SystemManager Event Trap Utility (Ver.5.3)
Release Memo

July 2016

1) Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.
   In addition, Microsoft product names included in this guide are registered trademarks of Microsoft Corporation in the United States and other countries.
2) EXPRESSCLUSTER X and EXPRESSSCOPE are registered trademark of NEC Corporation.
3) In addition, proper nouns such as company names and product names included in this guide are trademarks or registered trademarks of their respective companies.
4) The "TM" mark and the R mark are not reflected in this document.

This document uses the following abbreviations to describe some product names:

Product Name	Abbreviation
Microsoft(R) Windows(R) Operating System	Windows
Microsoft(R) Windows(R) Server 2008	Windows 2008
Microsoft(R) Windows(R) Server 2008 R2	Windows 2008 R2
Microsoft(R) Windows(R) Server 2012	Windows 2012
Microsoft(R) Windows(R) Server 2012 R2	Windows 2012 R2

It describes any machine to which SystemManager Manager Ver5.0 or later is installed as a manager (machine).

It sometimes refers to SystemManager Event Trap Utility as Event Trap Utility.

Table of Contents

List of Tables

List of Figures

1 Operating Environment

This chapter describes system requirements that must be met in order to install SystemManager Event Trap Utility.

1.1 System Requirements

Table 1-1 System Requirements for Windows Versions

OS*1	Windows 2008 (32bit/64bit *4) Windows 2008 R2 (64bit *4) Windows 2012 (64bit *4) Windows 2012 R2 (64bit *4)
Memory*2	OS memory requirement + 10MB
Disk capacity*3	Required size: 20MB

*1: This product is available only in the OS of the same language as the linked SystemManager (Version 5 or later).

*2: Note that if users add additional message definitions, additional memory space will be needed to incorporate them.

*3: This size indicates the value derived from totaling the cumulative size of programs and message definition files included in the installer and that of files required for operating the system. The size of the files required for system operation can be changed.

Note that if users add additional message definition files, the disk capacity will increase by the size of them.

*4: The system runs in the 32-bit compatible mode when used on a 64-bit OS.

1.2 Required Software

This section describes the required software for SystemManager Event Trap Utility.

Table 1-2 Required Software for Event Trap Utility

Software Name	Version
ESMPRO/Base *1	8.0*2

*1: This software is not included in MasterScope Media. It must be provided by customers. Normally, the software is bundled by the ESMPRO products.

*2: You can confirm the version of your ESMPRO/BASE with %windir%\Express.ini. Check the CurrentVersion key in the NVBASE section from %windir%\Express.ini.

2 Function Overview

Event Trap Utility transfers messages to SystemManager (Ver5 or later) Manager.

It supports the following products as transfer sources:

- Windows versions of SystemManager (Ver3 or earlier)
- ESMPRO products

Note: Message link requires appropriate message definition files.
The message definition files for SystemManager (Ver3 or earlier) and some ESMPRO products are already embedded within Event Trap Utility.

2.1 Message Link with Windows Versions of SystemManager (Ver3 or earlier)

Event Trap Utility transfers messages received by SystemManager (Ver3 or earlier) Manager to SystemManager (Ver5 or later) Manager. Install Event Trap Utility to a machine on which SystemManager (Ver3 or earlier) Manager is running.

The blue line indicates the flow of messages from SystemManager (Ver3 or earlier) Agent. Note that SNMPTraps received by SystemManager (Ver3 or earlier) Manager are also to be transferred.

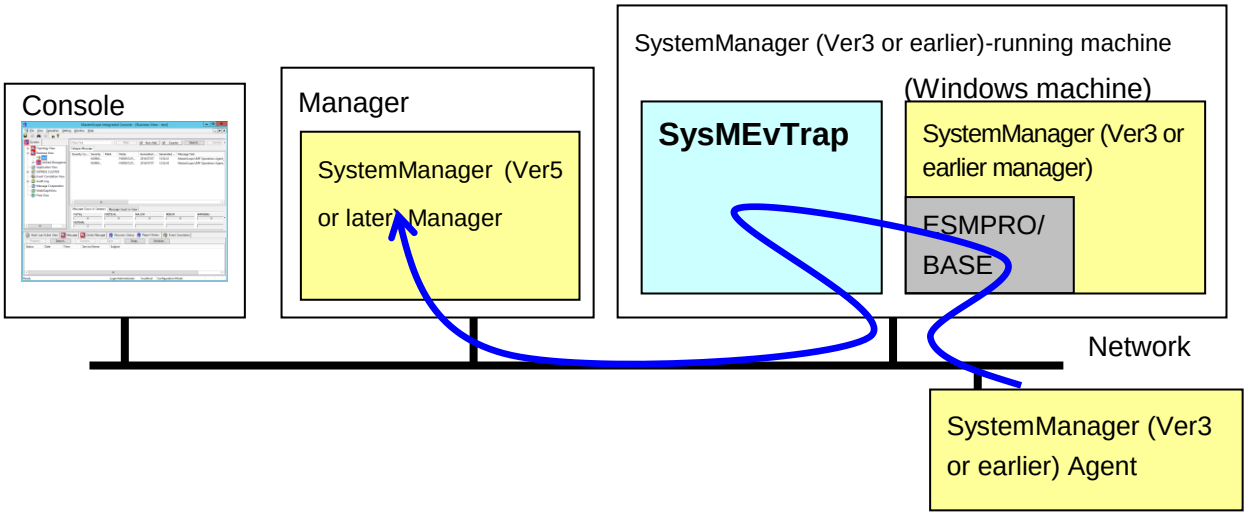

Figure 2-1: Schematic View of Message Link with Windows versions of SystemManager (Ver3)

Note: SystemManager Event Trap Utility only supports SNMPv1.

2.2 Message Link with ESMPRO Products

Event Trap Utility can transfer messages from ESMPRO products to SystemManager (Ver5 or later) Manager. Install Event Trap Utility to a machine on which an ESMPRO product is running.

The following figure illustrates a message link from ESMPRO/ServerManager and ESMPRO/ServerAgent.

The blue line indicates the flow of messages from ESMPRO/ServerAgent. Note that SNMPTraps received by ESMPRO/BASE are also to be transferred.

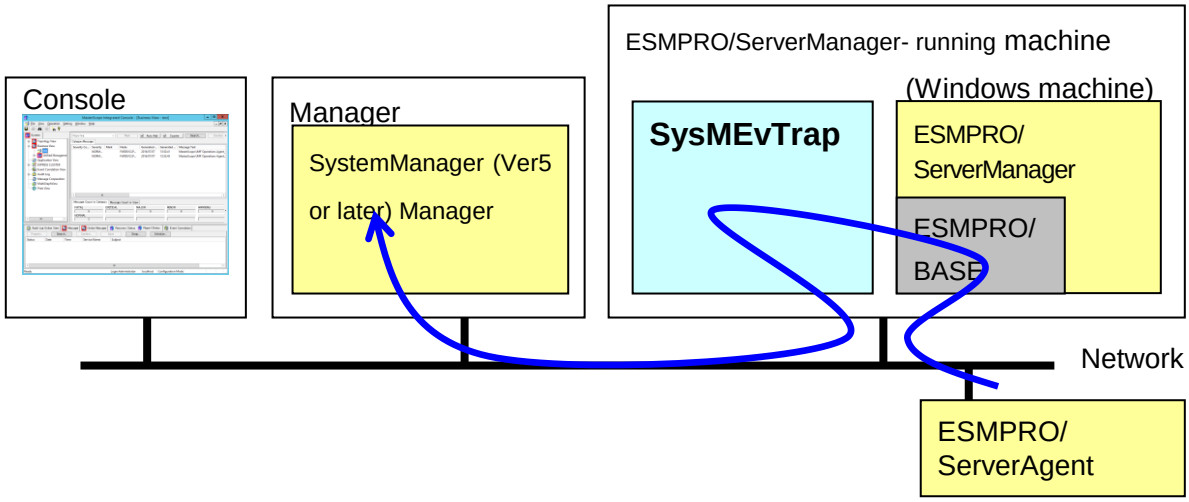

Figure 2-2: Schematic View of Message Link with ESMPRO/ServerManager

Note1: Other ESMPRO products (for example, ESMPRO/Netvisor) are configured in a manner similar to

Note2: SystemManager Event Trap Utility only supports SNMPv1.

Note3: SystemManager Event Trap Utility is capable of interacting with what is displayed in the ESMPRO alert viewer.

The trap from the ESMPRO data viewer is not reported to Event Trap Utility, and linkage is not allowed.

Messages of the SNMP report (PET (Platform Event Trap)) is sent from BMC (EXPRESSSCOPE engine) mounted in the Express5800 server to SystemManager (Version 5 or later).

However, they cannot be analyzed by Event Trap Utility due to its data structure.

The reported messages cannot be checked.

3 New functions and enhanced functions

3.1 Supporting SNMP traps from the NEC Tape Storage Products (T30A, T60A) and EM cards

A message definition file for SNMP traps from the NEC Tape Storage Products (T30A, T60A) and EM cards is now supported.

This allows SNMP traps defined in the file to be displayed on the SystemManager monitoring terminal by default.

4 Preparing for Installation

Before you install SystemManager Event Trap Utility, confirm and perform the following task:

4.1 Registering the Hostname of a Target Manager

To specify a host name for the destination manager, configure an environment where a machine on which SystemManager Event Trap Utility is installed can resolve network addresses based on host names.

4.2 Installing Visual C++ 2013 Redistributable Packages

The VisualC++ 2013 library runtime components must be installed in advance.

Obtain and install the “Microsoft Visual C++ 2013 Redistributable Package (x86)” from the Microsoft website or the following location on the MasterScope Media.

D:\tools\SysMgr\SysMEvTrap\Windows\runtime\vcredist_x86.exe

* In this section, the optical drive is assumed to be the D drive. Change this in accordance with your environment.

5 Installation

This chapter describes the procedure to be followed when installing a new SystemManager Event Trap Utility of single configuration.

For information on SystemManager Event Trap Utility of cluster configuration, refer to "8.2 Duplex Setup".

5.1 Installation procedure

MasterScope Media includes the installation module for Event Trap Utility.

Please install it by performing the following procedure.

1. Log on to Windows with an account that has administrative rights.

2. Insert MasterScope Media into the optical device.

3. Double-click “setup.exe” in the following path to start the installer.

   D:\tools\SysMgr\SysMEvTrap\Windows\setup.exe

   *This example assumes the optical device to be drive D. The setting should be changed appropriately according to your environment.

