Express5800

NEC

NEC ESMPRO Manager Ver. 5.7
Installation Guide (Windows)

E5.75-01-WEB

Contents

Notations Used in This Document

Notations used in the text

In addition to safety-related symbols urging caution, 3 other types of notations are used in this document. These notations have the following meanings.

Important	Indicates critical items that must be followed when operating software.
Note	Indicates items that must be confirmed when operating software.
Tips	Indicates information that is helpful to keep in mind when using this server.

Abbreviations of Operating Systems

Windows Operating Systems (OS) are referred to as follows.

Notations in this document	Official names of Windows
Windows Server 2012 R2	Windows Server 2012 R2 Standard
	Windows Server 2012 R2 Datacenter
Windows Server 2012	Windows Server 2012 Standard
	Windows Server 2012 Datacenter
Windows Server 2008 R2	Windows Server 2008 R2 Standard
	Windows Server 2008 R2 Enterprise
	Windows Server 2008 R2 Datacenter
Windows Server 2008	Windows Server 2008 Standard
	Windows Server 2008 Enterprise
	Windows Server 2008 Datacenter
	Windows Server 2008 Foundation
	Windows Server 2008 Standard 32-bit
	Windows Server 2008 Enterprise 32-bit
	Windows Server 2008 Datacenter 32-bit
Windows 8.1	Windows 8.1 Pro 64-bit Edition
	Windows 8.1 Pro 32-bit Edition
	Windows 8.1 Enterprise 64-bit Edition
	Windows 8.1 Enterprise 32-bit Edition
Windows 8	Windows 8 Pro 64-bit Edition
	Windows 8 Pro 32-bit Edition
	Windows 8 Enterprise 64-bit Edition
	Windows 8 Enterprise 32-bit Edition
Windows 7	Windows 7 Professional 64-bit Edition
	Windows 7 Professional 32-bit Edition
	Windows 7 Ultimate 64-bit Edition
	Windows 7 Ultimate 32-bit Edition
	Windows 7 Enterprise 64-bit Edition
	Windows 7 Enterprise 32-bit Edition
Windows Vista	Windows Vista Business 64-bit Edition
	Windows Vista Business 32-bit Edition
	Windows Vista Enterprise 64-bit Edition
	Windows Vista Enterprise 32-bit Edition
	Windows Vista Ultimate 64-bit Edition
	Windows Vista Ultimate 32-bit Edition

Windows XP	Windows XP Professional x64 Edition
	Windows XP Professional

Trademarks

EXPRESSCLUSTER is a registered trademark of NEC Corporation.

Microsoft, Windows, Windows Vista, Windows Server are registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

VMware, VMware ESXi are registered trademarks or trademarks of VMware, Inc. in the United States and other countries.

Intel and Intel vPro are registered trademarks or trademarks of Intel Corporation in the United States and other countries.

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

Warnings and Additions to This Document

1. Unauthorized reproduction of the contents of this document, in part or in its entirety, is prohibited.
2. The contents of this document may change without prior notice.
3. Do not make copies or alter the document content without permission from NEC Corporation.
4. Every effort has been made to ensure the completeness of this document. However, if you have any concerns, or discover errors or omissions, please contact your retailer.
5. Regardless of these 4 items, NEC Corporation does not take responsibility for effects resulting from operations.
6. The sample values used in this document are not the actual values.

Keep this document nearby so that you may refer to it as necessary.

Latest editions

This document was created based on the information available at the time of its creation. The screen images, messages and procedures **may differ from the actual screens, messages and procedures.** Substitute as appropriate when content has been modified.

External Libraries

This product contains libraries (“external libraries”) provided by the third party suppliers ("suppliers"). Assume and agree these libraries' license documents and NOTICE files before using this product.

License documents and NOTICE files of external libraries are stored in the following folders:

*<The folder in which this product is installed>¥ESMWEB¥wbserver

*<The folder in which this product is installed>¥ESMWEB¥wbserver¥webapps¥axis2¥WEB-INF¥lib

*<The folder in which this product is installed>¥ESMWEB¥wbserver¥webapps¥esmpro¥WEB-INF¥lib

* LICENSE under the<The folder in which this product is installed>¥ESMWEB¥jre

If the external libraries require to include their source code with this product, see the folder below.

¥SM575_E¥MANAGER¥MGR¥SRC

External Libraries are listed in "External Libraries and their copyright."

Notwithstanding any of the terms in the Agreement or any other agreement you may have with NEC:

a) "Suppliers" provide the libraries WITHOUT WARRANTIES OF ANY KIND and, such Suppliers DISCLAIM ANY AND ALL EXPRESS AND IMPLIED WARRANTIES AND CONDITIONS INCLUDING, BUT NOT LIMITED TO, THE WARRANTY OF TITLE, NON-INFRINGEMENT OR INTERFERENCE AND THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE EXTERNAL LIBRARIES;

b) In no event are the suppliers liable for any direct, indirect, incidental, special, exemplary, punitive or consequential damages, including but not limited to lost data, lost savings, and lost profits, with respect to the external libraries; and,

c) NEC and the suppliers are not liable to you, and will not defend, indemnify, or hold you harmless for any claims arising from or related to the external libraries.

External Libraries and their Copyright

activation	Copyright©Sun Microsystems, Inc.
annogen	Copyright©The Codehaus.
antlr	Developed by jGuru.com, http://www.ANTLR.org and http://www.jGuru.com, Copyright©Terence Parr
Apache Axiom	Copyright©The Apache Software Foundation
Apache Axis	The Apache Software Foundation
Apache Axis2	Copyright©The Apache Software Foundation
Apache Commons Discovery	The Apache Software Foundation
Apache commons-codec	Copyright©The Apache Software Foundation
Apache commons-fileupload	Copyright©The Apache Software Foundation
Apache commons-httpclient	Copyright©The Apache Software Foundation
Apache commons-io	Copyright©The Apache Software Foundation
Apache commons-logging	Copyright©The Apache Software Foundation
Apache Derby	Copyright©The Apache Software Foundation
Apache geronimo-activation	Copyright©The Apache Software Foundation
Apache geronimo-annotation	Copyright©The Apache Software Foundation
Apache geronimo-java-mail	Copyright©The Apache Software Foundation
Apache geronimo-stax-api	Copyright©The Apache Software Foundation
Apache httpcore	Copyright©The Apache Software Foundation
Apache httpcore-nio-4.0	Copyright©The Apache Software Foundation
Apache Log4J	Copyright©The Apache Software Foundation
Apache Neethi	Copyright©The Apache Software Foundation
Apache Rampart	Copyright©The Apache Software Foundation
Apache Struts	Copyright©The Apache Software Foundation
Apache Tomcat	Copyright©The Apache Software Foundation
Apache Woden	Copyright©The Apache Software Foundation
Apache WSS4J	Copyright©The Apache Software Foundation
Apache Xalan	Copyright©The Apache Software Foundation
Apache Xerces	Copyright©The Apache Software Foundation
Apache XML Schema	Copyright©The Apache Software Foundation
Apache XML Security	Copyright©The Apache Software Foundation
Apache XMLBeans	Copyright©The Apache Software Foundation
Apache xml-commons	Copyright©The Apache Software Foundation
asm	Copyright©INRIA, France Telecom

asm-attrs	Copyright©INRIA, France Telecom
backport-util-concurrent	Copyright©Distributed Computing Laboratory, Emory University
bcprov-jdk	Copyright©The Legion Of The Bouncy Castle (http://www.bouncycastle.org)
c3p0	Copyright©Machinery For Change, Inc.
cglib	Copyright©cglib
dom4j	Copyright©MetaStuff, Ltd.
DWR	Copyright©Joe Walker
ehcache	Copyright©Luck Consulting Pty Ltd
Flot	Copyright©IOLA and Ole Laursen
ForceRedraw	Copyright©Pascal Beyeler
Hibernate	Copyright©Red Hat Middleware, LLC.
imrsdk	Copyright© Intel Corporation
jalopy	Copyright©Marco Hunsicker.
jaxb-api	Copyright©Sun Microsystems, Inc.
jaxb-impl	Copyright©Sun Microsystems, Inc.
jaxb-xjc	Copyright©Sun Microsystems, Inc.
jaxen	Copyright©The Werken Company.
JAX-RPC	http://java.net/projects/jax-rpc
JAX-WS	Copyright©Sun Microsystems, Inc.
JCIFS	Copyright©The JCIFS Project
jettison	Copyright©Envoi Solutions LLC
jibx-bind	Copyright©Dennis M. Sosnoski
jibx-run	Copyright©Dennis M. Sosnoski
Jline	Copyright©Marc Prud'hommeaux
JNA	https://github.com/twall/jna#readme
JQuery	Copyright©John Resig
JQuery UI	Copyright ©2011 Paul Bakaus, http://jqueryui.com/
JRE	Copyright©Sun Microsystems, Inc.
JSch	Copyright©JCraft, Inc.
JSONIC	Copyright©Hidekatsu Izuno
jsr173-api	Copyright©The Apache Software Foundation
jta	Copyright©Sun Microsystems, Inc.
KVMLib	Copyright©Intel Corporation
libiconv	Copyright©Free Software Foundation, Inc.

libxml2	Copyright©Daniel Veillard. All Rights Reserved.
mail	Copyright©Sun Microsystems, Inc.
msvcp90	Copyright©Microsoft
msvcr90	Copyright©Microsoft
OpenSAML	Copyright©Internet2.
OpenSSL	Copyright©The OpenSSL Project
prototype.js	Copyright©Sam Stephenson
sblim cim-client	http://sourceforge.net/apps/mediawiki/sblim/index.php?title=CimClient
sortable	Copyright©Stuart Langridge
Table Drag and Drop JQuery plugin	Copyright©Denis Howlett <denish@isocra.com>
Treeview JQuery plugin	Copyright©2007 Jörn Zaefferer
vSphere Web Services SDK	http://communities.vmware.com/community/vmtn/developer/forums/managementapi
WISEMAN	Copyright©Sun Microsystems, Inc.
WSDL4J	Copyright©IBM Corp
wstx	Copyright©The Codehaus Foundation
zlib	Copyright©Jean-loup Gailly and Mark Adler

NEC ESMPRO Manager Ver. 5.7

1 General Description

This chapter explains NEC ESMPRO Manager.

1. Introduction

2. About Downloading Latest NEC ESMPRO

Describes about Downloading Latest NEC ESMPRO.

3. System Requirements

Describes about the need environment of NEC ESMPRO Manager.

1. Introduction

Read this document so as to gain an adequate understanding of the contents.

The contents in this document are intended for users who fully understand features and operations of OS related to this utility.

If you want to know operations of OS, or if there is any unclear point, see the online help of each OS.

NEC ESMPRO Manager is a software designed for reducing operational management costs by remotely managing servers.

NEC ESMPRO Manager has the following features.

Note Some models of managed servers may not support all functions. See "Managed Server" at "System Requirements".

- **Rebuilding even if OS on the managed server has failed.**

  Even if OS on the managed server is inoperable (in the state of OS's stall, BIOS Power On Self Test (POST), or DC OFF), NEC ESMPRO Manager allows you to collect the managed server's hardware information and control the power supply.

- **Operation while viewing the managed server's screen.**

  While key-in and mouse operations are enabled, the managed server's screen can be viewed on the remote browser at any time during POST just after the managed server is turned ON and even after Windows or Linux has been booted.

  Note After Windows or Linux starts up, login to EXPRESSSCOPE Engine series, key input and mouse operation are possible from remote KVM.

- **Operation of more than one managed server at a time.**

  By specifying a group, you can provide power control or change a setting for managed servers through a single operation.

- **Specification of remote operation time.**

  The managed server can be turned OFF or information can be collected at pre-specified time, so NEC ESMPRO Manager is available for nighttime batch processing.

- **Easy operation through the Internet.**

  The managed server can be operated with a web browser. If you use Internet's standard Secure Socket Layer (SSL) for NEC ESMPRO Manager, you enable secure remote operation from an external network.

- **Update of firmware and software on the managed server. (NEC ExpressUpdate)**

  NEC ExpressUpdate is the function that manages versions of modules like firmware and software on the managed server and that updates the modules.

  NEC ExpressUpdate can download the update packages automatically for the managed server, and install them without stopping the system.

2. About Download of Latest NEC ESMPRO

See the following URL for NEC ESMPRO information. You can download the latest version of NEC ESMPRO from URL.

http://www.58support.nec.co.jp/global/download/index.html

3. System Requirements

NEC ESMPRO Manager requires the following hardware and software:

3.1 PC for Management

Important

About product license
NEC ESMPRO Manager can be used on a single OS per license.

• Hardware

- Machine: A computer on which OS supported by NEC ESMPRO Manager can be installed
  Intel Pentium 4 1.3GHz or higher, or equivalent compatible processor is recommended.
- Memory: Memory required for running OS plus 512MB or more (1GB or more is recommended.)
- Free hard disk space: 400MB or more

• Software

- OS:
  Windows Server 2012 R2
  Windows Server 2012
  Windows Server 2008 R2 (up to SP1)
  Windows Server 2008 (up to SP2) *1
  Windows 8.1
  Windows 8
  Windows 7 (up to SP1)
  Windows Vista (up to SP2)
  Windows XP (up to SP3 for 32-Bit, up to SP2 for 64-Bit Edition)

  *1 Windows Server 2008 Foundation SP2 is not supported.

Important

- NEC ESMPRO Manager is available on neither Windows Server 2003, nor Windows Server 2003 R2.
- NEC ESMPRO Manager is available on neither Server Core, nor Minimal Server Interface.

- Web client: Internet Explorer 8.0 / 10.0 / 11.0
  Firefox ESR 24 (Windows / Linux)

Important

- If you use NEC ESMPRO Manager from a browser, install JRE 7 and above. On a point of the security, the latest version is recommended. If JRE is not installed, some pages are not displayed correctly.
- Java Applet and Java scripts must be executable. Please set the web browser to play animation in web pages.
- 1024 by 768 pixels or more are recommended as a screen area in display properties.
- The browser must be latest status such as applying a patch.
  If the status is not updated such as preinstalled, some pages may not be displayed correctly.

⧫ Number of managed servers: Addition of server licenses permits a single NEC ESMPRO Manager to manage a maximum of 1000 servers.

3.2 Managed server

A server to be managed by NEC ESMPRO Manager is as follows:

- Baseboard Management Controller (BMC)

  About the managed server integrated BMC, see "Appendix C Managed Components Summary" in "NEC ESMPRO Manager Ver.5 Setup Guide".

  Note The required environment varies depending on the connection type with the managed server. See "Chapter1 3.3 Requirements for Connection between PC for Management and Managed Server".

- Simple Network Management Protocol (SNMP)

  If you use SNMP monitoring function, the following software is need on managed server. (No matter if BMC is integrated or not.)

  - NEC ESMPRO Agent (Ver. 4.1 and above)
  - The following ft server are supported.

  Express5800/ft server [R320c-M4/R320c-E4]

  Note The following servers are not supported.
  - NEC ESMPRO Agent (Windows) for other vendor's server (up to Ver. 4.4)
  - NEC ESMPRO Agent (Linux) for other vendor's server (up to Ver. 4.2.22-1)

- Firmware

  If you use NEC ExpressUpdate function that manages versions of modules like firmware and software, the following software or EXPRESSSCOPE Engine 3 is required on the managed server.

  - NEC ExpressUpdate Agent

- ESXi

  ESXi5.0 / 5.1

- RAID system

  If you manage RAID system using Universal RAID Utility on the managed server, the following software is required on the managed server.

  - Universal RAID Utility Windows Edition (Ver2.1 or later)
  - Universal RAID Utility Linux / VMware ESX Edition (Ver2.4 or later)

- vPro

  About the managed server based on vPro, see "Appendix C Managed Components Summary" in "NEC ESMPRO Manager Ver.5 Setup Guide".

Note
- If Windows Firewall is enabled, communication will be interrupted.
  See Appendix "Chapter4 2 Port numbers / Protocols" and open the required ports.
- NEC ESMPRO Manager and a managed server needs to be the same OS language.

3.3 Requirements for connection between PC for Management and managed server

Provide an environment in accordance with the connection type to be used.

- **LAN connection**
  - **TCP/IP network**

Note

- Do not use a cross cable to connect PC for Management and managed server.
- If you use the managed server integrated BMC, LAN port that BMC uses depends on the type of BMC. Some BMC uses standard LAN port. Other BMC uses a Management LAN Port. There are 2 types of managed servers on that BMC uses standard LAN port to connect with NEC ESMPRO Manager: one type is permitted to use only LAN1 port, and the other type is permitted to use both LAN1 and LAN2 ports. See "Appendix C Managed Servers Summary" in "NEC ESMPRO Manager Ver.5 Setup Guide".

