HITACHI
Inspire the Next

For Windows Systems

Job Management Partner 1/Software Distribution

Setup Guide

3020-3-S80-80(E)

■ Relevant program products

P-2642-1197 Job Management Partner 1/Software Distribution Manager version 09-51 (for Windows Server 2003, Windows XP Professional, and Windows 2000)

P-2642-1397 Job Management Partner 1/Software Distribution Client version 09-51 (for Windows Server 2003, Windows XP, Windows 2000, Windows NT 4.0, Windows Me, and Windows 98)

P-2A42-1197 Job Management Partner 1/Software Distribution Manager version 09-51 (for Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista)

P-2C42-1397 Job Management Partner 1/Software Distribution Client version 09-51 (for Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista)

P-1B42-2J72 Job Management Partner 1/Software Distribution Network Node Manager Linkage version 07-00 (for HP-UX)

P-2642-1C77 Job Management Partner 1/Software Distribution Internet Gateway version 07-00 (for Windows Server 2003, Windows XP Professional, Windows 2000, and Windows NT Server 4.0)

P-2642-1D77 Job Management Partner 1/Software Distribution HTTP Gateway version 07-00 (for Windows Server 2003, Windows XP, Windows 2000, Windows NT 4.0, Windows Me, and Windows 98)

■ Trademarks

■ Microsoft product screen shots

Microsoft product screen shots reprinted with permission from Microsoft Corporation.

■ Restrictions

Information in this document is subject to change without notice and does not represent a commitment on the part of Hitachi. The software described in this manual is furnished according to a license agreement with Hitachi. The license agreement contains all of the terms and conditions governing your use of the software and documentation, including all warranty rights, limitations of liability, and disclaimers of warranty.

Material contained in this document may describe Hitachi products not available or features not available in your country.

No part of this material may be reproduced in any form or by any means without permission in writing from the publisher.

Printed in Japan.

■ Issued

June 2013: 3020-3-S80-80(E)

■ Copyright

Summary of amendments

The following table lists changes in the manuals 3020-3-S79-80(E), 3020-3-S80-80(E), 3020-3-S81-80(E), and 3020-3-S82-80(E) for JP1/Software Distribution 09-51 and product changes related to these manuals.

Changes	Location
Windows 8 and Windows Server 2012 are now supported.	Desc. and Planning Guide: *1.3.6*, *2.2.1*, *2.2.2*, *2.5.2*, *2.5.3*, *2.5.4*, *2.5.5*, *2.5.6*, *2.5.8*, *2.7.1*, *2.7.2*, *2.7.6*, *2.13.3*, *2.13.7*, *2.14.5*, *5.1.5*, *6.6.1*, *Appendix A.2*, *Appendix C.23*, *C.61*, *C.62*, *Appendix F* Setup Guide: *1.1.1*, *1.1.2*, *2.1.4*, *2.1.6*, *2.1.25*, *3.1.16*, *4.6*, *5.4*, *6.3*, *7.3.2*, *7.4.1*, *7.4.5*, *7.5.1*, *7.5.4*, *9.5.2*, *11.1.1*, *11.1.2* Admin. Guide 1: *2.2.3*, *2.2.5*, *2.2.9*, *2.2.10*, *3.2.2*, *6.2.6*, *6.2.10*, *6.5.3*, *6.6.4*, *11.1.2*, *11.7*, *Appendix F* Admin. Guide 2: *1.1.1*, *4.26.20*, *4.28*, *6.6.4*, *6.6.7*, *7.2.1*, *Appendix A*, *A.1*, *A.2*, *A.3*, *A.4*, *A.5*, *A.6*, *Appendix E*
Microsoft SQL Server 2012 can now be used as a relational database program.	Desc. and Planning Guide: *2.6.5*, *5.2.6*, *5.4.2* Setup Guide:*7.1.1*, *7.3.2*, *7.5.4*, *7.6*, *11.1.1*, *11.1.2*, *Appendix A.2*, *Appendix F* Admin. Guide 2: *6.3.2*
Software information can now be collected for additional Microsoft Office products. In addition, greater detail about Microsoft Office products is now provided.	Desc. and Planning Guide: *2.2.1*
Software information can now be collected for additional anti-virus products.	Desc. and Planning Guide: *2.2.2*

Legend:

Desc. and Planning Guide: *Job Management Partner 1/Software Distribution Description and Planning Guide* (3020-3-S79(E)), for Windows systems

Setup Guide: *Job Management Partner 1/Software Distribution Setup Guide* (3020-3-S80(E)), for Windows systems

Admin. Guide 1: *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1* (3020-3-S81(E)), for Windows systems

Admin. Guide 2: *Job Management Partner 1/Software Distribution Administrator's Guide Volume 2* (3020-3-S82(E)), for Windows systems

In addition to the above changes, minor editorial corrections have been made.

Preface

This manual describes how to set up a JP1/Software Distribution system.

It explains the installation and setup procedures, creation of a relational database, and management of your system configuration.

This manual is part of a related set of manuals for *JP1/Software Distribution for Windows*. The manuals in the set, including this manual, are listed below. Read the applicable manual according to your need.

Job Management Partner 1/Software Distribution Description and Planning Guide, for Windows systems

Read this manual first.

This manual provides a brief overview of JP1/Software Distribution's concepts and facilities. It also provides examples of typical ways in which JP1/Software Distribution can be set up and used. The manual also includes instructions on how to install JP1/Software Distribution and explains important points you should consider before installing and using JP1/ Software Distribution.

Job Management Partner 1/Software Distribution Setup Guide, for Windows systems

This manual describes the installation and setup procedures for JP1/Software Distribution, database creation, and management of your system configuration.

Job Management Partner 1/Software Distribution Administrator's Guide Volume 1, for Windows systems

This manual describes in detail the facilities and operation of the managing server, such as for distributing software, acquiring and managing inventory, and collecting files.

This manual also describes operations at a client.

Job Management Partner 1/Software Distribution Administrator's Guide Volume 2, for Windows systems

This manual describes how to link JP1/Software Distribution with other products, and how to take corrective action if a problem has occurred. This manual also describes differences in functionality between the Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista Edition of JP1/Software Distribution Client.

Job Management Partner 1/Software Distribution Automatic Installation Tool Description and Reference, for Windows systems

This manual describes how to create AIT files and recorder files that are required for packaging non-Hitachi software.

Job Management Partner 1/Software Distribution Administrator Kit Description and Operator's Guide

This manual describes Job Management Partner 1/Software Distribution Administrator Kit Description and Operator's Guide, which is used for automatically installing JP1/Software Distribution Client.

Job Management Partner 1/Remote Control Description and Operator's Guide

This manual describes JP1/Remote Control and the remote control facility of JP1/Software Distribution.

Note

In this manual, *JP1* is an abbreviation for *Job Management Partner 1*.

■ Intended readers

This manual is intended for the following readers:

- Administrators who use JP1/Software Distribution to distribute software or to collect and manage asset information
- System administrators who intend to install and set up a JP1/Software Distribution system
- Users who have a basic understanding of Microsoft Windows operations
- Users who have a basic understanding of networks
- Users who have a basic understanding of relational databases
- Users who have a basic understanding of Microsoft SQL Server or Oracle (for those using Microsoft SQL Server or Oracle)

■ Related publications

This manual is part of a related set of manuals. The manuals in the set are listed below (with the manual numbers):

- *Job Management Partner 1/Software Distribution Description and Planning Guide* (3020-3-S79(E)), for Windows systems#
- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1* (3020-3-S81(E)), for Windows systems#
- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 2* (3020-3-S82(E)), for Windows systems#
- *Job Management Partner 1/Software Distribution Automatic Installation Tool Description and Reference* (3020-3-S83(E)), for Windows systems#
- *Job Management Partner 1/Software Distribution Administrator Kit Description and Operator's Guide* (3020-3-S84(E))
- *Job Management Partner 1/Remote Control Description and Operator's Guide* (3020-3-S87(E))
- *Job Management Partner 1/Software Distribution Manager Description and Administrator's Guide* (3000-3-841(E))
- *Job Management Partner 1/Software Distribution Client Description and User's Guide* (3020-3-S85(E)), for UNIX systems
- *Job Management Partner 1/Software Distribution Workstation Description and Operator's Guide* (3000-3-817(E))
- *Job Management Partner 1/Asset Information Manager Description* (3020-3-S76(E))
- *Job Management Partner 1/Asset Information Manager Planning and Setup Guide* (3020-3-S77(E))
- *Job Management Partner 1/Asset Information Manager Administrator's Guide* (3020-3-S78(E))
- *Job Management Partner 1/Client Security Control Description, User's Guide and Operator's Guide* (3020-3-S71(E))
- *Job Management Partner 1/Automatic Job Management System 2 Description* (3020-3-K21(E))
- *Job Management Partner 1/Automatic Job Management System 2 Planning and Administration Guide* (3020-3-K22(E))
- *Job Management Partner 1/Automatic Job Management System 2 Operator's Guide* (3020-3-K24(E))
- *Job Management Partner 1/Automatic Job Management System 2 Command Reference* (3020-3-K25(E))
- *Job Management Partner 1/Automatic Job Management System 2 Linkage Guide* (3020-3-K27(E))
- *Job Management Partner 1/Automatic Job Management System 2 Messages* (3020-3-K28(E))
- *Job Management Partner 1/Automatic Job Management System 3 Introduction* (3020-3-S01(E))
- *Job Management Partner 1/Automatic Job Management System 3 Overview* (3020-3-S02(E))
- *Job Management Partner 1/Automatic Job Management System 3 System Design (Configuration) Guide* (3020-3-S03(E))
- *Job Management Partner 1/Automatic Job Management System 3 System Design (Work Tasks) Guide* (3020-3-S04(E))
- *Job Management Partner 1/Automatic Job Management System 3 Administration Guide* (3020-3-S07(E))
- *Job Management Partner 1/Automatic Job Management System 3 Troubleshooting* (3020-3-S08(E))
- *Job Management Partner 1/Automatic Job Management System 3 Operator's Guide* (3020-3-S09(E))
- *Job Management Partner 1/Automatic Job Management System 3 Command Reference 1* (3020-3-S10(E))
- *Job Management Partner 1/Automatic Job Management System 3 Command Reference 2* (3020-3-S11(E))
- *Job Management Partner 1/Automatic Job Management System 3 Linkage Guide* (3020-3-S12(E))
- *Job Management Partner 1/Automatic Job Management System 3 Messages 1* (3020-3-S13(E))
- *Job Management Partner 1/Automatic Job Management System 3 Messages 2* (3020-3-S14(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Overview* (3021-3-318(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 System Design (Configuration) Guide* (3021-3-319(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 System Design (Work Tasks) Guide* (3021-3-320(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Configuration Guide 1* (3021-3-321(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Configuration Guide 2* (3021-3-322(E))

- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Administration Guide* (3021-3-323(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Troubleshooting* (3021-3-324(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Operator's Guide* (3021-3-325(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Command Reference 1* (3021-3-326(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Command Reference 2* (3021-3-327(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Linkage Guide* (3021-3-328(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Messages 1* (3021-3-329(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Automatic Job Management System 3 Messages 2* (3021-3-330(E))
- *Job Management Partner 1/Integrated Management - Manager Configuration Guide* (3020-3-R77(E))
- *Job Management Partner 1/Integrated Management - Manager Administration Guide* (3020-3-R78(E))
- *Job Management Partner Version 10 Job Management Partner 1/Integrated Management - Manager Configuration Guide* (3021-3-306(E))
- *Job Management Partner Version 10 Job Management Partner 1/Integrated Management - Manager Administration Guide* (3021-3-307(E))
- *Job Management Partner 1/Base User's Guide* (3020-3-R71(E))
- *Job Management Partner 1/Base Messages* (3020-3-R72(E))
- *Job Management Partner 1/Base Function Reference* (3020-3-R73(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Base User's Guide 1* (3021-3-301(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Base Messages* (3021-3-302(E))
- *Job Management Partner 1 Version 10 Job Management Partner 1/Base Function Reference* (3021-3-303(E))
- *HiRDB Version 8 Messages* (3020-6-358(E))

#: In this manual, common parts of manual names, such as *Job Management Partner 1/Software Distribution*, may be omitted.

■ How to use the manual

- Unless noted otherwise, this manual assumes that the version of the JP1/Software Distribution product that is used at the connection destination is JP1/Software Distribution Manager 09-51 for Windows or JP1/Software Distribution Manager 06-72 for UNIX, and that the version of JP1/Software Distribution Client for UNIX that is used is 09-00. If the system at the connection destination is using an earlier version of JP1/Software Distribution, only the facilities supported by that version are available.
- For details about the differences in terminology and facilities for JP1/Software Distribution for UNIX, see *D.2 Differences with JP1/Software Distribution for UNIX* in the manual *Description and Planning Guide*.
- For details about the functional differences with Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista Edition JP1/Software Distribution Client, see *A. Functions Provided in the Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista Edition of JP1/Software Distribution Client* in the manual *Administrator's Guide Volume 2*.

■ About online help

JP1/Software Distribution provides online help.

JP1/Software Distribution online help (for JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system))

The JP1/Software Distribution online help combines the following manuals:

- *Job Management Partner 1/Software Distribution Description and Planning Guide*, for Windows systems
- *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems
- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems
- *Job Management Partner 1/Software Distribution Administrator's Guide Volume 2*, for Windows systems
- *Job Management Partner 1/Software Distribution Automatic Installation Tool Description and Reference*, for Windows systems

JP1/Software Distribution Client online help (for JP1/Software Distribution Client (client))

The JP1/Software Distribution Client Help contains information about clients that is extracted from the above manuals.

This online help enables the user to search the entire set of help documents for a desired item.

To access online help, use the **Help** menu in any window of JP1/Software Distribution or the **Help** button in any dialog box. To use the online help, you must have Microsoft Internet Explorer 5.01 or later installed.

■ Conventions: Abbreviations for product names

This manual uses the following abbreviations for names of products associated with JP1/Software Distribution:

Abbreviation	Full name or meaning
HTTP Gateway	Job Management Partner 1/Software Distribution HTTP Gateway
Internet Gateway	Job Management Partner 1/Software Distribution Internet Gateway
JP1/Client Security Control or JP1/CSC	Job Management Partner 1/Client Security Control - Agent
	Job Management Partner 1/Client Security Control - Manager
JP1/Remote Control	Job Management Partner 1/Remote Control Agent
	Job Management Partner 1/Remote Control Manager
JP1/Software Distribution	Job Management Partner 1/Software Distribution Client
	Job Management Partner 1/Software Distribution Manager
Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista Edition of JP1/Software Distribution Client	The edition of JP1/Software Distribution Client that runs on Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista
Windows CE Edition of JP1/Software Distribution Client	The edition of JP1/Software Distribution Client that runs on Windows CE .NET 4.1

This manual uses the following abbreviations for the names of other products:

Abbreviation	Full name or meaning
AIX	AIX(R)
AMT	Intel Active Management Technology
HIBUN FDE	HIBUN AE - English version FDE
HP NNM	HP Network Node Manager Software version 6 or earlier
	HP Network Node Manager Starter Edition Software version 7.5 or earlier
InstallShield	InstallShield(R)
Itanium 2	Intel Itanium(R) 2 processor

Abbreviation				Full name or meaning
JP1/AJS				Job Management Partner 1/Automatic Job Management System 2
				Job Management Partner 1/Automatic Job Management System 3
JP1/Asset Information Manager				Job Management Partner 1/Asset Information Manager
JP1/Base				Job Management Partner 1/Base
JP1/IM	JP1/IM			Job Management Partner 1/Integrated Management - Manager
	JP1/IM - View			Job Management Partner 1/Integrated Management - View
JP1/PFM/ SSO[#1]	JP1/PFM/SSO[#1]			Job Management Partner 1/Performance Management/ SNMP System Observer
	JP1/SSO			Job Management Partner 1/Server System Observer
Linux				Linux(R)
MBSA				Microsoft(R) Baseline Security Analyzer
Microsoft Internet Explorer				Microsoft(R) Internet Explorer(R)
				Windows(R) Internet Explorer(R)
Microsoft Internet Information Services				Microsoft(R) Internet Information Services 6.0
				Microsoft(R) Internet Information Services 7.0
Microsoft Internet Information Services 5.0				Microsoft(R) Internet Information Services 5.0
Microsoft SQL Server				Microsoft(R) SQL Server(R) 2000
				Microsoft(R) SQL Server(R) 2005
				Microsoft(R) SQL Server(R) 2008
				Microsoft(R) SQL Server(R) 2012
				Microsoft(R) SQL Server(R) 7.0
MS-DOS				Microsoft(R) MS-DOS(R)
Oracle				Oracle8i
				Oracle9i
Pentium				Intel Pentium(R)
UNIX				UNIX(R)
Visual Test				Visual Test 4.0
				Visual Test 6.0
				Visual Test 6.5
Windows	Windows 98			Microsoft(R) Windows(R) 98 Operating System
	Windows Me			Microsoft(R) Windows(R) Millennium Edition Operating System
	Windows NT	Windows 2000	Windows 2000 Advanced Server	Microsoft(R) Windows(R) 2000 Advanced Server Operating System

Abbreviation				Full name or meaning
Windows	Windows NT	Windows 2000	Windows 2000 Datacenter Server	Microsoft(R) Windows(R) 2000 Datacenter Server Operating System
			Windows 2000 Professional	Microsoft(R) Windows(R) 2000 Professional Operating System
			Windows 2000 Server	Microsoft(R) Windows(R) 2000 Server Operating System
		Windows 7		Microsoft(R) Windows(R) 7 Enterprise
				Microsoft(R) Windows(R) 7 Professional
				Microsoft(R) Windows(R) 7 Ultimate
		Windows 8		Microsoft(R) Windows(R) 8
				Microsoft(R) Windows(R) 8 Enterprise
				Microsoft(R) Windows(R) 8 Pro
		Windows NT 4.0	Windows NT Server 4.0	Microsoft(R) Windows NT(R) Server Network Operating System Version 4.0
			Windows NT Workstation 4.0	Microsoft(R) Windows NT(R) Workstation Operating System Version 4.0
		Windows Server 2003#2	Windows Server 2003#2	Microsoft(R) Windows Server(R) 2003 R2, Datacenter Edition
				Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
				Microsoft(R) Windows Server(R) 2003 R2, Standard Edition
				Microsoft(R) Windows Server(R) 2003, Datacenter Edition
				Microsoft(R) Windows Server(R) 2003, Enterprise Edition
				Microsoft(R) Windows Server(R) 2003, Standard Edition
			Windows Server 2003 (x64)	Microsoft(R) Windows Server(R) 2003 R2, Datacenter x64 Edition
				Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
				Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
				Microsoft(R) Windows Server(R) 2003, Datacenter x64 Edition
				Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
				Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
		Windows Server 2008#3	Windows Server 2008#3	Microsoft(R) Windows Server(R) 2008 Datacenter
				Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(R)
				Microsoft(R) Windows Server(R) 2008 Enterprise

Abbreviation				Full name or meaning
Windows	Windows NT	Windows Server 2008#3	Windows Server 2008#3	Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(R)
				Microsoft(R) Windows Server(R) 2008 Standard
				Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(R)
			Windows Server 2008 R2	Microsoft(R) Windows Server(R) 2008 R2 Datacenter
				Microsoft(R) Windows Server(R) 2008 R2 Enterprise
				Microsoft(R) Windows Server(R) 2008 R2 Standard
		Windows Server 2012		Microsoft(R) Windows Server(R) 2012 Datacenter
				Microsoft(R) Windows Server(R) 2012 Standard
		Windows Vista		Microsoft(R) Windows Vista(R) Business
				Microsoft(R) Windows Vista(R) Enterprise
				Microsoft(R) Windows Vista(R) Ultimate
		Windows XP	Windows XP Home Edition	Microsoft(R) Windows(R) XP Home Edition Operating System
			Windows XP Professional	Microsoft(R) Windows(R) XP Professional Operating System
Windows 95				Microsoft(R) Windows(R) 95 Operating System
WSUS	WSUS 2.0			Microsoft(R) Windows Server(R) Update Services 2.0
	WSUS 3.0			Microsoft(R) Windows Server(R) Update Services 3.0
WUA	WUA 2.0			Windows(R) Update Agent 2.0
	WUA 3.0			Windows(R) Update Agent 3.0

#1

In descriptions that are explicitly about JP1/SSO, any references to JP1/PFM/SSO do not apply to JP1/SSO.