4. Install Event Trap Utility. Click [Next].

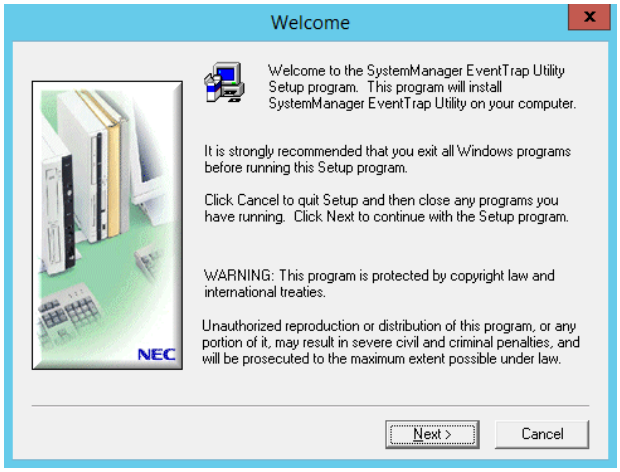

Figure 5-1: Event Trap Utility Installation (Welcome)

5. Confirm the Event Trap Utility installation destination. Click [Next] if it is correct.
   Click [Browse] to change the installation destination.

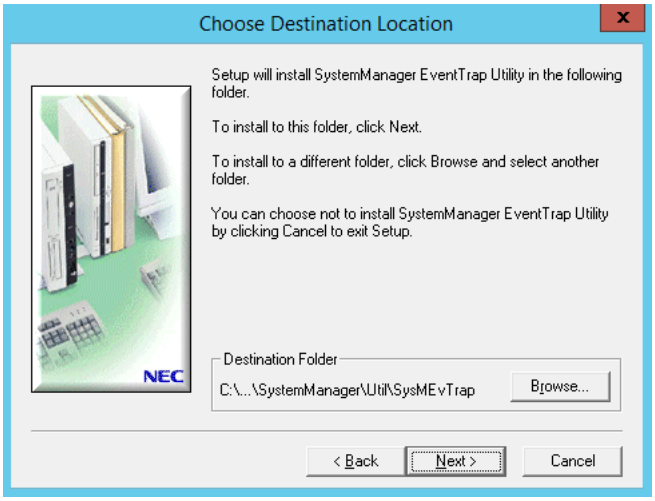

Figure 5-2: Event Trap Utility Installation (Select Installation Destination)

Note: Some characters cannot be used for folder paths to which Event Trap Utility is installed.
For details, refer to "7.7 About folder paths used in Event Trap Utility".

6. Specify the host name or IP address of the destination manager and then click the [Next] button.
   *"localhost" is specified for the hostname by default.

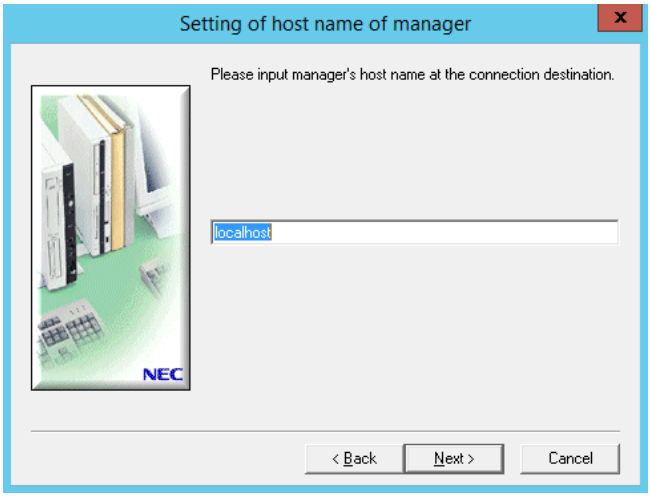

Figure 5-3: Event Trap Utility Installation (Enter Hostname)

7. Specify a desired port number for the target manager and click [Next].
   *The port number is 12520 by default.

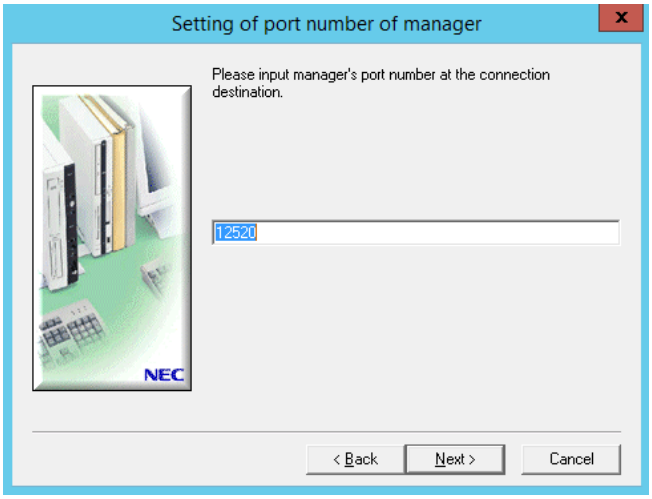

Figure 5-4: Event Trap Utility Installation (Enter Port Number)

8. Confirm your installation settings. Click [Next] if they are correct. To start the installation process, click [Next].
   To change settings, click [Back] and make appropriate changes.

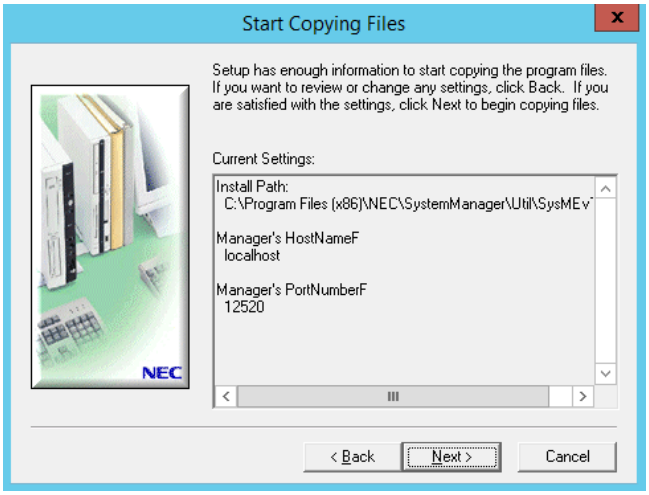

Figure 5-5: Event Trap Utility Installation (Selected Settings)

9. When the installation process finishes normally, the following window appears.

   Click [Finish].

   Next, start Event Trap Utility, and restart ESMPRO/BASE.

   The ESMPRO/BASE service is registered as the “ESM Base Service“.

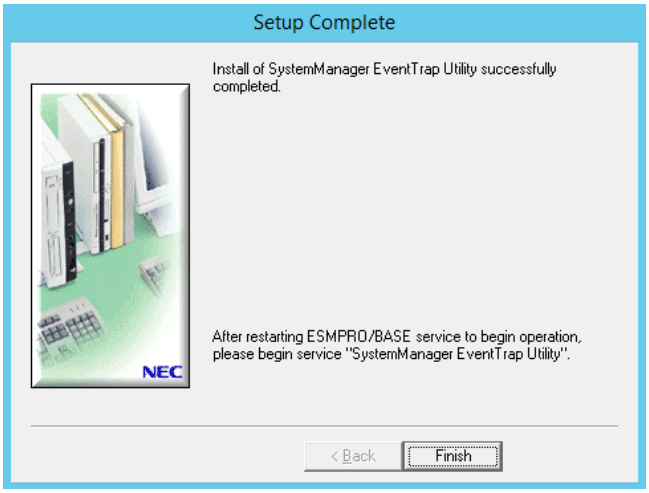

Figure 5-6: Event Trap Utility Installation (Complete)

Event Trap Utility has now been installed.

Refer to "8.1 Property File" to configure Event Trap Utility.

5.1.1 Notes

(1) About an event where installation or uninstallation takes a long time

[Event]

When users install or uninstall Event Trap Utility from a EXPRESSCLUSTER X environment, the process may take a long time.

This event occurs only when EXPRESSCLUSTER X1.0 for Windows is being used.

[Cause]

This event is ascribed to a problem between the “EXPRESSCLUSTER Shutdown Hook” module (clphookstdn.exe) in EXPRESSCLUSTER X1.0 for Windows and InstallShield(ver5). Clphookstdn.exe is a process that hooks a shutdown process from the Start menu and issues a warning message.

[Solution]

You can avoid this problem by following these steps in both the active system and the standby system before establishing Event Trap Utility.

The following example shows a case where EXPRESSCLUSTER X is installed to drive C:

1) Confirm that a “EXPRESSCLUSTER Shutdown Menu Hook” shortcut is found under “C:\Documents and Settings\All Users\Start Menu\Program\Startup.”
2) Move the above shortcut to another location so that it cannot be started from Startup.
3) When you have moved the shortcut, restart the machine or log off from it.
4) After logging in to the active system and the standby system, use Task Manager to confirm that clphookstdn.exe has not started.
5) When you have completed the above steps in both the active system and the standby system, establish the environment by following the procedure document.
6) Once you have established the environment for both systems, return the shortcut to its original position and restart the machine or log off from it.

*The above operation temporarily disables the start of the “EXPRESSCLUSTER Shutdown Hook.” It will not have any impact on EXPRESSCLUSTER X operations and, consequently, will not pose any problem.

6 Uninstallation

This chapter describes the procedure to follow when uninstalling SystemManager Event Trap Utility.

6.1 For Windows Versions

This section describes the procedure to uninstall a Windows version of SystemManager Event Trap Utility.

6.1.1 Uninstallation procedure

1. Log on to Windows with an account that has administrative rights.

2. Insert MasterScope Media into the optical device.

3. Double-click “setup.exe” in the following path to start it.

   D:\tools\SysMgr\SysMEvTrap\Windows\setup.exe

   *This example assumes the optical device to be drive D. The setting should be changed appropriately according to your environment.

4. When you are sure you want to uninstall the Event Trap Utility, you may click [Yes]. When you click [Yes], the Utility will be uninstalled. If you want to cancel the uninstallation process, click [No]. The process will be terminated.