- **Modem connection** (Only available for BMC connection)
  - **Phone line**
  - **Modem**

Use a modem that supports the following functions:

Baud rate	:	19.2Kbps
Data bits	:	8bit
Parity	:	None
Stop bits	:	1bit
Flow control	:	Hardware (CTS/RTS)

Note

- Use the modem recommended for NEC Express 5800 series on the managed server.
- Connect the modem to the serial port 2 on the managed server.

  - **Other Information**

When BMC send alert to PC for Management via modem, it is necessary the following:

- Dial-up router or PPP server

- **Direct connection** (Only available for BMC connection)
  - **RS-232C cross cable**

The serial port for direct connection on ESMPRO server. NEC ESMPRO Manager must be set following on OS.

Bits per speed	: Be set a same value with a value of BMC configuration on a managed server. The default value of BMC configuration is 19.2Kbps.
Data bits	: 8bit
Parity	: None
Stop bits	: 1bit
Flow control	: Hardware (CTS/RTS)

Important

- Do not use an interlink cable.
- Connect RS-232C cross cable to serial port 2 on the managed server.
- Some models of managed servers do not permit use of any RS-232C cross cable other than the specified one. See Maintenance Guide provided with the server.

3.4 Notes on managed servers and network devices

This section explains particular notes on managed servers and network devices.

- **Use of network switch / router**

  If the managed server installed BMC that uses a standard LAN port or loaded Advanced Remote Management Card, and there is network switch / router between PC for Management and the managed servers, set the network switch / router to receive Gratuitous ARP. See each document of the switch / router about how to set it.

  If Gratuitous ARP cannot be received, managed server that is power-off status is not connected.

- **Use of a layer-2 / layer-3 switching hub**

  Set "Disable" for Spanning Tree Protocol (STP) function of the switching hub or STP of the port to which a managed server is connected.

  Set "Enable" for the auto-negotiation function of the port to which a managed server is connected.

- **Use of DHCP**

  In case that BMC on the managed server uses a standard LAN port, communication between NEC ESMPRO Manager and System BIOS or BMC is not compatible with a DHCP environment.

  Be sure to use a fixed IP address with NEC ESMPRO server in which NEC ESMPRO Manager is to be installed.

  To use a managed server in a DHCP environment, start DianaScope Agent or NEC ESMPRO Agent Extension.

- **Setting of Teaming for standard LAN with OS (providing redundancy or multiplexing with multiple network adapters) on the managed server installed BMC that uses a standard LAN port**

  The managed server installed BMC that uses a standard LAN port shares the embedded standard LAN controller between BMC, System BIOS and OS, but BMC and System BIOS do not support LAN teaming modes including Adapter Fault Tolerance (AFT) and Adaptive Load Balancing(ALB). So if AFT mode or ALB mode was made available by OS, NEC ESMPRO Manager can communicate with BMC and System BIOS only under the following conditions while Failover does not occur.

  - If Receive Load Balancing (RLB) is set with ALB, disable RLB. (If RLB cannot be disabled, NEC ESMPRO Manager cannot communicate with BMC.)
  - Make the teaming-set address ("preferred primary") identical to LAN1 IP address and MAC address in BMC configuration information.
  - Even if the configuration of LAN2 for BMC on the managed server is available, do not set LAN2 in BMC configuration information.
  - See "Appendix B B.1 On the managed server that BMC uses standard LAN port" in "NEC ESMPRO Manager Ver.5 Setup Guide" if you install DianaScope Agent or NEC ESMPRO Agent Extension on the managed server whose OS is Windows.

    Note that NEC ESMPRO Manager cannot communicate with BMC when you use RLB or Fast Ether Channel (FEC) teaming mode on the managed server.

- **Setting of Teaming for LAN that DianaScope Agent or NEC ESMPRO Agent Extension uses with OS (providing redundancy or multiplexing with multiple network adapters) on the managed server installed BMC that uses a Management LAN port**

  If the teaming setting is made available for LAN port that DianaScope Agent uses on the managed server installed BMC that uses a Management LAN port, see "Appendix B B.2 On the managed server that BMC uses a Management LAN port" in "NEC ESMPRO Manager Ver.5 Setup Guide".

- **Change of the hardware of a default gateway or an alert receiver**

  In case that there is a gateway between a PC for Management and a managed server, re-configure BMC on the managed server after the change the hardware of the gateway. In case that there is not gateway between an alert receiver and a managed server, re-configure BMC on the managed server after the change the hardware of the alert receiver. BMC on the managed server can know MAC address of the new hardware by setting BMC configuration.

- **Use of a dialup router or a PPP server**

  If an alert receiver via modem uses Windows Remote Access Service, select "Allow any authentication including clear text" about the encryption on the Windows Remote Access Service properties.

- **Restrictions on use of the standard serial port 2 (COM2)**

  The standard serial port 2 (COM2) on a managed server cannot be used for connecting another device in the following cases because BMC occupies the serial port 2.

  - The managed server compatible with Serial over LAN (SOL) and set enable on following BMC Configuration items:

    "Remote control (WAN/Direct)"

    "Redirection (LAN)"

    "Redirection (WAN/Direct)"
  - Connection via modem or direct connection has been made.
  - Direct connection has been set in BMC configuration information. (Even if NEC ESMPRO Manager and managed server are not connected, BMC occupies the serial port 2 (COM2).)

  Note See "Appendix C Managed Components Summary" in "NEC ESMPRO Manager Ver.5 Setup Guide" to confirm whether that your server supports SOL.

NEC ESMPRO Manager Ver. 5.7

2 Installation

This chapter explains installation of NEC ESMPRO Manager.

1. Before Installation

Describes about necessary setting before NEC ESMPRO Manager installation.

2. Installation

Describes about installation procedure of NEC ESMPRO Manager.

3. After Installation

Describes about necessary setting after NEC ESMPRO Manager installation.

1. Before Installation

Be sure to read this page before installing NEC ESMPRO Manager.

Security settings – Setting up NEC ESMPRO User Group

To make the applications run on PC for Management have proper access rights, NEC ESMPRO User Group is needed. NEC ESMPRO User Group name must be determined during the installation. The Manager setup names it "Administrators" by default.

If you want to specify another user group name, you must create it before installing NEC ESMPRO Manager and specify the group name during installation. NEC ESMPRO User Group is case sensitive. Also, to make this security feature function effectively, install NEC ESMPRO Manager on a hard drive formatted with NTFS.

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

Confirming the disk space required for operation

Prepare sufficient free space in the folder you specified at installation. By default, the installation folder is "¥Program Files¥ESMPRO" on the system drive.

The following files are added at operation. See them before you calculate the required disk space.

- About 10MB as a management area.
- About 10KB per server.
- Maximum of 60KB per IPMI information collection of a server.
- About 1KB per alert.

Setting access permissions

When installing NEC ESMPRO Manager in an already existing folder, NEC ESMPRO Manager will not operate unless the access permissions required for NEC ESMPRO Manager operation have been set. When installing NEC ESMPRO Manager in a folder that does not exist, the following access permissions are set by the installer:

Administrators Full Control(All)(All)

Everyone Read(RX)(RX)

SYSTEM Full Control(All)(All)

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

Remote installation of NEC ESMPRO Manager

When installation of NEC ESMPRO Manager completes, you need to reboot the system.

Careful attention is needed to install the program in the environment where reboot cannot be performed from the Start menu, such as on Remote Desktop of Windows XP.

Tips

OS can be restarted by running the following command at Command Prompt:
Ex.) When you want to restart the system immediately: shutdown -r -t 0

Installation for multisession terminal server or Remote Desktop Server access

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

- **For Windows Server 2008**

  Use [Install Application on Terminal Server] in [Control Panel].

- **For Windows Server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2**

  Use [Install Application on Remote Desktop Server] in [Control Panel].

Important

If you do not follow the procedure above, a message indicating the occurrence of the error during the setup is displayed and the setup stops.

If an older version of NEC ESMPRO Manager has been already installed

- If NEC ESMPRO Manager Ver. 4.1 or later has been already installed, you can update it to this version. If any version other than the above has been installed, uninstall it before installation.
- Note that if you perform update installation from NEC ESMPRO Manager Ver. 5.0 or prior with Web Component installed, Web Component will be uninstalled at the update installation.
- If you perform update installation from older version of NEC ESMPRO Manager, the registered information is inherited.
- Note that "BMC Remote Control Tool" for out-of-band management included in NEC ESMPRO Manager Ver. 4.43 / Ver. 4.51 will be removed and cannot be accessed if you update your NEC ESMPRO Manager to this version.

If DianaScope Manager has been installed

If DianaScope Manager has been installed, you can update it to this version. The information registered to DianaScope Manager will be inherited.

Sample of Script Component

When you changed a sample of Script Component and saved it as the original file name, change the file name before performing update installation. If you perform update installation without doing that, the sample will be overwritten and the changes might be initialized.

If NEC Management Workstation Application (MWA) has been installed

If MWA has been installed, you cannot install NEC ESMPRO Manager. Uninstall MWA.

Changing language settings in Windows (ex. In the case of using MUI)

When changing the language settings in Windows, make sure "Japanese" is not selected in the settings below. "Japanese" is not supported, and therefore installation will fail.

You must also make consistent language settings, that is, choose the same language (except Japanese) in the settings below.

- **Windows XP**

  Control Panel - Regional and Language Options - [Regional Options] tab
  - [Languages] tab
  - [Advanced] tab

- **Windows Server 2008 / Windows Server 2008 R2 / Windows Vista / Windows 7**

  Control Panel - Region and Language - [Formats] tab
  - [Location] tab
  - [Keyboards and Language] tab
  - [Administrative] tab

- **Windows Server 2012 / Windows Server 2012 R2 / Windows 8 / Windows 8.1**

  Control Panel - Language - Change date, time, or number formats - [Formats] tab
  - [Location] tab
  - [Administrative] tab

Important Do not change language settings after installation of NEC ESMPRO Manager.
Otherwise it does not work properly.

The path of the installer

If you update NEC ESMPRO Manager to the same version as the installed version, start the installer from the same path as the installation of the last time.

2. Installation

This page describes fresh installation and update installation of NEC ESMPRO Manager.

Be sure to read "Before Installation" and install this product.

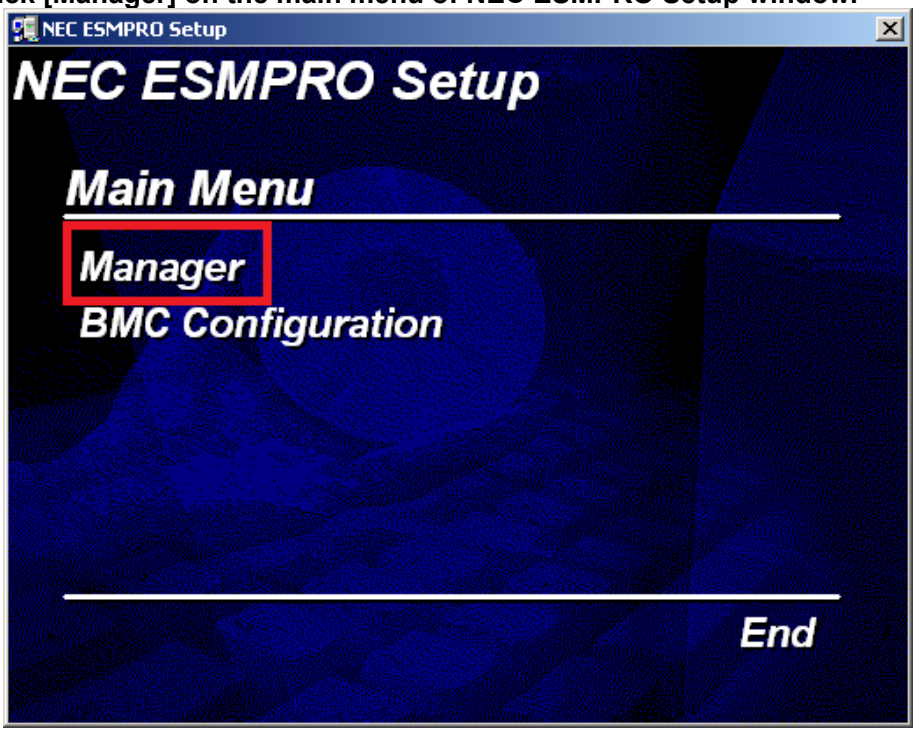
2.1 Installation procedure

Important Windows Server 2003 and Windows Server 2003 R2 is not supported.

1. **Sign-in (Log on) to the system with the built-in Administrator (or an account having administrative privilege).**
2. **Save the downloaded "SM575_E.ZIP" file in a folder of your choice, and unzip it.**

   Important If you store the setup program in a folder that is too deep in the hierarchy, the program may not be run correctly.
3. **Run the setup program "¥SM575_E¥ESMMENU¥SETUP.EXE".**

   If User Account Control is enabled, User Account Control window appears. Click [Continue] to proceed.
4. **Click [Manager] on the main menu of NEC ESMPRO Setup window.**

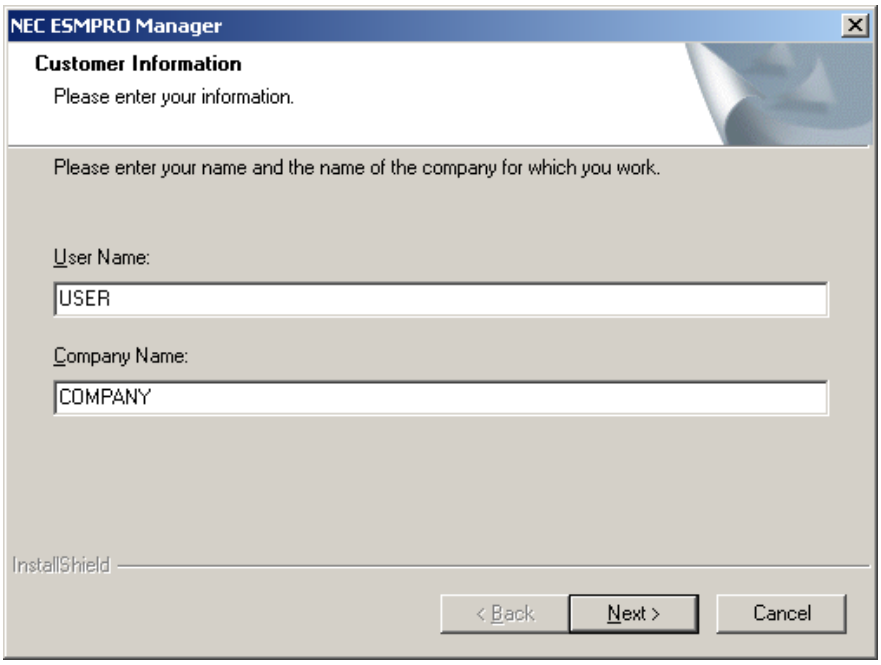


Important If you double-click the menu, two identical dialog boxes appear. Click [Exit] to close one of the dialog boxes.

Tips The displayed menu varies depending on the environment.

5. Enter the user information. (For update installation, this is not displayed.)

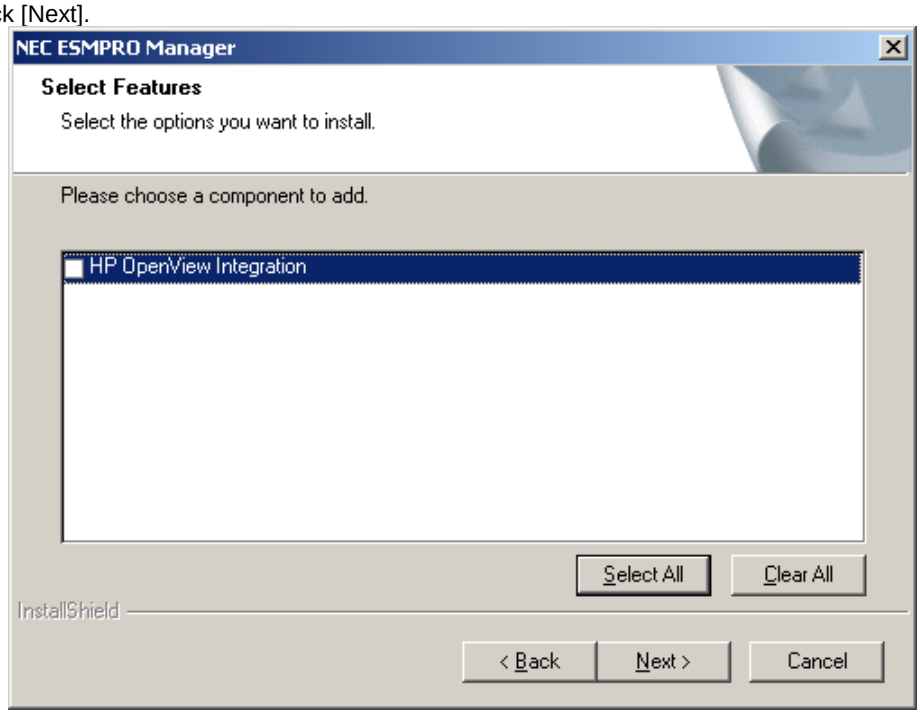
Enter your user name and company name, and then click [Next].