#2

In descriptions that are explicitly about Windows Server 2003 (IPF) or Windows Server 2003 (x64), any references to Windows Server 2003 do not apply to Windows Server 2003 (IPF) or Windows Server 2003 (x64).

#3

In descriptions that are explicitly about Windows Server 2008 R2, any references to Windows Server 2008 do not apply to Windows Server 2008 R2.

■ Conventions: Acronyms

This manual also uses the following acronyms:

Acronym	Full name or meaning
AIF	Application Information File
API	Application Programming Interface
ASP	Active Server Pages
BIOS	Basic Input Output System
CD-R	Compact Disc Recordable
CD-ROM	Compact Disc Read Only Memory

Acronym	Full name or meaning
CF	Compact Flash
CGI	Common Gateway Interface
CPU	Central Processing Unit
CSV	Comma Separated Value
DB	Database
DBA	Database Administrator
DBMS	Database Management System
DHCP	Dynamic Host Configuration Protocol
DLL	Dynamic Linking Library
DNS	Domain Name System
DoS	Denial of Service
DVD	Digital Versatile Disk
FD	Floppy Disk
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Security
ICMP	Internet Control Message Protocol
ID	Identifier
IP	Internet Protocol
IPF	Itanium(R) Processor Family
ISAPI	Internet Server Application Programming Interface
LAN	Local Area Network
MAC	Media Access Control
MIB	Management Information Base
MO	Magneto-Optical disk
MS-DOS	Microsoft Disk Operating System
NAT	Network Address Translation
NIC	Network Interface Card
ODBC	Open Database Connectivity
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
PME	Power Management Event
PPP	Point to Point Protocol

Acronym	Full name or meaning
RDBMS	Relational Database Management System
RWU	Remote-Wake-UP
SCSI	Small Computer System Interface
SD	Secure Digital
SID	System Identifier
SMBIOS	System Management Basic Input Output System
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
UNC	Universal Naming Convention
URI	Uniform Resource Identifier
USB	Universal Serial Bus
UTC	Coordinated Universal Time
UUID	Universally Unique Identifier
VPN	Virtual Private Network
WAN	Wide Area Network
WINS	Windows Internet Name Service
WMI	Windows Management Instrumentation
WS	Workstation
WWW	World Wide Web
XML	Extensible Markup Language

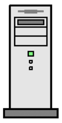
■ Conventions: Diagrams

This manual uses the following conventions in diagrams:

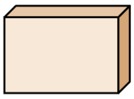
- PC or workstation

- Notebook computer

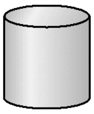
- Server



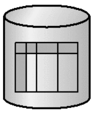
- Program



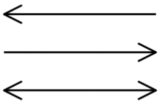
- File



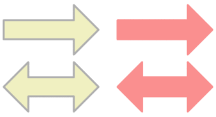
- Relational database



- Flow of control

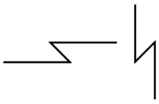


- Flow of data

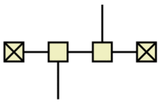


- Input/output operation

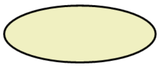
- Communication line



- Network (LAN)

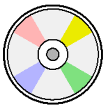


- Network (WAN)

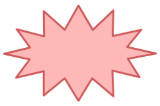


- Modem

- CD-ROM



- Problem



■ Conventions: Fonts and symbols

The following table explains the fonts used in this manual:

Font	Convention
Bold	**Bold** type indicates text on a window, other than the window title. Such text includes menus, menu options, buttons, radio box options, or explanatory labels. For example: • From the **File** menu, choose **Open**. • Click the **Cancel** button. • In the **Enter name** entry box, type your name.
Italics	*Italics* are used to indicate a placeholder for some actual text to be provided by the user or system. For example: • Write the command as follows: `copy` *source-file target-file* • The following message appears: `A file was not found. (file =` *file-name*`)` *Italics* are also used for emphasis. For example: • Do *not* delete the configuration file.
`Code font`	A `code font` indicates text that the user enters without change, or text (such as messages) output by the system. For example: • At the prompt, enter `dir`. • Use the `send` command to send mail. • The following message is displayed:

Font	Convention
`Code font`	`The password is incorrect.`

The following table explains the symbols used in this manual:

Symbol	Convention
|	In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: `A|B|C` means A, or B, or C.
`{ }`	In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: `{A|B|C}` means only one of A, or B, or C.
`[ ]`	In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: `[A]` means that you can specify `A` or nothing. `[B|C]` means that you can specify `B`, or `C`, or nothing.
`...`	In coding, an ellipsis (...) indicates that one or more lines of coding are not shown for purposes of brevity. In syntax explanations, an ellipsis indicates that the immediately preceding item can be repeated as many times as necessary. For example: `A, B, B, ...` means that, after you specify `A, B,` you can specify B as many times as necessary.

■ Conventions: KB, MB, GB, and TB

This manual uses the following conventions:

- 1 KB (kilobyte) is 1,024 bytes.
- 1 MB (megabyte) is $1{,}024^2$ bytes.
- 1 GB (gigabyte) is $1{,}024^3$ bytes.
- 1 TB (terabyte) is $1{,}024^4$ bytes.

■ Conventions: References to other manuals

Within the group of manuals *Description and Planning Guide*, *Administrator's Guide Volume 1*, *Administrator's Guide Volume 2*, and *Automatic Installation Tool Description and Reference*, a reference in one manual to another manual is indicated in the following format:

For details about *AAA*, see *n.n.n BBB* in the manual *CCC*.

AAA

The topic to be referenced.

n.n.n

The chapter or section number to be referenced. This number may be followed by a number or letter in parentheses.

BBB

The title of the chapter or section to be referenced.

CCC

The abbreviated name of the manual to be referenced. Common parts of manual names, such as *Job Management Partner 1/Software Distribution* and *for Windows systems*, are omitted.

■ Conventions: Version numbers

The version numbers of Hitachi program products are usually written as two sets of two digits each, separated by a hyphen. For example:

- Version 1.00 (or 1.0) is written as 01-00.
- Version 2.05 is written as 02-05.
- Version 2.50 (or 2.5) is written as 02-50.
- Version 12.25 is written as 12-25.

The version number might be shown on the spine of a manual as *Ver. 2.00*, but the same version number would be written in the program as *02-00*.

Contents

1 Overview of JP1/Software Distribution Installation

This chapter explains how to install individual programs and components of JP1/Software Distribution.

1.1 Supported OSs and organization of components

JP1/Software Distribution consists of two programs, JP1/Software Distribution Manager and JP1/Software Distribution Client.

Each program consists of several facilities, called *components*. For installation of each JP1/Software Distribution program, the user selects desired components and then installs them.

This section describes the OSs supported for each program and the organization of the components.

1.1.1 Supported OSs

The table below shows the operating systems applicable to each program.

The OSs supported for JP1/Software Distribution Client depend on whether the program is used as a relay system or as a client.

Table 1–1: Operating systems applicable to JP1/Software Distribution

Program	Applicable OSs
JP1/Software Distribution Manager	• Windows 8 (Windows 8, Enterprise, Pro) • Windows Server 2012 (Standard, Datacenter) • Windows 7 (Enterprise, Professional, Ultimate) • Windows Server 2008 R2 (Standard, Enterprise, Datacenter) • Windows Server 2008 (Standard, Enterprise, Datacenter) • Windows Vista • Windows Server 2003 (Standard Edition, Enterprise Edition) • Windows Server 2003 (x64) • Windows XP (Professional) • Windows 2000 (Professional, Server, Advanced Server)
JP1/Software Distribution Client (relay system)	• Windows 8 (Windows 8, Enterprise, Pro) • Windows Server 2012 (Standard, Datacenter) • Windows 7 (Enterprise, Professional, Ultimate) • Windows Server 2008 R2 (Standard, Enterprise, Datacenter) • Windows Server 2008 (Standard, Enterprise, Datacenter) • Windows Vista • Windows Server 2003 (Standard Edition, Enterprise Edition) • Windows Server 2003 (x64) • Windows XP (Professional) • Windows 2000 (Professional, Server, Advanced Server) • Windows NT 4.0
JP1/Software Distribution Client (client)	• Windows 8 (Windows 8, Enterprise, Pro) • Windows Server 2012 (Standard, Datacenter) • Windows 7 (Enterprise, Professional, Ultimate) • Windows Server 2008 R2 (Standard, Enterprise, Datacenter) • Windows Server 2008 (Standard, Enterprise, Datacenter) • Windows Vista • Windows Server 2003 • Windows Server 2003 (IPF) • Windows Server 2003 (x64) • Windows XP • Windows 2000

Program	Applicable OSs
JP1/Software Distribution Client (client)	• Windows NT 4.0 • Windows Me • Windows 98

OS issues pertaining to the installation and operation of JP1/Software Distribution are discussed below.

Notes on supported OSs

- This software does not support Remote Desktop in Windows 8, Windows 7, Windows Vista, Windows XP, or Windows 2000 Server. In these environments, install and operate JP1/Software Distribution on the local console.
- The Server Core option of Windows Server 2008 or Windows Server 2012 is not supported.
- The Fast User Switching feature of Windows XP is not supported.

  If you have used Fast User Switching, restart the PC before installing or operating JP1/Software Distribution.
- Do not disable the startup programs registered by JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system).

  The following programs are registered as the startup programs:
  - AlertTsk.exe
  - dmplogmg.exe
  - dmpsetup.exe
  - smclogin.exe
  - Remote Control Agent
  - Remote Control Chat

Note that JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system) do not support Remote Desktop, Fast User Switching, or Terminal Server on other OSs either. The installation, operation, and functions of JP1/Software Distribution Client (client) is also subject to limitations when used in virtualized environments of these OSes. For details, see *2.13.7 Notes on using a client* in the manual *Description and Planning Guide*.

JP1/Software Distribution operation monitoring has preconditions in addition to those shown here. For details, see *2.5.2 Prerequisites for monitoring operation status* in the *Description and Planning Guide*.

1.1.2 Organization of components

This subsection provides an overview of the functions of the components of each program.

The available components depend on whether JP1/Software Distribution Client is installed as a relay system or as a client.

(1) Components of JP1/Software Distribution Manager

The table below lists and describes the components of JP1/Software Distribution Manager.

Note that some components may not be available depending on the operating system used.

Table 1–2: Components of JP1/Software Distribution Manager

Component	Overview of functions
Server	Functions as a managing server. The Server includes the following subcomponents: • *Server core facility*[#1] Functions as the core of a managing server. If JP1/Software Distribution Manager is installed as a relay system, this core facility also provides client facilities. • *Remote Installation Manager*

Component	Overview of functions
Server	Provides the GUI of a managing server. Normally, the Remote Installation Manager is installed in the same PC as the Server. However, if a relational database is used, the Remote Installation Manager can be installed in a different PC. If you are installing Remote Installation Manager on a separate PC, make sure that the versions of Server and Remote Installation Manager are the same. To link to JP/IM, JP1/IM - View must be installed on the target PC. • *Database Manager*#1 Provides functions for relational database creation and maintenance. • *AMT Linkage* Provides functions for controlling clients using AMT.
Asset Information Manager Subset#1, #2	Provides the GUI for totaling and referencing inventory information as well as GUI functions for managing software operating status. To use this facility, you must create a relational database for Asset Information Manager Subset when you install JP1/Software Distribution Manager. It is normal to install Asset Information Manager Subset on a separate PC from the server in order to distribute the PC workload. When you install Asset Information Manager Subset on a separate PC, you must also install Remote Installation Manager.
WSUS Linkage#1	Manages WSUS from JP1/Software Distribution. Install this program on the WSUS server.
OpenView Linkage#3	Manages JP1/Software Distribution from HP NNM version 7.5 or earlier. Install this facility in the PC in which HP NNM is installed.
OpenView Gateway Server#3	Provides the gateway function for accessing Manager's management information from HP NNM version 7.5 or earlier. Install this facility in the PC in which the Server core facility of the Server component is installed.
Packager#4	Packages software to be remote-installed.
Automatic Installation Tool#4	Functions as the tool for creating scripts for automatic installation of software. The Automatic Installation Tool can be installed on a dedicated PC only.
Remote Control Manager	Functions as the controller for remote control. *Chat* Provides the facility for chatting with Remote Control Manager or Remote Control Agent. To link to JP/IM, JP1/IM - View must be installed on the target PC.
Remote Control Agent#4	Functions as the agent for remote control.

#1

This component cannot be installed on Windows 8, Windows 7 or Windows Vista systems.

#2

To install Asset Information Manager Subset, Microsoft Internet Information Services must have already been installed.

One of the following Web browsers must also be installed.

- Microsoft Internet Explorer 6 SP1 or later
- Windows Internet Explorer 7
- Windows Internet Explorer 8

#3

This component cannot be installed when the OS is Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, Windows Vista, or Windows Server 2003 (x64).

#4

This component can be installed only on a relay manager. Note that Remote Control Agent cannot be used with a PC on which another product providing the remote control facility has already been installed. If you have installed Remote Control Agent on such a PC, you must uninstall it.

(2) Components of JP1/Software Distribution Client (relay system)

The following table lists and describes the components of JP1/Software Distribution Client (relay system):

Table 1–3: Components of JP1/Software Distribution Client (relay system)

Component	Overview of functions
Relay system	Functions as a relay system. Also provides the facilities of a managing server relative to lower clients and the facilities of a client relative to higher systems. A relay system includes the following subcomponents: • *Relay system core facility* This is the relay system installer. • *Remote Installation Manager* This is the GUI for executing distribution management on the relay system. • *AMT Linkage* Provides functions for controlling clients using AMT.
Packager	Packages the software to be remote-installed.
Automatic Installation Tool	Functions as the tool for creating scripts for automatic installation of software. The Automatic Installation Tool can be installed on a dedicated PC only.
Remote Control Agent#	Functions as the agent for remote control. *Chat* Provides the facility for chatting with Remote Control Manager or Remote Control Agent.

#

Remote Control Agent cannot be used with a PC on which another product providing the remote control facility has already been installed. If you have installed Remote Control Agent on such a PC, you must uninstall it.

(3) Components of JP1/Software Distribution Client (client)

The table below lists and describes the components of JP1/Software Distribution Client (client).

Note that some components may not be available depending on the operating system used.

Table 1–4: Components of JP1/Software Distribution Client (client)

Component	Overview of functions
Client	Functions as a client. A client includes the following subcomponents: • *Package Setup Manager* Remote-installs software distributed from a managing server, based on an instruction from the client. • *Additional facilities* Facilities for operating the client on the basis of a user-created program. Normally, these do not need to be installed. • *Distribution facility using Visual Test 6.0*#1 • *Distribution facility using Visual Test 6.5*#1 Facility for using Visual Test 6.0 or Visual Test 6.5 to distribute software from other companies. You can install either the *distribution facility using Visual Test 6.0* or the *distribution facility using Visual Test 6.5*. • *AMT Linkage*#2 Provides functions for controlling clients using AMT.
Packager	Packages software to be remote-installed.
Automatic Installation Tool	Functions as the tool for creating scripts for automatic installation of software. The Automatic Installation Tool can be installed on a dedicated PC only.

Component	Overview of functions
Startup Kit Support Tool#3	Program required in order to create an installation set using the startup kit provided by JP1/Software Distribution Administrator Kit. To install this component, JP1/Software Distribution Administrator Kit must have been installed.
Remote Control Agent#4	Functions as the agent for remote control. *Chat* Provides the facility for chatting with Remote Control Manager or Remote Control Agent.
Help	Provides Help for Client.

#1

This component cannot be installed when the OS is Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, Windows Vista, or Windows Server 2003 (x64).

#2

This component can be installed only when the OS is Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003 (no Service Pack, or Service Pack 1) or Windows XP Professional (Service Pack 1 or later).

#3

This component cannot be installed on Windows 8, Windows Server 2012, Windows Server 2003, Datacenter Edition, Windows Server 2003 (IPF), Windows 2000 Datacenter Server, Windows Me, or Windows 98.

#4

Remote Control Agent cannot be used with a PC on which another product providing the remote control facility has already been installed. If you have installed Remote Control Agent on such a PC, you must uninstall it.

1.2 Installing JP1/Software Distribution

This section describes the JP1/Software Distribution installation procedures for a new installation. It also describes installation by overwriting.

In addition, the section describes how to use the pre-installation facility to install JP1/Software Distribution Client (client) and provides notes on using the remote installation facility of JP1/Software Distribution to upgrade JP1/Software Distribution Client.

For details about how to upgrade JP1/Software Distribution, see *A. How to Upgrade and Migrate JP1/Software Distribution*.

1.2.1 Procedure for a new installation of JP1/Software Distribution

For a new installation, you install higher system programs first in the sequence indicated below.

To install a new JP1/Software Distribution:

1. Install JP1/Software Distribution Manager

   Install JP1/Software Distribution Manager in the managing server PC.

2. Create a relational database.

   You must create it using Database Manager. For details about how to create a relational database, see *7. Setting Up a Relational Database*.

3. Install JP1/Software Distribution Client (relay system).

   Install JP1/Software Distribution Client (relay system) in any relay system PCs.

4. Install JP1/Software Distribution Client (client).

   Install JP1/Software Distribution Client (client) in the client PCs.

   Although installation can be performed from a medium, using an installation set created by JP1/Software Distribution Administrator Kit is more convenient when there are many client computers. For details about how to use an installation set to install JP1/Software Distribution Client (client), see *1.2.4 Using an installation set to install JP1/Software Distribution Client (client)*.

Notes on installation

- After installing JP1/Software Distribution Manager or JP1/Software Distribution Client, you must restart the computer before installing other software.
- You must specify a directory on a local drive for the installation directory or for any directory that needs to be specified during setup. If you specify a directory on a network drive, the system is not guaranteed to run correctly.