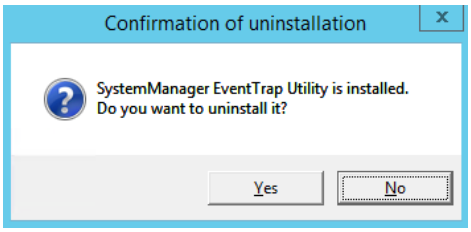

Figure 6-1: Uninstallation (Confirmation)

5. A confirmation dialog is displayed. Click [OK].

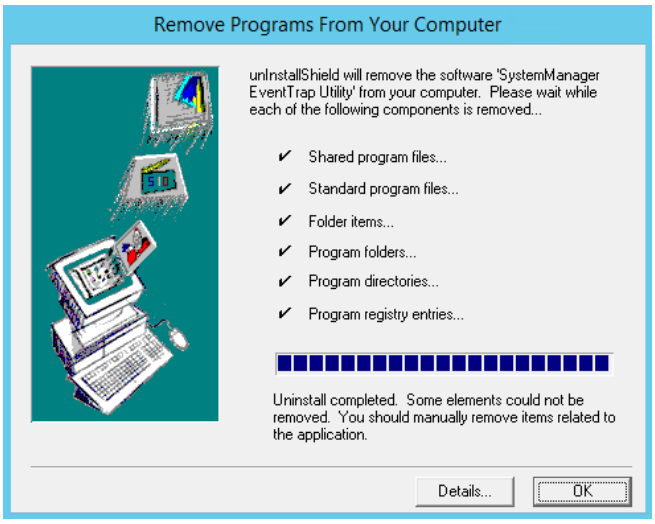

Figure 6-2: Uninstallation (Confirmation)

6. When the uninstallation process has finished normally, the following window appears. Click [Finish].

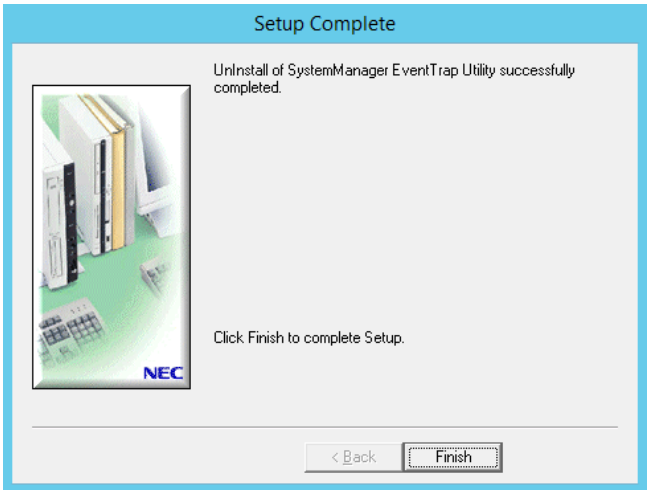

Figure 6-3: Uninstallation (Complete)

Event Trap Utility has now been uninstalled.

6.1.2 Notes

- If you uninstall Event Trap Utility in a duplex environment, manually remove all the files related to it from the shared disk.
- Manually cancel the settings that were made for EXPRESSCLUSTER X.
- If your environment has EXPRESSCLUSTER X1.0 for Windows, it may take some time to complete the installation and uninstallation processes. For details, refer to "5.1.1 Notes".

7 Notes

7.1 Dependency on ESMPRO/BASE Service

This note is intended for only the Windows versions of Event Trap Utility.

No dependencies are set between the “SystemManager Event Trap Utility Service“ or one of SystemManager Event Trap Utility services and the “ESM Base Service” or one of ESMPRO/BASE services.

7.2 Encoding Notification Messages

Messages displayed on the Manager console of SystemManager (Ver. 5 or later) might become unreadable in the following cases.

- False recognition with an automated determination process

  When SystemManager captures data reported from the agents and SNMPtrap data, it performs its own automated determination process on those data based on the Japanese character codes (it supports SJIS and EUC only).

  As the automated determination process cannot correctly identify characters in messages in the following cases, it may not display them properly. If that is the case, it assumes that the characters are encoded in SJIS.

  - ✓ When the number of characters in a message to be captured is small
  - ✓ When the number of characters in a message to be captured is small (for example, when the same character appears repeatedly)
  - ✓ When a messages includes characters that exist in the same code ranges in both SJIS and EUC Specifically, they are SJIS codes for single-byte katakana.

- Kanji characters beyond SJIS Kanji Plane 3

  As SystemManager does not support characters beyond SJIS Kanji Plane 3 (those after character code 0xEAA5), it cannot display them properly.

- Characters that cannot be converted by using API on Windows

  Manager of SystemManager (Ver5 or later) has been implemented in unicode.

  Event Trap Utility uses MultiByteToWideChar() function, a Win32 API, to convert data to be notified to that in unicode. Then, if the data includes a code that cannot be converted with this API, the code can neither be converted nor displayed properly on the console due to the API specifications.

7.3 Range of SpecificCode Numeric Values

The SpecificCode numeric values that can be handled range from 0 to 2147483647.

7.4 About delay in message notification

When the originating node name of a message is no known, Event Trap Utility will try to lookup the hostname from the IP address to resolve the node name. When the node name is not registered on neither hosts file nor DNS, it may take noticeable time for the resolution causing delay in message notification. If you are experiencing message delays and message's node field showing an IP address, consider registering the node name to the host file or to the DNS to speed up the name resolution process.

7.5 Case of the connection to the Manager is disconnected for long time

Event Trap Utility retries several times to reestablish the connection if the connection to the Manager is disconnected. If the connection cannot be reestablished for a long period of time and reaches a retry limit, Event Trap Utility will stop.

To change the retry behavior, please refer to "8.1 Property File".

7.6 In Case of Stop of ESMPRO/BASE

Event Trap Utility retries the startup check processing more than one time if startup of ESMPRO/BASE installed in the same host cannot be checked. If startup of ESMPRO/BASE cannot be checked even after retrying, Event Trap Utility stops according to the default setting.

To change the settings related to stopping, see "8.1.1 Property file for Event Trap Utility control processes".

7.7 About folder paths used in Event Trap Utility

For folder paths to be used in Event Trap Utility, you should use single-byte blank characters and printable characters (excluding the following characters).

/ * ? " < > | % & ; ^

To specify a one-byte space for the folder path of the installation destination, however, enclose the value of the “ImagePath” registry key in double quotation marks (“”) after installation as described in “7.10 When starting the Event Trap Utility service fails”.

Then, restart the Event Trap Utility service.

7.8 About Restarting ESMPRO/BASE

If you restarted ESMPRO/BASE, ensure that you also restart SystemManager Event Trap Utility after that.

Unless you restart it, a new occurrence of an alert will not be reported to SystemManager.

7.9 About Reinstalling ESMPRO/BASE

When you have reinstalled ESMPRO/BASE, ensure that you will also reinstall SystemManager Event Trap Utility.

Otherwise, the start of SystemManager Event Trap Utility fails because some initial settings used by it cannot be read.

7.10 When starting the Event Trap Utility service fails

If error message “SystemManager EventTrap Utility is not a valid Win32 application.” is output to the event log when starting the Event Trap Utility service failed, start the registry editor and verify the following entries.

Path:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SystemManager EventTrap Utility

Key name: ImagePath

Enclose the entire value in double quotation marks (“”) when a space is included in the value of “ImagePath”.

7.11 Order of starting and stopping linked product services

Start the services in the following order:

1. SystemManager Manager service
2. Event Trap Utility service
3. ESMPRO/BASE service

Even if the SystemManager Manager service is not running when starting the Event Trap Utility service, Event Trap Utility becomes operable by starting the SystemManager Manager service during the Event Trap Utility retry period.
For information about connection retries between Event Trap Utility and SystemManager Manager, refer to "7.5 Case of the connection to the Manager is disconnected for long time".

Stop the services in the reverse order.

7.12 SNMP traps from the NEC Tape Storage Products (T30A, T60A)

Note that SNMP traps from the NEC Tape Storage Products behave as described below.
To use a particular trap, add or change the definition as described below.

When the message definition file is updated, be sure to restart Event Trap Utility.
For the setting items of the message definition file, refer to "8.3 Message Definition Files ".

・For the following Enterprise, GenericCode, and SpecificCode traps, the message "The format is undefined." is displayed in the message view of the monitoring terminal.

```
Enterprise: 1.3.6.1.4.1.119.1.83.1.31
GenericCode: 6
SpecificCode: 200
Enterprise: 1.3.6.1.4.1.119.1.83.1.41
GenericCode: 6
SpecificCode: 200
```

To use these traps, add the following definitions in the message definition file.

```
Enterprise: 1.3.6.1.4.1.119.1.83.1.31
GenericCode: 6
SpecificCode: 200
```

```
#Severity:
Summary: t30aEventTrapTestTrap
Detail: (FC=TP98) TIME(%3%) %5%
Action: Test trap.
AlertType: Tape Library
ESMKind: T30A
Source: T30A_Event
EventID: 0x400000C8

Enterprise: 1.3.6.1.4.1.119.1.83.1.41
GenericCode: 6
SpecificCode: 200
#Severity:
Summary: t60aEventTrapTestTrap
Detail: (FC=TQ98) TIME(%3%) %5%
Action: Test trap.
AlertType: Tape Library
ESMKind: T60A
Source: T60A_Event
EventID: 0x400000C8
```

The above traps provide information to determine the degree of severity among 2 (information), 3 (warning), and 4 (abnormal). Note, however, that a fixed value should be specified for the Severity term in Event Trap Utility.
If omitted, 2 (information) is assumed.

・EventID cannot be displayed in the message view of the monitoring terminal.
To display EventID, copy the value of the EventID term to the Detail section of the message definition file.

(Copy example)

```
Enterprise: 1.3.6.1.4.1.119.1.83.1.31
GenericCode: 6
SpecificCode: 1
Severity: 4
Summary: t30aEventTrapEmergencyDrive
Detail: (FC=TP01) TIME(%3%) %5% EventID: 0xC0000001
Action: Please carry out processing corresponding to the CHK code.
AlertType: Tape Library
ESMKind: T30A
Source: T30A_Event
EventID: 0xC0000001
```

For SNMP traps from the NEC Tape Storage Products, note that the EventID value cannot be

displayed even if the template setting of the SystemManager manager function in "8.3.6 Mapping between a template and its linked data" is changed.

8 Remarks

8.1 Property File

8.1.1 Property file for Event Trap Utility control processes

It is the property file for control processes in SystemManager Event Trap Utility.

The following table shows user-editable items in the property file.

Unless absolutely necessary, you should not change the value of any property.

If you should change it to an inappropriate value, the behavior of Event Trap Utility will be unpredictable.

- List of setting items

Table 8-1 Property file for control processes setting parameter

parameter	description	default	Minimum	Maximum
INVOKE_RETRY_COUNT	Number of restarts of each process started by the SystemManager Event Trap Utility control process.	3	0	100
INVOKE_RETRY_CONTINUE	Indicates whether to reset the number of restarts of each process started by the SystemManager Event Trap Utility control process.*1 (TRUE: Yes, FALSE: No)	FALSE		

*1: When set to TRUE, the number of restarts will be reset when the SystemManager Event Trap Utility control process normally starts the other processes normally.

When set to FALSE, the number of restarts will not be reset and SystemManager Event Trap Utility will stop when any process started by the control process stops the number of times exceeding INVOKE_RETRY_COUNT.

- About path to store the property file

  The property file for Event Trap Utility control processes is stored in the following location:

Table 8-2 Path to Location where Property File Is Stored

OS	Location
Windows	<*INSTALL_HOME*>\FrameworkManager\config\SysMEvTrap_cntl.properties

Note: <*INSTALL_HOME*> is the directory specified when you installed SystemManager.

In Windows, you specify the directory with the installer when installing it.

In any 32-bit environment, the specified default is set to

C:¥Program Files¥NEC¥SystemManager¥Util¥SysMEvTrap.

