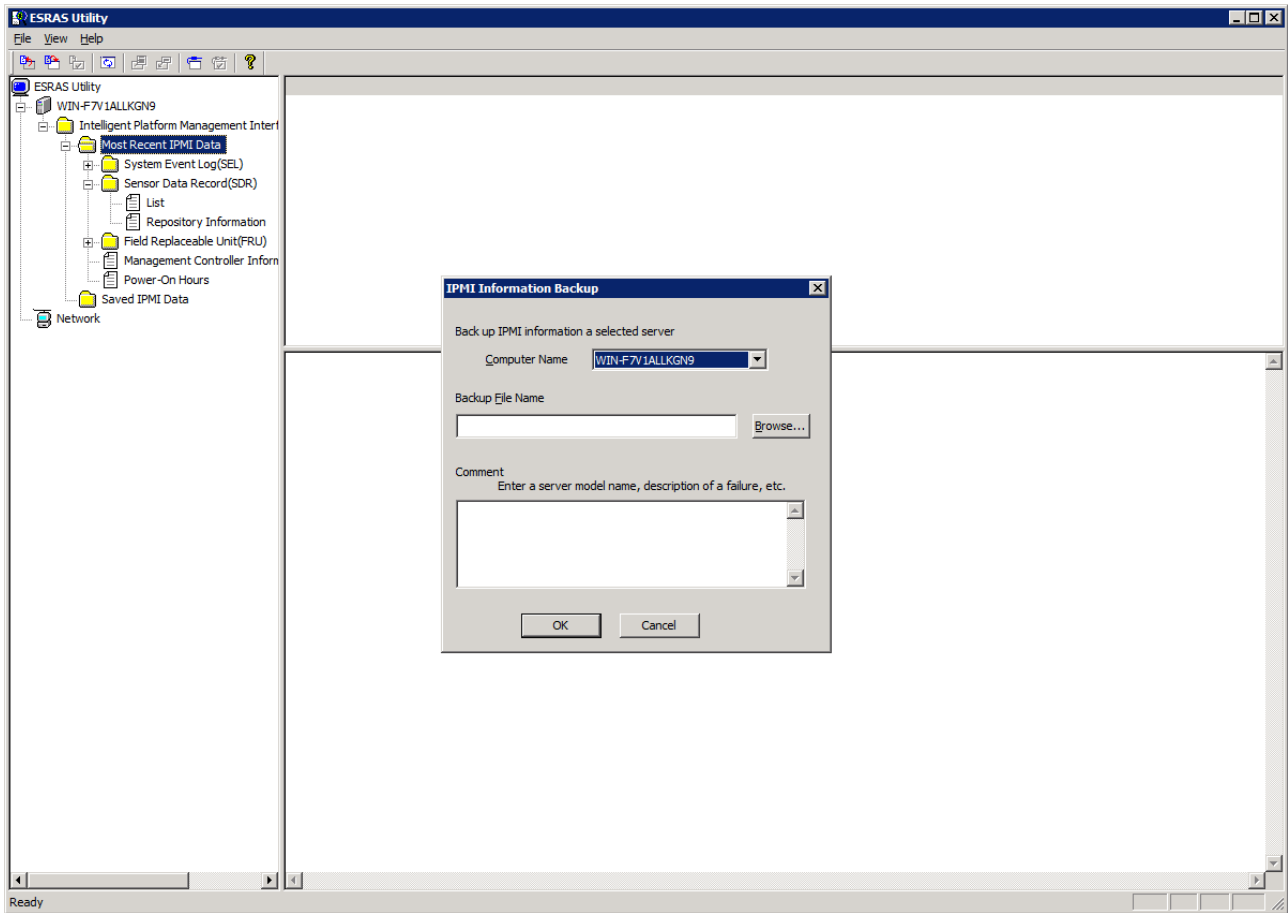


Figure 103 IPMI information backup

### iii. ESRAS Utility

On the ESRAS Utility, click “File”, “Back up the current IPMI Information...”. Specify a destination which has a write privilege, and click “OK”.



**Figure 104 ESRAS Utility IPMI information Backup dialog**

## Appendix B Comparison of EXPRESSSCOPE Engine Series Features

---

EXPRESSSCOPE Engine series have different features available for NEC ESMPRO Manager depending on the version.

**Table 61 EXPRESSSCOPE Engine Series Features**

NEC ESMPRO Manager	EXPRESSSCOPE Engine	EXPRESSSCOPE Engine 2	EXPRESSSCOPE Engine 3
Automatic Power Distribution	X	X	○
System BIOS Setting	X	X	○
Network Property	○	○	◎
Network Service	X	X	○
User Account	X	X	○
SNMP Alert	○	○	○
SNMP Alert Level Setting	○	○	◎ (The report can be set individually)
Mail Alert	X	X	○
ECO	X	○ (Selection of ECO level)	◎ (Watt value can be specified)
BMC Backup/Restore	X	X	○
BMC Reset	X	X	○
NEC ExpressUpdate via Management Controller	X	X	○

# Revision History

---

Revision	Date	Detail
1.0e	Sep 30 2015	New Document
1.35e	Nov 5 2018	Support NEC ESMPRO Manager v6