  However, you can specify (in UNC format) a directory on a network drive as the operation history storage directory or as the operation history backup directory.
- After installing JP1/Software Distribution Manager on Windows Server 2008 or Windows Server 2012, the following messages might be output to the Windows event (system) log. However, this does not cause any operational problem.
  - The Remote Install Service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.
  - The Hitachi Alert Process Service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.
  - The Hitachi SMC Service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.
- After installing JP1/Software Distribution Client on Windows Vista, Windows 7, Windows 8, Windows Server 2008, or Windows Server 2012, the following messages might be output to the Windows event (system) log. However, this does not cause any operational problem.
  - The Client Install Service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.

- The Hitachi Alert Process Service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.
- The Hitachi SMC Service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.

1.2.2 Installing JP1/Software Distribution by overwriting

You can overwrite the existing JP1/Software Distribution program with the same or a newer version of the program. By installing the same version, you can change the installation settings or restore the original settings. To change or correct installation settings by overwriting the same version, use the maintenance wizard; for details, see *1.3 Changing installation settings*.

The programs that can be overwritten depend on the installation target system. The following table shows the programs that can be overwritten by target system:

Table 1–5: Programs that can be overwritten depending on the target system

Program to be installed		Installation target system			
		Central manager	Relay manager	Relay system	Client
JP1/Software Distribution Manager	Central manager	Y	N	N	Y#
	Relay manager	Y	Y	N	N
JP1/Software Distribution Client	Relay system	N	N	Y	Y
	Client	Y#	N	N	Y

Legend: Y: Can be installed; N: Cannot be installed.

#
The program is not overwritten. Two programs are installed separately.

The notes below apply to overwrite installation. For notes about upgrading, see *A.1 Upgrading JP1/Software Distribution*.

- When a program is overwritten, the previous settings before upgrading are inherited. During installation, each dialog box displays the existing settings; you can change settings as necessary.
- To overwrite Asset Information Manager Subset, stop the services in the following order:
  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (when JP1/CSC is linked)

  If you use Asset Information Manager Subset after you have performed overwrite installation, start the services in the reverse order from which they were stopped.
- If you overwrite Asset Information Manager Subset, **Startup type** for Asset Information Synchronous Service is set to **Manual**. If necessary, change it to **Automatic**.
- For details about how to perform overwrite installation of JP1/Software Distribution Manager, see *11.1.5 How to reconfigure a cluster system environment*.
- After reinstalling JP1/Software Distribution Manager or JP1/Software Distribution Client, you must restart the computer before installing other software.
- After installing JP1/Software Distribution Manager on Windows Server 2008 or Windows Server 2012, the following messages might be output to the Windows event (system) log. However, this does not cause any operational problem.
  - The Remote Install Service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.
  - The Hitachi Alert Process Service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.

  - The Hitachi SMC Service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.
- After installing JP1/Software Distribution Client on Windows Vista, Windows 7, Windows 8, Windows Server 2008, or Windows Server 2012, the following messages might be output to the Windows event (system) log. However, this does not cause any operational problem.
  - The Client Install Service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.
  - The Hitachi Alert Process Service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.
  - The Hitachi SMC Service is marked as an interactive service. However, the system is configured to not allow interactive services. This service may not function properly.

! Important note

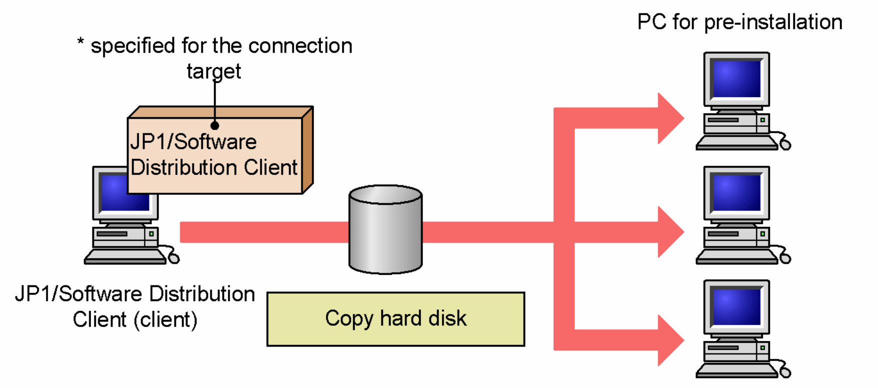
You cannot overwrite your existing version of JP1/Software Distribution with an earlier version. Once you install JP1/Software Distribution 07-00 or later, do not attempt to overwrite it with JP1/Software Distribution 06-71 or earlier. If you do, you will not be able to uninstall it successfully.

1.2.3 Using the pre-installation facility to install JP1/Software Distribution Client (client)

The pre-installation facility of JP1/Software Distribution Client (client) can be used to install JP1/Software Distribution Client (client) without creating client-specific information or temporary files. This is a convenient facility for distributing a pre-installed PC to clients or for testing a PC before distributing it. Installing JP1/Software Distribution Client (client) in a single PC and simply copying its hard disk is much more efficient than installing it in all the PCs one computer at a time.

The following figure provides an overview of installing JP1/Software Distribution Client (client) using the pre-installation facility:

Figure 1–1: Installing JP1/Software Distribution Client (client) using the pre-installation facility


* specified for the connection target
JP1/Software Distribution Client
JP1/Software Distribution Client (client)
Copy hard disk
PC for pre-installation

To create a copy source PC environment for distributing JP1/Software Distribution Client (client) using the pre-installation facility:

1. Install JP1/Software Distribution Client (client).

   Install JP1/Software Distribution Client (client) according to the procedure described in *3.1 How to install JP1/ Software Distribution Client*.
2. Specify * in **Specify Connection Destination** as the host name or IP address of the connection destination.

   When * is specified as the connection destination, no client-specific information is created in the installed directories.
3. Complete the installation of JP1/Software Distribution Client (client).

   A PC in which JP1/Software Distribution Client (client) is installed using the pre-installation facility has been created. You can now copy its hard disk to other PCs.

To test the operation of such a PC before copying its hard disk to other PCs:

1. Install JP1/Software Distribution Client.
   Install JP1/Software Distribution Client (client) according to the procedure described in *3.1 How to install JP1/Software Distribution Client*. For this step, specify in **Specify Connection Destination** the host name or IP address of the connection destination to be used in the test.
2. Run an operation verification test.
   Run an operation verification test in the test environment.
3. From the **Start** menu, choose **Setup** and start client setup.
4. On the **Connection Destination** page, change the connection destination from the host name or IP address in the test environment to *, and then click the **OK** button.
   Changing the connection destination to * deletes the client-specific information used for the test and the temporary files related to the connection destination, and initializes the settings.
5. Complete the installation of JP1/Software Distribution Client (client).
   A PC in which JP1/Software Distribution Client (client) is installed using the pre-installation facility has been created. You can now copy its hard disk to other PCs.

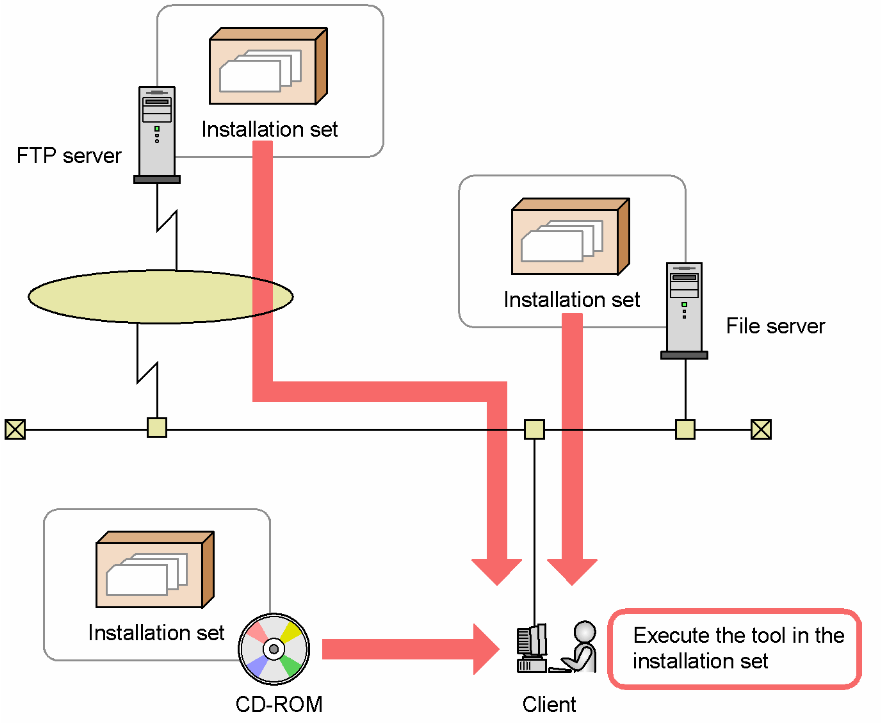
1.2.4 Using an installation set to install JP1/Software Distribution Client (client)

This subsection provides an overview of using an installation set to install JP1/Software Distribution Client (client). For details about creating an installation set and using the installation set for installation, see the *Job Management Partner 1/Software Distribution Administrator Kit Description and Operator's Guide*.

If you install Startup Kit Support Tool of JP1/Software Distribution Client (client) and JP1/ Software Distribution Administrator Kit on the same PC, you can then create an *installation set* that can be used to execute automatic installation of JP1/Software Distribution Client. An installation set contains programs of JP1/Software Distribution Client (client) and their setup information. Client users can then use the installation set stored on a CD-ROM, in a file server, or at an FTP server to execute automatic installation of JP1/ Software Distribution Client (client).

The following figure provides an overview of automatic installation using an installation set:

Figure 1–2: Automatic installation using an installation set



The following capabilities become available when you use an installation set to execute automatic installation of JP1/Software Distribution Client (client):

- Providing installation sets that are appropriate to different network environments

  Installation sets containing the same setup information for different network environments can be stored on the CD-ROM, in the file server, or at the FTP server, enabling automatic installation of JP1/Software Distribution Client (client) in any network environment. The JP1/Software Distribution products need not be actually installed in the file server or at the FTP server.
- Specifying the connection destination as appropriate to the IP address of the client

  An installation set can provide the appropriate connection destination for each range of client IP addresses. During automatic installation, the connection destination corresponding to the IP address of the particular client is selected automatically. Therefore, even when there are multiple connection destinations for the clients, automatic installation can be achieved at multiple clients using only one installation set.
- Displaying the Register in ID Group and Update User Information dialog boxes during installation

  You can include information other than just setup information in an installation set. For example, if you include in the installation set the ID groups in which clients can register and the user inventory items to be acquired, you can register each client in appropriate ID groups during installation and display immediately after installation a dialog box that prompts for entry of user information.
- Using the automatic installation facility to install a relay system

  When a new relay system is installed, one method is to first install Client on the applicable PCs. By using an installation set to install Client and then remote-installing JP1/Software Distribution Client (relay system) in these clients, you can easily install a relay system at a different location.

1.2.5 Notes on using the remote installation facility to distribute JP1/Software Distribution

When you need to upgrade a JP1/Software Distribution Client relay system or client, you can use JP1/Software Distribution to remote-install the upgraded version. The method of remote installation is the same as for other Hitachi program products.

For the JP1/Software Distribution Client that has been installed remotely, the client settings existing prior to the installation are inherited.

The following points should be noted about using the remote installation facility to distribute JP1/Software Distribution Client:

(1) Notes about programs and components

- You can remotely install the components listed below for each program. When you install JP1/Software Distribution Client (client), you can select the components to be installed remotely.

  When installing JP1/Software Distribution Client (relay system)

  - Relay system
  - Remote Control Manager
  - Remote Control Agent
  - Packager

  When installing JP1/Software Distribution Client (client)

  - Client
  - Remote Control Agent
  - Packager
  - Online Help
- The following describes how to perform remote installation of AMT Linkage on a relay system with version 08-00 or earlier.

  On the relay system, Microsoft .NET Framework 1.1, 2.0, 3.0, or 3.5 must have already been installed.

  1. On the higher system, upgrade the JP1/Software Distribution Manager version to 08-10 or later.

During upgrading, install AMT Linkage.

2. Package *JP1/SoftwareDistribution-Manager-installation-directory*`\DMAMT`.

   During packaging, set the installation-target directory as follows:

   Drive: None

   Directory: `%NETMDMP%`

3. Distribute the package to the relay system.
4. Perform remote installation of the relay system with version 08-10 or later.

   AMT Linkage is installed.

- JP1/Software Distribution Client (client) cannot be remote-installed on a PC on which Startup Kit Support Tool or Client Installation by Web (a component of JP1 Version 7i or earlier) has been installed. You can remotely install JP1/Software Distribution Client (client) on a PC where the Automatic Installation Tool has been installed; however, the Automatic Installation Tool will not be overwritten. Make sure that you manually install Startup Kit Support Tool and Automatic Installation Tool.
- JP1/Software Distribution Client (relay system) cannot be remote-installed on a PC on which Startup Kit Support Tool or Client Installation by Web (a component of JP1 Version 7i or earlier) has been installed.

  You can remotely install JP1/Software Distribution Client (relay system) on a PC that has the Automatic Installation Tool installed on it. However, the Automatic Installation Tool will not be overwritten. You must install the Automatic Installation Tool manually.

(2) Notes about remote installation

- If a Job Management Partner 1/Software Distribution Client dialog box is displayed when a Job Management Partner 1/Software Distribution Client (relay system) installation is performed, the installation will fail. Close any Job Management Partner 1/Software Distribution Client dialog box before starting an installation. Extra care must be taken due to the fact that the following dialog boxes are sometimes automatically displayed:
  - Message notification dialog boxes
  - Dialog boxes displayed when a job error occurs
  - Deletion confirmation dialog boxes for shortcuts that fail to start from Software Distribution Client Startup
  - Update User Information dialog box: At system boot
  - Update User Information dialog box: At periodic execution
  - Hold or Cancel Software Distribution Job dialog box
  - Shutdown or Restart confirmation dialog box
- The disk at the remote installation target requires about three times as much space as for the JP1/Software Distribution Client that is to be installed remotely.
- Do not remote-install JP1/Software Distribution together with other packages.
- To distribute JP1/Software Distribution Client by remote installation, you must use the Packager whose version matches the version of the JP1/Software Distribution Client.
- When you create the packaging or remote installation job, you cannot specify in **Start external program** on the **External Program** page an external program that starts immediately after installation or when an installation error occurs.
- When you create the packaging or remote installation job, if **Reinstallation** is specified in **Hitachi program product installation** on the **Installation Method** page, the same components will be installed again.

  If **New installation** is selected, the following components will be installed in addition to a component that has already been installed:

  When JP1/Software Distribution Client (relay system or client) was installed

  - Remote Control Agent
- Restarting the computer or manipulating the JP1/Software Distribution Client menu during installation processing results in an installation error.

  Clicking the **Cancel** button in the dialog box that shows the installation status cancels the installation processing.
- If dialog boxes are set not to be displayed during installation, no message is displayed even when the computer needs to be restarted after completion of JP1/Software Distribution Client installation.

- Do not execute any other jobs on the relay system or client where remote installation of JP1/Software Distribution Client is underway. Before you execute another job, make sure that remote installation has been completed.
- To complete remote installation of JP1/Software Distribution Client, manually restart the computer after remote installation has finished and before you install any other products.
- When remote installation of JP1/Software Distribution Client version 08-10 or later is performed on a client whose version is 08-00 or earlier, the dialog box display settings during the installation depend on the settings used by the target client.

  When remote installation of JP1/Software Distribution Client version 08-00 or earlier is performed, the dialog box display settings are ignored during the installation. All dialog boxes are displayed during the installation.
- The installation set created by JP1/Software Distribution Administrator Kit cannot be used from the remote installation facility. The remote installation facility can be used to distribute the installation set to a client machine. The distributed installation set must be manually executed from the client machine.
- You can check the execution results of remote installation as follows:

  Installation of JP1/Software Distribution Client (relay system):

  > Use the Job Status window of the managing server to check the results. In the Detailed Information dialog box (displayed from the Job Status window), **Maintenance code** is the return code for the execution results.

  Installation of JP1/Software Distribution Client (client):

  > A message is displayed at the client indicating that JP1/Software Distribution Client (client) is being installed. When installation is complete, a return code indicating completion is displayed in the message box.
  >
  > If dialog boxes are set not to be displayed during installation, a message box reporting the termination is not displayed. To determine whether or not the installation has been successful, check the job execution result on the higher system.

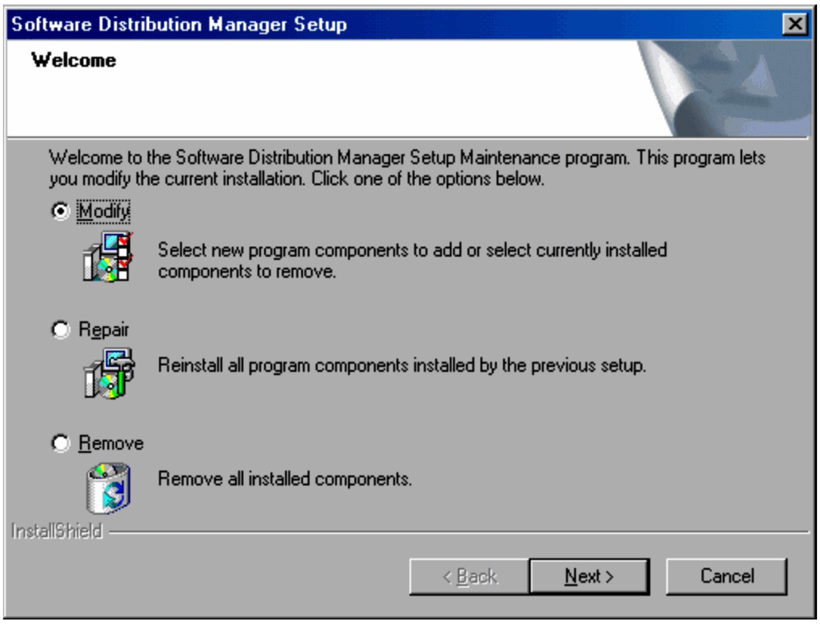
  For details about the return codes, see *6.2.3 List of maintenance codes* in the manual *Administrator's Guide Volume 2*.

1.3 Changing installation settings

You use the *maintenance wizard* to add a component that was once installed or to delete an installed component. The maintenance wizard enables you to reinstall a component using its previous setup information or to uninstall existing products.

To start the maintenance wizard, start the installer from the CD-ROM containing the product that has already been installed. If you attempt to use the same version of installer to overwrite the product, the maintenance wizard starts and displays the Welcome dialog box:

Figure 1–3: Welcome dialog box



Software Distribution Manager Setup

Welcome

Welcome to the Software Distribution Manager Setup Maintenance program. This program lets you modify the current installation. Click one of the options below.

● Modify

Select new program components to add or select currently installed components to remove.

○ Repair

Reinstall all program components installed by the previous setup.

○ Remove

Remove all installed components.

The contents of the Welcome dialog box are the same for JP1/Software Distribution Manager and JP1/Software Distribution Client. Choose **Modify**, **Repair**, or **Remove**.

Modify

Choose this option to add new components or remove installed components.

Choosing **Modify** and then clicking the **Next** button displays the Select Manager Type dialog box for JP1/Software Distribution Manager or the Select Components dialog box for JP1/Software Distribution Client.