The user name and the company name entered here are information NEC ESMPRO Manager manages. There are no influences to the user registration information of OS.

6. Select features to be added.

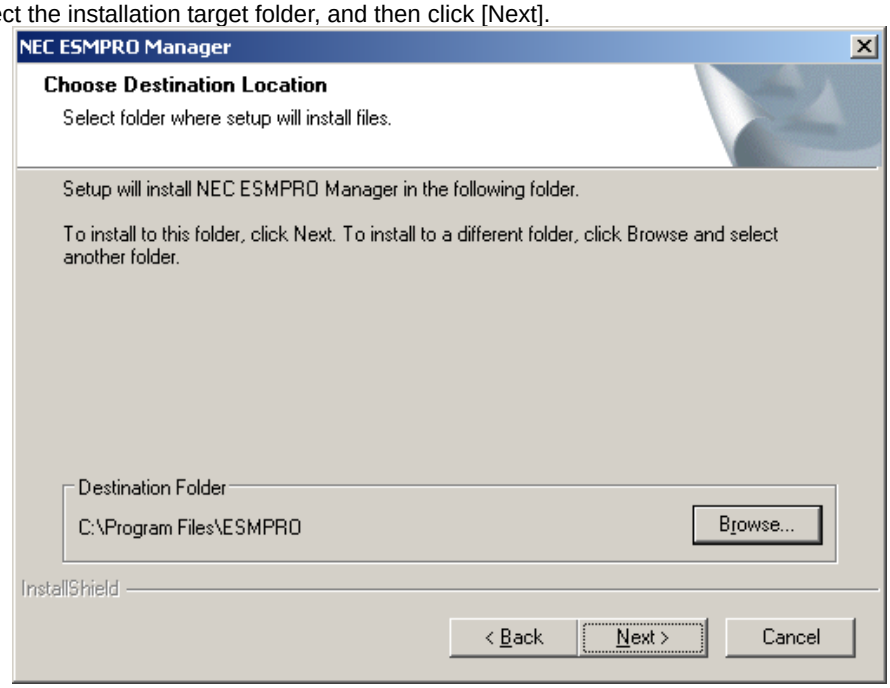
Features that can be added to NEC ESMPRO Manager are listed. Select features you want to add and click [Next].



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

7. Select the installation destination. (For update installation, this is not displayed.)

Select the installation target folder, and then click [Next].

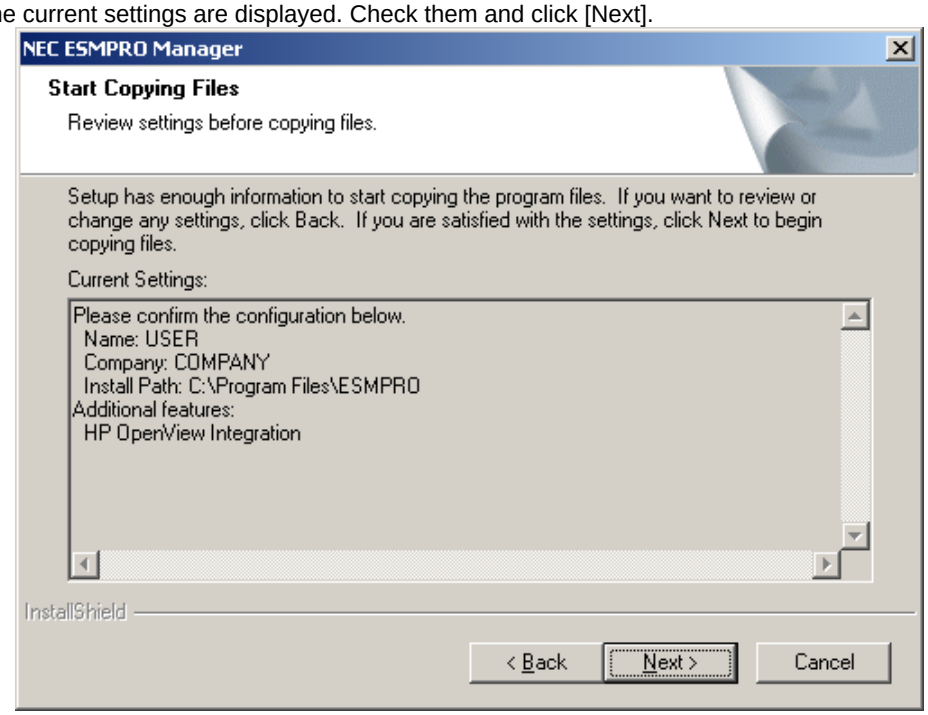


Important

The default directory for 64-bit OS is "[system drive]:¥Program Files (x86)".
You cannot specify "[system drive]:¥Program Files" for the installation directory in the 64-bit OS.

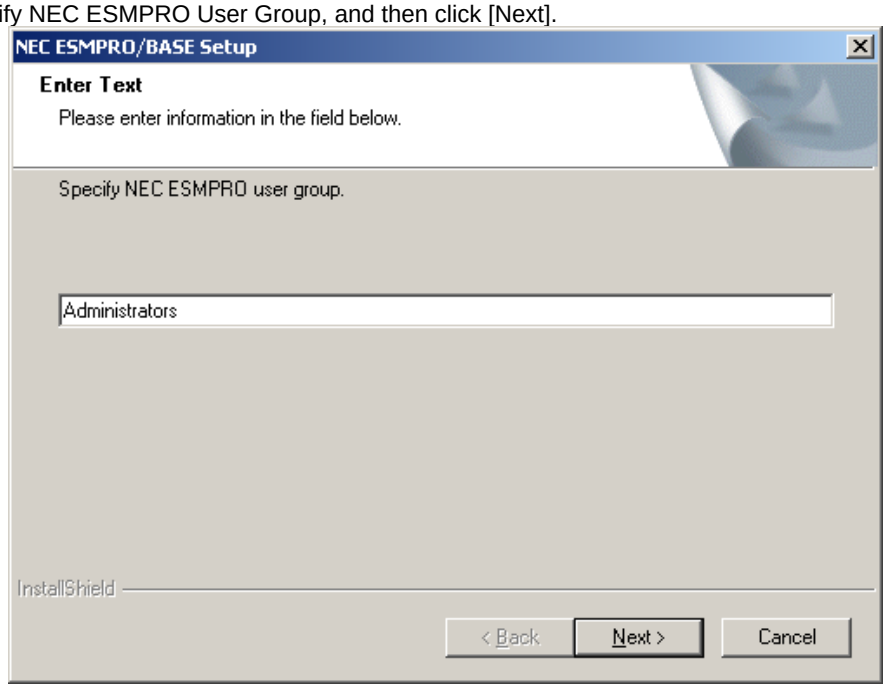
8. Check the current settings.

The current settings are displayed. Check them and click [Next].



9. Enter NEC ESMPRO User Group. (For update installation, this is not displayed.)

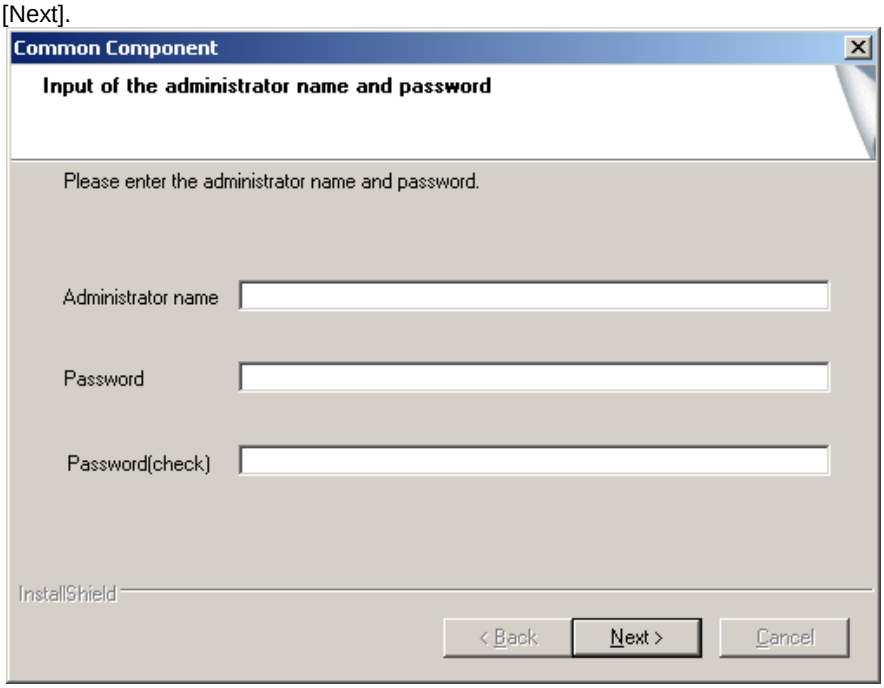
Specify NEC ESMPRO User Group, and then click [Next].



10. Enter the administrator name and the password.

(For update installation from DianaScope Manager and NEC ESMPRO Manager Ver. 5, this is not displayed.)

Create NEC ESMPRO Manager administrator. Specify the administrator name and password, and then click [Next].



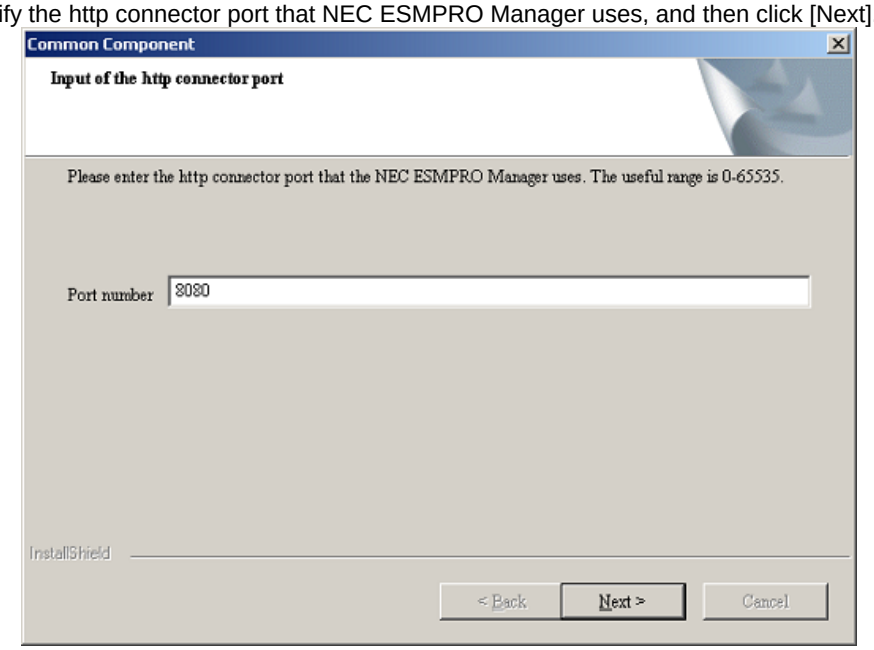
Note

- Specify the administrator name with 1 to 16 alphanumeric characters, and the password with 6 to 16 alphanumeric characters.
- Administrator name is the user name to operate NEC ESMPRO Manager with the administrator authority.

11. Input of the http connector port.

(For update installation from DianaScope Manager and NEC ESMPRO Manager Ver. 5, this is not displayed.)

Specify the http connector port that NEC ESMPRO Manager uses, and then click [Next].

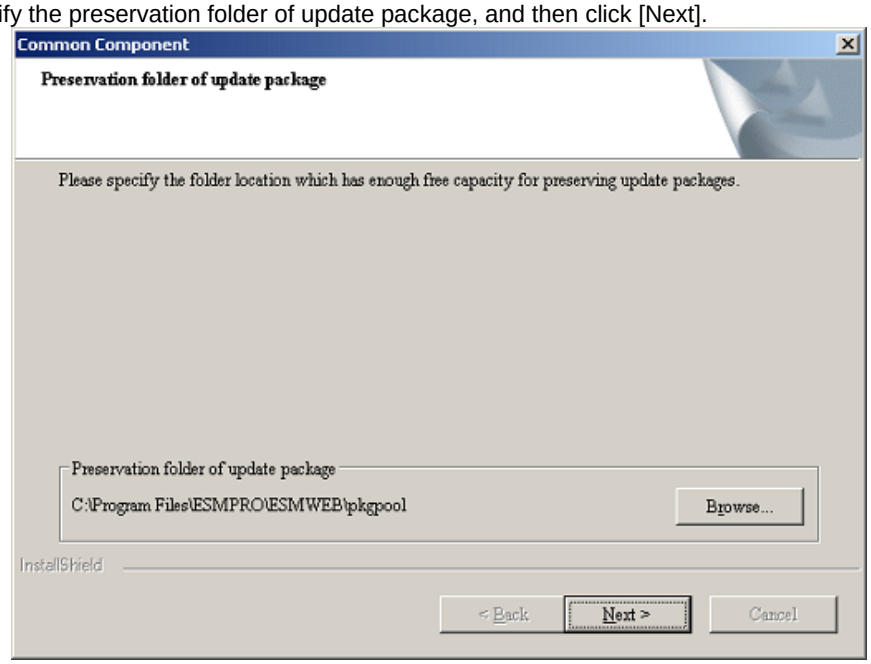


Note The useful range of the http connector port is 0-65535.

12. Enter preservation folder of update package.

(For update installation, this is not displayed in case that the folder has been specified.)

Specify the preservation folder of update package, and then click [Next].



Tips This folder will be used as a repository of update packages for NEC Express Update.

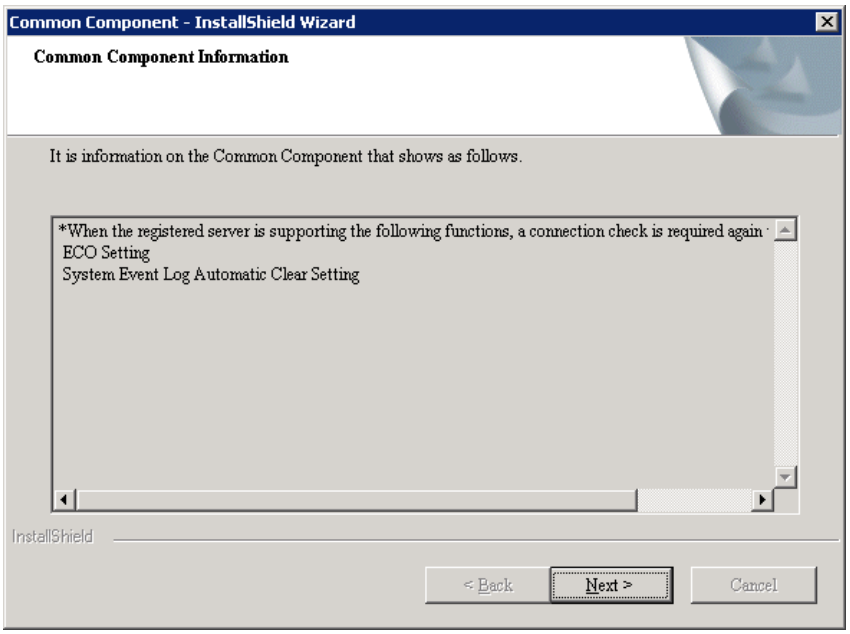
Note This folder is required plenty of space. The default preservation folder is "Installation target folder¥ESMWEB¥pkgpool".

Wait until the installation completes. Some installation windows are displayed during the installation. If you click [Cancel], the installation can be aborted but the installed files are not deleted.

13. Check the information on Common Component.

(This is displayed for update installation from NEC ESMPRO Manager Ver. 5.01.)