In any 64-bit environment, it is set to

C:\Program Files (x86)\NEC\SystemManager\Util\SysMEvTrap.

When a cluster configuration is adopted, the property file resides in the following location:

Table 8-3 Path to Location where Property File Is Stored

OS	Location
Windows	<*Given folder in the shared drive*>\FrameworkManager*config*\SysMEvTrap_cntl.properties

- About the file format

The following shows the format for the property file:

```
INVOKE_RETRY_COUNT=<Number of restarts of each process>
INVOKE_RETRY_ CONTINUE =<Indicates whether to reset the number of restarts of each process>
```

The following shows a property file in which the default values are populated:

```
NVOKE_RETRY_COUNT=3
INVOKE_RETRY_CONTINUE=FALSE
```

8.1.2 Property file for Event Trap Utility operation

The host or port number of a target manager can be changed by changing an appropriate value in the property file of SystemManager Event Trap Utility.

Unless absolutely necessary, you should not change the value of any property.

If you should change it to an inappropriate value, the behavior of Event Trap Utility will be unpredictable.

- List of setting items

  The following table shows user-editable items in the property file.

Table 8-4 Setting items in the property file for operation

Parameter	Description	Default Value	Minimum	Maximum
MNG_HOST [required]	Target manager's hostname or IP address.	Localhost		
MNG_PORT	Target manager's port number.	12520	1025	65535
MNG_CLOSE_RETRY_SW	Indicator for whether to retry disconnecting a manager. (TRUE: Yes, FALSE: No)	TRUE		
MNG_CONNECT_RETRY_COUNT	Number of retries to connect to a manager.	10	0	1000
MNG_CONNECT_RETRY_INT	Time interval between retries to connect to a manager (in seconds).	60	5	3600
MNG_CONNECT_CHECK_RETRY_TIME	Waiting time before connecting to a manager (in seconds).	15	5	3600
MNG_RESPONSE_TIME	Time to wait for a response from a manager (in seconds).	15	1	1800
MNG_RETRY_COUNT	Number of retries allowed to send data to a manager until data transmission succeeds.	5	0	100
TRANSFER_FILE_SIZE	Maximum size of the transfer file for data transmission (unit: MB).	2	1	50
TRANSFER_FILE_GENE	Maximum number of generations for the transfer file for data transmission.	5	2	16

TRANSFER_WATCH_INT	Time interval for monitoring the transfer file for data transmission (in seconds).	1	1	3600

- About path to store the property file

  The property file for Event Trap Utility operation is stored in the following location:

Table 8-5 Path for storing the property file for operation

OS	Location
Windows	<*INSTALL_HOME*>\FrameworkManager\config\SysMEvTrap.properties

Note: <*INSTALL_HOME*> indicates the directory specified when installing Event Trap Utility.
In Windows, you specify the directory with the installer when installing it.
By default, it is C:\Program Files\NEC\SystemManager\Util\SysMEvTrap.

When a cluster configuration is adopted, the property file resides in the following location:

Table 8-6 Path for storing the property file for operation

OS	Location
Windows	<Given folder in the shared drive>\FrameworkManager\config\SysMEvTrap.properties

- About the file format

The following shows the format for each property file:

```
MNG_HOST=<Target manager's hostname>
MNG_PORT=<Target manager's port number>
MNG_CLOSE_RETRY_SW=<Indicator whether to retry disconnecting a manager (TRUE, FALSE)>
MNG_CONNECT_RETRY_COUNT=<Number of retries to connect to a manager. (*1)>
MNG_CONNECT_RETRY_INT=<Time interval between retries to connect to a manager (in seconds) (*1)>
MNG_CONNECT_CHECK_RETRY_TIME=<Waiting time before connecting to a manager (in seconds)>
MNG_RESPONSE_TIME=<Time to wait for a response from a manager (in seconds)>
MSG_RECV_ACK_SW=<Indicator whether a mode to confirm that data has reached a manager is present when sending data (TRUE) (*3)>
MNG_RETRY_COUNT=<Number of retries allowed to send data to a manager until data transmission succeeds (*2)>
TRANSFER_FILE_DIR=<Directory to store the transfer file for data transmission (*3)>
TRANSFER_FILE_SIZE=<Maximum size of the transfer file for data transmission (MB)>
TRANSFER_FILE_GENE=<Maximum number of generations for the transfer file for data transmission>
TRANSFER_WATCH_INT=<Time interval for monitoring the transfer file for data transmission>
SYSMGR_DEF_FILE=<Directory to store def files for Event Trap Utility (*3)>
```

*1: This value is only valid if MNG_CLOSE_RETRY_SW=TRUE.

*2: This value is only valid if MSG_RECV_ACK_SW=TRUE.

*3: Do not change. Unintended behavior might occur.

The following shows the respective property files in which the default values are populated:

```
MNG_HOST=localhost
MNG_PORT=12520
MNG_CLOSE_RETRY_SW=TRUE
MNG_CONNECT_RETRY_COUNT=10
MNG_CONNECT_RETRY_INT=60
MNG_CONNECT_CHECK_RETRY_TIME=15
MNG_RESPONSE_TIME=15
MSG_RECV_ACK_SW=TRUE
MNG_RETRY_COUNT=5
TRANSFER_FILE_DIR=\FrameworkManager\transfer
TRANSFER_FILE_SIZE=2
TRANSFER_FILE_GENE=5
TRANSFER_WATCH_INT=1
SYSMGR_DEF_FILE=\FrameworkManager\trapdef
```

8.2 Duplex Setup

SystemManager Event Trap Utility supports duplex systems.

This section explains the procedure used to set up a duplex environment for SystemManager Event Trap Utility in a duplex system.

SystemManager Event Trap Utility supports EXPRESSCLUSTER X.

For information on such as setting up EXPRESSCLUSTER X, refer to EXPRESSCLUSTER X manuals.

The following descriptions are provided based on the assumption that cluster and cluster group definitions for EXPRESSCLUSTER X have been set. Specifically, the clusters and their groups must be defined so that the shared DISK may be referenced. Assign any drive as the shared DISK.

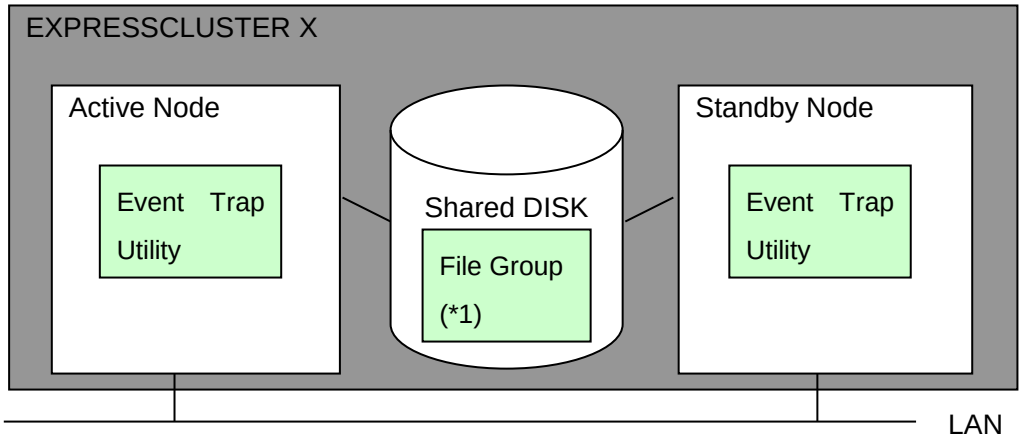

Figure 8-1: Duplexed Structure Diagram (Windows Versions)

*1: The file group consists of property and data files used by Event Trap Utility.
The group must be placed under the arbitrary drive that was assigned as the shared DISK.

*2: This document does not describe the procedure used to establish duplex ESMPRO/BASE.
Please do so by referring to separate ESMPRO/BASE manuals.

Note: This document does not describe the procedure used to establish duplex ESMPRO/BASE.

Note: This document uses the following values to describe the procedure;

- Assume drive X for the arbitrary drive that is assigned as the shared DISK
- Assume X:\\share\SysMgr\Util for the folder to which files for Event Trap Utility will be copied
  Create this folder before starting the procedure.
- <*INSTALL_HOME*> indicates the SysMEvTrap installation directory.
  In any 32-bit environment, the specified default is set to
  C:\Program Files\NEC\SystemManager\Util\SysMEvTrap.
  In any 64-bit environment, it is set to
  C:\Program Files (x86)\NEC\SystemManager\Util\SysMEvTrap.

1. Installing SystemManager Event Trap Utility in the active node

   Install SystemManager Event Trap Utility in the active node.

   For details, refer to "5 Installation".

2. Setting up Event Trap Utility files in the active node

   When the following command is executed, the property file and data file used by Event Trap Utility are placed in the specified folder in the shared disk.

   The directory you will specify must be an appropriate folder within the shared DISK.

><*INSTALL_HOME*>\FrameworkManager\bin\SysMEvTrap_Cluster.bat source-dir dest-dir TRUE

Parameter description:

source-dir: Installation path

By default, it is C:\Program Files\NEC\SystemManager\Util\SysMEvTrap.

dest-dir: Directory in which to store data within the shared DISK

Specify "X:\\share\SysMgr\Util".

TRUE: Specify whether the files are actually to be copied to the shared directory. In the active system, specify TRUE so that the files may be copied.

3. Installing SystemManager Event Trap Utility in the standby node as well

   Install SystemManager Event Trap Utility in the standby node.

   For details, refer to "5 Installation".

4. Setting up Event Trap Utility files in the standby node

   When the following command is executed, the property file and data file used by Event Trap Utility are placed in the specified folder in the shared disk.

   The directory you will specify must be an appropriate folder within the shared DISK.

><INSTALL_HOME>\FrameworkManager\bin\SysMEvTrap_Cluster.bat source-dir dest-dir FALSE

Parameter description:

source-dir: Installation path

By default, it is C:\Program Files\NEC\SystemManager\Util\SysMEvTrap.

dest-dir: Directory to store data within the shared DISK

Specify "X:\\share\SysMgr\Util".

FALSE: Specify whether the files are actually to be copied to the shared directory. As the files are not to be copied in the standby system, specify FALSE.

5. Changing the start attribute of the Event Trap Utility service

Select [Settings] -> [Control Panel] -> [Administrative Tools] -> [Services] from the Start menu to display the Services window.

Change the start attribute of “Event Trap Utility Service” to “Manual” with the following operation:

In the Services window, select the above service and display [Property] from the right-click menu. Change [Startup type] to [Manual].

Note that you must follow this setting procedure in both the active node and the standby node.

6. Setup by EXPRESSCLUSTER X

Creates the failover group for the servers to which Event Trap Utility is installed.

The resource settings for the failover group are described below.

The following two resources must be set.