Modify the manager type or installation components in the displayed dialog box and proceed with installation in the same manner as in the case of new installation. When installation is complete, the Maintenance Complete dialog box is displayed.

Repair

Choose this option to re-install all components that were installed previously.

Choosing **Repair** and then clicking the **Next** button displays a dialog box indicating the processing status. When re-installation is complete, the Maintenance Complete dialog box is displayed.

Remove

Choose this option to remove all components and uninstall the product.

Choosing **Remove** and then clicking the **Next** button starts uninstallation. For details about the confirmation dialog box that is displayed during uninstallation, see *1.4 Uninstalling JP1/Software Distribution*. When uninstallation is complete, the Maintenance Complete dialog box is displayed.

1.4 Uninstalling JP1/Software Distribution

This section describes how to *uninstall* JP1/Software Distribution.

1.4.1 Uninstallation procedures

There are two ways to uninstall JP1/Software Distribution:

- By choosing **Add/Remove Programs** or **Programs and Features** from **Control Panel**
- By using the **Remove** option of the maintenance wizard

With both methods, the following verification messages are displayed during uninstallation:

- `Do you want to completely remove the selected application and all of its components?`

  This message is always displayed. Clicking the **OK** button will start uninstallation.
- `Delete the symbol registered in OpenView NNM.`

  This message is displayed when OpenView Gateway Server is deleted. Select **Yes** or **No**.
- `Delete from network automatically adding the client to the managing servers system configuration.`

  This message is displayed when the Server core facility of a relay manager, Relay System, or Client is deleted. Select **Yes** or **No**.

  If you selected **No**, or if you selected **Yes** but message transmission to the higher system has failed, delete the uninstalled host at the higher managing server. For details about how to delete hosts at the managing server, see *9.1 Maintaining the system configuration information manually*.

When uninstallation is complete, the Maintenance Completed dialog box is displayed.

1.4.2 Precautions about uninstallation

You should note the following points about uninstalling JP1/Software Distribution.

- To uninstall JP1/Software Distribution in a Windows NT environment, you must log on using Administrator permissions or the user name of the administrator who installed the program.
- First terminate the JP1/Software Distribution program and then execute uninstallation. If uninstallation is executed while a JP1/Software Distribution program that was started from the JP1/Software Distribution icon group is still running, the program may be terminated abnormally.
- If Asset Information Manager Subset has been installed, you must stop the IIS Admin Services before uninstalling JP1/Software Distribution.
- If the **Create Software Distribution Client Startup folder** check box was selected during setup, then when multiple users log on to a single PC using their individual IDs in a Windows NT environment in which JP1/Software Distribution Client is installed, a **Software Distribution Client Startup** folder is created for each user. If JP1/Software Distribution Client is uninstalled under such a circumstance, only the folder of the user who executes the uninstallation is deleted. The other users must delete their own **Software Distribution Client Startup** folders.
- In the case of a PC on which JP1/Software Distribution Client and JP1/Software Distribution Manager are both installed or on which JP1/Software Distribution Client relay system and client are both installed, only the environment of the program for which uninstallation was executed is uninstalled. The other program environment is not deleted.
- JP1/Software Distribution Encryption Option does not have a dedicated uninstaller. It is uninstalled when its prerequisite program (such as JP1/Software Distribution Manager (relay manager), or JP1/Software Distribution Client) is uninstalled.
- When Asset Information Manager Subset is used, uninstalling JP1/Software Distribution may not delete the installation folders and files and Microsoft Internet Information Service's virtual directory. If you re-install JP1/Software Distribution, make sure that these remaining folders are deleted.

- During uninstallation, if you choose **Yes** for the message `Information about this host will be deleted from the system configuration information managed by the higher host. OK?`, the host ID management file for that host will be deleted, and thus host IDs become invalid.
- If Asset Information Manager Subset uses Microsoft SQL Server or Oracle as the database, uninstalling JP1/Software Distribution does not delete the database tables. You must use the DBMS facility to delete these tables. If you use Embedded RDB, uninstalling JP1/Software Distribution also deletes the database tables. If you may need these tables after uninstallation, be sure to make a backup before executing uninstallation.
- If you uninstall JP1/Software Distribution immediately after installing it in a relay system or client, the **Error has occurred in host ID management information** dialog box may be displayed. This is normal.
- If you are using the software operation monitoring function when you uninstall the product, the system may be unable to delete the software operation monitoring module located in the JP1/Software Distribution installation target directory `\BIN`. If this happens, restart the PC.
- If the error message `Client Install Service could not be deleted` is displayed, the JP1/Software Distribution Client service remains running. If this happens, first confirm that it is OK to stop the JP1/Software Distribution Client service. Then, choose **Control Panel**, **Administrative Tools**, and **Services**, and manually stop the service.

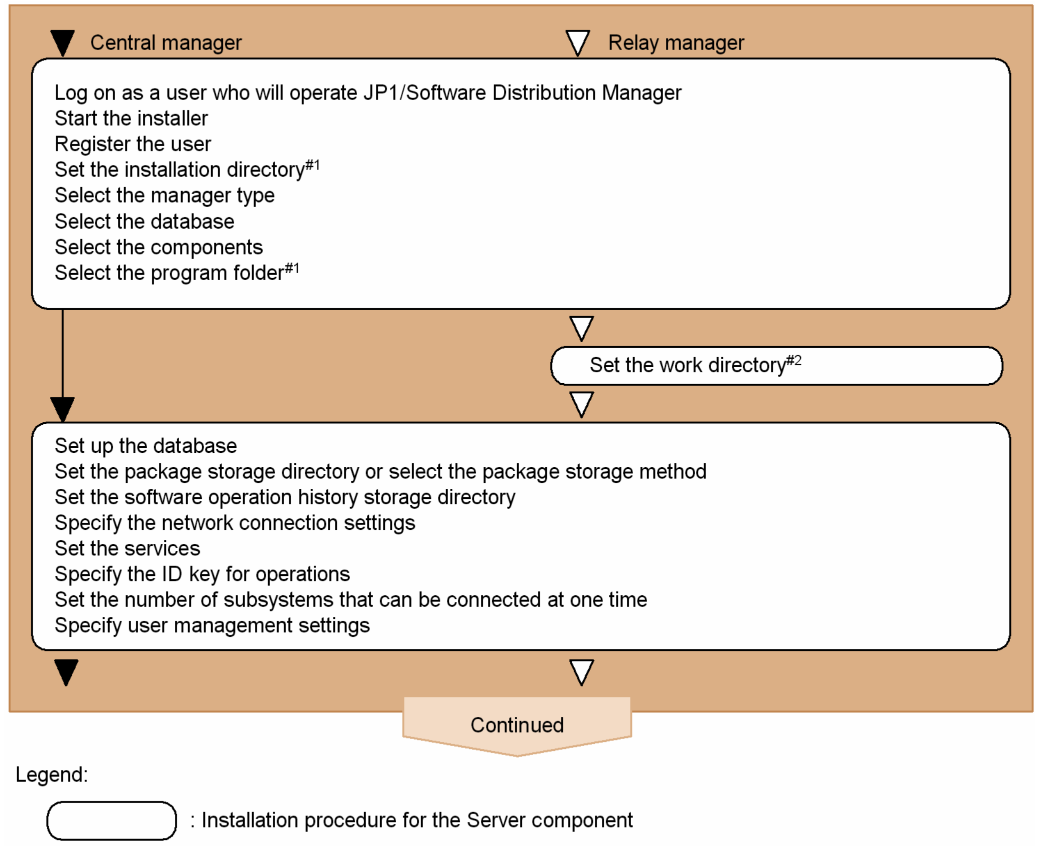
2 Installing JP1/Software Distribution Manager

This chapter explains how to install JP1/Software Distribution Manager and its components.

2.1 How to install JP1/Software Distribution Manager

Figures 2-1 and 2-2 show the procedure for installing JP1/Software Distribution Manager as the central manager or a relay manager.

Figure 2–1: JP1/Software Distribution Manager installation procedure (1/2)



Log on as a user who will operate JP1/Software Distribution Manager
Start the installer
Register the user
Set the installation directory#1
Select the manager type
Select the database
Select the components
Select the program folder#1

Set the work directory#2

Set up the database
Set the package storage directory or select the package storage method
Set the software operation history storage directory
Specify the network connection settings
Set the services
Specify the ID key for operations
Set the number of subsystems that can be connected at one time
Specify user management settings

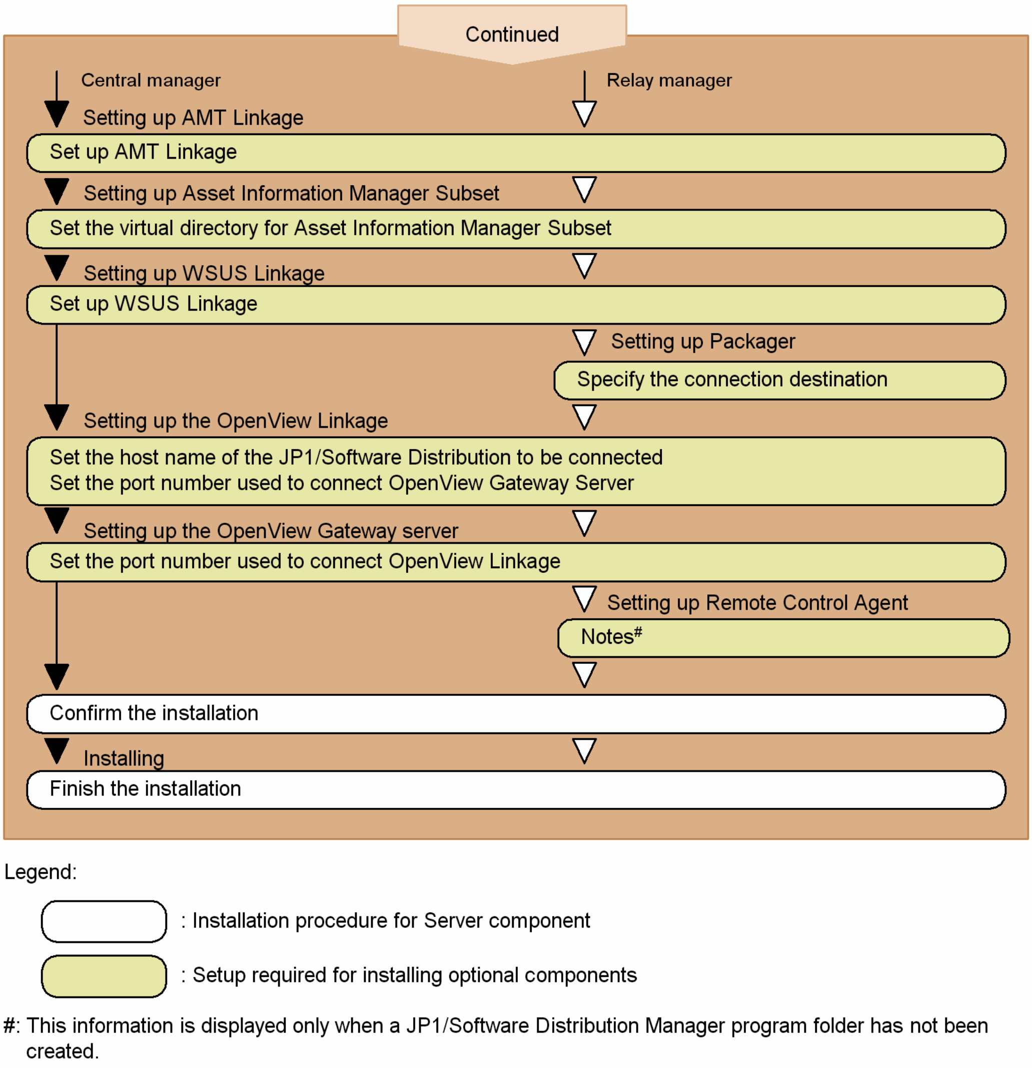
Legend:

▭ : Installation procedure for the Server component

#1 This information is displayed only when a JP1/Software Distribution Manager program folder has not been created.

#2 This information is displayed only when Server core facility of Server is selected.

Figure 2–2: JP1/Software Distribution Manager installation procedure (2/2)


Continued
Central manager
Relay manager
Setting up AMT Linkage
Set up AMT Linkage
Setting up Asset Information Manager Subset
Set the virtual directory for Asset Information Manager Subset
Setting up WSUS Linkage
Set up WSUS Linkage
Setting up Packager
Specify the connection destination
Setting up the OpenView Linkage
Set the host name of the JP1/Software Distribution to be connected
Set the port number used to connect OpenView Gateway Server
Setting up the OpenView Gateway server
Set the port number used to connect OpenView Linkage
Setting up Remote Control Agent
Notes#
Confirm the installation
Installing
Finish the installation
Legend:
: Installation procedure for Server component
: Setup required for installing optional components

#: This information is displayed only when a JP1/Software Distribution Manager program folder has not been created.

If you select any of **Asset Information Manager Subset**, **WSUS Linkage**, **Packager**, **OpenView Linkage**, **OpenView Gateway Server**, or **Remote Control Agent** as installation components in addition to **Server**, you must also set up the selected components during installation.

You can install Remote Control Manager of the Server on a separate machine from the Server. In such a case, Server core facility is not installed. For details about how to install Remote Installation Manager, see *2.2 Installing Remote Installation Manager*.

You can install Asset Information Manager Subset on a separate machine from Server core facility, in which case Remote Installation Manager is required.

For notes about installing Asset Information Manager Subset and how to install Asset Information Manager Subset on a separate machine from JP1/Software Distribution, see *2.3 Installing Asset Information Manager Subset*.

You install WSUS Linkage on the WSUS server and OpenView Linkage on an HP Network Node Manager. For details about how to install only these components from the JP1/Software Distribution Manager installation medium, see *2.4 Installing JP1/Software Distribution on a WSUS server* and *2.5 Installing JP1/Software Distribution Manager in HP Network Node Manager*.

OpenView Gateway Server must be installed on the same PC as the Server core facility of the Server.

2.1.1 Logging on

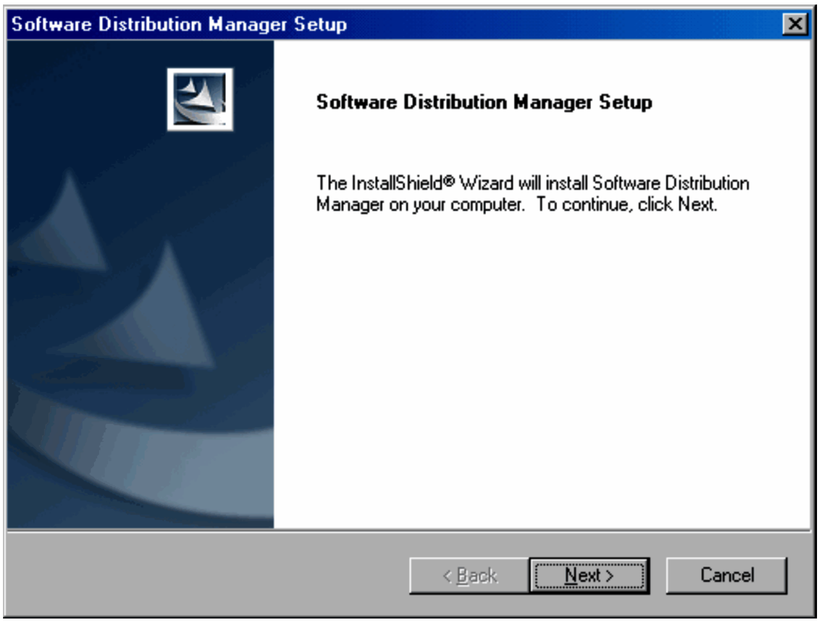
Log on using a user name with Administrator permissions. This is the user who will operate JP1/Software Distribution Manager.

2.1.2 Starting the installer

Insert the provided medium into the CD-ROM drive and install the program following the instructions of the installer.

When the installer starts, the JP1/Software Distribution Manager installation program starts, and the Software Distribution Manager Setup dialog box is displayed.

Figure 2–3: Software Distribution Manager Setup dialog box



Software Distribution Manager Setup

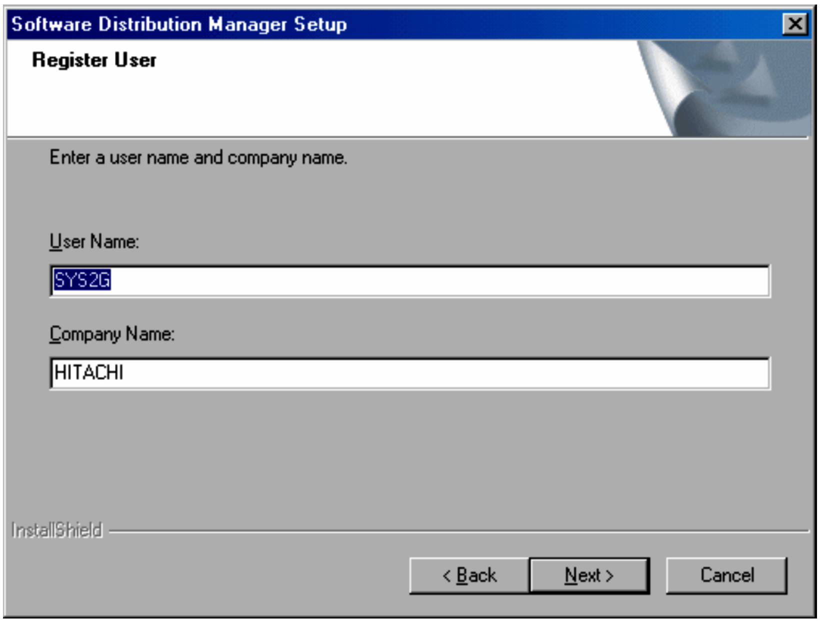
The InstallShield® Wizard will install Software Distribution Manager on your computer. To continue, click Next.

Click the **Next** button to continue with installation. To stop installation, click the **Cancel** button. In the subsequent dialog boxes, clicking the **Back** button displays the immediately preceding dialog box.

2.1.3 Registering the user

Register the user name and company name in the Register User dialog box.

Figure 2–4: Register User dialog box



Software Distribution Manager Setup

Register User

Enter a user name and company name.