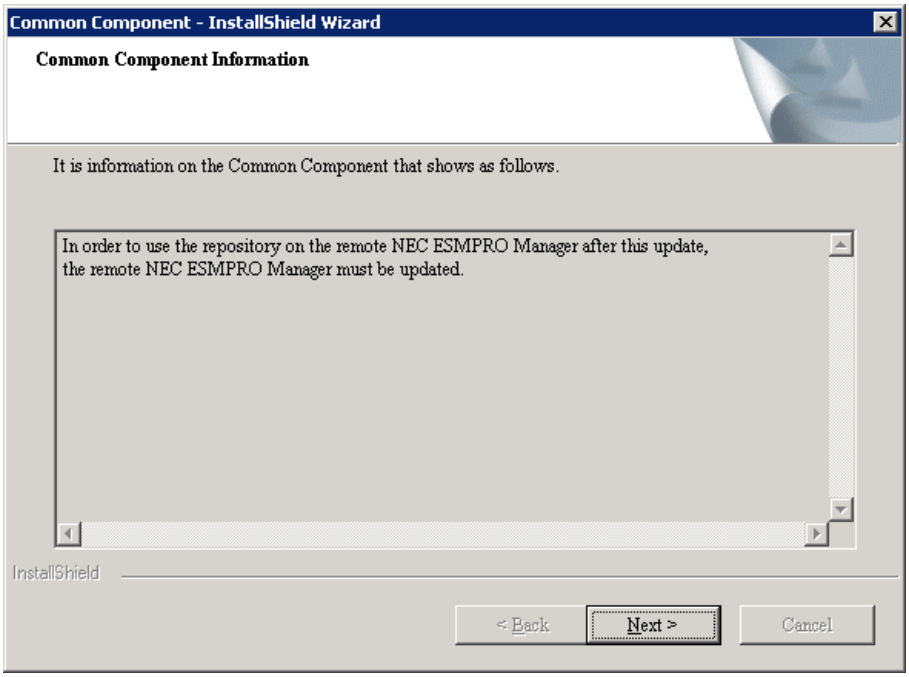
Check the information and click [Next].



14. Check the information on Common Component.

(This is displayed for update installation from NEC ESMPRO Manager Ver. 5 when you set the remote repository on Environment.)

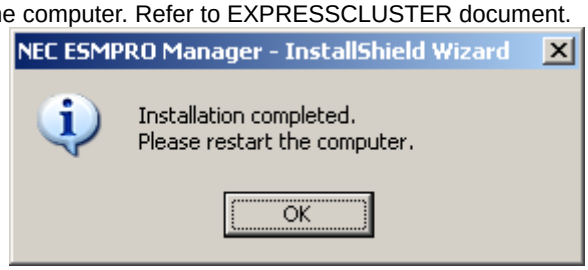
Check the information and click [Next].



15. The installation completes.

Click [OK] and then restart OS (the system will not automatically restart.).

* If this computer is intended to be used in EXPRESSCLUSTER system, you need to do some extra work before restarting the computer. Refer to EXPRESSCLUSTER document.



Note

- The displayed messages vary depending on the environment.
- If this computer is intended to be used in EXPRESSCLUSTER system, you need to do some extra work before restarting the computer. Refer to EXPRESSCLUSTER document.

2.2 Notes on installation

Message on NEC ESMPRO Manager install

Depending on OS, installing NEC ESMPRO Manager the message that "Windows Explorer has stopped working" might be displayed. However, installation was normally completed. The system does not have the influence.

Program Compatibility Assistant dialog box

A message "This program might not have installed correctly" may popup after installing NEC ESMPRO Manager complete. In such a case, you can safely click [This program installed correctly] or［Cancel] button to close the dialog because the installation is done successfully.

3. After Installation

Login

When the installation of NEC ESMPRO Manager completes, check that you can login to it.

1.Access to the following address on a Web browser on the web client.

http://"*the computer name installed NEC ESMPRO Manager*":"*HTTP connection port number*"/esmpro/

This is an example of address to access with HTTP connection port "8080" from the web browser on PC for Management.

http://localhost:8080/esmpro/

* If EXPRESSCLUSTER system is installed, access to the following address.

http://" *Floating IP (FIP) or Virtual computer name*":"*HTTP connection port number*"/esmpro/

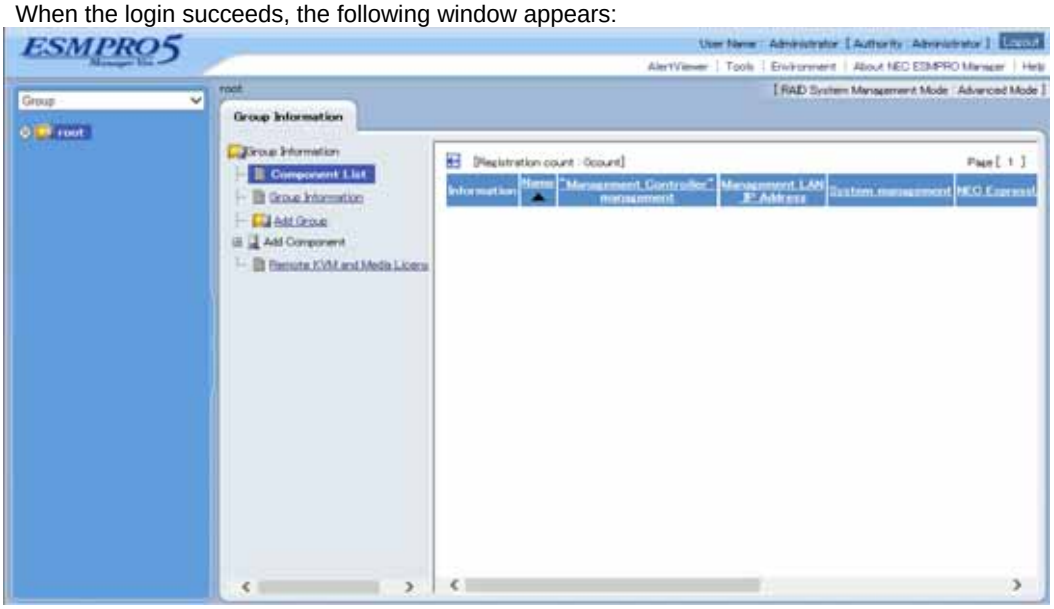
Tips

- NEC ESMPRO Manager can be started up by clicking its icon created on the desktop after the installation.
- When you use NEC ESMPRO Manager from Web Client, login to NEC ESMPRO Manager locally, then add the Web Client address from [Environment] - [Access Control].

2.NEC ESMPRO Manager login window opens.

Enter the administrator name and the password that were registered at the installation, and click [Login] button.

When the login succeeds, the following window appears:



Note The area on which commands, such as [AlertViewer], [Tools] are displayed is called [Header Menu]. Use these commands on [Header Menu] to operate NEC ESMPRO Manager.

Setting environment

You can change the optional setting of NEC ESMPRO Manager.

Click [Environment] on [Header menu] to check the setting. For details, see the online help.

- **Set a modem**

  The modem that is used to connect with a managed server must be set on OS on PC for Management. If PC for Management has plural modem driver on Windows, input the modem name to use the connection in DianaScopeModemAgent.ini file under the sytem32 folder. The modem names are shown on device manager on Windows. The following is an example of DianaScopeModemAgent.ini file.

```
modem=Standard 56000 bps modem
```

SSL

If you need to login to NEC ESMPRO Manager using SSL, you must change the setting of NEC ESMPRO Manager. Perform the procedure that is necessary in order to use SSL with NEC ESMPRO Manager as follows:

1.Create a key

The Key tool is needed for creating the key using with SSL. The Key tool is contained in JRE. Create the key as follows:

In the case of NEC ESMPRO Manager installed in "C:¥Program Files¥ESMPRO":

Windows (32 bits):

```
C:¥Program Files¥ESMPRO¥ESMWEB¥jre¥bin¥keytool" -genkey -alias tomcat -keyalg RSA
```

Windows (64bits):

```
"C:¥Program Files (x86)¥ESMPRO¥ESMWEB¥jre¥bin¥keytool" -genkey -alias tomcat -keyalg RSA
```

Some messages are displayed with dialog style. Input the information about the creator of the key.

You need to set the same password as the keystore password to the key password for <sdo>.

The following is shown an example.

```
Enter keystore password: ******
What is your first and last name?
      [Unknown]: Scott Oaks
What is the name of your organizational unit?
      [Unknown]: SMCC
What is the name of your organization?
      [Unknown]: Sun Microsystems
What is the name of your City or Locality?
      [Unknown]: New York
What is the name of your State or Province?
      [Unknown]: NY
What is the two-letter country code for this unit?
      [Unknown]: US
Is <CN=Scott Oaks, OU=SMCC, O=Sun Microsystems, L=New York, S=NY, C=US> correct?
    [no]: yes
Enter key password for <sdo>
(RETURN if same as keystore password): ******
```

Confirm that the key was created.

```
%USERPROFILE%¥.keystore
```

Tips %USERPROFILE% means C:¥Document and Settings¥<logon user>

2.Change the setting of NEC ESMPRO Manager.

Edit the server.xml file to enable SLL. The server.xml is in the folder ESMWEB¥wbserver¥conf on NEC ESMPRO Manager installed folder. Open the server.xml file with an editor tool, search the description of <Connector> which is specified port number 8443, and delete the comment form "<!-" and "->". Modify the port number if you need.

Add the keystore file path and the password that is specified at the time creating the keystore, in the description of <Connector>.

```
<--Define a SSL HTTP/1.1 Connector on port 8443-->
<!--NOTES: Delete these lines
<Connector port="8443"    NOTES: Change it if you need.
    maxHttpHeaderSize="8192"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
    enableLookups="false" disableUploadTimeout="true"
    acceptCount="100" scheme="https" secure="true" SSLEnabled="true"
    clientAuth="false" sslProtocol="TLS"
    keystoreFile="<the directory that contains keystore>/.keystore"
    keystorePass="<the password>"
    useBodyEncodingForURI="true"  NOTES: Add these lines.
     />
-->    NOTES:Add these lines.
```

3.Reboot PC for Management.

Reboot the server installed NEC ESMPRO Manager.

4.Login.

Confirm to login to NEC ESMPRO Manager with "https:".

Make access to the following address using the web browser on the web client.

https://" the computer name installed NEC ESMPRO Manager":" port number that is specified in server.xml"/esmpro/

An example of address to access from the web browser on PC for Management is shown.

https://localhost:8443/esmpro/

SSL Setup for LDAP/ActiveDirecroty

To use SSL connection between NEC ESMPRO Manager and the authentication server of LDAP/ActiveDirectory, please import certificate into a keystore of JRE which NEC ESMPRO Manager uses. The certificate can be imported by entering the following commands in a command prompt.

C:¥Program Files¥ESMPRO¥ESMWEB¥jre¥bin>keytool.exe -import -trustcacerts -alias ldapsrv -file C:¥ldap¥client.pem -keystore ..¥lib¥security¥cacerts

Note

- If NEC ESMPRO Manager is running on the Windows Vista and later versions of Windows, Administrator privileges may be required.
- Change "C:¥Pogram Files¥ESMPRO" according to the installed environment.
- Change "C:¥ldap¥client.pem" according to the location and the file name of the certificate.
- A default password of a keystore is "changeit".

Changing the port number

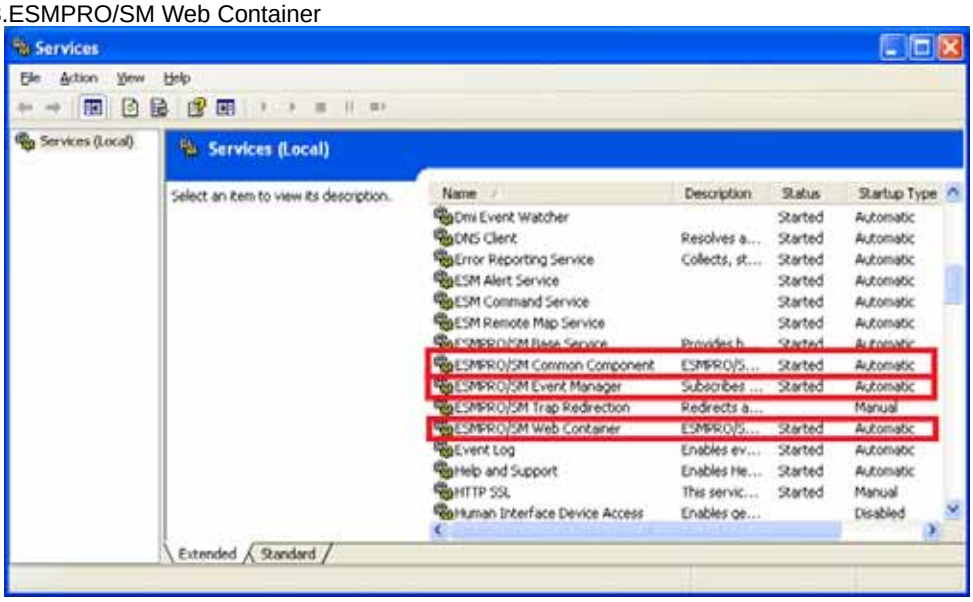
You can change the available port number after installation of NEC ESMPRO Manager.

An example of address to access in HTTP connection port "8080".

1. Stop the following three services.

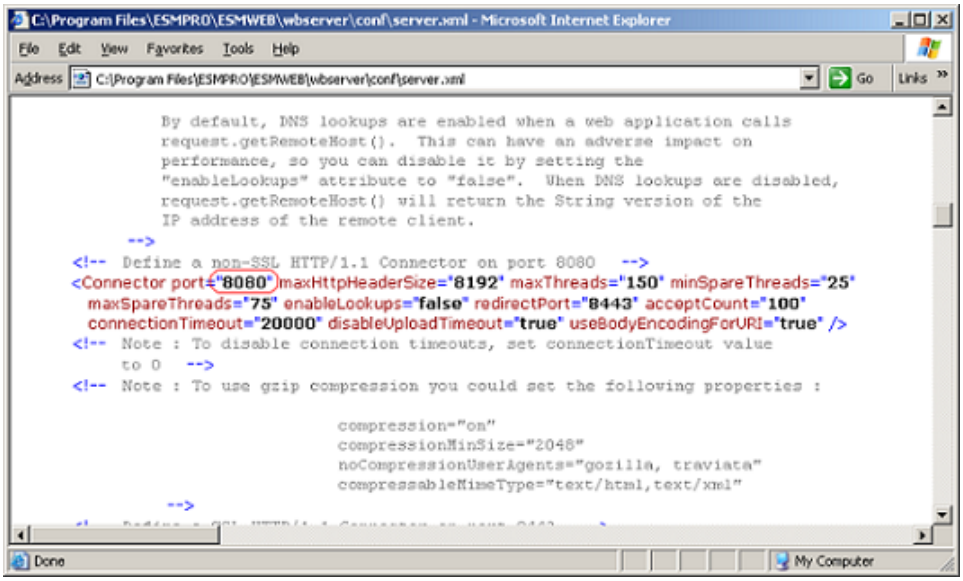
♦ **Stop procedure**

1. ESMPRO/SM Event Manager
2. ESMPRO/SM Common Component
3. ESMPRO/SM Web Container



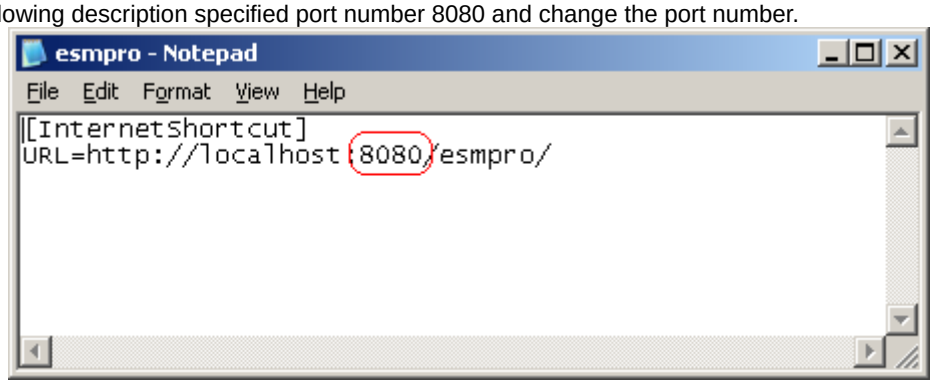
2. Edit the port number in the "server.xml" setting file of ESMPRO/SM Web Container service.

The "server.xml" file is on "NEC ESMPRO Manager installed folder"¥ESMWEB¥wbserver¥conf. In this file, you search the following <Connector> description specified port number 8080 and change the port number.



3. Edit shortcut file "esmpro".

The "esmpro" file is on "NEC ESMPRO Manager installed folder"¥ESMWEB. In this file, you search the following description specified port number 8080 and change the port number.