Table 8-7 Type of resources that must be set

Type of resource	Value
Disk resource or Mirror disk resource	Any drive characters (x in the setting of this document)
Service resource	SystemManager EventTrap Utility

When the failover group has already been created, right click the created failover group, and then select [Add Resource] from the displayed pop-up menu. The [Resource Definition] dialog box is displayed.

First, set up the shared disk. For [Type], select [disk resource] or [mirror disk resource], and then enter the group name of the shared disk in the [Name] text box.

After that, set up the disk in accordance with the instructions in the dialog box.

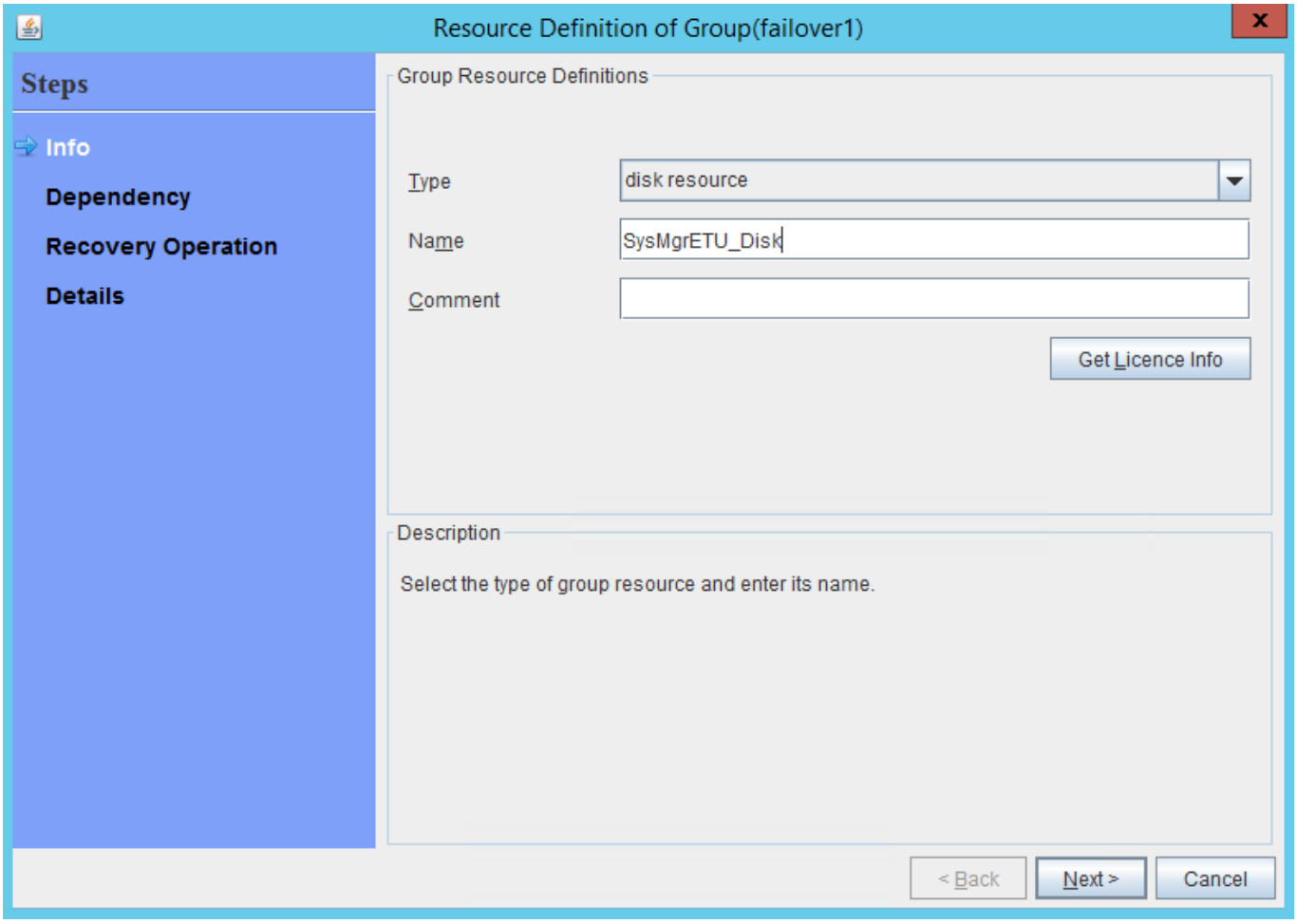

Figure 8-2: Disk resource

Next, set the service resources.

For [Type], select [service resource] in the Resource Definition Dialog, and enter the service resource name in the [Name] text box.

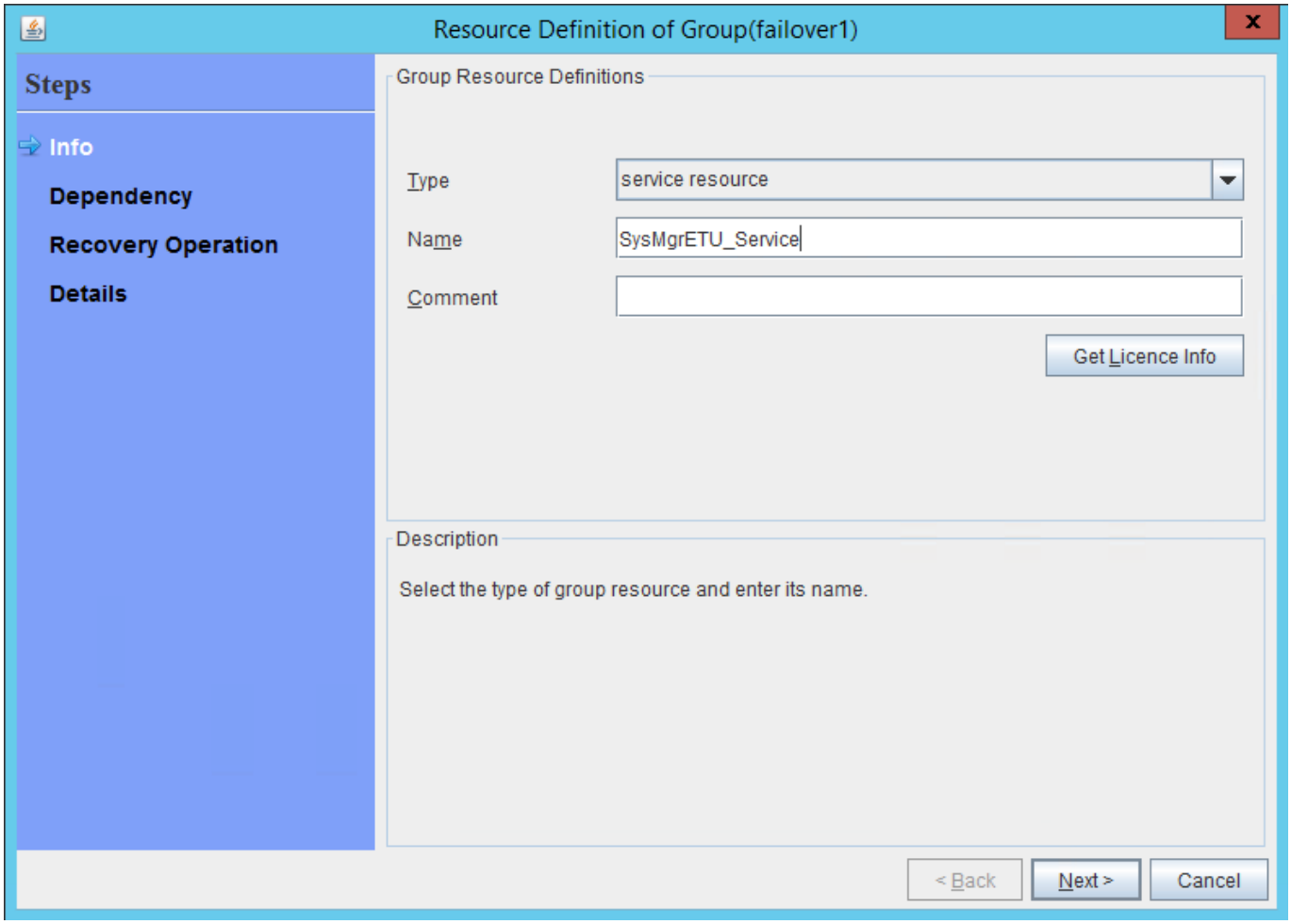

Figure 8-3: Service resource

To set up the dependencies, clear the [Follow the default dependency] check box, and then add the shared disk to the resources that are depended on.

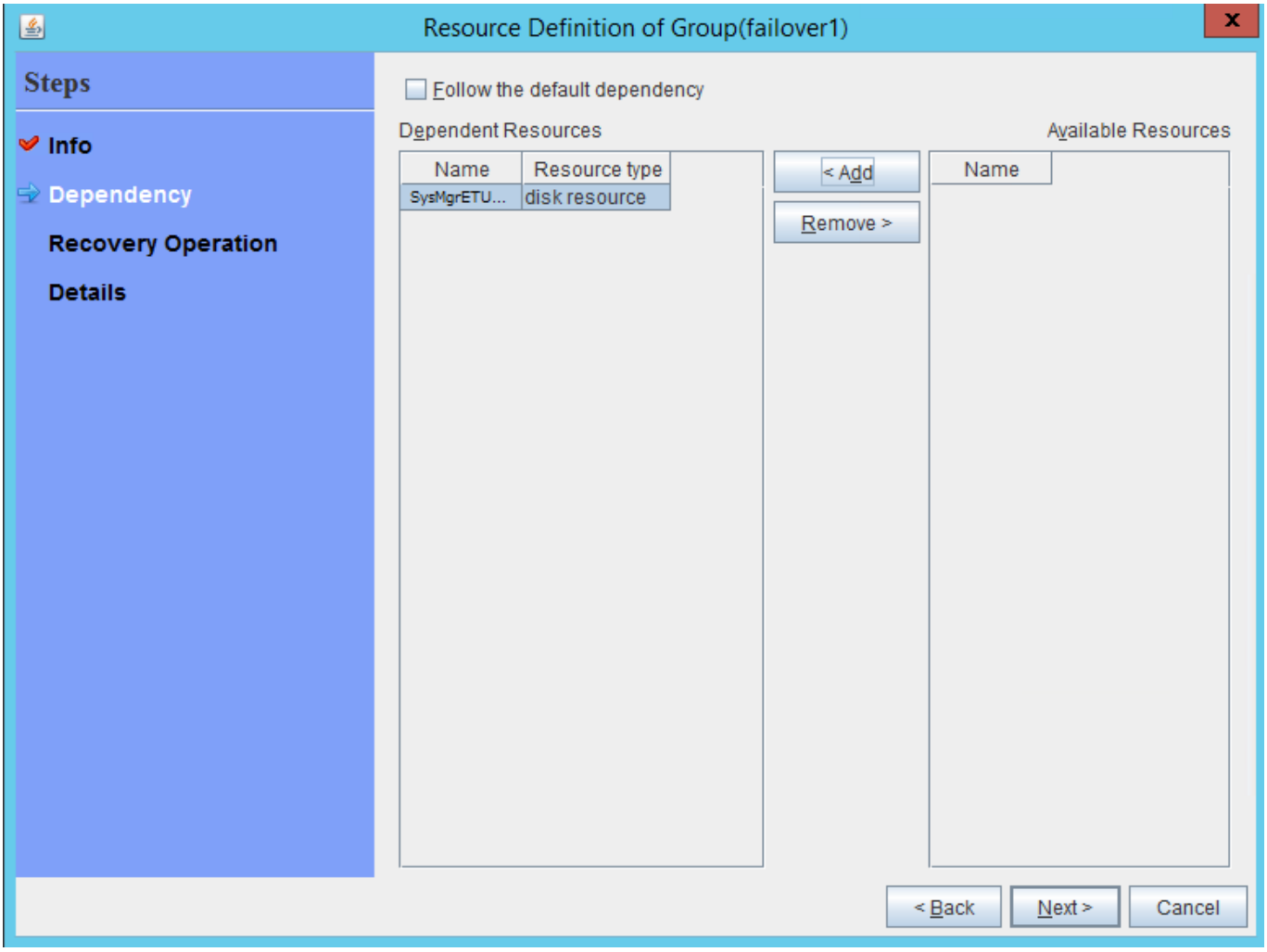

Figure 8-4: Dependencies of service resources

Specify the Windows service name for the product in the [Service Name] text box.