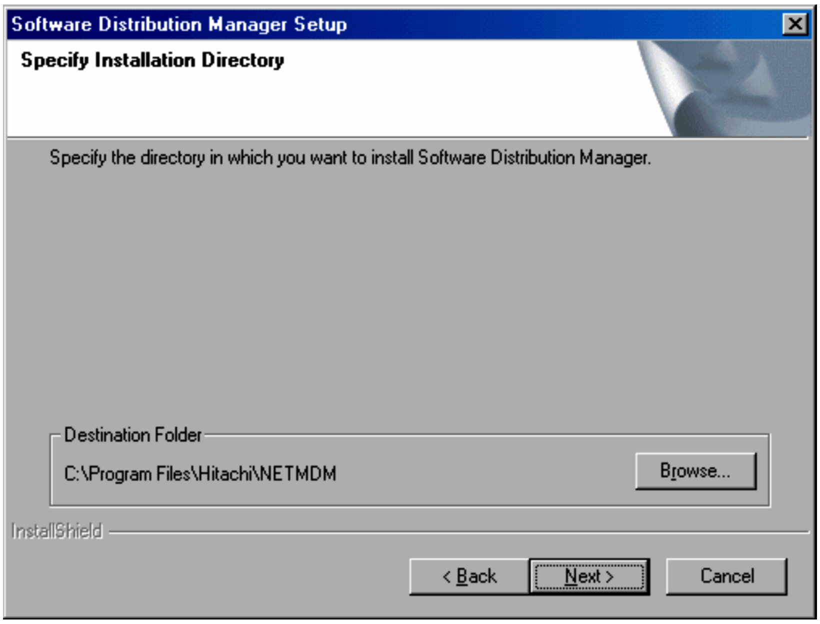
User Name: SYS2G

Company Name: HITACHI

2.1.4 Specifying the installation directory

Specify the directory in which JP1/Software Distribution Manager is to be installed. This dialog box is displayed only during a new installation. In an upgrade, JP1/Software Distribution Manager is installed automatically in the existing installation directory.

Figure 2–5: Specify Installation Directory dialog box



Software Distribution Manager Setup

Specify Installation Directory

Specify the directory in which you want to install Software Distribution Manager.

Destination Folder: C:\Program Files\Hitachi\NETMDM

The default installation target is `C:\Program Files\Hitachi\NETMDM` (`C:` indicates the drive on which the OS has been installed). If JP1/Software Distribution Manager is to be installed on a computer that is running a 64-bit version of Windows Server 2012, Windows Server 2008 or Windows Server 2003 (x64), the default installation directory is `C:\Program Files (x86)\Hitachi\NETMDM`. In this case, replace references in the manual to *Program Files* with *Program Files (x86)*.

To change the default installation directory, click the **Browse** button to select the desired directory. You should note the following about changing the installation directory:

- Specify the installation target directory, using alphanumeric characters, spaces, and the following special characters:
  `_ \ . : ( )`
- Check that the installation directory does not end with `\`. For example, do not specify `C:\NETMDM\`.
- Do not specify a drive name only as the installation directory. For example, do not specify `C:`.
- When installing OpenView Linkage on a PC whose `NtfsDisable8dot3NameCreation` is set to `1` in the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem`, do not include any spaces in the installation target directory. If a space is included, OpenView Linkage cannot be used.

If you are using Embedded RDB for the database, make sure that the disk where you are installing JP1/Software Distribution Manager has at least the following amount of space:

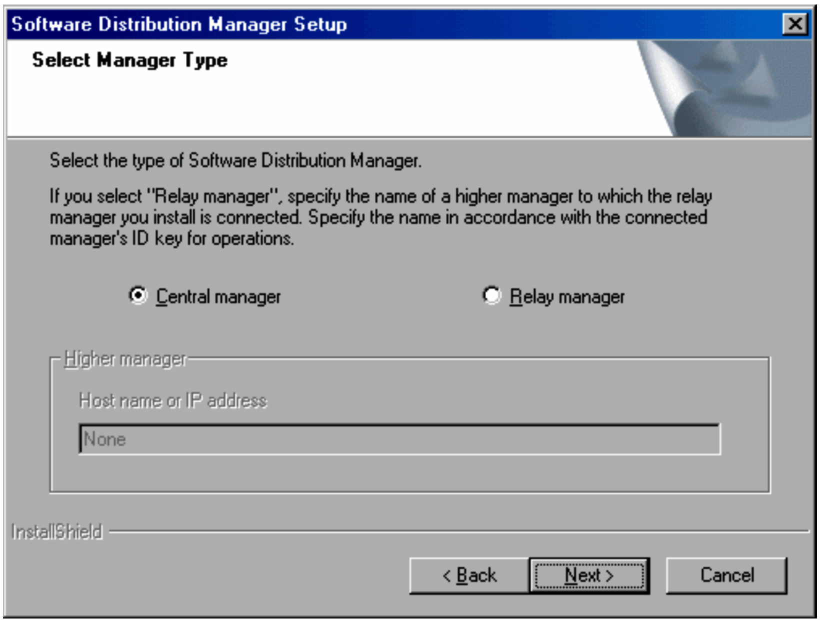
disk space required by database + 10 (GB)

Insufficient disk space may result in abnormal termination of Embedded RDB. See *5.3.3(1) Disk space required for JP1/Software Distribution Manager* in the manual *Description and Planning Guide* for information on disk space requirements for databases.

2.1.5 Selecting the manager type

Select a JP1/Software Distribution Manager type. To use JP1/Software Distribution Manager as the central manager, select **Central manager**; to use it as a relay manager, select **Relay manager**. When **Relay manager** is selected, specify the host name or IP address of the higher manager to which the relay manager is to be connected, in accordance with the ID key for operations of the connection destination. The default is **Central manager**.

Figure 2–6: Select Manager Type dialog box



Software Distribution Manager Setup

Select Manager Type

Select the type of Software Distribution Manager.

If you select "Relay manager", specify the name of a higher manager to which the relay manager you install is connected. Specify the name in accordance with the connected manager's ID key for operations.

● Central manager ○ Relay manager

Higher manager

Host name or IP address: None

In the case of an upgrade, you should note the following:

- If JP1/Software Distribution Manager was installed as a **Relay manager**, you cannot select **Central manager**.
- If JP1/Software Distribution Client was installed, you cannot select **Relay manager**.

2.1.6 Selecting the database

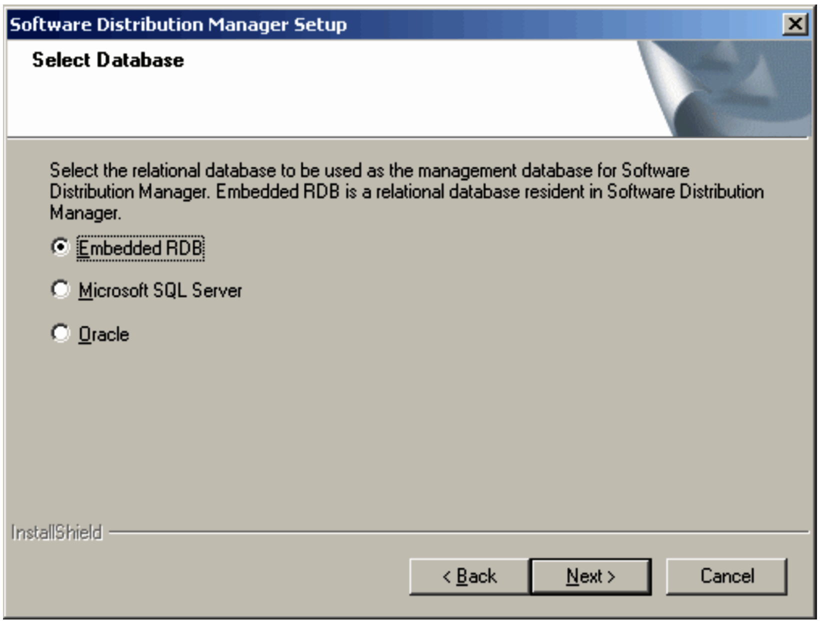
Select the database to be used as JP1/Software Distribution Manager's management database. This dialog box is displayed the first time any of Server, Asset Information Manager Subset, or OpenView Linkage is installed.

The following are the supported databases:

- Embedded RDB
- Microsoft SQL Server
- Oracle[#]

#: Not displayed when the OS is Windows Server 2012 or Windows Server 2008.

Figure 2–7: Select Database dialog box



Software Distribution Manager Setup

Select Database

Select the relational database to be used as the management database for Software Distribution Manager. Embedded RDB is a relational database resident in Software Distribution Manager.

● Embedded RDB

○ Microsoft SQL Server

○ Oracle

The default is **Embedded RDB**, which is the database that is included in JP1/Software Distribution Manager.

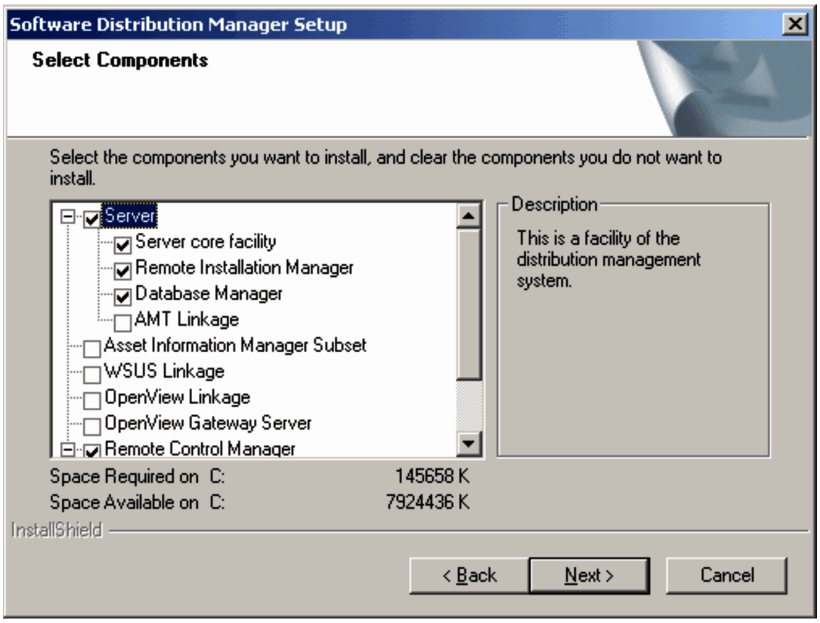
If you select **Embedded RDB** as the database and install Asset Information Manager Subset, the `tmp` folder is created immediately under the Asset Information Manager Subset installation drive. Do not delete this `tmp` folder because it is needed in order to use Embedded RDB.

If **Embedded RDB** cannot be selected because JP1/Software Distribution Manager for JP1 Version 7i or earlier using the basic database is to be overwritten, use the procedure described in *A.2 Changing the database type* to install JP1/Software Distribution Manager.

2.1.7 Selecting the components

Select the components or subcomponents you wish to install. In the case of an upgrade, you can add components or subcomponents, but you cannot delete any installed components or subcomponents.

Figure 2–8: Select Components dialog box



Software Distribution Manager Setup

Select Components

Select the components you want to install, and clear the components you do not want to install.

- ☑ Server
  - ☑ Server core facility
  - ☑ Remote Installation Manager
  - ☑ Database Manager
  - □ AMT Linkage
- □ Asset Information Manager Subset
- □ WSUS Linkage
- □ OpenView Linkage
- □ OpenView Gateway Server
- ☑ Remote Control Manager

Description

This is a facility of the distribution management system.

Space Required on C: 145658 K

Space Available on C: 7924436 K

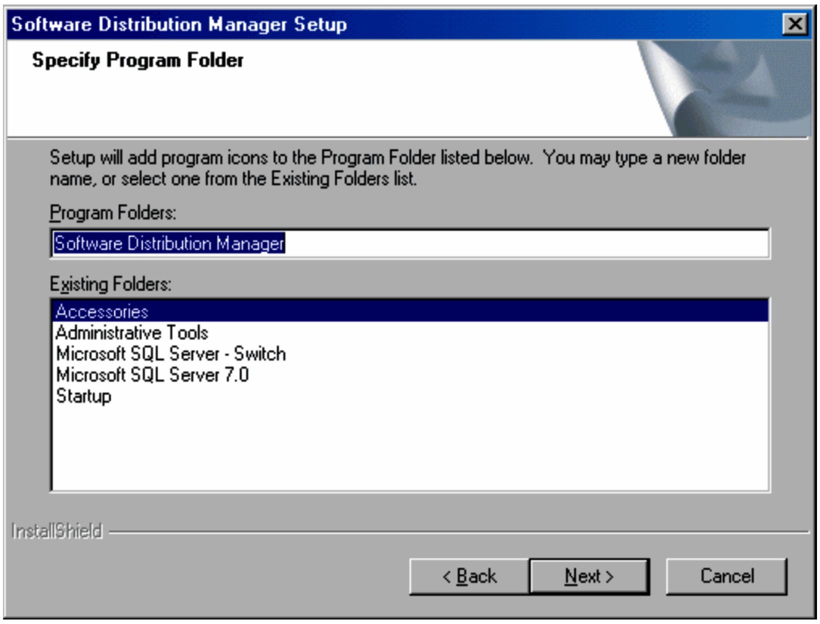
The components that are displayed depends on the selected server type, such as **Central manager** or **Relay manager**. For details about the components that can be installed when JP1/Software Distribution Manager is used as the central manager or as a relay manager, see *1.1 Supported OSs and organization of components*.

Subcomponents are displayed in the tree hierarchy under the component name.

2.1.8 Selecting the program folder

Select the program folder in which the JP1/Software Distribution Manager icon is to be registered. The Specify Program Folder dialog box appears only during new installation. For an upgrade, the existing program folder is used automatically.

Figure 2–9: Specify Program Folder dialog box



Software Distribution Manager Setup

Specify Program Folder

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the Existing Folders list.

Program Folders:

Software Distribution Manager

Existing Folders:

Accessories
Administrative Tools
Microsoft SQL Server - Switch
Microsoft SQL Server 7.0
Startup

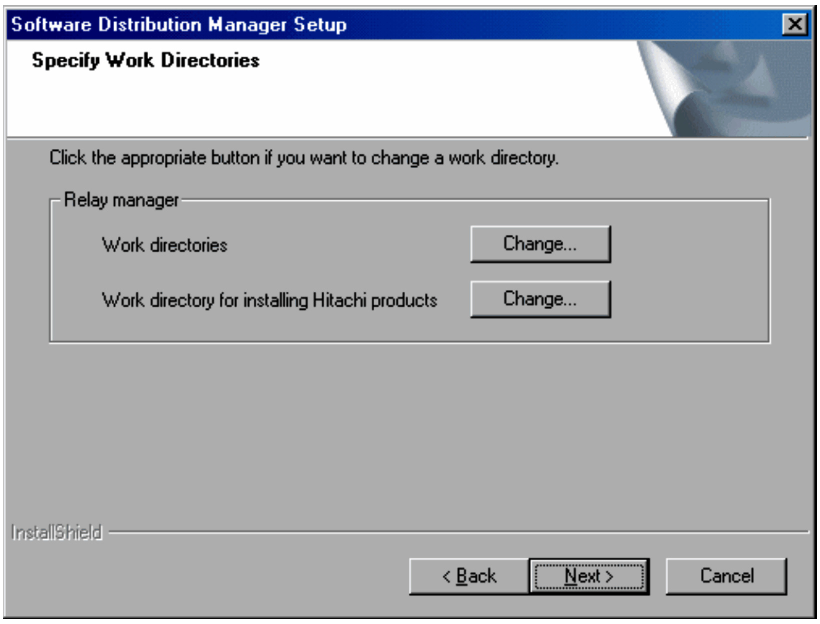
The default is for the icon to be registered in the **Software Distribution Manager** group. You can select an existing program folder or you can create a new program folder. Note that you cannot specify a program folder name that includes a backslash (\).

Click the **Next** button to continue with installation.

2.1.9 Specifying work directories

When **Relay manager** was selected in order to install the Server core facility of the Server, the Specify Work Directories dialog box appears. Clicking the **Change** button to the right of each item lets you change that work directory.

Figure 2–10: Specify Work Directories dialog box



Software Distribution Manager Setup

Specify Work Directories

Click the appropriate button if you want to change a work directory.

Relay manager

Work directories [Change...]

Work directory for installing Hitachi products [Change...]

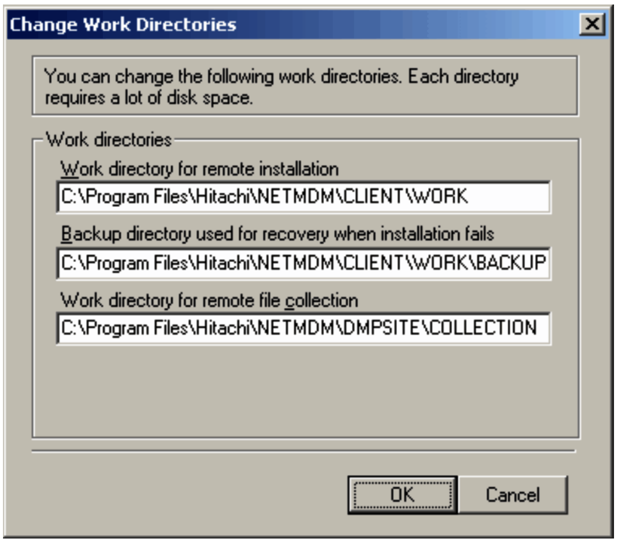
(1) Change Work Directories

This dialog box enables you to change each default work directory that is used by a relay manager for remote installation or remote collection. If you change these default work directories, set a directory for remote installation and another directory for remote collection, and do not use those directories for any other purpose. Express a work directory as alphanumeric characters, spaces, and the following special characters:

`_ \ . : ( )`

Clicking the **OK** button displays the Specify Work Directories dialog box again.

Figure 2–11: Change Work Directories dialog box



Change Work Directories

You can change the following work directories. Each directory requires a lot of disk space.

Work directories

Work directory for remote installation: C:\Program Files\Hitachi\NETMDM\CLIENT\WORK

Backup directory used for recovery when installation fails: C:\Program Files\Hitachi\NETMDM\CLIENT\WORK\BACKUP

Work directory for remote file collection: C:\Program Files\Hitachi\NETMDM\DMPSITE\COLLECTION

Work directory for remote installation

This directory is used by the client facility of the relay manager for installing packages. It requires the same amount of space as any package that is to be installed. Normally, you should specify a directory with at least 50 MB of free space.

Backup directory used for recovery when installation fails

This directory is used for saving a backup of software to be remote-installed by the client facility of the relay manager.

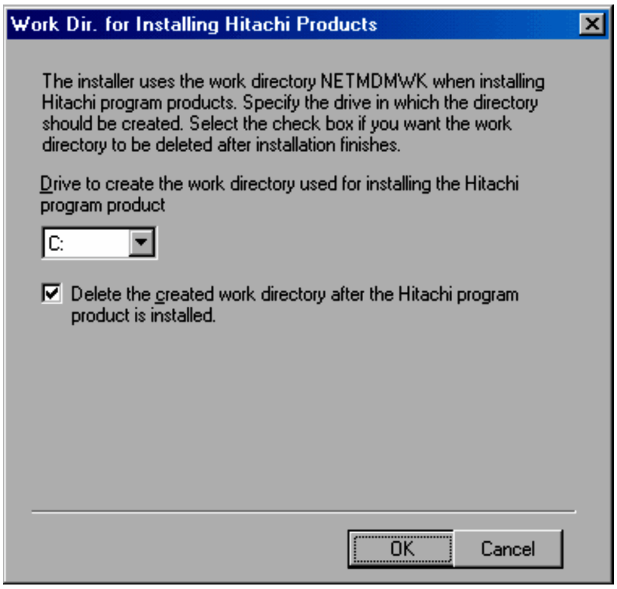
Work directory for remote file collection

This directory retains the collected files that are collected by executing a *Collect files from client to relay system* job until the managing server executes an *Acquire collected files from relay system* job or a *Delete collected files from relay system* job.