4. Start the following three services.

♦ **Start procedure**

1. ESMPRO/SM Web Container
2. ESMPRO/SM Common Component
3. ESMPRO/SM Event Manager

Coexistence with Tomcat

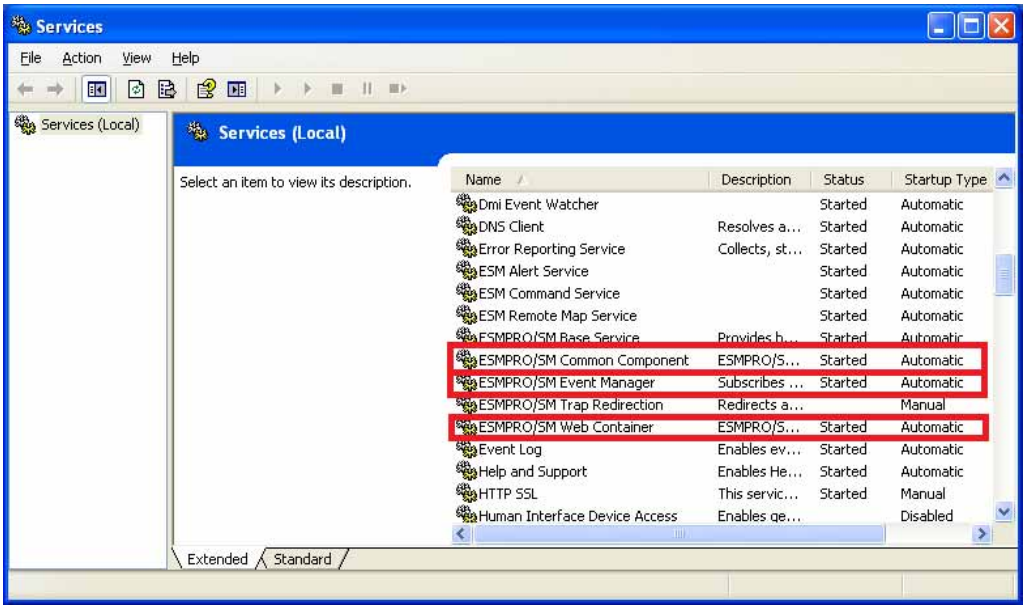
When NEC ESMPRO Manager and Tomcat are installed same computer, the application software installed later will not be running correctly.

In this case, you can avoid it by the following way.

1. If the following three services have started, stop the services.

♦ **Stop procedure**

1. ESMPRO/SM Event Manager
2. ESMPRO/SM Common Component
3. ESMPRO/SM Web Container



2. If Tomcat service has started, stop the service.

3. Edit the server port number and connector port number in the "server.xml" setting file of ESMPRO/SM Web Container service.

The "server.xml" file is on the <The folder in which this product is installed>¥ESMWEB¥wbserver¥conf. In this file, you search the following description specified <Server port="8105" …> <Connector port = "8109" …> and change the port number to unused number.

- **server port number**

File Edit Format View Help

```
<!-- Example Server Configuration File -->
<!-- Note that component elements are nested corresponding to their
     parent-child relationships with each other -->

<!-- A "Server" is a singleton element that represents the entire JVM,
     which may contain one or more "Service" instances.  The Server
     listens for a shutdown command on the indicated port.

     Note:  A "Server" is not itself a "Container", so you may not
     define subcomponents such as "Valves" or "Loggers" at this level.
 -->

<Server port="8105" shutdown="SHUTDOWN">

  <!-- Comment these entries out to disable JMX MBeans support used for the
       administration web application -->
  <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
  <Listener className="org.apache.catalina.core.JasperListener" />
  <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />
  <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener" />
  <Listener className="org.apache.catalina.core.ThreadLocalLeakPreventionListener" />

  <!-- Global JNDI resources -->
  <GlobalNamingResources>

    <!-- Test entry for demonstration purposes -->
    <Environment name="simpleValue" type="java.lang.Integer" value="30"/>

    <!-- Editable user database that can also be used by
         UserDatabaseRealm to authenticate users -->
    <Resource name="UserDatabase" auth="Container"
              type="org.apache.catalina.UserDatabase"
       description="User database that can be updated and saved"
           factory="org.apache.catalina.users.MemoryUserDatabaseFactory"
          pathname="conf/tomcat-users.xml" />
```

- **connector port number**

File Edit Format View Help

```
                         noCompressionUserAgents="gozilla, traviata"
                         compressableMimeType="text/html,text/xml"
       -->

    <!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
    <!--
    <Connector port="8443" maxHttpHeaderSize="8192"
               maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
               enableLookups="false" disableUploadTimeout="true"
               acceptCount="100" scheme="https" secure="true" SSLEnabled="true"
               clientAuth="false" sslProtocol="TLS" />
    -->

    <!-- Define an AJP 1.3 Connector on port 8009 -->
    <Connector port="8109"
               enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />

    <!-- Define a Proxied HTTP/1.1 Connector on port 8082 -->
    <!-- See proxy documentation for more information about using this. -->
    <!--
    <Connector port="8082"
               maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
               enableLookups="false" acceptCount="100" connectionTimeout="20000"
               proxyPort="80" disableUploadTimeout="true" />
    -->

    <!-- An Engine represents the entry point (within Catalina) that processes
         every request.  The Engine implementation for Tomcat stand alone
         analyzes the HTTP headers included with the request, and passes them
         on to the appropriate Host (virtual host). -->

    <!-- You should set jvmRoute to support load-balancing via AJP ie :
    <Engine name="Catalina" defaultHost="localhost" jvmRoute="jvm1">
    -->

    <!-- Define the top level container in our container hierarchy -->
```

4. Start the following three services.

♦ **Start procedure**

1. ESMPRO/SM Web Container
2. ESMPRO/SM Common Component
3. ESMPRO/SM Event Manager

5. Start Tomcat service.

Note

- Specify the port numbers of NEC ESMPRO Manager and Tomcat not to overlap.
  If you change the port number of NEC ESMPRO Manager, see the preceding clause "Change the Port Number".
- When you use SSL communication on Tomcat or connect Tomcat with Apache, you may need to change another port number. See Tomcat is Document for detail.

Update installation from an older version of NEC ESMPRO Manager

If you perform update installation from NEC ESMPRO Manager of less than Ver. 5.0, the managed servers originally registered in Operation Window do not show up on Web GUI of NEC ESMPRO Manager.

In such a case, execute Auto Registration on Web GUI first with "System management" enabled and "IP Address Range Search" specified so that all IP addresses of the managed servers are included.

Note

- Only managed servers of DianaScope Manager show up on Web GUI right after update installation if DianaScope Manager was previously installed.
- Following managed objects in Operation Window are not migrated to Web GUI.
  - Maps
  - Server icons representing NEC ESMPRO Agent Ver.4.0 or before.

Receiving SNMP Trap from iStorage T series

NEC ESMPRO Manager Ver. 5.71 or later has a built-in support for SNMP trap from iStorage T series.
If you preconfigured NEC ESMPRO Manager to receive trap from iStorage T series using alert definition file, remove such customizations and reboot the computer so that the built-in support is enabled.The trap enterprise of iStorage T series is shown below.

Also note that If you use WebSAM AlertManager, you may have to reconfigure the report setting since alert type for iStorage T series is now “Tape Library”.

[Location of the alert definition file]

%ESMWORK%¥public¥trap

%ESMWORK% is written in the following registry;

Key ：(32bit OS)HKEY_LOCAL_MACHINE¥SOFTWARE¥NEC¥NVBASE

(64bit OS)HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥NEC¥NVBASE

Name：WorkDir

[Enterprise for iStorage T series]

Managed Server	Enterprise
T30A	1.3.6.1.4.1.119.1.83.1.31
T60A	1.3.6.1.4.1.119.1.83.1.41
T100A	1.3.6.1.4.1.211.4.1.1.126.3.5
T700A	1.3.6.1.4.1.211.4.1.1.126.3.2

NEC ESMPRO Manager Ver. 5.7

3

Uninstallation

This chapter explains uninstallation of NEC ESMPRO Manager.

1. Uninstallation

Describes about uninstallation procedure of NEC ESMPRO Manager.

1. Uninstallation

This page describes how to uninstall NEC ESMPRO Manager.

1.1 Uninstallation procedure

Important

- Uninstallation performed immediately after the system restarts may fail.
  If an error message appears, try again after waiting for a while.
- If this computer is intended to be used in EXPRESSCLUSTER system, you need to do some extra work before restarting the computer. Refer to EXPRESSCLUSTER document.

1. **Sign-in (Log on) to the system with the built-in Administrator (or an account having administrative privilege).**
2. **Exit all running applications.**
3. **Perform uninstallation.**

   Startup [Programs and Features] (or [Add or Remove Programs]) from [Control Panel].

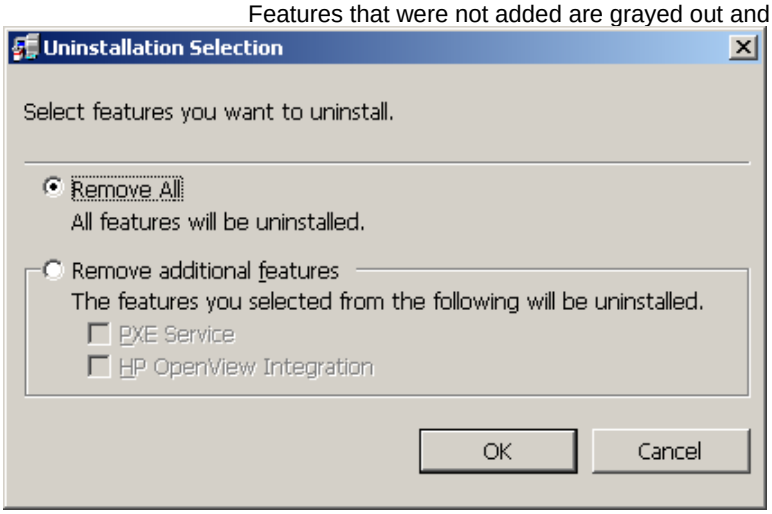
   Select NEC ESMPRO Manager from the list of the installed programs to remove it.
4. **Select features you want to remove.**

   Select the item to be uninstalled, and click [OK].

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

   Remove additional features : Removes features you selected.

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

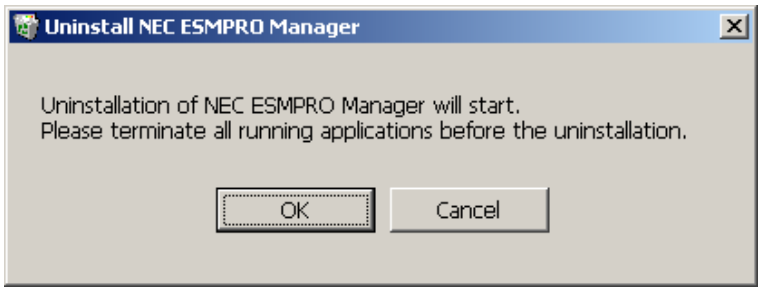


Tips If no features are added, this dialog box is not displayed.

5. Confirmation for uninstallation.

Confirm that any applications related to NEC ESMPRO are not running, and click [OK].

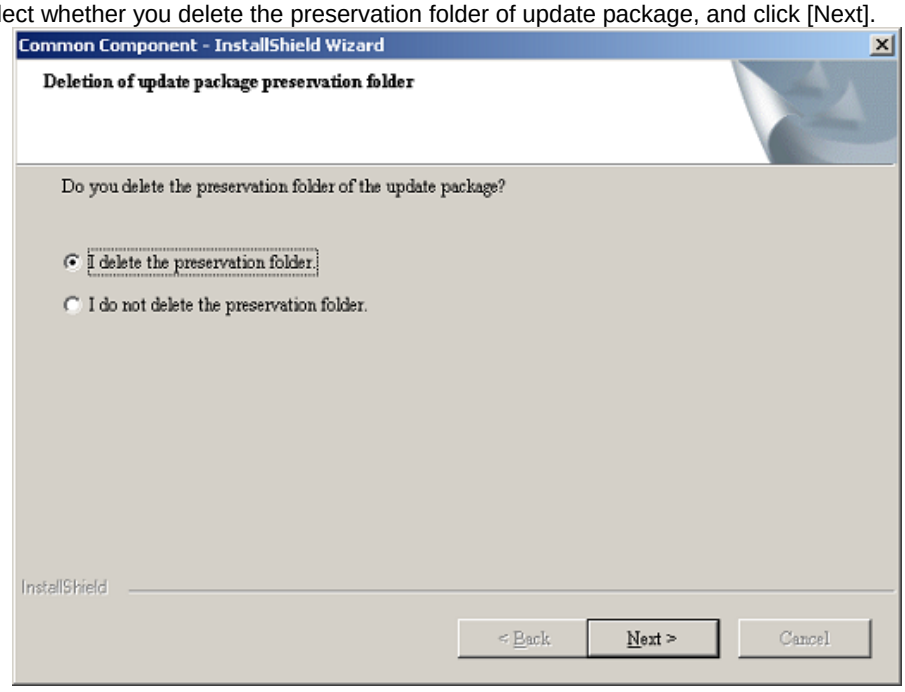
The selected features will be uninstalled.



6. Confirmation for deletion of the folder.

(If there is no folder of update package, this dialog box is not displayed.)

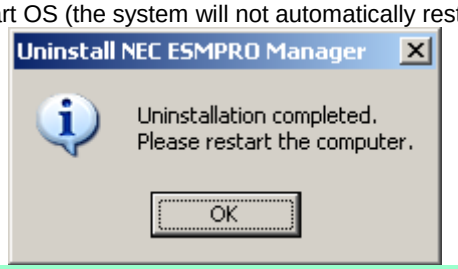
Select whether you delete the preservation folder of update package, and click [Next].



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

7. The uninstallation completes.

Click [OK] and then restart OS (the system will not automatically restart.).



Note The displayed messages vary depending on the environment.

1.2 Notes on Uninstallation

Message after NEC ESMPRO Manager Uninstall

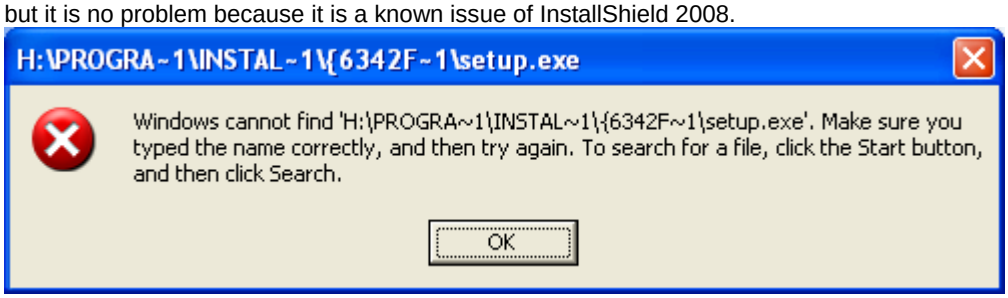
Depending on OS, uninstalling NEC ESMPRO Manager the message that "Windows Explorer has stopped working" might be displayed. However, uninstallation was normally completed. The system does not have the influence.

Program Compatibility Assistant dialog box

A message "This program might not have uninstalled correctly" may popup after uninstalling NEC ESMPRO Manager complete. In such a case, you can safely click [This program uninstalled correctly] or [Cancel] button to close the dialog because the uninstallation is done successfully.

Message at reactivation

The following message might be displayed at the time of the first system reboot after ESMPRO uninstall, but it is no problem because it is a known issue of InstallShield 2008.



Alarm category of HP OpenView Network Node Manager

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

NEC ESMPRO Manager Ver. 5.7

4 Appendix

1. Notes

Describes about note when using NEC ESMPRO Manager.

2. Port numbers / Protocols

Describes about the port numbers and port Protocols NEC ESMPRO Manager uses.

3. Services

Describes about the service list NEC ESMPRO Manager uses.

1. Notes

Check the following points after installing NEC ESMPRO Manager:

1.1 NEC ESMPRO Manager

♦ Installation

- If you install NEC ESMPRO Manager on Windows Server 2008 and later, do not delete user account "Administrator" from "Impersonate a client after authentication" of "Local Security Policy".
- NEC ESMPRO Manager cannot be downgraded to the older version. If you want to use the older version, uninstall the current version and then install new version.

  Note: All the registered information will be deleted as the result of the uninstalling.
- If installer displays either of the following message, execute the installation again.

  "It failed in the writing in a necessary file of Common Component."