Set the following service name.

Service name: SystemManager EventTrap Utility

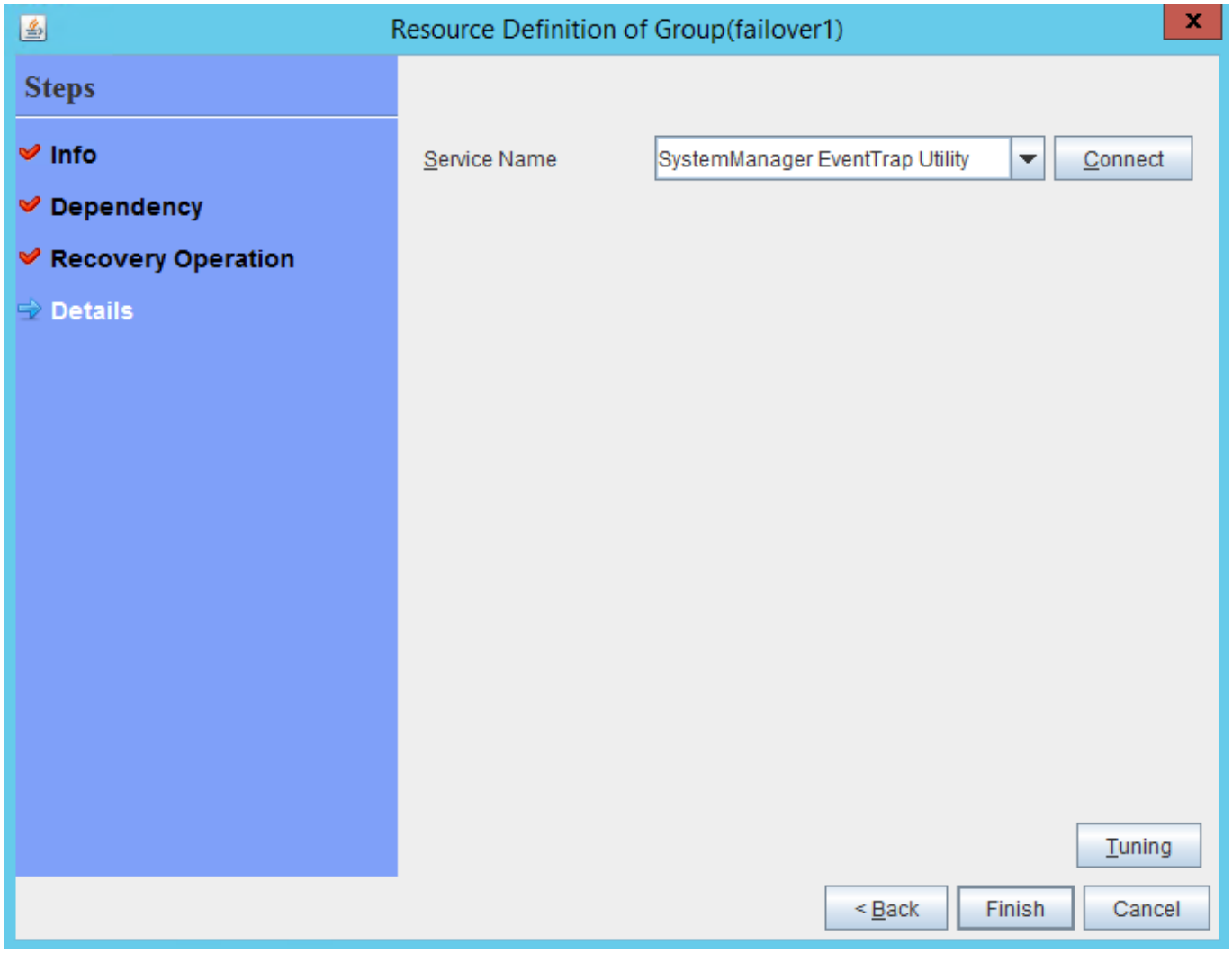

Figure 8-5: Selecting service source

7. Dependencies on the ESMPRO/BASE services

ESMPRO/BASE must be started up on the server where Event Trap Utility starts up.

(See "7.6 In Case of Stop of ESMPRO/BASE".) By registering ESMPRO/BASE in the resource of the same failover group as the Event Trap Utility, etc., be sure to perform the setting so that ESMPRO/BASE starts up in the Event Trap Utility operation system.

* Order of startup/stop of ESMPRO/BASE

Perform the setting so that ESMPRO/BASE starts up after Event Trap Utility.

Additionally, perform the setting so that Event Trap Utility stops after ESMPRO/BASE.

8. End of duplex setup

   The duplex Event Trap Utility has now been set up.

8.3 Message Definition Files

The data reported by SystemManager Event Trap Utility are to be displayed in the message view of SystemManager. Those data are created based on what is defined in its corresponding message definition file.

This section describes the content of Windows version of the message definition file and mapping between the content items and those displayed in the message view.

8.3.1 Message definition files

- **Path to the location where message definition files are stored**

  The message definition file for SystemManager (Ver3 or earlier) is placed in the Event Trap Utility installation directory during installation.

Note: The same message definition files as those provided with shipments of SystemManager Ver3.3 are stored under the installation directory.

Table 8-8 Message Definition File Location Path (Regular Installation)

Type	Path
Windows Version	*<INSTALL_HOME>*\FrameworkManager\trapdef

Note: *<INSTALL_HOME>* indicates the directory specified when installing Event Trap Utility.
Specify this during installation for Windows.
In any 32-bit environment, the specified default is set to
C:\Program Files\NEC\SystemManager\Util\SysMEvTrap.
In any 64-bit environment, it is set to
C:\Program Files(x86)\NEC\SystemManager\Util\SysMEvTrap.

It is placed in the following directory for the cluster configuration.

Table 8-9 Message Definition File Location Path (Duplex Environment)

Type	Path
Windows Version	*<Defined folder in shared drive>*\FrameworkManager\trapdef

Note: Directories for language environments are provided under each directory above.
The message definition file will be selected and run under the directory that matches your language environment.

- **Character code for message definition files**

  The message definition files support only SJIS character codes. Ensure that you describe message definition files in SJIS.

- **Specifications for message definition file names**

Ensure that you suffix every message definition file with ".def".

- **Items in a message definition file**

  Event Trap Utility reads all the message definition files (.def) present in the storage directory path described above in the order of the definition filenames (in the order of ASCII sorting).

8.3.2 About setting items in the message definition file

The following explains the parameters to be defined in the message definition file.

For cross references between each parameter and its corresponding item in the message view on the console, refer to the "8.3.5 Mapping to items in the message view on a console".

Items where "×" is specified for [Initial View] are not displayed in the SystemManager message view. To display them in the message view, set up the template for the manager function of SystemManager. For how to set up the message definition file and template, see "8.3.6 Mapping between a template and its linked data".

Table 8-10 Parameter Description

Parameter Name	Initial View	Omissible	Description
Enterprise:<Value>	○	No	Set a value that will be entered into the Enterprise clause in SNMP traps. If any values are applicable, set an asterisk (*).
GenericCode:<Value>	○	No	Set a value that will be entered into the Generic-trap clause in SNMP traps. An asterisk (*) cannot be used for this item.
SpecificCode:<Value>	○	No	Set a value that will be entered into the Specific-trap clause in SNMP traps. If any values are applicable, set an asterisk (*).
Summary:<Value>	×	Yes	Specify the summary of the message. Specify a character string of up to 512 bytes. *Omission of this setting makes its corresponding display item a blank.
Logging:<Value>	×	Yes	Specify whether the message must be received or not. Specify "1" when you need to receive it and otherwise "0". *Omission of this value is interpreted as specifying "1" (receive).
Severity:<Value>	○	Yes	Specify the severity of the message. Either 2 (information), 3 (warning), or 4 (abnormal) can be specified. *Omission of this value is interpreted as specifying "2" (information).
AlertType:<Value>	○	Yes	Specify the type of the message. Specify a character string of up to 128 bytes. *Omission of this setting makes its corresponding display item a blank.
Pattern 1 TimeStamp:1 <Time> <Offset> Pattern 2 TimeStamp:2 <TimeWithOffset>	○	Yes	Specify the time when the message was generated It can be specified in the following two formats: □Specification format 1 Specify a generated time. When a message occurs, this indicates the number of seconds elapsed since January 1, 1970 (at Greenwich standard time). It must be of type INTEGER. <Offset>: Specify "an offset of the generated time." It must be of type INTEGER. □Specification format 2

			Specify “a generated time + offset.” *Omission of this setting makes its corresponding display item a blank.
ESMKind:<Value>	○	Yes	Specify a component of the message. Specify a character string of up to 512 bytes. *Omission of this setting makes its corresponding display item a blank.
Action:<Value>	×	Yes	Specify the action for the message. Specify a character string of up to 512 bytes. *Omission of this setting makes its corresponding display item a blank.
Detail:<Value>	○	Yes	Specify the detail of the message. Specify a character string of up to 1024bytes. *Omission of this setting makes its corresponding display item a blank.
Source:<Value>	×	Yes	Use this setting when interacting with ESMPRO/ServerAgent. Specify the “source” of the event log of the event log monitoring message in ESMPRO/ServerAgent. Specify a character string of up to 512 bytes. *Omission of this setting makes its corresponding display item a blank. (Supplement) When interacting with ESMPRO/ServerAgent, it is defined so that it may correspond to the “source” of the monitored Windows event log.
EventID:<Value>	×	Yes	Use this setting when interacting with ESMPRO/ServerAgent. Specify the “Event ID” of the event log of the event log monitoring message in ESMPRO/ServerAgent. Specify a desired value in the range of 0 to 65535. *Omission of this setting makes its corresponding display item a blank. (Supplement) When interacting with ESMPRO/ServerAgent, it is defined so that it may correspond to the “Event ID” of the monitored Windows event log.
AgentAddress:<Value>	○	Yes	It is the hostname that generates the message. Normally, you do not have to specify it because the hostname will be obtained from the OS information, based on the network information included in a received SNMPTrap. Specify a host name or IP address to change the message source host name to another value. When a host name is specified, that value is used as the source host name. When an IP address is specified, the specified IP address is displayed. For more information on how to generate the generating hostname and generating IP address, refer to the note item “About the generating hostname and generating IP address” described later. Specify a character string of up to 1023bytes.