(2) Work Dir. for Installing Hitachi Products

You can change the drive of the work directory for installing Hitachi program products (`NETMDMWK` directory). Clicking the **OK** button after specifying the settings displays the Specify Work Directories dialog box again.

Figure 2–12: Work Dir. for Installing Hitachi Products dialog box



Work Dir. for Installing Hitachi Products

The installer uses the work directory NETMDMWK when installing Hitachi program products. Specify the drive in which the directory should be created. Select the check box if you want the work directory to be deleted after installation finishes.

Drive to create the work directory used for installing the Hitachi program product: C:

☑ Delete the created work directory after the Hitachi program product is installed.

Drive to create the work directory used for installing the Hitachi program product

Select the drive in which you wish to create the directory used for installing Hitachi program products. Do not specify a network drive; if a network drive is specified, operations cannot be guaranteed.

Delete the created work directory after the Hitachi program product is installed.

You can choose whether or not to delete the work directory after the Hitachi program product has been installed. To delete the work directory, select the **Delete the created work directory after the Hitachi program product is installed** check box. This option is selected as the default.

The following points should be noted about selecting the **Delete the created work directory after the Hitachi program product is installed** check box:

- In Windows NT, you must have the appropriate permissions to read, write, and delete the created drive in order to select the **Delete the created work directory after the Hitachi program product is installed** check box. If these permissions have not been granted, installation of a Hitachi program product will fail.
- Even though the **Delete the created work directory after the Hitachi program product is installed** check box has been selected, the `NETMDMWK` directory may remain after installation. In such a case, the directory will be deleted when the computer is restarted or during polling.

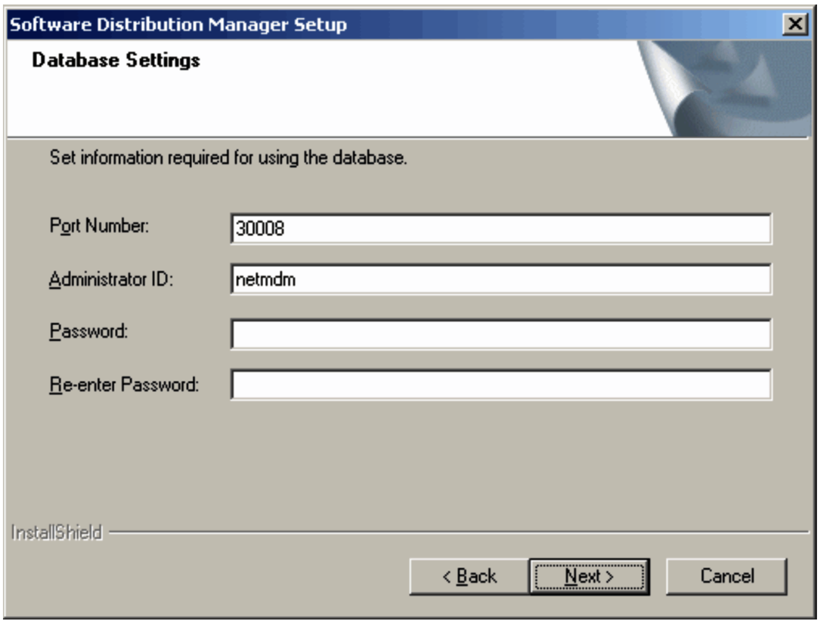
2.1.10 Setting up the database

Select the database to be used to record the information managed by JP1/Software Distribution and specify information needed in order to use the database. The Database Settings dialog box is displayed the first time any of **Server**, **Asset Information Manager Subset**, or **OpenView Linkage** is being installed. The actual dialog box that is displayed depends on the database to be used.

(1) For Embedded RDB

If you select **Embedded RDB** in the Select Database dialog box, the following window appears:

Figure 2–13: Database Settings dialog box (for Embedded RDB)



Software Distribution Manager Setup

Database Settings

Set information required for using the database.

Port Number: 30008

Administrator ID: netmdm

Password:

Re-enter Password:

Port Number

Specify the port number to be used to connect to Embedded RDB. The default is `30008`.

Administrator ID

Specify the login ID to be used to connect to Embedded RDB. This ID must be expressed as 1 to 8 alphanumeric characters beginning with an alphabetic character. The default is `netmdm`.

Password

Enter a password that will be used to connect to Embedded RDB. Express the password as 1 to 30 alphanumeric characters beginning with an alphabetic character. Spaces are not permitted.

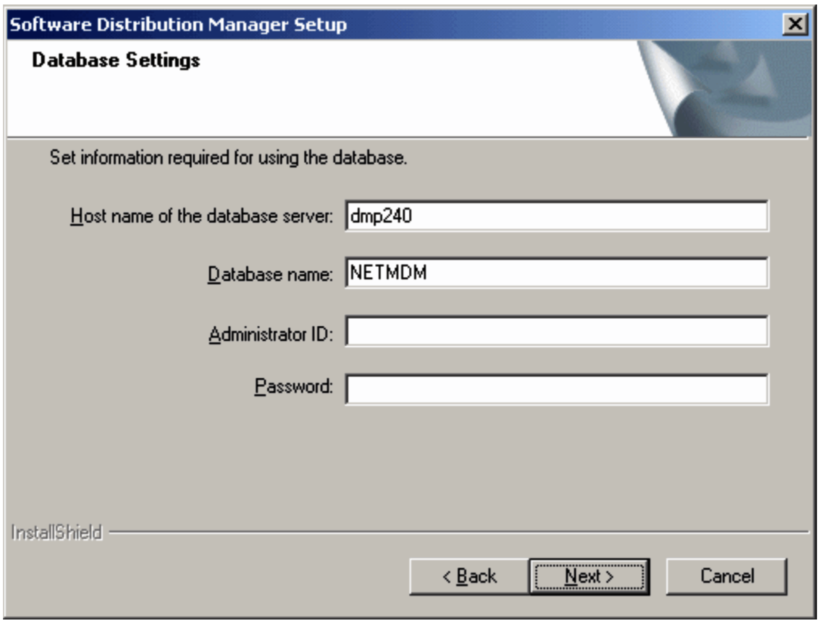
Re-enter Password

Re-enter the password that was entered in **Password**.

(2) For Microsoft SQL Server

If you select **Microsoft SQL Server** in the Select Database dialog box, the following window appears:

Figure 2–14: Database Settings dialog box (for Microsoft SQL Server)



Software Distribution Manager Setup

Database Settings

Set information required for using the database.

Host name of the database server: dmp240

Database name: NETMDM

Administrator ID:

Password:

Host name of the database server

Specify the host name of Microsoft SQL Server. The default is the local host name.

When using named instances, specify the host name in the format shown below. The permitted maximum length of a host name is 64 characters including the instance name.

database-server's-host-name\instance-name

Database name

Specify the name of the database. The default is `NETMDM`.

Administrator ID

Specify the login ID to be used to connect to Microsoft SQL Server.

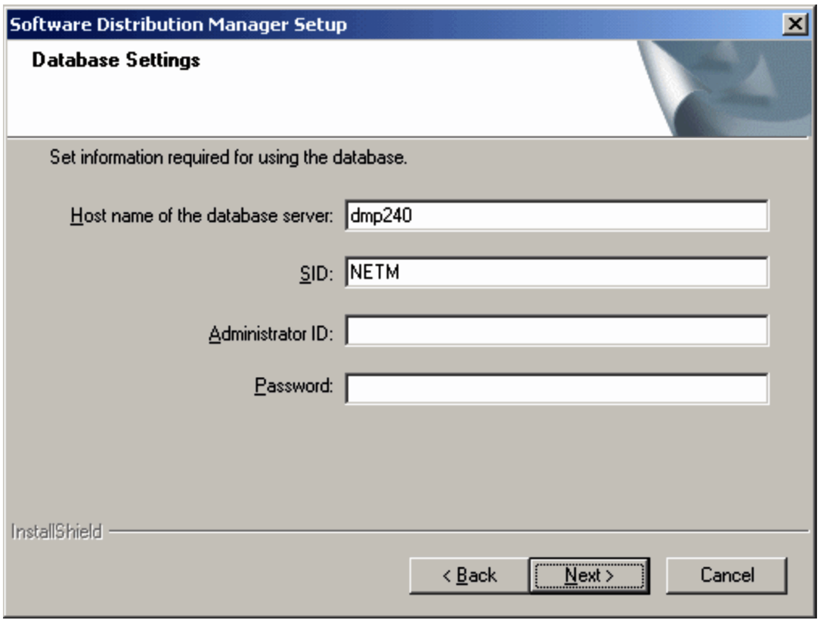
Password

Specify the password for connecting to Microsoft SQL Server. The permitted maximum length is 30 characters.

(3) For Oracle

If you select **Oracle** in the Select Database dialog box, the following window appears:

Figure 2–15: Database Settings dialog box (for Oracle)



Software Distribution Manager Setup

Database Settings

Set information required for using the database.

Host name of the database server: dmp240

SID: NETM

Administrator ID:

Password:

Host name of the database server

Specify the host name of Oracle Database Server. The default is the local host name.

SID

Specify the Oracle SID. The default is `NETM`.

Administrator ID

Specify the login ID to be used to connect to Oracle.

Password

Specify the password for connecting to Oracle. The permitted maximum length is 30 characters.

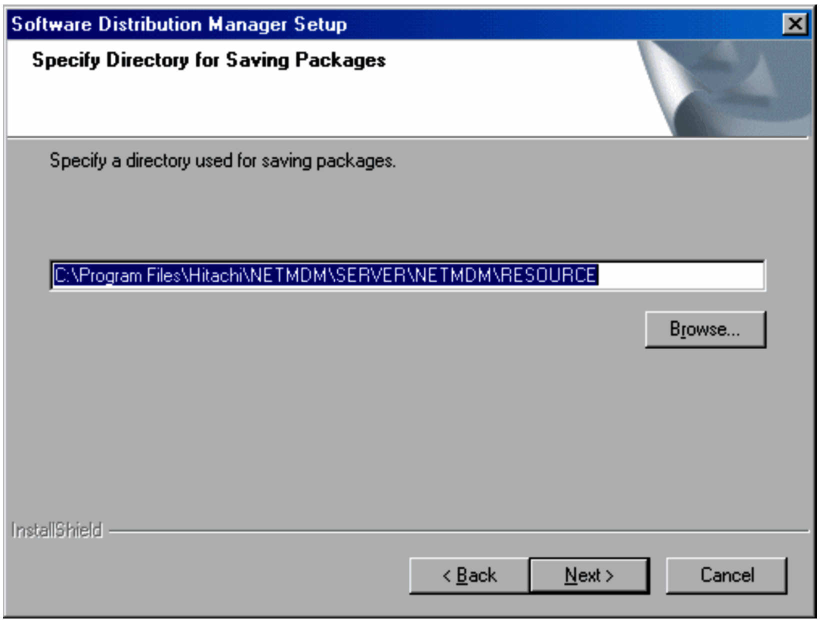
2.1.11 Setting the package storage directory

When you are installing the Server, you specify the database for storing packages and the storage directory. The actual dialog box that is displayed depends on the type of database used for logging JP1/Software Distribution management information.

(1) For Embedded RDB or Oracle

If you select **Embedded RDB** or **Oracle** in the Select Database dialog box and install the Server core facility of the Server, the Specify Directory for Saving Packages dialog box is displayed.

Figure 2–16: Specify Directory for Saving Packages dialog box



Software Distribution Manager Setup

Specify Directory for Saving Packages

Specify a directory used for saving packages.

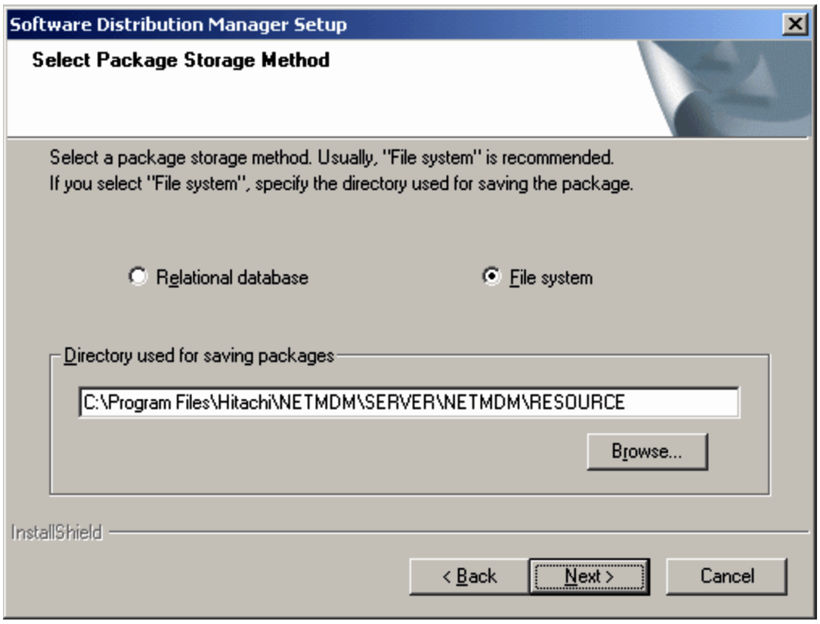
C:\Program Files\Hitachi\NETMDM\SERVER\NETMDM\RESOURCE

Specify in this dialog box the directory for saving packages. To change the default package storage directory, click the **Browse** button and select a desired directory.

(2) For Microsoft SQL Server

If you select **Microsoft SQL Server** in the Select Database dialog box and install the Server core facility of the Server, the Selecting Package Storage Method dialog box is displayed.

Figure 2–17: Select Package Storage Method dialog box



Software Distribution Manager Setup

Select Package Storage Method

Select a package storage method. Usually, "File system" is recommended.
If you select "File system", specify the directory used for saving the package.

○ Relational database ● File system

Directory used for saving packages

C:\Program Files\Hitachi\NETMDM\SERVER\NETMDM\RESOURCE

If you use Microsoft SQL Server for logging JP1/Software Distribution management information, you can select either the relational database (Microsoft SQL Server) or the file system for storing packages. Although use of the file system is recommended, Microsoft SQL Server is also available as the package storage database. The default is **File system**.

If you select the file system, specify the directory for saving packages.

Directory used for saving packages

To change the default package storage directory, click the **Browse** button and select a desired directory.

(3) Notes about setting the package storage directory

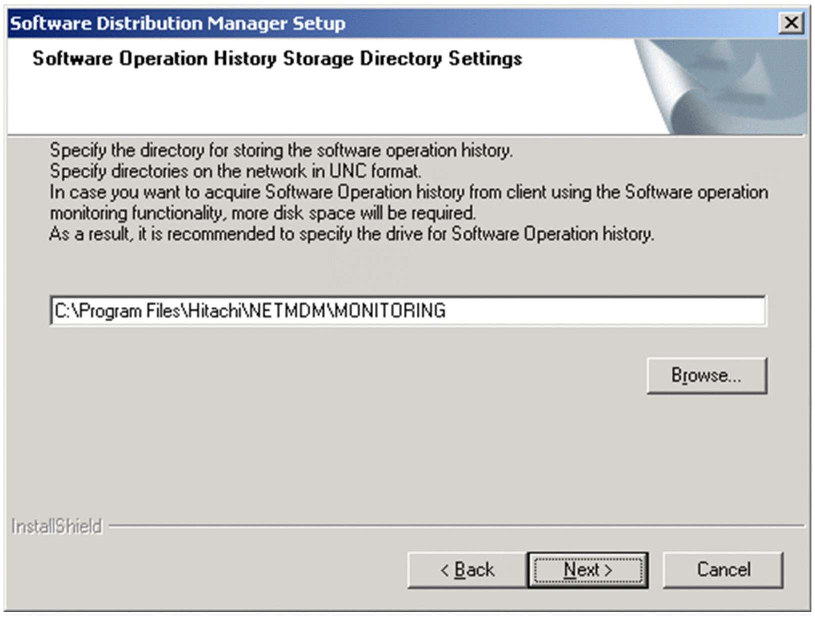
You should note the following if you change the package storage directory when you upgrade your system or change installation settings:

- You must move any package data in the old package storage directory to the new package storage directory.
  If such packages are not moved, a job that already existed before the change, such as a remote installation job, will result in an error.
- If you have changed the package storage directory from relational database to file system, execute **Transfer resource from database to file system** from Database Manager after installation has been completed. For details about how to use Database Manager, see *7.5.3 Transferring resources from the database to the file system (Microsoft SQL Server)*.

2.1.12 Setting the software operation history storage directory

To monitor the software activity status and collect the operation history, you must specify a directory for storing the operation history for each client. This dialog box is displayed when the Server core facility of the Server is installed.

Figure 2–18: Software Operation History Storage Directory Settings dialog box



Software Distribution Manager Setup

Software Operation History Storage Directory Settings

Specify the directory for storing the software operation history.
Specify directories on the network in UNC format.
In case you want to acquire Software Operation history from client using the Software operation monitoring functionality, more disk space will be required.
As a result, it is recommended to specify the drive for Software Operation history.

C:\Program Files\Hitachi\NETMDM\MONITORING

Operation history requires a large amount of disk space. We recommend that you provide a dedicated drive for storing the operation history.

The operation history storage directory cannot be directly under the drive, such as `D:\`. To change the default operation history storage directory, click the **Browse** button and specify a desired directory.

To specify a network drive for the operation history storage directory, use the UNC format (`\\`*network-drive-name* `\`*shared-name*). A format that includes a drive letter, such as `G:\NETM\MONITORING`, is not permitted. Express a network drive as 1 to 127 characters. The permitted symbols include `-`, _, `\`, `.`, `:`, `(`, and `)`. You must specify an existing directory for the operation history storage directory.

To change the operation history storage directory after installation, restart the installer and then specify the necessary settings. To change the operation history storage directory, you must migrate the operation history. For details about migrating the operation history, see *6.10 Notes on software operation monitoring* in the manual *Administrator's Guide Volume 1*.

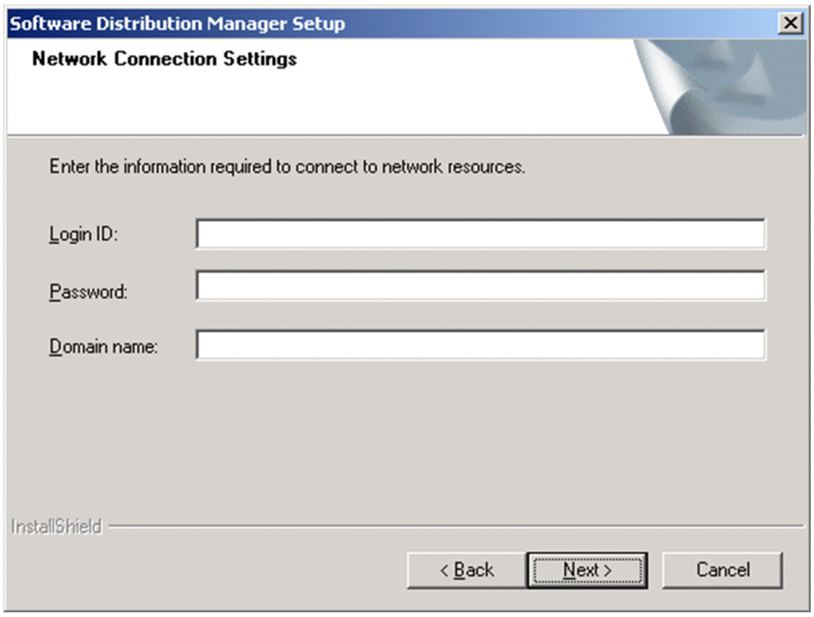
Operation history will be stored for each client under the `OPERATION` directory that is created under the directory specified on this page. The amount of operation history per client depends on the type of operations. As a guideline, assume about 4 megabytes per day if Web access logs are acquired and about 1 megabyte per day if Web access logs are not acquired.