  "Close of necessary file for Common Component failed."
- You must logout from the web browser that is login to NEC ESMPRO Manager before NEC ESMPRO Manager is updated. After NEC ESMPRO is updated during login, some error may be displayed on any web browser. When the error is displayed, you must close web browser that is login to NEC ESMPRO Manager and restart the following services.

  ♦ Stop procedure

  1. ESMPRO/SM Event Manager
  2. ESMPRO/SM Common Component
  3. ESMPRO/SM Web Container

  ♦ Start procedure

  1. ESMPRO/SM Web Container
  2. ESMPRO/SM Common Component
  3. ESMPRO/SM Event Manager
- After NEC ESMPRO Manager is updated, NEC ESMPRO Manager on the web browser may display incorrectly.

  Take the following steps to avoid it.

  [Internet Explorer 8]

  1. Click [Safety] menu.
  2. Select [Delete Browsing History].
  3. Select the checkbox for [Temporary Internet Files].
  4. Click [Delete] button.

  [Internet Explorer 10, 11]

  1. Click [Tools].
  2. Select [Delete Browsing History].
  3. Select the checkbox for [Temporary Internet Files].
  4. Click [Delete] button.

[Firefox]

1. Click [Tools].
2. Click [Options] menu.
3. Select [Advanced].
4. Select [Network].
5. Click [Clear Now] in [Offline Web Content and User Data] section.
6. Click [OK].

Setting a Windows Firewall

If the Windows Firewall is enabled, communication of NEC ESMPRO Manager with a web client and a managed server will be interrupted and the system will not work correctly.

To use NEC ESMPRO Manager with Windows Firewall enabled, open the required ports.

Note For ports used by NEC ESMPRO Manager, see "Chapter4 2 Appendix Port numbers / Protocols".

Use of two or more NEC ESMPRO Manager

A single managed component can be controlled remotely by up to three NEC ESMPRO Manager.

Follow these notes on the remote control:

- Use only one NEC ESMPRO Manager for "management controller" management of the managed component.
- Use only one NEC ESMPRO Manager for RAID system management and NEC ExpressUpdate of the managed component. If you register the managed component on two or more NEC ESMPRO Manager, you must set "unregistration" for RAID system management and NEC ExpressUpdate of the managed component.
- Use one NEC ESMPRO Manager for all EM cards and CPU blades on one blade enclosure.

Power OFF, Power Cycle, Reset, and Dump

Since power control is provided by hardware regardless of the state of the managed server is OS, the system may be damaged. Be careful of operation under power control.

Power OFF, Power Cycle, Reset with BIOS Setup Utility active

If you use the managed server integrated BMC, do not execute Power Off, Power Cycle or Reset while BIOS Setup Utility is active on the managed server. Otherwise, the alert setting of BMC configuration will be disabled.

Shutdown OS

NEC ESMPRO Manager commands one of the agent modules on the managed component to shutdown OS. The order of priority for the shutdown function is NEC ESMPRO Agent Extension, NEC ESMPRO Agent and NEC ExpressUpdate Agent.

NEC ESMPRO Agent Extension or NEC ExpressUpdate Agent shutdowns OS regardless the setting "Permit Remote Shutdown / Reboot" on NEC ESMPRO Agent.

IPMI information collection

While a managed server is tuned OFF, some records of management controller information and FRU (Field Replaceable Unit) information cannot be read in.

The current status of some sensors cannot be read in either while the managed server is turned OFF.

Restriction on concurrent connection to Remote Console

When a single NEC ESMPRO Manager is operating the remote console of a managed server, another Manager cannot execute the remote console function for the managed server. A managed server can transmit redirection data to only a single NEC ESMPRO Manager.

Remote console before OS boot or during DOS program running

If a graphic screen is displayed on a managed server, data cannot be displayed correctly on CUI (Character User Interface) remote console. CUI remote console screen is displayed only when the managed server displays a text screen.

In case of interruption to Remote Console

After BMC on a managed server establishes communication via WAN/Direct connection, communication with DianaScope Agent or NEC ESMPRO Agent Extension may ends up with a timeout or the remote console may not be updated any more. This is because priority is given to communication with BMC.

To restart the remote console, use [Restart Redirection] button on NEC ESMPRO Manager.

Display of a special character

CUI remote console screen is not displayed correctly in the following cases:

- **Special character**

  Ruled lines, arrows correctly and en-size left arrows cannot be displayed.

- **User definition font**

  User definition font cannot be displayed.

In case of display of illegally keyed data on the remote console

If you use the managed server integrated BMC, unintentionally keyed data may appear on a managed server in the following conditions when NEC ESMPRO Manager issues a command to BMC:

- WAN/Direct connection.
- Special Administration Console (SAC) screen at Windows boot or CUI remote console under Linux is accessed.

In case of key-in failure on the remote console

- During DOS boot or access to the removable media immediately after the managed server is power switch is turned ON, data cannot be keyed in from the remote console or the keyed data display may be delayed.
- Remote Console is realized by using SOL function of IPMI conformity and the Serial Redirection function of BIOS.

  Data cannot be keyed in from the remote console when the firmware (BIOS and so on) or the software requires the key code that VT100 terminal emulator (the hyper-terminal and so on) cannot control.

  Refer to the document of each firmware or software for the details.

RAID EzAssist Configuration Utility

To operate RAID EzAssist for a SOL-incompatible managed server from CUI remote console via LAN, set the item "Console Redirection" to "Disable" on BIOS Setup Utility screen, reboot the system, and then boot RAID EzAssist Configuration Utility.

Power management

- If you set the value on the managed server which does not support power management, you cannot put back the value to "unsetting". Set "zero" to each value, it is accepted as "unsetting".
- The electric power value might not necessarily reach even the value of Power Cap value.

  The electric power control lowers the power consumption of the system by lowering the frequency of CPU / Memory.

  When CPU / Memory Throttling value reaches 100%, the electric power value does not fall any more.

Note For more detail about Power Monitoring and Power Control Function, reference the following site.
http://www.58support.nec.co.jp/global/download/index.html
[Others] - [Technology paper]

CPU blade auto registration

When "Check Connection" of "CPU blade auto registration" was failed. You can execute "Check Connection" on "Server Properties" - "Connection Setting".

If a specified IP address is set from a CPU blade to another CPU blade during "CPU blade auto registration" process (ex. when you replace CPU blade and execute "CPU blade auto registration"), NEC ESMPRO Manager may not be able to connect CPU blade because old information remains in ARP table on PC for Management. Wait for a few minutes and try "Check Connection".

Coexistence of NEC ESMPRO Manager with DianaScope Agent or NEC ESMPRO Agent Extension on the same server

If the managed server is installed Advanced Remote Management Card or EXPRESSSCOPE Engine series (BMC uses exclusive LAN port (management LAN port)), NEC ESMPRO Manager can manage the server itself installed. If the managed server is installed BMC that uses the standard LAN port, NEC ESMPRO Manager on the managed server cannot manage itself.

You can install NEC ESMPRO Manager and NEC ESMPRO Agent Extension (formerly DianaScope Agent) on the same server, but the communication with BMC on the server is prevented by local loopback function of OS and BMC cannot receive any packets from NEC ESMPRO Manager.

EM Card registration

- When you resister EM Card, you need to set valid on SNMP management and "Management Controller" management each other.
- If the connection is failed at "Auto Registration" or "Check Connection", it is not recognized as EM Card because both management is invalid. In this case, set correct connection setting and execute "Check Connection" again.
- If you register EM Card from Operation Window, EM Card is registered invalid status on NEC ESMPRO Manager. So you need to execute "Check Connection" to manage it.

Remote Control

When all the following conditions are satisfied, remote control cannot be executed from NEC ESMPRO Manager.

- NEC ESMPRO Manager is installed on the server whose OS is Windows since Windows Vista or Windows Server 2008 and later.
- The managed server has either following BMC.
  - BMC uses standard LAN port
  - Advanced Remote Management Card or equivalent BMC
- The managed server has been power off.

  If you manage the server satisfied above condition, install NEC ESMPRO Manager on the server whose OS is the older version of Windows Vista or Windows Server 2008, for example Windows XP.

Display of the monitoring window

If you exit and restart the monitoring window of NEC ESMPRO Manager with AlertViewer started, the displayed AlertViewer window is rewritten and the window may not be properly displayed.

In such a case, exit the monitoring window and AlertViewer once, and then restart them.

Versions of NEC ESMPRO Manager and NEC ESMPRO Agent

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

Coexistence of NEC ESMPRO Manager with other vendor's SNMP management application

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

[Work Around]

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

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

Usage of DHCP

As NEC ESMPRO Manager manages the system according to its IP Address, do not use a DHCP which assigns IP address dynamically on OS on which NEC ESMPRO Manager and NEC ESMPRO Agent are installed.

Setting SNMP trap destination

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

On the other hand, you may need to specify 127.0.0.1 for a computer not connected to the network. For more information, see "Settings on Standalone Environments Without Network Connections" below.

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

Component : {unknown server}

Address : 127.0.0.1

change IP address to 127.0.0.1 on the properties of the server by selecting [Connection Setting] from [Server setting].

Settings on standalone environments without network connections

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

- Specify 127.0.0.1 for Start Address and End Address as a range for Auto Registration.
- Specify 127.0.0.1 for SNMP trap destination.

If you have already registered server, execute Auto Registration after deleting it.

NEC ESMPRO User Group

Since security for NEC ESMPRO Manager is managed by NEC ESMPRO User Group (by default, Administrators), NEC ESMPRO Manager never starts without accessing this group.

Note the following:

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

To upgrade your OS

Otherwise uninstall NEC ESMPRO Manager first and upgrade OS. To upgrade OS to other than the following OS, uninstall NEC ESMPRO Manager first and upgrade OS.

- Windows Vista
- Windows 8.1

Display of the Information of server state/constitution

In case that NEC ESMPRO Manager has been updated from Ver. 5.23 and below, the display of the selected item on [Information of server state/constitution] may take long time with the hardware constitution of the managed server.

Perform the followings in this case:

- Change the "Update Interval" value of "Automatically update display" setting from 5 seconds (default value) to 60 seconds.

  The changing of the automatic update interval by JavaScript will reduce the load of NEC ESMPRO Agent on the managed server, and so allows NEC ESMPRO Manager to display DataViewer quickly.

  <settings>

  [Environment] - [Option] - [Automatically update display] - [Update Interval]

Display of the network speed

- When you monitor Linux servers, Speed will not be displayed on the network general view of [Information of server state]. In such a case, check it on the monitored server.
- When you monitor Windows servers which have network interfaces of which speeds are 10Gbps or over, Speed may not be displayed correctly on the network general view of [Information of server state]. In such a case, check it on the monitored servers.
- When you monitor Windows Server 2008 and later servers which have network interfaces with which a cable is not connected, an incorrect value (4,294 Mbps) may be displayed for the Speed on the network general view of [Information of server state].

Display of the network status

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

Display of the teamed network interfaces

Depending on OS, if network interfaces are teamed, the network information may not be properly displayed on [Information of server state]. Check it on the monitored server

Power saving mode of OS

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

System event log when installing NEC ESMPRO Manager on Windows Vista

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

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

Application event log when installing NEC ESMPRO Manager

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

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

In addition to the above, there is ESMPROProvider as a provider name.

Source and Description might somewhat vary depending on OS.

Replacing a managed server

After replacing monitored server, even if the server name and IP address remains the same, delete the corresponding server icon and execute AutoRegistration.

Otherwise, the replaced server is not recognized and the server status and the configuration information is not correctly displayed.

Auto Registration

- Even if managed servers that are registered only to Operation Window are out of the search range for Auto Registration, they are listed in the Auto Registration list and registered to NEC ESMPRO Manager as managed servers.
- If any server that is not supported, such as NEC ESMPRO Agent Ver.4.1 or prior, is included in the search range for Auto Registration, the server is not registered to NEC ESMPRO Manager. However, it is registered to Operation Window.
- After you register a CPU blade managed via only SNMP to create the chassis information, to register another CPU blade on the same chassis with the management controller enabled, delete the previously registered CPU blade managed via SNMP and register it again.
- Do not perform other operations or move to another window during Auto Registration or Check Connection.
- If a server for which Check Connection is not performed is included in the search range for Auto Registration, be sure to execute Check Connection for it before Auto Registration.
- After auto-discovery is finished from web browser, the server icon is also put on Operation Window. Change the icon location manually if you feel the location is not appropriate.

Manually registering server on Operation Window

When manually registering server on Operation Window from menu [View]-[Icon Palette], Web GUI cannot show the corresponding component.

In such a case, do Auto Registration on Web GUI.

Changing properties of the monitored server on Operation Window

When changing properties (below) of the monitored server on Operation Window,

Web GUI cannot show the corresponding changes.

- Alias
- IP Address
- SNMP Community Name
- UUID

Changing properties must be done via Web GUI - Connection Setting.

Note "Alias" on Operation Window and that on Web GUI are saved respectively.

Changing Status Polling Interval

The default value for SNMP status polling interval is 1 minute.

To change it, change the value set in [Server Status Polling Interval (min)] on the server icon displayed on Operation Window.

Recovery from system error

If a system error occurs, follow the instruction displayed on the window.

If no instruction is displayed, restart the browser.

If communication with a monitored server becomes disabled

If communication with a monitored server becomes disabled due to server down or network problem during display of the status of the server, the server icon of the group or chassis shows unknown status. In this case, the status color of the configuration information tree item may not indicate the latest status. Click the server icon from the group or chassis to display the latest information.

Changing the configuration of the servers

If you change the configuration of the servers (such as attaching or removing HDDs) with [Information of server state/constitution] tree displayed, the changes will not be reflected to [Information of server state/constitution] tree. After changing the configuration, click the target server icon displayed in [Group] or [Chassis] tree to update [Information of server state/constitution] tree.

Display of the Information of EM Card state/constitution

To update the monitoring display in case of EM Card configuration such as removing/mounting CPU blade, switching power redundancy mode, reselect EM card icon from Group/Chassis tree.

If the page cannot be displayed on web browser

When you start NEC ESMPRO Manager or application that is installed after NEC ESMPRO Manager installation, the web browser may displays "The page cannot be displayed." or "The server cannot be found." and the page cannot be displayed. In this case, the port number of NEC ESMPRO Manager and other application may be overlapped. See the procedure on "Coexistence with Tomcat" in "6.1 After Installation".

RAID operation

See User's Guide of Universal RAID Utility (after Ver.2.1) installed on the managed server for notes about the operation of RAID system with [Information of server state] navigation tree.

Alert driven status control function

The alert driven status control function which is supplied as a Windows application cannot be used on the Web browser interface. If the function is enabled, there is the possibility that you misunderstand the status of the managed servers, because the server status color on the web browser of the client side changes by starting, operating, or exiting AlertViewer (Windows application) on the web server side. Disabling the alert driven status control function is recommended.

Suspend Periods Setting

When you set a suspend period schedule for a group, NEC ESMPRO Manager deletes the same schedule which has already been set for the managed component.

Please be careful that the group schedule is deleted from the managed component if you move the managed component from the group to another group.

The default setting of EXPRESSSCOPE Engine 3

You can change BMC Configuration Information from [BMC Setting] of NEC ESMPRO Manager.

For details of [BMC Setting], see the online help of NEC ESMPRO Manager.

Refer to EXPRESSSCOPE Engine 3 User's Guide about difference between NEC ESMPRO Manager's default value and a value which 'BMC Initialization' function will set.

Standby BMC Configuration Setting

It may take a few minutes to set the Standby BMC Configuration.

If the setting is failed, please set it again after waiting for a few minutes.

DHCP setting for Advanced Remote Management Card

If you change DHCP setting to [Enable] on [BMC setting] of NEC ESMPRO Manager, Advanced Remote Management Card may not be able to send the alert to the destinations.

The reason is that MAC address for the destination becomes unsuitable in the case that enabling DHCP changes the address range.

Set DHCP setting for Advanced Remote Management Card using BMC configuration tools on the managed server.

1.2 NEC ExpressUpdate

Installation of NEC ExpressUpdate Agent

To use the function of "Installing NEC ExpressUpdate Agent", following configurations are necessary.

*1 Change following configurations with the user belongs to Administrators group.

*2 See"Chapter4 2 Appendix Port numbers / Protocols" for network ports and protocols which this function uses.