(Notes)

◆ About how parameters are displayed on the SystemManager console

The maximum specifiable size for the parameter values in the message definition files is as described above, but it is different from the maximum data length the SystemManager console can display.

Note that for this reason, the values defined for the parameters in a message definition file may not be displayed in entirety on the SystemManager console.

◆ About the generating hostname and generating IP address

This section describes how to generate the hostname and IP address that generate messages.

The source host name is the node name displayed in the node item of the message reported to SystemManager.

➢ When the parameter “AgentAddress” is omitted in the message definition file

- Generating hostname
  Hostname obtained by resolving the name based on an IP address generated from the network information contained in the received SNMPTrap.
  If the name resolution cannot be performed, the IP address is displayed as the source host name.
- Generating IP address
  IP address generated from the network information contained in the received SNMPTrap.

➢ When the parameter "AgentAddress" is specified in the message definition file

- Generating hostname
  Hostname specified in "AgentAddress" in the message definition file.
  If the IP address is specified in this item, the IP address is displayed as the source host name.
- Generating IP address
  IP address obtained by resolving the name based on the hostname specified in the AgentAddress parameter in the message definition file.

Note: Notes on the name resolution mentioned above are described in "7.4 About delay in message notification" Please, refer to the section.

◆ Compatibility with message display methods in ESMPRO

Methods to display alerts for ESMPRO other than the message definition file method mentioned above are not supported.

For example, the display method using dll is not supported.

◆ Compatibility with message definition files in ESMPRO

The items in the message definition file used to display alerts in ESMPRO are interchangeable with those for Event Trap Utility, except the TimeStamp and AgentAddress parameters.

- The TimeStamp parameters are specified differently in Event Trap Utility and ESMPRO. If the TimeStamp parameter cannot be specified by using the two definition patterns, omit specifying it.
- The AgentAddress parameter is an Event Trap Utility proprietary parameter.

◆ About the AgentAddress and TimeStamp parameters

Any values can be specified for both AgentAddress and TimeStamp parameters for a newly created message definition file; however, do not change both parameters for the Event Trap Utility message definition file that is placed during installation.

8.3.3 Specifiable special characters in the message definition file

8.3.3.1 List of specifiable special characters in the message definition file

The special characters that can be specified in message definition files are listed in "Table 8-11 List of special characters usable for message definition"

"Value" in the table will be replaced with the information in the received "variable-length data." For the replacement information, refer to "8.3.3.3 About replacing special characters".

Table 8-11 List of special characters usable for message definition

Special Character	Meaning	How It Is Displayed on Console
\CARRIAGE\	Indicates Carriage Return.	The message detail dialog box will begin a

	Use it as \CARRIAGE\\NEWLINE\. It means a new line.	new line. In the message view, it will be replaced with a blank.
\NEWLINE\	Indicates Line Feed. Use it as \CARRIAGE\\NEWLINE\. It means a new line.	The message detail dialog box will begin a new line. In the message view, it will be replaced with a blank.
\HORIZTAB\	Indicates a horizontal tab.	The message detail dialog box will display it as a tab. In the message view, it will be replaced with a blank.
%all	Outputs all the items of the received variable-length data as ”OID= Value”.	1.3.6.119.2.3.26.1.1.0= AAA 1.3.6.119.2.3.26.1.2.0= 2
%OID%	Displays Value in the entry that matches the specified OID, from the received variable-length data. For example, if “%1.3.6.119.2.3.26.1.1%” is specified, the entry with this OID (1.3.6.119.2.3.26.1.1) will be extracted.	Value will be displayed
%#%	Outputs the number of the received pieces of variable-length data.	10
%*%	Outputs all the items of the received variable-length data as [INDEX number]”＋”OID (type): Value”. (however, OID will be output as a number as it is)	[1] 1.3.6.119.2.3.26.1.1.0 (OctetString): 1 [2] 1.3.6.119.2.3.26.1.2.0 (OctetString): 2
%n%	Displays Value in the specified n^{th} entry, from the received variable-length data.	Value will be displayed
%+n%	Displays the specified n^{th} entry as ”OID : Value”, from the received variable-length data. (however, OID will be output as a number as it is)	1.3.6.119.2.3.26.1.2.0 : 2
%-n%	Displays the specified n^{th} entry as ”[INDEX number]”＋”OID (type): Value”, from the received variable-length data. (however, OID will be output as a number)	[2] 1.3.6.119.2.3.26.1.2.0 (OctetString): 2
%>+n%	Outputs continuously the n^{th} or later received variable-length data as ”OID :Value”. (however, OID will be output as a number as it is)	1.3.6.119.2.3.26.1.6.0: 6 1.3.6.119.2.3.26.1.7.0: 7
%>-n%	Outputs continuously the n^{th} or later received variable-length data as ”[INDEX number]”＋”OID (type): Value”. (however, OID will be output as a number as it is)	[1] 1.3.6.119.2.3.26.1.1.0 (OctetString): 1 [2] 1.3.6.119.2.3.26.1.2.0 (OctetString): 2
%C%	Outputs the community character string of SNMPTrap. Normally, it is the received	private

	community value.	
%o%	Outputs data in the form of Enterprise+"0"+SpecificCode. Normally, it is the content of the Enterprise parameter and that of the SpecificCode parameter in the message definition file. If it does not match the contents, the received value will be used.	.1.3.6.1.2.1.16.0.2
%e%	Outputs Enterprise using ObjectID in the form of a number. Normally, it is the content of the Enterprise parameter in the message definition file. If there are no Enterprise parameters that match this setting, the received Enterprise value will be used.	.1.3.6.1.4.1.119.1.26.2
%G%	Outputs the generic trap number. Normally, it is the content of the GenericCode parameter in the message definition file. If there are no GenericCode parameters that match this setting, the received GenericCode value will be used.	6
%S%	Outputs the specific trap number. Normally, it is the content of the SpecificCode parameter in the message definition file. If there are no SpecificCode parameters that match this setting, the received SpecificCode value will be used.	2
%T%	Value stored in the received data. Time from when the source module was started to when a message is sent	22283

(Notes)

(1) When the information that corresponds to a special character cannot be obtained, t he special character will be displayed on the console as it is.

For example, assume that Detail is defined as follows:

Detail: Error-Code = %4%

When the received variable-length data has no 4th entry, the special character will not be replaced and will be displayed as defined similarly to the following:

Error-Code = %4%

Other special characters such as Severity may be changed to their default value b y Event Trap Utility.

8.3.3.2 List of parameters for which special characters can be specified in the message definition file

The parameters for which special characters can be specified in the message definition file are listed in the "Table 8-12 List of usable and unusable special characters in parameters".

Table 8-12 List of usable and unusable special characters in parameters

Parameter Name	Can Special Characters Be Used
Enterprise	No
GenericCode	No
SpecificCode	No
Summary	Yes
Logging	Only %OID% and %n% are available.
Severity	Only %OID% and %n% are available.
AlertType	Yes
TimeStamp	Only %OID% and %n% are available.
ESMKind	Yes
Action	Yes
Detail	Yes
Source	Yes
EventID	Only %OID% and %n% are available.
AgentAddress	Only %OID% and %n% are available.

8.3.3.3 About replacing special characters

As described before, a special character specifiable in a message definition file will be replaced with the received “variable-length data” in the place where it is specified. The following summarizes the types of data handled in the replacement:

- OCTET_STRING data

  When obtaining data from the received “variable-length data," the binary data may not be displayed if it is of OCTET_STRING type.

  Encoding is performed based on “automatic determination.”

  Note: If the number of characters is small, auto judgment might not work properly, resulting in incorrect display. For details about auto judgment, refer to “7.2Encoding Notification Messages”.

- Numeric data

  In Event Trap Utility, a special character will be replaced with a decimal number whenever it is replaced with numeric data.

  Note: In configuration of the message link to ESMPRO/ServerAgent, there is a function that can replace a numerical value to which a special meaning is assigned on the side of ESMPRO/ServerAgent with an appropriate character string.
  Event Trap Utility does not support this function. Consequently, such values will be displayed as they are.

- OBJECT IDENTIFIER data

  In Event Trap Utility, a special character will be replaced with a number(s) and dot(s) (“.”) whenever it is replaced with OBJECT IDENTIFIER data.

- IP address data

  In Event Trap Utility, a special character will be replaced with a dot notation whenever it is replaced with IP address data.

8.3.4 About updating the message definition file

The message definition files can be customized.

Users can change parameters (such as changing a severity) in the current message definition file or add a new message definition file.

To put those changes in force, users must restart SystemManager Event Trap Utility.