2.1.13 Specifying the network connection settings

If you use a network drive for the operation history storage directory or operation history backup directory, you must set the authentication information required in order to connect to the network drive. These settings are not required if you have specified a local drive for the operation history storage directory. For details about the authentication information to be set, see *2.5.8 Collecting operation history and suppression history* in the manual *Description and Planning Guide*.

The authentication information set here can be changed on the **Network Connection** page at the time of setup.

Figure 2–19: Network Connection Settings dialog box



Software Distribution Manager Setup

Network Connection Settings

Enter the information required to connect to network resources.

Login ID:

Password:

Domain name:

Login ID

Specify the login ID used to connect to the network drive, expressed as 1 to 30 alphanumeric characters and symbols. None of the following symbols can be used:

`\ / * : ; , + < = > ? | [ ]`

If you specify a network drive for the operation history storage directory and operation history backup directory, make sure that you also specify the password and domain name.

Password

Specify the password used to connect to the network drive, expressed as 1 to 30 alphanumeric characters and symbols. Spaces are not permitted.

Domain name

Specify the domain name used to connect to the network drive, expressed as 1 to 127 alphanumeric characters and symbols. None of the following symbols can be used:

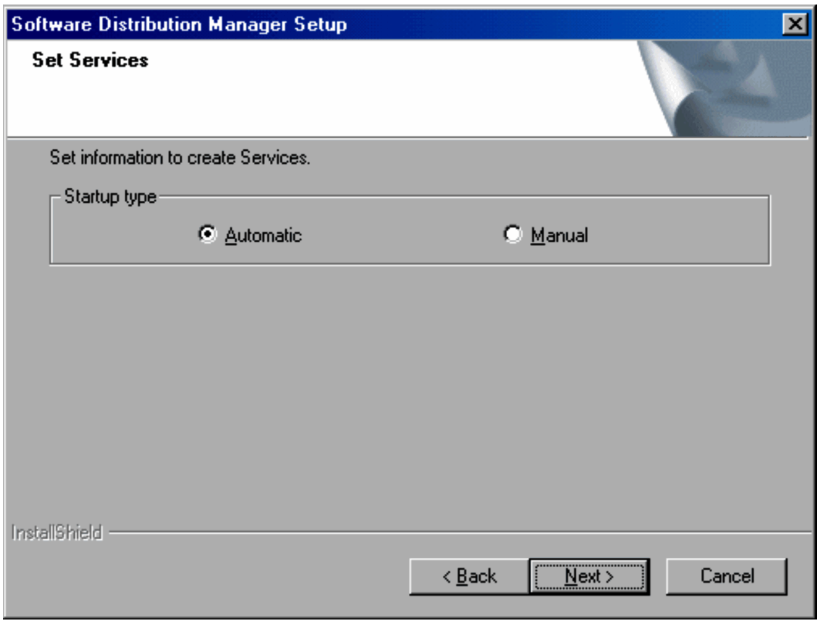
`\ / * : ; , + < = > ? | [ ]`

2.1.14 Setting up services

Specify the startup type of services. These settings are the same as when the Remote Install Server properties are displayed by choosing **Control Panel**, **Administrative Tools**, and then **Services**.

This dialog box is displayed the first time the Server core facility of the Server is installed. If the Remote Install Server services already exist, this dialog box is not displayed.

Figure 2–20: Set Services dialog box



Software Distribution Manager Setup

Set Services

Set information to create Services.

Startup type

● Automatic ○ Manual

Startup type

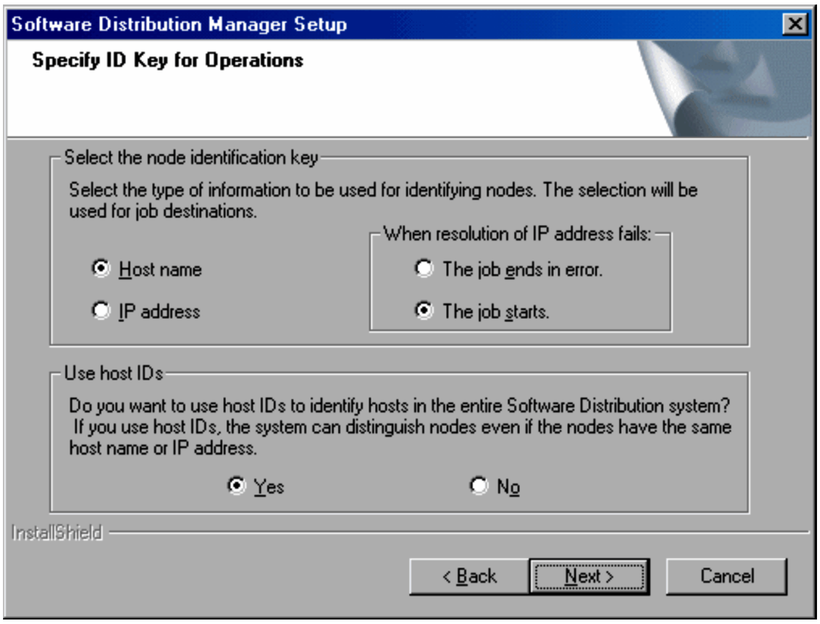
Select **Automatic** or **Manual**. The default is **Automatic**.

2.1.15 Specifying the ID key for operations

Specify the key for managing hosts and identifying destinations on the network (*ID key for operations*). This dialog box is displayed when the Server core facility of the Server or Asset Information Manager Subset is installed.

You can change these settings during setup.

Figure 2–21: Specify ID Key for Operations dialog box



Software Distribution Manager Setup

Specify ID Key for Operations

Select the node identification key

Select the type of information to be used for identifying nodes. The selection will be used for job destinations.

● Host name

○ IP address

When resolution of IP address fails:

○ The job ends in error.

● The job starts.

Use host IDs

Do you want to use host IDs to identify hosts in the entire Software Distribution system? If you use host IDs, the system can distinguish nodes even if the nodes have the same host name or IP address.

● Yes ○ No

The ID key for operations includes the node identification key and use of host IDs. For **Select the node identification key**, select a node identification key. For **Use host IDs**, specify whether or not host IDs are to be used.

Select the node identification key

For communication between hosts, specify either **Host name** or **IP address** as the information for identifying the communication destination host. Select **Host name** or **IP address** to match the *ID key for operations* setting at the destination host. The default is **Host name**. When **Host name** is selected, specify the **When resolution of IP address fails:** option.

If you are migrating a JP1 Version 7i system using a basic database to a JP1 Version 8 system and changing the ID key for operations, you must first delete some information. For details about the information to be deleted, see *4.2.8(2) Notes on changing the node identification key*.

When resolution of IP address fails:

Specify whether or not a job that results in an error because a destination IP address cannot be resolved is to be terminated. The default is **The job starts**. When **The job starts** is selected, the status of a job for which an IP address cannot be resolved becomes **Waiting for transmission**. The status of a job addressed to a nonexistent destination becomes **Waiting for transmission** and remains unchanged.

In an environment in which a WINS server is used, the destination address cannot be resolved if the destination client PC is turned off during job execution. Thus, if you select **The job ends in error**, you will not be able to execute jobs at night or on weekends by automatically starting the client by polling at system startup. In such a case, you should select **The job starts**.

When **The job starts** is selected and a job to be executed includes an address that cannot be resolved, processing at the remote installation manager slows down.

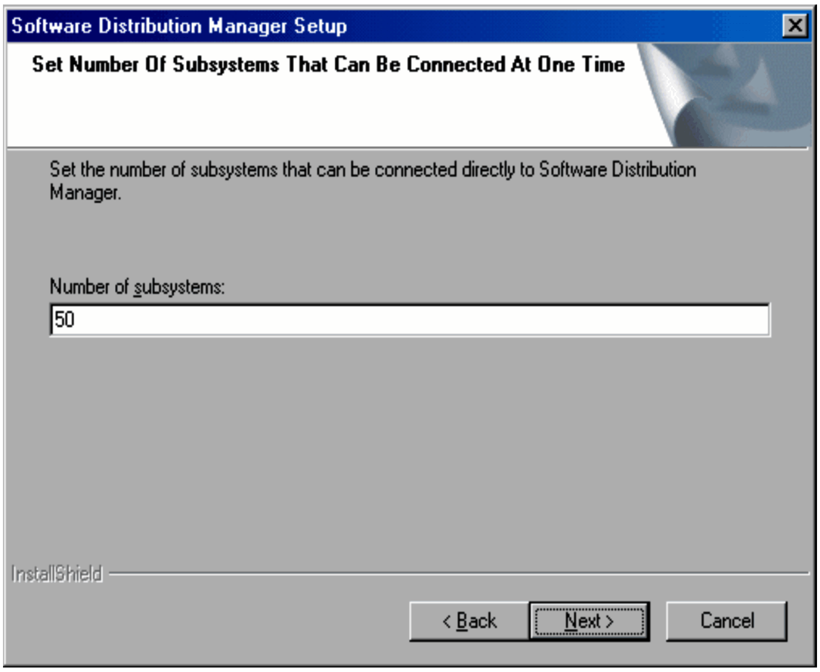
Use host IDs

Select whether host IDs are to be used for identifying and managing hosts throughout the entire JP1/Software Distribution system. The default is **Yes**.

2.1.16 Setting the number of subsystems that can be connected simultaneously

Specify the number of subsystems that can be connected at one time to JP1/Software Distribution Manager. This dialog box is displayed when the Server core facility of the Server is installed.

Figure 2–22: Set Number Of Subsystems That Can Be Connected At One Time dialog box



Software Distribution Manager Setup

Set Number Of Subsystems That Can Be Connected At One Time

Set the number of subsystems that can be connected directly to Software Distribution Manager.

Number of subsystems: 50

Use the formulas shown below to determine the setting.

Number of subsystems that can be connected simultaneously =

Number of systems to be connected directly + number of Packagers to be connected **x** 2

The permitted number of subsystems that can be connected simultaneously depends on the type of database selected:

Database	Minimum value	Maximum value	Default
Embedded RDB	4	100	30
Microsoft SQL Server or Oracle	4	256	50

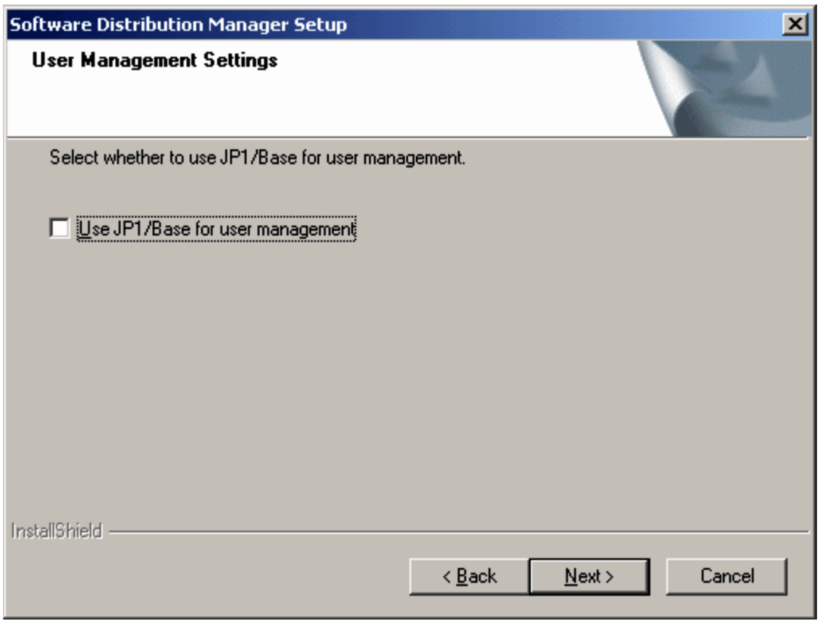
This setting enables you to limit the number of subsystems that can be connected simultaneously. Once the number of connections reaches the value specified here, the system rejects additional connection requests from subsystems. The specified value becomes the number of socket connections. Each socket connection is counted from the time it is established until the time it is released.

You can change this setting during setup. If the network traffic becomes heavy and many packet collisions occur, you can reduce the traffic by specifying a smaller value to decrease the number of concurrent subsystem connections.

2.1.17 Setting user management

Select whether or not to link JP1/Base in order to manage JP1/Software Distribution users. This dialog box is displayed when **Server core facility** of **Server** is installed.

Figure 2–23: User Management Settings dialog box



Software Distribution Manager Setup

User Management Settings

Select whether to use JP1/Base for user management.

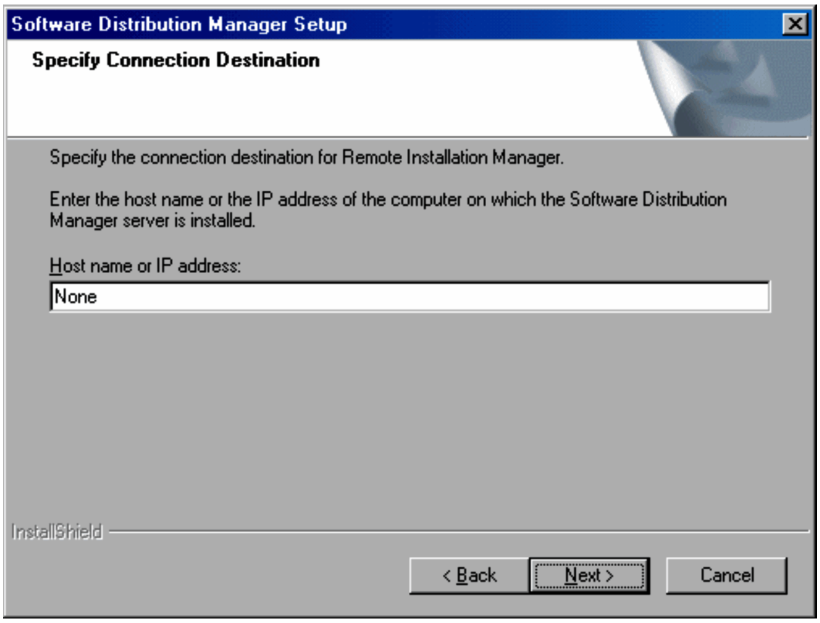
□ Use JP1/Base for user management

To link JP1/Base to manage JP1/Software Distribution users, select the check box. By default, this check box is not selected.

2.1.18 Specifying the connection destination (Remote Installation Manager)

When only the Remote Installation Manager facility of **Server** is being installed on a separate PC from the server, the Specify Connection Destination dialog box appears so that you can specify the connection destination server. Specify in this dialog box the server to which connection from the Remote Installation Manager is to be established. Make sure that the version of the server to be connected matches the version as the Remote Installation Manager. You can change the connection destination when Remote Installation Manager starts.

Figure 2–24: Specify Connection Destination dialog box



Software Distribution Manager Setup

Specify Connection Destination

Specify the connection destination for Remote Installation Manager.

Enter the host name or the IP address of the computer on which the Software Distribution Manager server is installed.

Host name or IP address: None

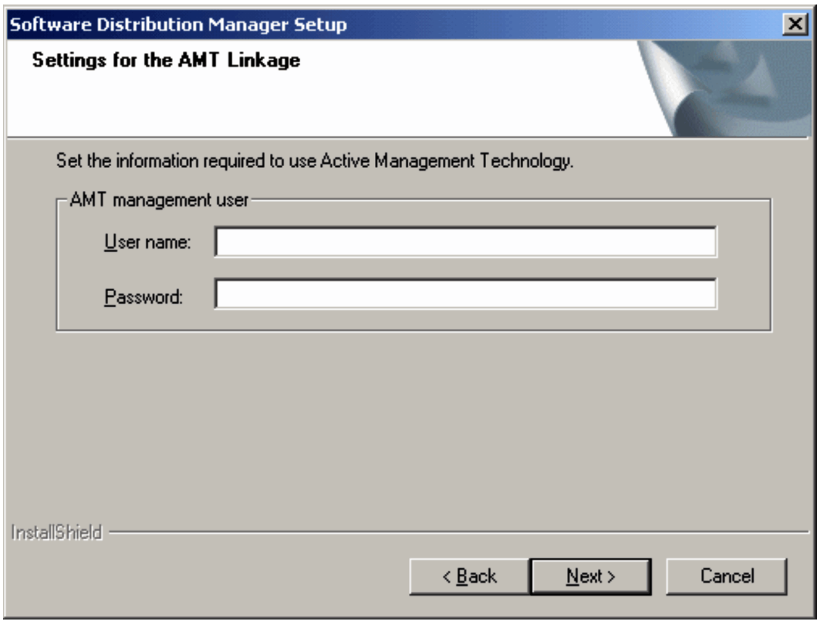
For the connection destination, specify the host name or IP address of the PC on which the Server core facility of the Server is installed. The default is **None**.

For a PC on which only Remote Installation Manager has been installed, there is no need to specify settings on the **Database Environment** page of a setup dialog box. The settings of the connection destination PC take effect.

2.1.19 Setting up AMT Linkage

Set information that is needed for controlling the client using AMT Linkage.

Figure 2–25: Settings for the AMT Linkage dialog box



Software Distribution Manager Setup

Settings for the AMT Linkage

Set the information required to use Active Management Technology.

AMT management user

User name:

Password:

AMT management user

Sets the information needed to access the client's AMT. The user name and password must match the client's settings.

User name

Specifies the user name used to access the client's AMT, expressed as up to 60 characters.

Password

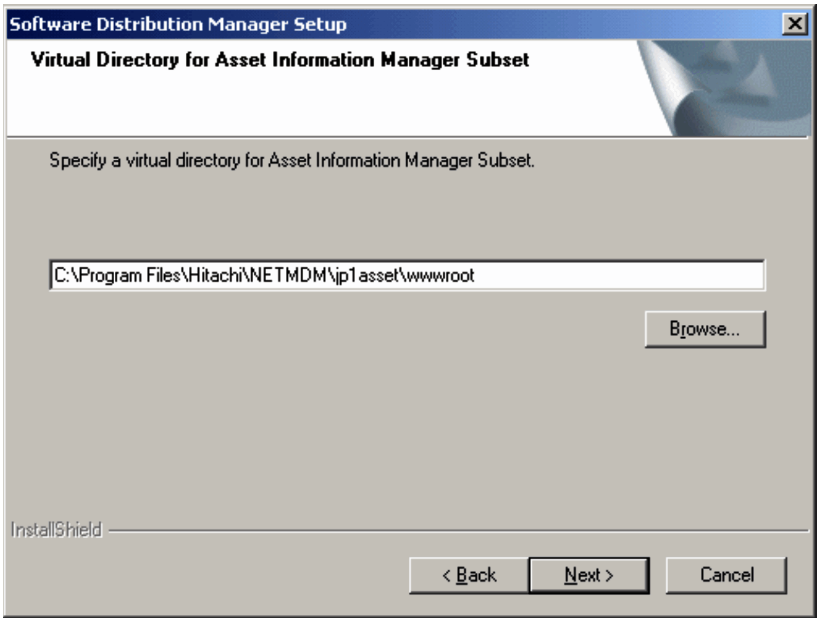
Specifies the password used to access the client's AMT, expressed as up to 60 characters.