- **Windows XP**
  1) Configure Windows Firewall Configuration.
     - [Control Panel] - [Security Center] - [Windows Firewall] Select [General] tab and uncheck [Don't allow exceptions].
     - Select [Exceptions] tab and check [File and Printer Sharing].
  2) Configure File Sharing
     - [Control Panel] - [Appearance and Themes] - [older Options] Select [View] tab and uncheck [Use simple file sharing].
- **Windows Vista**
  1) Configure Windows Firewall
     - [Control Panel] - [Security] - [Windows Firewall] - [Allow a program through Windows Firewall]-Select [Exceptions] tab and check [File and Printer Sharing].
  2) Configure File Sharing.
     - [Control Panel] - [Appearance and Personalization] - [Folder Options]-Select [View] tab and uncheck [Use Sharing Wizard].
  3) Configure UAC.
     - [Control Panel] - [User Accounts] - [User Accounts] - [Turn User Account Control on or off]-uncheck [Use User Account Control (UAC) to help protect your computer]
- **Windows 7**
  1) Configure Windows Firewall.
     - Select [File and Printer Sharing] on [Control Panel] - [System and Security] - [Windows Firewall] - [Allow a program or feature through Windows Firewall] and click [OK].
  2) Configure Configuration.
     - [Control Panel] - [User Account and Family Safety] - [User Accounts] - [Change User Account Control settings]-Select [Never notify]
- **Windows Server 2008**
  1) Configure Windows Firewall.
     - [Control Panel] - [Security] - [Windows Firewall] - [Allow a program through Windows Firewall]-Select [Exceptions] tab and check [File and Printer Sharing].
  2) Configure UAC Configuration.
     - [Control Panel] - [User Accounts] - [User Accounts] - [Turn User Account Control on or off]-uncheck [Use User Account Control (UAC) to help protect your computer].

- **Windows Server 2008 R2**

  1) Configure Windows Firewall.
     - Select [File and Printer Sharing] on [Control Panel] - [System and Security] - [Windows Firewall] - [Allow a program or feature through Windows Firewall] and click [OK].

  2) Configure UAC.

- [Control Panel] - [User Accounts] - [User Accounts] - [Change User Account Control settings]-Select [Never notify].

- **Windows Server 2008 R2 Core**

  1) Configure Windows Firewall.

     1-1) Make up the remote PC to change "Windows Server 2008 R2 is Windows Firewall settings" remotely.

     1-2) Input below command on the managed server to enable remote configuration of Windows Firewall.

     netsh advfirewall set currentprofile settings remote management enable.

     1-3) Input [mmc] at [Run...] window on remote PC.

     1-4) File-Add/Remove Snap-in...-Add [Windows Firewall with Advanced Security].

     In the select computer window, input the host name of the managed server.

     You can get host name of the managed server with [hostname] command.

     1-5) [Inbound Rules]-Select [File and Printer Sharing] and execute [Enable Rule].

- **Windows 8, Windows Server 2012 and later**

  "NEC ExpressUpdate Agent" cannot be installed on OS remotely.

- **Linux OS**

  *1 See document of the distribution for configuration.

  1) Configure Firewall.
     - Enable remote SSH login.

  2) Configure SSH.
     - Enable root login with SSH.

       Typically, open the sshd configuration file [/etc/sshd/sshd_config] and set "PermitRootLogin" option to "yes".

1.3 Managed Servers

Setting Windows Firewall

If Windows Firewall is enabled, communication with the management machine will be interrupted and the system will not work correctly. To use NEC ESMPRO Manager Windows Firewall enabled, open the required ports.

Note For ports used by NEC ESMPRO Manager, see "Chapter4 2 Appendix Port numbers / Protocols"

Support for SOL

The SOL system implements CUI remote console via LAN by the following method: BMC or vPro gets redirection data that has been output to the serial port 2 by System BIOS or console–less OS and transmits the data via the LAN. If the remote console has been set in BMC configuration information, the serial port 2 (COM2) cannot be used for connecting another device such as UPS because BMC occupies the serial port 2.

See "Appendix C Managed Components Summary" in "NEC ESMPRO Manager Ver.5 Setup Guide" to confirm the managed server supports SOL.

The remote console of Linux or SAC of Windows can be used when the managed server support SOL. However, there are the following notes:

- Use of serial port 2 is restricted. See "Notes on Managed Servers and Network Devices".
- In case of the managed server based on vPro, NEC ESMPRO Manager does not support the remote console of SAC of Windows.

There are the following notes in the managed server which does not support SOL:

- Do not attempt to boot Windows or Linux on the managed server when you use Remote Control function with utility boot mode via LAN connection. Booting of Windows or Linux may result in a failure.
- To operate RAID EzAssist for a SOL–incompatible managed server from CUI remote console via LAN, set the item［Console Redirection] to [Disable］on
- BIOS Setup Utility screen, reboot the system, and then boot RAID EzAssist Configuration Utility.

Power control with BIOS Setup Utility Active

If you use the managed server integrated BMC, do not control the power supply while BIOS Setup Utility is active on the managed server. Otherwise, the alert setting of BMC configuration will be disabled.

CUI Remote Console of DOS

To execute CUI remote console function of DOS screen, select [Server］-［Console Redirection］and change［ACPI Redirection］to［Disable］on BIOS Setup Utility screen of the managed server if［ACPI Redirection] exists on［Console Redirection］.

CUI Remote Console after Windows boot

- If the managed server does not support SOL, Remote Console of SAC of Windows cannot be executed via LAN.
- To execute CUI remote console function of SAC screen after Windows boot, select [Server]-[Console Redirection] and change [ACPI Redirection] to [Enable] on BIOS Setup Utility screen of the managed server. When [ACPI Redirection] is set to [Enable] on BIOS Setup Utility screen, CUI remote console function cannot be executed after POST.
  If [ACPI Redirection] does not exist on [Console Redirection] menu, confirm that [Console Redirection after POST] is enabled.

Shutdown OS

When the following operation is performed on the managed server running Windows Server 2008 or later, the cancellation dialog box may not be displayed.

- OS shutdown by NEC ESMPRO Manager.
- OS shutdown by scheduled running function.

Shutdown OS during DC-OFF state by scheduled running

When [Agent Setting] - [Shut down OS after DC-ON during Scheduled Running Halt] on NEC ESMPRO Manager is enabled, DianaScope Agent or NEC ESMPRO Agent Extension shutdowns OS if the managed server is powered up during the down period (DC OFF state time by scheduled running).
Only if the managed server is powered up from NEC ESMPRO Manager, DianaScope Agent or NEC ESMPRO Agent Extension does not shutdown OS. However, in case that any error is occurred during booting, DianaScope Agent or NEC ESMPRO Agent Extension may shutdown OS even though power up by NEC ESMPRO Manager.

1.4 BMC Configuration

BMC Configuration tool

Among BMC configuration information tools there are some tools which cannot be used to setup NEC ESMPRO Manager.

- NEC MWA Agent cannot be used.
- If NEC MWA is stored in EXPRESSBUILDER DVD-ROM, [A setup of a system management] stored in the same EXPRESSBUILDER DVD-ROM cannot be used.
- The Console-less function of EXPRESSBUILDER cannot be used when NEC MWA is stored in the same EXPRESSBUILDER DVD-ROM.

In case of exchange of PC for Management

If a PC for Management as an alert receiver has been exchanged, register the managed server is BMC configuration information again even when IP address of PC for Management remains unchanged. Otherwise, BMC may fail to recognize the alert receiver.

Function "Obtain an IP Address automatically (DHCP)"

The managed server included BMC that uses a Management LAN port supports the function "Obtain an IP Address automatically (DHCP)".

1. Following version of NEC ESMPRO Manager modules supports the setting of the function.

Managed server	DianaScope
The managed server that integrates EXPRESSSCOPE Engine series. DianaScope Manager Ver.1.07.01 or later	DianaScope Manager Ver.1.07.01 or later
	DianaScope Agent Ver.2.03.05 or later
	DianaScope Configuration Ver.1.02 or later
The managed server installed Advanced Remote Management Card.	DianaScope Manager Ver.1.11.00 or later
	DianaScope Agent Ver.2.06.00 or later
	DianaScope Configuration Ver.1.02 or later

When you use the module that does not support the setting of the function "Obtain an IP Address automatically (DHCP)" for the managed server that supports the function, note followings :

- If DianaScope Agent does not support the setting of the function, DianaScope Agent always set [disable] for the function when it registers BMC configuration. DianaScope Agent also set [disable] when it writes BMC configuration information file.
- If DianaScope Configuration does not support the setting of the function, DianaScope Configuration always set [disable] for the function when it writes BMC configuration information file.
- If [System Management] tool on EXPRESSBUILDER does not support the setting of the function, the tool always set [disable] for the function when it registers BMC configuration. The tool also set [disable] when it writes BMC configuration information file.
- If remote console feature of EXPRESSBUILDER does not support the setting of the function, the tool always set "disable" for the function when it registers BMC configuration.

- If NEC ESMPRO Manager does not support the setting of the function, NEC ESMPRO Manager cannot set disable for the function nor change IP address when DianaScope Agent support the setting of the function and the function has been set enable.

2. Advanced Remote Management Card

   If the managed server has been installed Advanced Remote Management Card, BMC may not immediately obtain IP address after BMC is set to obtain IP address by DHCP.

   Please turn the managed server AC-OFF and then AC-ON because BMC try to obtain IP address whenever the managed server is turned AC-ON.

Port that BMC uses

In case that Linux on the managed server uses port 623, NEC ESMPRO Manager cannot communicate with BMC that uses standard LAN port.

Perform following settings:

1. Add the following entries in services files (/etc/services) to reserve port 623.

```
asf-rmcp 623/tcp ASF Remote Management and Control Protocol
asf-rmcp 623/udp ASF Remote Management and Control Protocol
```

2. Reboot OS.

Initialization of BMC Configuration Information setting

When you set［Default value］on BMC Configuration Information with DianaScope Agent or NEC ESMPRO Agent Extension, or create New Configuration with [System Management Tool] started from EXPRESSBUILDER, each items of BMC Configuration Information are initialized.

If the managed server integrates EXPRESSSCOPE Engine series, Advanced Remote Management Card, following items for BMC Web server are also initialized because they are shared with BMC Configuration Information:

DHCP Configuration

IP Address

Subnet Mask

Default Gateway

How to set the Web server is following:

- Select［System Management Tool] on［Tool]. Started from EXPRESSBUILDER DVD-ROM, and then select［Web server of BMC].
- Login to Web server of BMC, and then select［Configuration］－[Network］.

1.5 Web client

◆Language setting on Web browser

NEC ESMPRO Manager and Web client needs to be the same OS language.

Do not change your browser language setting.

⧫ Operation from two or more browsers

NEC ESMPRO Manager cannot be operated using two or more browser windows by one Web client. When you use the browser which has tabbed browsing, NEC ESMPRO Manager cannot be operated using two or more tab.

⧫ Downloading Configuration Information File

When you try to download the file from［Configuration Information File］of [Linkage Service］on NEC ESMPRO Manager, Internet Explorer may block the download. Internet Explorer will also display the message on the information bar.

In this case, you can download the file with following settings:

1. Click information bar on Internet Explorer.
2. Click［Download File].
3. Read the confirmation message carefully, and select [Save].

⧫ Java Plug-in version

To login to EXPRESSSCOPE Engine series through NEC ESMPRO Manager, Java plug-in of the web browser must be version 5.0 and above. If JRE plug-in version is 1.4.2_11 and below, the web browser may stall.

⧫ Internet Explorer

- The "login to EXPRESSSCOPE Engine series" screen might not be displayed on Internet Explorer.

  In this case, add URL of EXPRESSSCOPE Engine series to "Add this Web site to the zone".

  1. Select［Internet Options］on [Tools］menu of Internet Explorer.
  2. Click [Security] tab.
  3. Click [Local Internet］zone, and then click [Sites] button.
  4. Enter URL of EXPRESSSCOPE Engine series on [add this Web site to the zone］.

     For example: If EXPRESSSCOPE Engine series has IP address 192.168.0.100, URL is "http://192.168.0.100".
  5. Click [Add] button, and then click [OK]

- The screen including Java Applet might not be displayed on Internet Explorer.

  Through the following procedure, the situation can be avoided.

  - Disable the check box.

    [Java control panel] - [Advanced] tab [Enable the next-generation Java Plug-in].

Note on using Internet Explorer since version 8

If you login to NEC ESMPRO Manager Ver.5 from Web client using Internet Explorer for a long time, according to Internet Explorer restriction (for detail, see Microsoft Knowledge Base 830555), memory usage of Internet Explorer on Web client will increase. (About 10MB a day at maximum.)

So, do following processes if you use it for a long time after login from Web client.

- Logout Web client regularly. The increased memory by Internet Explorer restriction will be released by logout.

Using Firefox

The screen including Java Applet might not be displayed on Firefox. Through the following procedure, the situation can be avoided.

- Modify the version of Java Plug-in of web browser.
- Use Internet Explorer.
- Disable the check box.
  [Java control panel] - [Advanced] tab [Enable the next-generation Java Plug-in].

Using AlertViewer

In some environments, a pop-up window must be allowed on a browser to use AlertViewer.

If the pop-up window is not allowed, AlertViewer may not work properly.

[Back] button of the browser

NEC ESMPRO Manager cannot be operated using browser functions like [Back] button. The screen contents cannot be displayed correctly on browsers.

Choose a necessary link or a button again in that case.

Automatic logout

NEC ESMPRO Manager logs out automatically when you do not operate a screen for more than 30 minutes.

When you continue the operation, login to NEC ESMPRO Manager again.

1.6 Applications run on PC for Management

NEC ESMPRO User Group

To use applications run on PC for Management, let the user belong as a member of NEC ESMPRO User Group (by default, Administrators).

Coexistence of NEC ESMPRO Manager with other vendor's SNMP management application

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

[Work Around]

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

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

Note that if you set to use SNMP Trap Service, the name of NetWare server (host) that sent a trap via IPX protocol cannot be identified.

Transfer of DMI events on Inter-Manager Communication

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

Installing other DMI management application and manager on the same machine

In case when other DMI management application is installed to the same machine, receiving DMI events with AlertViewer may not work properly.

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

Monitoring Ver. 3.2 or prior version of NEC ESMPRO Agent and DMI Agents

A function for monitoring Ver. 3.2 or prior version of NEC ESMPRO Agent and DMI Agents has been removed from NEC ESMPRO Manager Ver. 4.3 or later. As a result, Manager behaves as follows.

- By performing auto-discovery, server icons are registered on Operation Window.
- SNMP traps and DMI events sent from monitored servers are displayed on AlertViewer properly.
- If［Watch Server Status] properties are "On" for Ver. 3.0 or prior version of NEC ESMPRO Agent, the status color is displayed in gray (unknown). Set "Off" for［Watch Server Status］properties or delete the icon of Agent.
- Status of DMI Agents is not monitored through DMI even if "Watch Server Status" properties are "On".
- The information of Ver. 3.0 or prior version of NEC ESMPRO Agent and DMI Agents is not viewed on DataViewer or GraphViewer, and not collected by Automatic Data Collection function.
- Monitoring storages for NEC ESMPRO Agent Ver. 3.0 to Ver. 3.1 is not supported.

Receiving DMI events from the machine belonging to multiple networks

Receiving DMI events from the machine (with multiple IP addresses) belonging to multiple networks may not be available.

Using NEC ESMPRO Manager on a machine with a high load

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

  If you use the machine with an extremely high load such as when 100% of CPU has been used for a long time period, the message "Communication with NVBase System Service became invalid" may appear. Manager applications communicate with a service (NVBase System Service). The above message appears when the communication is timed-out due to high load.

  If this message appears, decrease the load on the machine and restart the application.

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

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

  - The icon for the machine is grayed out on Operation Window.
  - The following error messages are displayed when DataViewer is started.

    Could not collect information on the host.

    Refer to Recovery Action for errors in DataViewer Help.
  - The machine information becomes "Unknown" on DataViewer

Transmitting and receiving packets between NEC ESMPRO Manager and NEC ESMPRO Agent

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

In addition, note that a large amount of data is flown in server management by DMI (Set "On" for DMI Agent displayed on a server icon on Operation Window).

* Server management by DMI is for other vendor's server client on which DMI is installed. You do not need to use DMI for managing machines on which NEC ESMPRO Agent is installed.

- At autodiscovery of servers on Operation Window.
- At a specified interval after specifying regular autodiscovery on Operation Window.
- When deleted server where DMI agent is checked for its properties on Operation Window.
- When DMI Agent is registered on Operation Window.
- When DMI Agent is turned OFF on Operation Window.
- When DMI Agent is turned ON on Operation Window.
- When Remote Wake UP is executed on Operation Window.
- Irregularly, after specifying inter-manager communication on Operation Window.
- At receiving SNMP Trap.
- At receiving DMI event.
- At startup of OS, for all DMI agents registered at Operation Window.