8.3.5 Mapping to items in the message view on a console

The items in the message definition files correspond to those displayed in the message view on a console. The following shows the default mapping:

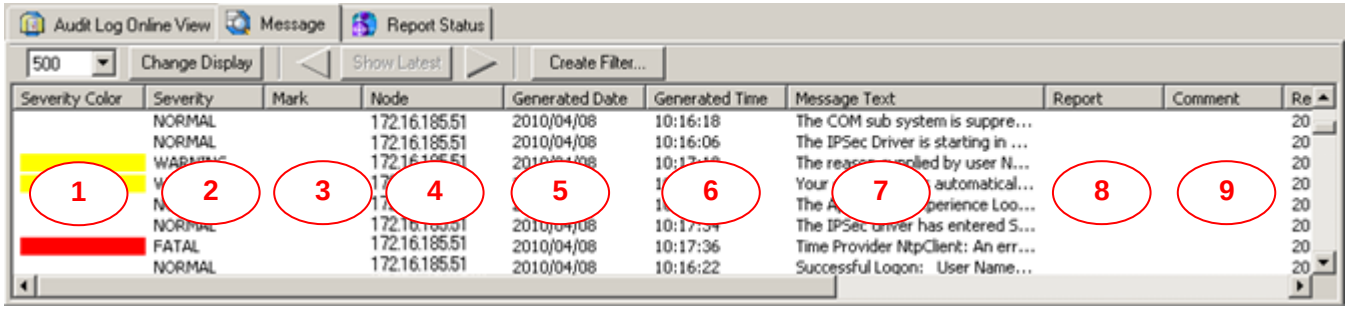

Figure 8-6: Message View (1/2)

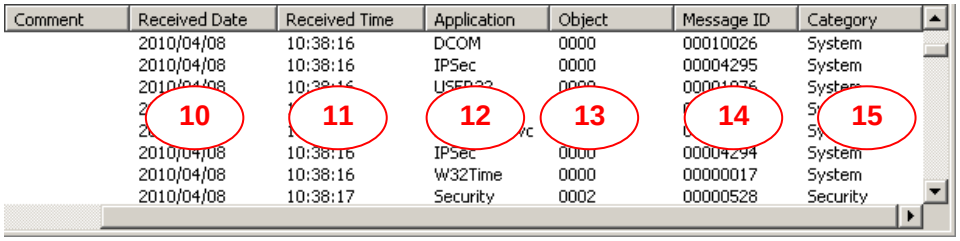

Figure 8-7: Message View (2/2)

Table 8-13 Mapping between Displayed Items in the Message View and Items in the Message Definition File

Number	Displayed Item	Item Name in Message Definition File	Meaning of Item	Supplement to Mapping
(1)	Severity Color	—	Displays the color based on the importance of each message and any added User Mark.	—
(2)	Severity	Severity	Displays a severity set in each alert.	Severity=2: Normal Severity=3: Warning Severity=4: Abnormal
(3)	Mark	—	Displays each assigned user mark.	—

(4)	Node	AgentAddress	Displays the node name or IP address that reported each message.	—
(5)	Generated Date	TimeStamp	Displays the date on which each message was generated on a node.	Date on which a failure was detected on SystemManager Agent
(6)	Generated Time	TimeStamp	Displays the time at which each message was generated on a node.	Time at which a failure was detected on SystemManager Agent
(7)	Message Text	Detail	Displays the text of each message.	—
(8)	Report	—	Displays the reporting status of each message.	—
(9)	Comment	—	Displays "Yes" for each message if it is annotated.	—
(10)	Received Date	—	Displays the date on which each message was received by the message monitoring function.	Date on which SystemManager Manager received each message from Event Trap Utility.
(11)	Received Time	—	Displays the time at which each message was received by the message monitoring function.	Time at which SystemManager Manager received each message from Event Trap Utility.
(12)	Application	ESMKind	Displays the name of the application that output each message.	—
(13)	Object	—	Object name that output each message. Permanent	—
(14)	Message ID	Enterprise, GenericCode, SpecificCode	Displays the ID of each message.	Event Trap Utility maps Enterprise, GenericCode, or SpecificCode to this.
(15)	Category	AlertType	Category to which each message belongs.	—

8.3.6 Mapping between a template and its linked data

You can customize the items of a message you want to display in [Message Text] of the message view on the console by changing the settings of a template in the SystemManager manager function. For the detailed method of specifying a template, refer to SystemManager manual.

The following provides the mapping table between the keywords in the template and data items transmitted by Event Trap Utility:

Table 8-14 Mapping between Template Keywords and Data Items Transmitted by Event Trap Utility

Keyword in Template	Data Transmitted by Event Trap Utility
%ENTERPRISE%	Replaced with the value of the Enterprise parameter in the message definition file. For a message that is not defined in the message definition file, it will be replaced with the value of Enterprise in the message.
%GENERICCODE%	Replaced with the value of the GenericCode parameter in the message definition file. For a message that is not defined in the message definition file, it will be replaced with the value of GenericCode in the message.
%SPECIFICCODE%	Replaced with the value of the SpecificCode parameter in the message definition file. For a message that is not defined in the message definition file, it will be replaced with the value of SpecificCode in the message.
%IPADDRESS%	Replaced with the generating IP address of a message. For more information on the generating IP address, refer to the note item “About the generating hostname and generating IP address” in the “Table 8-10 Parameter Description”.
%LOGGING%	Replaced with the value of the Logging parameter in the message definition file. When the Logging parameter is omitted in the message definition file, it will be a blank.
%DETAILMESSAGE%	Replaced with the value of the Detail parameter in the message definition file. When the Detail parameter is omitted in the message definition file, it will be a blank.
%SUMMARY%	Replaced with the value of the Summary parameter in the message definition file. When the Summary parameter is omitted in the message definition file, it will be a blank.
%SOURCENAME%	Replaced with the value of the Source parameter in the message definition file. When the Source parameter is omitted in the message definition file, it will be a blank.
%ALERTTYPE%	Replaced with the value of the AlertType parameter in the message definition file.

	When the AlertType parameter is omitted in the message definition file, it will be a blank.
%RECOVERYACTION%	Replaced with the value of the Action parameter in the message definition file. When the Action parameter is omitted in the message definition file, it will be a blank.
%RESOURCENAME%	Replaced with the generating hostname of a message. For more information on the generating hostname, refer to the note item “About the generating hostname and generating IP address” in the “Table 8-9: Parameter Description.”
%COMPONENTNAME%	Replaced with the value of the ESMKind parameter in the message definition file. When the ESMKind parameter is omitted in the message definition file, it will be a blank.
%TRAPRECEIVEPROTOCOL%	Replaced with the protocol of a message. Permanently, “UDP.”
%SEVERITY%	Replaced with the value of the Severity parameter in the message definition file.
%TRAPTYPE%	Replaced with the value that corresponds to the value of GenericCode in the message definition file. For GenericCode=0 – 5 in the message : 0 For GenericCode=6 in the message : 1 When receiving a message without the message definition :2
%EVENTID%	Replaced with the value of the EventID parameter in the message definition file.
%TIMEZONE%	Replaced with the value of Offset of the TimeStamp parameter in the message definition file. When the TimeStamp parameter is omitted in the message definition file, it will be a blank.
%ALERTOCCURREDTIME% %ALERTOCCURREDTIME_STR% (in the format of YYYY/MM/DD HH:MM:SS)	Replaced with the value of Time of the TimeStamp parameter in the message definition file. When the TimeStamp parameter is omitted in the message definition file, it will be a blank.
%TIMEZONEOFFSET%	Replaced with the value of the Time Zone in which Event Trap Utility is running.
%ARRIVALTIME% %ARRIVALTIME_STR% (in the format of YYYY/MM/DD HH:MM:SS)	Replaced with the GMT time when Event Trap Utility receives the message.

* For details of the message definition file, refer to "8.3.1 Message definition files" in this document.

8.4 Version Upgrade

This section describes the procedure to be followed when upgrading SystemManager Event Trap Utility from version 4.

1. Making a backup of files required for Event Trap Utility

If you changed the following files, manually make a backup of those files before upgrading Event Tap Utility. After installing the new version, manually reflect the changes to the corresponding files of the new version. Those backed up files will also be used when restoring the current version to the original by downgrading.

Message definition files

For information on the file path, refer to "8.3.1 Message definition files".

○**Property file for Event Trap Utility control processes**

For information on the file path, refer to "8.1.1 Property file for Event Trap Utility control processes".

○**Property file for Event Trap Utility operation**

For information on the file path, refer to "8.1.2 Property file for Event Trap Utility operation".

2. Uninstalling the Event Trap Utility you are using

Uninstall the version of Event Trap Utility you are now using. For details of the uninstallation method, refer to the release memo for your version of Event Trap Utility.

3. Installing a new version of Event Trap Utility

Install the new version of Event Trap Utility to which you want to upgrade. For details of the installation method, refer to "5 Installation".

4. Reflecting the changes

If you changed the files described above, manually reflect the changed items in those files.

Before doing this operation, stop Event Trap Utility. To put those changed files in effect, restart Event Trap Utility.

○**Message definition files**

・ When you added a new message definition file

If you added a new message definition file, manually copy the added message definition file from "<*dest-dir*>\SysMEvTrap\FrameworkManager\trapdef" or the directory in which to store backup data to "<*INSTALL_HOME*>\FrameworkManager\trapdef" or the installation directory.

Note: <dest-dir> indicates the directory in which to store backup data.
<*INSTALL_HOME*> indicates the directory specified when installing Event Trap Utility.
If you are in a duplex environment, read <*INSTALL_HOME*> as ＜*Given folder in the shared drive*＞ or the data storage directory within the shared disk.

・ When you customized existing message definition files

If you customized existing message definition files, merge the customized items in each file with the corresponding message definition file in the installation directory (or in the data storage directory within the shared disk in the case of a duplex environment).

○**Property file for Event Trap Utility control processes（SysMEvTrap_cntl.properties）**

「Check the property items described in "8.1.1 Property file for Event Trap Utility control processes" and reflect the changed items in the file.

○**Property file for Event Trap Utility operation (SysMEvTrap.properties)**

「Check the property items described in "8.1.2 Property file for Event Trap Utility operation" and reflect the changed items in the file.

8.4.1 Note

The default value for the port number for a target manager has been changed from SystemManager Ver4 and Ver5 or later on the target side. For this reason, if your Event Trap Utility was connected with SystemManager (Ver4), make a backup of the property file for Event Trap Utility operation (SysMEvTrap.properties) before upgrading to the new version, and reflect the value of MNG_PORT to the file of the new version.

8.5 About Linking with ESMPRO/BASE

8.5.1 Reporting alert when Event Trap Utility stops

A new function has been introduced to report any alert that occurred while Event Trap Utility stopped when it is started.

This function only works for ESMPRO/BASE of version 8.0L or later.

The version of ESMPRO/BASE can be confirmed using %windir%\Express.ini.

Confirm the "CurrentVersion" key in the NVBASE section described in %windir%\Express.ini.

8.6 Error alerts

SystemManager Event Trap Utility reports some internally detected error alerts to SystemManager.

The following table describes the error alerts to be reported.

Table 8-15 Error alerts

Message	Cause	Action
Transfer file's tailer code is illegal. fileName=<file-name>	The alert information accumulation file that is used in the product cannot be read because an error occurred in that file.	A new accumulation file will be created automatically. Therefore, no action is required. *1

*1 However, alert information recorded after the corrupted part may not be reported to SystemManager because the alert information accumulation file cannot be read.

8.7 How to Check Event Trap Utility Version

The following commands allow you to check the Event Trap Utility version.

* Line feed is inserted in the following command. However, do not insert the line feed during execution of the command.

• Windows (32 bit)

reg query "HKEY_LOCAL_MACHINE\SOFTWARE\NEC\SystemManager EventTrap Utility" /v "CurrentVersion"

• Windows (x64)

reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NEC\SystemManager EventTrap Utility" /v "CurrentVersion"

(Example of output result in Windows (x64))

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\NEC\SystemManager EventTrap Utility
CurrentVersion REG_SZ 5.3.5

In the example above, 5.3.5 is the Event Trap Utility product version.

In Windows (32 bit), the version is displayed in the same way.