- About every one minute after DataViewer is started.
- About every one minute after GraphViewer is started.
- At a specified interval for a specified server, after setting Automatic Data Collection.
- Regular polling about every one minute to monitor server status.*

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

Setting SNMP trap destination

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

On the other hand, you need to specify 127.0.0.1 for a computer not connected to the network. For more information, see "Settings on Standalone Environments Without Network Connections" below.

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

Component : {unknown server}

Address : 127.0.0.1

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

Settings on standalone environments without network connections

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

- Specify 127.0.0.1 for Start Address and End Address as a range for Auto-discovering.
- Specify 127.0.0.1 for SNMP trap destination.

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

Threshold dialog box for the temperature sensor

For some servers, only the fatal status may be displayed on the dialog box for setting threshold values of the temperature sensor.

In this case, the sliders show yellow (Warning) and red (Fatal), but green is displayed as the actual status color when temperature of a target machine is lower than the specified Fatal limit.

Versions when using Inter-Manager Communication

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

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

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

Operations as a user who does not have Administrators privilege

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

If you perform a wrong operation by mistake, perform the following measure:

[Problem]

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

- When you have changed from Receive valid (green) to Receive invalid (red):
  Even though the status of each item appears to be changed to "Receive invalid (red)", the service (Alert Manager Socket(R) Service) does not actually stop. In such a case, alert messages can never be received but an unnecessary service is running. This results in a waste of resources. In addition, whenever you change this status to Receive valid (green), the following error message appears:
  "Failed to start the service. : (Alert Manager Socket(R) Service)"
- When you have changed from Receive invalid (red) to Receive valid (green):
  Although the following message appears, the status of each item is changed to "Receive valid (green)" for "Receive from Agent (TCP/IP)." However, alert messages cannot be received because the service (Alert Manager Socket(R) Service) failed to start.
  "Failed to start the service. : (Alert Manager Socket(R) Service)"

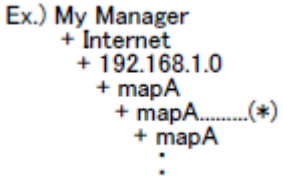
[Work Around]

If you have changed each item on “Receive from Agent (TCP/IP)” as user without Administrators privilege, take the following procedure:

- Logon as a user with Administrators privilege.
- If you have changed each item from Receive valid (green) to Receive invalid (red), restore it to "Receive valid (green)", and change it to "Receive invalid (red)" again.
- If you have changed each item from Receive invalid (red) to Receive valid (green), restore it to "Receive invalid (red)", and change it to "Receive valid (green)" again.

Maps to be specified at autodiscovery

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



This problem occurs when a map whose name is the same as its parent map was created at autodiscovery. In such a case, delete the second mapA (*) (in this example) to resolve the situation.

Setting Windows Firewall

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

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

[Target Ports]

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

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

Note For ports used by NEC ESMPRO Manager, see "Chapter4 2 Appendix Port numbers / Protocols".

<Monitoring a server where multiple IP addresses are set for a single network card>

[Problem]

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

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

[Work Around]

On Operation Window of NEC ESMPRO Manager, open [Properties] on the server icon, change IP address to another one that is set on the monitored server, and reboot PC for Management.

Autodiscovery of Blade Servers

When you execute Autodiscover and register blade servers, the number of slots for storing blades may be displayed differently from the actual one, and some blade images may be placed out of the frame. In such a case, follow the steps below to change map properties on Operation Window:

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

Autodiscovery of SIGMABLADE

When CPU blades are autodiscovered before EM Cards are done, the autodiscovered CPU blades will be registered directly under the network map that you specified at autodiscovery, not under a blade map. In such a case, delete the registered CPU blades, and autodiscover them again as follows:

<When EM Cards and CPU blades are in the same segment>

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

<When EM Cards and CPU blades are in different segments>

Register EM Cards first, and then autodiscover the corresponding CPU blades.

Display of the network speed on DataViewer

- When you monitor Linux servers, Speed will not be displayed on the network general view of DataViewer. In such a case, check it on monitored servers.
- When you monitor Windows servers which have network interfaces of which speeds are 10Gbps or over, Speed may not be displayed correctly on network general view of DataViewer. In such a case, check it on the monitored servers.
- When you monitor Windows Server 2008 and later servers which have network interfaces with which a cable is not connected, an incorrect value (4,294 Mbps) may be displayed for the Speed on the network general view of DataViewer.

Display of the network status on DataViewer

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

Display of the teamed network interfaces on DataViewer

Depending on OS, if network interfaces are teamed, the network information may not be properly displayed on DataViewer. Check it on the monitored server.

Display of the Memory Information on DataViewer

When you monitor a virtual machine running on Hyper-V with dynamic memory enabled, the following memory information may be displayed incorrectly.

In such a case, collapse DataViewer tree, then display the memory information again.

- Physical Memory Capacity
- Physical Memory Available
- Physical Memory Currently Used
- Physical Memory Percent Used

Display of the file system type on DataViewer

The file system type is displayed as "ReFS" on Web GUI when you use "Resilient File System (ReFS)", while the file system type on DataViewer (Windows GUI) is displayed as blank.

Display of the Information of EnclosureViewer

To update the monitoring display in case of EM Card configuration such as removing/mounting CPU blade, switching power redundancy mode, reselect EnclosureViewer - [Configure]Menu - [Reconstruct Tree].

2. Port numbers / Protocols

NEC ESMPRO Manager uses the following port numbers and protocols.

In case of two-way protocol, upper arrow shows that connection starts, and lower arrow shows that connection turns.

In case of port No. unknown, unused port is used to start connection.

[Web Client <->PC for Management]

Function	Web Client		Protocol /Direction	PC for Management	
	Component	Port No.		Port No.	Component
Management/ monitoring	web browser	Unknown	TCP -> <-	8080 (*1)	NEC ESMPRO Manager

*1 You can change the port number at the installation or see [Changing the port number].

[PC for Management <->Managed Server]

Function	PC for Management		Protocol /Direction	Managed Server	
	Component	Port No.		Port No.	Component
SNMP report to Manager	NEC ESMPRO Manager	162	UDP <-	Unknown	NEC ESMPRO Agent
TCP/IP report to Manager (TCP/IP in Band)	NEC ESMPRO Manager	31134 (*1)	TCP <- ->	Unknown	NEC ESMPRO Agent
Auto Registration Server Monitoring (SNMP)	NEC ESMPRO Manager	Unknown	UDP -> <-	161	NEC ESMPRO Agent
Auto Registration	NEC ESMPRO Manager	--	ICMP -> <-	--	NEC ESMPRO Agent
BMC Setting NEC ExpressUpdate	NEC ESMPRO Manager	Unknown	TCP -> <-	443(*2)	BMC
Alert from BMC	NEC ESMPRO Manager	162	UDP <-	623	BMC
Server Monitoring	NEC ESMPRO Manager	47117 (*3)	UDP -> <-	623	BMC
Information Collection (through BMC)	NEC ESMPRO Manager	47117 (*3)	UDP -> <-	623	BMC
Remote Batch	NEC ESMPRO Manager	47117 (*3)	UDP -> <-	623	BMC
Operation with Command Line I/F	NEC ESMPRO Manager	47117 (*3)	UDP -> <-	623	BMC
Power Control	NEC ESMPRO Manager	47117 (*3)	UDP -> <-	623	BMC
Remote Console (CUI, SOL)	NEC ESMPRO Manager	47117 (*3)	UDP -> <-	623	BMC

Remote Console (CUI, non-SOL)	NEC ESMPRO Manager	47115	UDP -> <-	2069	System BIOS
Remote Wake Up	NEC ESMPRO Manager	Unknown	UDP ->	10101	LAN Board
Information Collection (through NEC ESMPRO Agent Extension)	NEC ESMPRO Manager	Unknown	TCP -> <-	47120-47129 (*4)	DianaScope Agent NEC ESMPRO Agent Extension
Scheduled Running	NEC ESMPRO Manager	Unknown	TCP -> <-	47120-47129 (*4)	DianaScope Agent NEC ESMPRO Agent Extension
Search of NEC ExpressUpdate Agent, Universal RAID Utility ESXi5 server	NEC ESMPRO Manager	Unknown	UDP -> <-	427	NEC ExpressUpdate Agent Universal RAID Utility ESXi5
NEC ExpressUpdate, Universal RAID Utility	NEC ESMPRO Manager	Unknown	TCP -> <-	Unknown	NEC ExpressUpdate Agent Universal RAID Utility
NEC ExpressUpdate ,Universal RAID Utility event monitoring	NEC ESMPRO Manager	8080	TCP <- ->	Unknown	NEC ExpressUpdate Agent Universal RAID Utility
Remote installation of NEC ExpressUpdate Agent (When managed server's OS is Windows type)	NEC ESMPRO Manager	Unknown	UDP -> <-	137	OS
		Unknown	TCP -> <-	445	OS
Remote installation of NEC ExpressUpdate Agent (When managed server's OS is Linux type)	NEC ESMPRO Manager	Unknown	TCP -> <-	22	OS
Communication with the vPro	NEC ESMPRO Manager	Unknown	HTTP -> <-	16992	vPro
Remote Console	NEC ESMPRO Manager	Unknown	TCP -> <-	16994	vPro
Server Monitoring (WS-Man)	NEC ESMPRO Manager	Unknown	TCP -> <-	443	ESXi5
CIM Indication Subscription	NEC ESMPRO Manager	Unknown	TCP -> <-	5989	ESXi5
CIM Indication Receiving events	NEC ESMPRO Manager	6736 (*5)	TCP <- ->	Unknown	ESXi5

*1 The port number used by TCP/IP report to Manager can be changed in "TCP/IP Report Setting" screen of AlertViewer.

*2 BMC's port number can be changed on [BMC Setting] - [Network] - [Service].

*3 NEC ESMPRO Manager's port number used for communication with BMC can be changed on the "Environment" screen.

*4 The module uses the lowest unused port of the range.

*5 The port number can be changed on [Alert Receive Setting] - [CIM-Indication Setting] - [Port Number] of AlertViewer.

[Management PC -> EM Card]

Function	PC for Management		Protocol /Direction	EM Card	
	Component	Port No.		Port No.	Component
Information Collection	NEC ESMPRO Manager	47117(*1)	UDP -> <-	623	EM Card
	NEC ESMPRO Manager	47170-47179(*2)	TCP/IP <-	623	EM Card
	NEC ESMPRO Manager	47180-47189(*2)	UDP -> <-	623	EM Card
Auto Registration EM Card Monitoring (SNMP)	NEC ESMPRO Manager	Unknown	UDP -> <-	161	EM Card
EM Card Monitoring	NEC ESMPRO Manager	47117(*1)	UDP -> <-	623	EM Card
BMC configuration of CPU blade	NEC ESMPRO Manager	47117(*1)	UDP -> <-	623	EM Card
Operation with Command Line I/F	NEC ESMPRO Manager	47117(*1)	UDP -> <-	623	EM Card
SNMP Trap	NEC ESMPRO Manager	162	UDP <-	Unknown	EM Card
Ack sending for SNMP trap	NEC ESMPRO Manager	Unknown	UDP ->	5002	EM Card

*1 The NEC ESMPRO Manager uses a same port number for communication with BMC and EM card. The port number can be changed on the [Environment Setting] screen.
*2 The module uses the lowest unused port of the range.

[PC for Management <-> Other Vendor's Management Console]

Function	PC for Management		Protocol /Direction	Other Vendor's Management Console	
	Component	Port No.		Port No.	Component
SNMP Trap Redirection	NEC ESMPRO Manager	Unknown	UDP ->	162	Other Vendor's Management Console

[Inside of PC for Management]

Function	Component	Port No.	Protocol /Direction	Port No.	Component
NEC ESMPRO Manager	NEC ESMPRO Manager	1099	TCP -> <	1099	NEC ESMPRO Manager
NEC ESMPRO Manager	NEC ESMPRO Manager	51099-51107 (*1)	UDP -> <-	51099-51107 (*1)	NEC ESMPRO Manager
NEC ESMPRO Manager	NEC ESMPRO Manager	8105 8109	TCP -> <-	8105 8109	NEC ESMPRO Manager
NEC ESMPRO Manager Direct connection / Modem connection	NEC ESMPRO Manager	Unknown	TCP -> <-	47140-47149 (*1)	NEC ESMPRO Manager (DianaScope Modem Agent)

*1 The module uses the lowest unused port of the range.

[Applications run on PC for Management]

Function	Component	Port No.	Protocol /Direction	Port No.	Component
Inter-Manager Communication	NVBASE System Service	Unknown	TCP -> <-	8806	NVBASE System Service
AlertViewer	AlertViewer	Unknown	TCP -> <-	8807 (*1)	ESM Alert Service

*1 You can change the port number from [Tools] - [Port Settings] of AlertViewer.
Adding a Firewall exception is not needed.

3. Services

NEC ESMPRO Manager uses the following services.

Service Name	Process Name	Function
Alert Manager Main Service	AMVMain.exe	Various processing about reports.
Alert Manager HTTPS Service	AMMHTTP.exe	Forward Express Report(HTTPS) (*2)(*3)
Alert Manager ALIVE(S) Service	AMVALVS.exe	ExpressReportService reports.
Alert Manager Socket(R) Service	amvsckr.exe	Receiving TCP/IP In-bound report. (*1)
Dmi Event Watcher	dmieventwatcher.exe	Receiving DMI events.
ESM Alert Service	esmasvnt.exe	Receiving traps (alerts).
NVBASE System Service	nvbase.exe	Communication base for NEC ESMPRO Manager.
ESM Command Service	nvcmd.exe	Periodical command execution.
ESM Remote Map Service	nvrmapd.exe	Synchronizing Remote Map status color.
ESMPRO/SM Base Service	esmdsvnt.exe(*4) esmdsvap.exe	Server status watching.
ESMPRO/SM Trap Redirection	esmtrprd.exe	SNMP trap transferring function. (*2)
ESMPRO/SM Event Manager	jsl.exe	CIM indication Subscription / Receiving events
ESMPRO/SM Common Component	jsl.exe	Main service
ESMPRO/SM Web Container	jsl.exe	Web application server
DianaScope ModemAgent	DianaScopeModemAgent.exe	For modem/direct connection

*1 This service has stopped when "Receive from Agent (TCP/IP)" of the TCP/IP Report Setting is disabled.

*2 The startup is set as "Manual" by default.

*3 "Alert Manager HTTPS Service" is started and the startup is set as "Automatic" when "Express Report (HTTPS) from Manager" of Report Setting is enabled.

"Alert Manager HTTPS Service" is stopped and the startup is set as "Manual" when "Express Report (HTTPS) from Manager" of Report Setting is disabled.

*4 For ESMPRO/SM Base Service, esmdsvnt.exe is registered as a service process, and esmdsvap.exe is started and stopped on starting and stopping the service.

- **Dependencies of the services**

The dependencies of the services are the followings:

Alert Manager ALIVE(S) Service
Alert Manager HTTPS Service
Alert Manager Main Service
NVBASE System Service
  ESM Alert Service
    Alert Manager Socket(R) Service
    Dmi Event Watcher
  ESM Command Service
  ESM Remote Map Service
  ESMPRO/SM Base Service
  ESMPRO/SM Trap Redirection
  ESMPRO/SM Event Manager
ESMPRO/SM Common Component
    ESMPRO/SM Event Manager
ESMPRO/SM Web Container
DianaScope ModemAgent

- **Order of starting or stopping services**

To start or stop services, perform the following procedure.

⧫ Starting services

1. Alert Manager ALIVE(S) Service
2. Alert Manager HTTPS Service (*)
3. Alert Manager Main Service
4. NVBASE System Service
5. ESM Remote Map Service
6. ESM Command Service
7. ESM Alert Service
8. Dmi Event Watcher (*)
9. ESMPRO/SM Base Service
10. ESMPRO/SM Trap Redirection (*)
11. AlertManager Socket(R) Service (*)
12. ESMPRO/SM Web Container
13. ESMPRO/SM Common Component
14. ESMPRO/SM Event Manager
15. DianaScope ModemAgent

⧫ Stopping services

1. DianaScope ModemAgent
2. ESMPRO/SM Event Manager
3. ESMPRO/SM Common Component
4. ESMPRO/SM Web Container
5. AlertManager Socket(R) Service (*)
6. ESMPRO/SM Trap Redirection (*)
7. ESMPRO/SM Base Service
8. Dmi Event Watcher (*)
9. ESM Alert Service
10. ESM Command Service
11. ESM Remote Map Service
12. NVBASE System Service
13. Alert Manager Main Service
14. Alert Manager HTTPS Service (*)
15. Alert Manager ALIVE(S) Service

* May be stopped depending on the settings. In such a case, there is no need to start or stop the service.