2.1.20 Setting the virtual directory for Asset Information Manager Subset

When you install Asset Information Manager Subset for the first time, the window for setting the virtual directory for Asset Information Manager Subset is displayed.

Set the virtual directory for Asset Information Manager Subset that is used to store the data needed for execution of Asset Information Manager Subset and log files.

Figure 2–26: Settings for the Virtual Directory for Asset Information Manager Subset dialog box



Software Distribution Manager Setup

Virtual Directory for Asset Information Manager Subset

Specify a virtual directory for Asset Information Manager Subset.

C:\Program Files\Hitachi\NETMDM\jp1asset\wwwroot

Specify the absolute path of the virtual directory for Asset Information Manager Subset. To change the default path, click the **Browse** button and select the desired path.

When the installation is completed, the virtual directory for Asset Information Manager Subset is created in **Default Web Site**. The name of the virtual directory is `jp1asset`.

To set the virtual directory for Asset Information Manager Subset in a Web site other than **Default Web Site**, change it from the Asset Information Manager Subset setup after the installation is completed. For details about the Asset Information Manager Subset setup, see *10.1 Setting up Asset Information Manager Subset*.

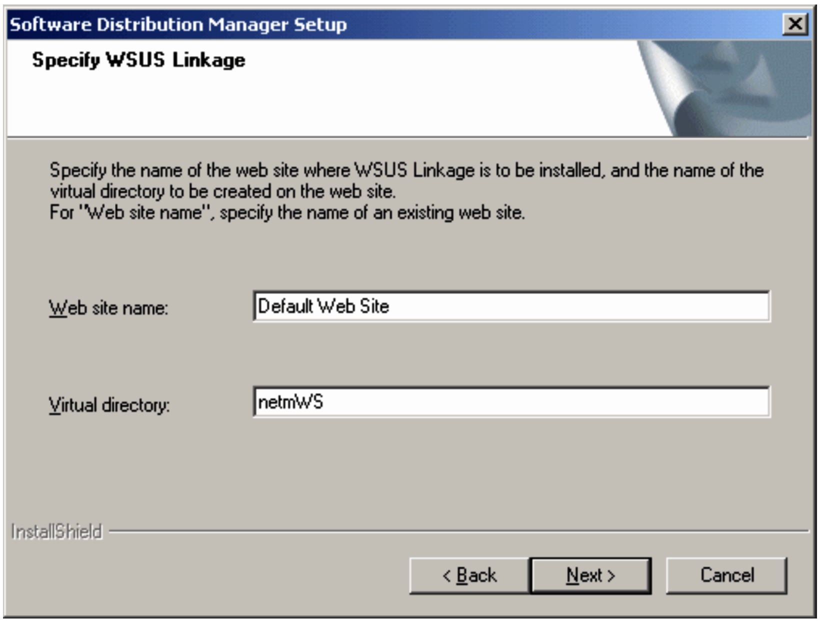
For details about how to install Asset Information Manager Subset, see *2.3 Installing Asset Information Manager Subset*.

2.1.21 Setting up WSUS Linkage

This dialog box is displayed when you install WSUS Linkage on a WSUS server. For details about how to install WSUS Linkage, see *2.4 Installing JP1/Software Distribution on a WSUS server*.

In this dialog box, set the Web site and virtual directory needed for JP1/Software Distribution to link with the Microsoft Internet Information Services of the WSUS server.

Figure 2–27: Specify WSUS Linkage dialog box



Software Distribution Manager Setup

Specify WSUS Linkage

Specify the name of the web site where WSUS Linkage is to be installed, and the name of the virtual directory to be created on the web site.
For "Web site name", specify the name of an existing web site.

Web site name: Default Web Site

Virtual directory: netmWS

Web site name

Specify an existing Web site name. The default is **Default Web Site.**

Virtual directory

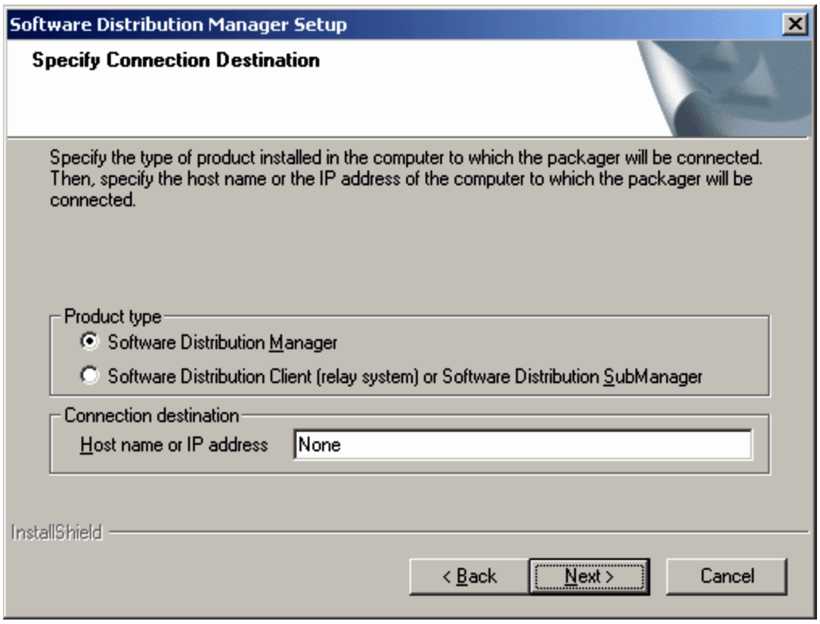
Specify a name for the new virtual directory to be created. The default is **netmWS**.

2.1.22 Specifying the connection destination (Packager)

Specify the connection destination of the Packager. The Specify Connection Destination dialog box is displayed when the Packager is being installed.

You can change the connection destination when the Packager starts.

Figure 2–28: Specify Connection Destination dialog box



Software Distribution Manager Setup

Specify Connection Destination

Specify the type of product installed in the computer to which the packager will be connected. Then, specify the host name or the IP address of the computer to which the packager will be connected.

Product type
● Software Distribution Manager
○ Software Distribution Client (relay system) or Software Distribution SubManager

Connection destination
Host name or IP address: None

Product type

Select either **Software Distribution Manager** or **Software Distribution Client (relay system) or Software Distribution SubManager**. The default is **Software Distribution Manager**.

Connection destination

Specify the host name or IP address of the connection destination of the Packager. The default is **None**.

2.1.23 Setting up OpenView Linkage

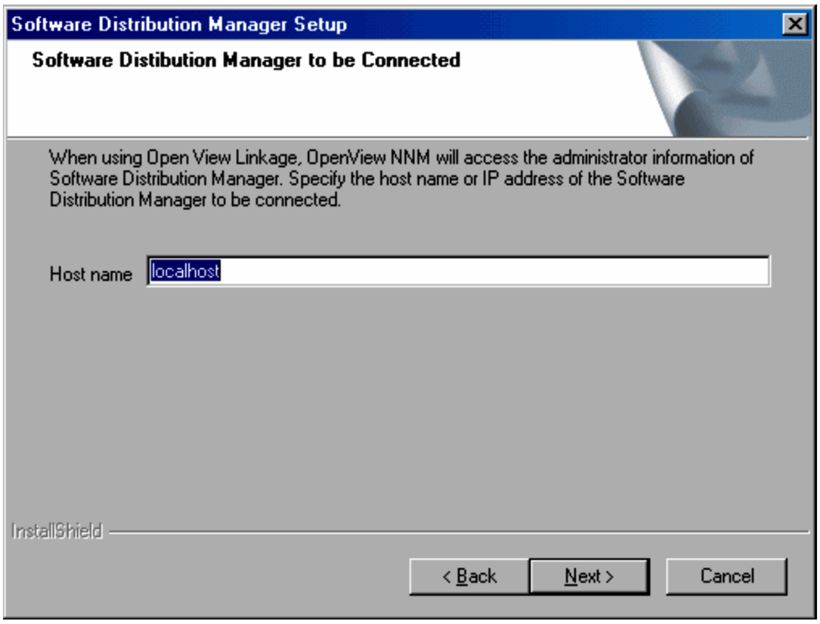
When you are installing OpenView Linkage, the Software Distribution Manager OpenView Linkage Setup dialog box is displayed. This subsection describes the settings. For details about how to install OpenView Linkage, see *2.5 Installing JP1/Software Distribution Manager in HP Network Node Manager*.

(1) Software Distribution Manager to be Connected

Specify the host name or IP address of the JP1/Software Distribution Manager to which HP NNM version 7.5 or earlier is to connect.

You can change this setting during setup.

Figure 2–29: Software Distribution Manager to be Connected dialog box



Software Distribution Manager Setup

Software Distibution Manager to be Connected

When using Open View Linkage, OpenView NNM will access the administrator information of Software Distribution Manager. Specify the host name or IP address of the Software Distribution Manager to be connected.

Host name: localhost

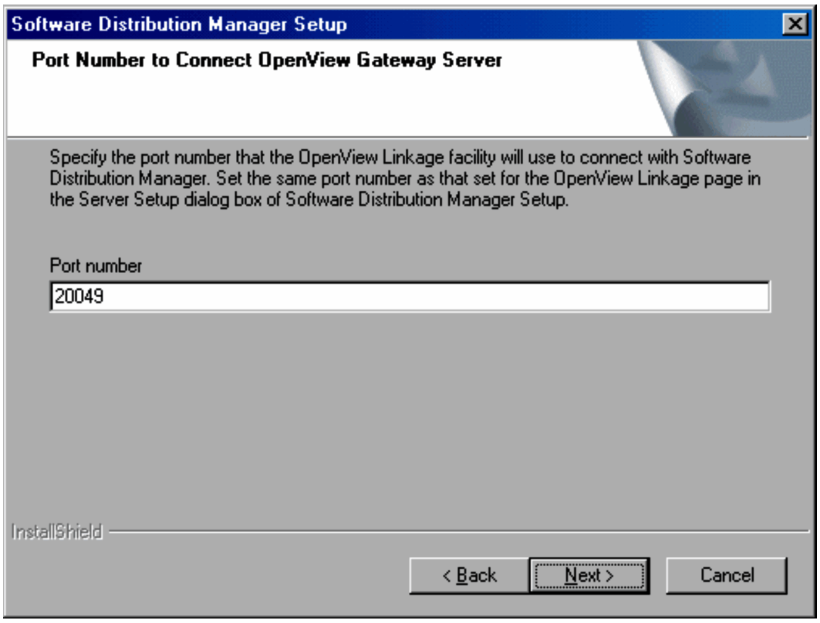
HP NNM accesses the management information of the specified JP1/Software Distribution Manager. Note that OpenView Gateway Server must be installed on the connection-destination JP1/Software Distribution Manager.

(2) Port Number to Connect OpenView Gateway Server

Specify the port number to be used by HP NNM version 7.5 or earlier to establish connection with JP1/Software Distribution Manager.

You can change this setting during setup.

Figure 2–30: Port Number to Connect OpenView Gateway Server dialog box



Software Distribution Manager Setup

Port Number to Connect OpenView Gateway Server

Specify the port number that the OpenView Linkage facility will use to connect with Software Distribution Manager. Set the same port number as that set for the OpenView Linkage page in the Server Setup dialog box of Software Distribution Manager Setup.

Port number: 20049

For **Port number**, specify the port number that has been specified on the **OpenView Linkage** tab of the Server Setup dialog box in the JP1/Software Distribution Manager setup. This port number is used when HP NNM accesses the management information of the JP1/Software Distribution Manager. The default is `20049`.

2.1.24 Setting up the OpenView gateway server

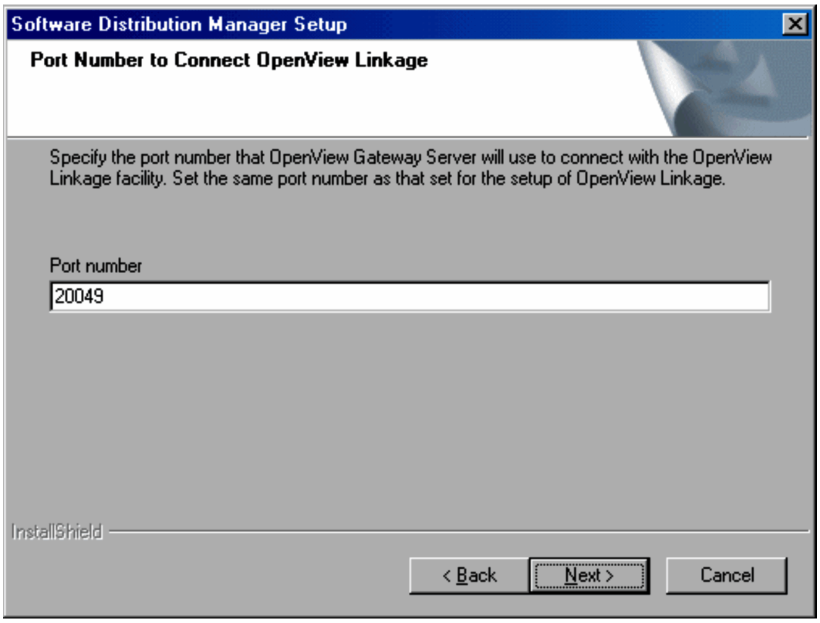
To use the OpenView Linkage facility to establish connection to JP1/Software Distribution Manager from HP NNM version 7.5 or earlier, you must install **OpenView Gateway Server** on the JP1/Software Distribution Manager PC. This subsection describes the setting that is required in order to install OpenView Gateway Server.

(1) Port Number to Connect OpenView Linkage

Specify the port number used by the OpenView Gateway Server to establish connection with OpenView Linkage.

You can change this setting during setup.

Figure 2–31: Port Number to Connect OpenView Linkage dialog box



Software Distribution Manager Setup

Port Number to Connect OpenView Linkage

Specify the port number that OpenView Gateway Server will use to connect with the OpenView Linkage facility. Set the same port number as that set for the setup of OpenView Linkage.

Port number: 20049

For **Port number**, specify the port number that has been specified in the Port Number to Connect OpenView Gateway Server dialog box during installation of OpenView Linkage. The default is `20049`.

2.1.25 Checking the Notes for the Remote Control Agent

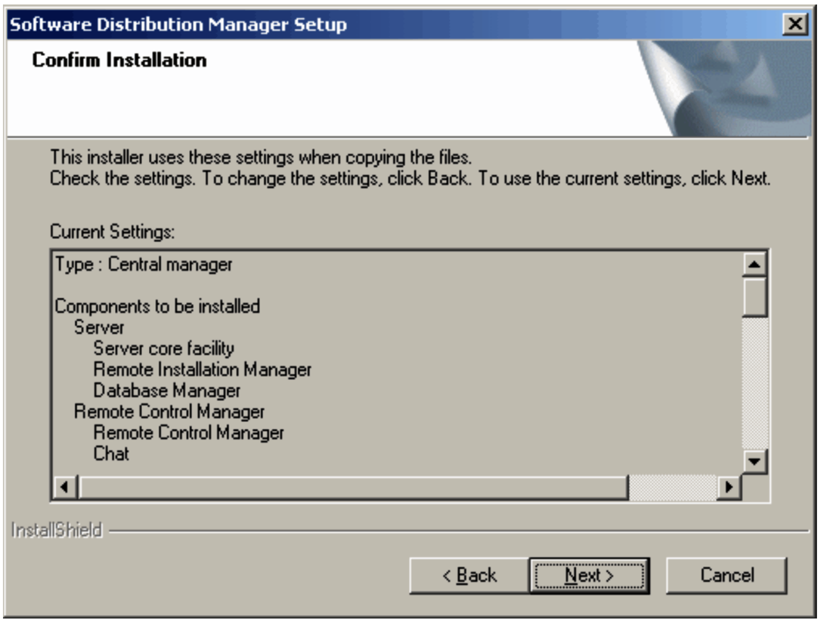
When you install a new Remote Control Agent, the Notes dialog box appears. The contents of this dialog box depend on whether Remote Control Agent is installed on a Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP, or Windows 2000 system or on a Windows NT 4.0, Windows Me, or Windows 98 system.

For details about the dialog box that is displayed, see *3.1.16 Checking the Notes for the Remote Control Agent*. For details about the notes, see the *Job Management Partner 1/Remote Control Description and Operator's Guide*.

2.1.26 Confirming the installation

Check the specified settings that are displayed in the Confirm Installation dialog box.

Figure 2–32: Confirm Installation dialog box



Software Distribution Manager Setup

Confirm Installation

This installer uses these settings when copying the files.
Check the settings. To change the settings, click Back. To use the current settings, click Next.

Current Settings:

```
Type : Central manager

Components to be installed
  Server
    Server core facility
    Remote Installation Manager
    Database Manager
  Remote Control Manager
    Remote Control Manager
    Chat
```

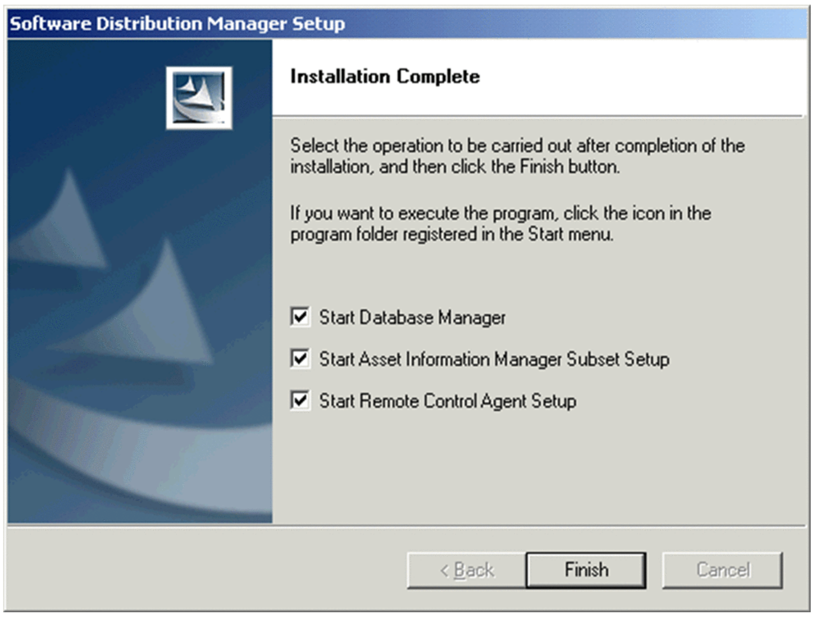
If you need to change any setting, click the **Back** button to display the corresponding dialog box and make the change. If no changes are needed, click the **Next** button. The system starts installation.

2.1.27 Finishing the installation

When installation is complete, the Installation Complete dialog box appears. There are two Installation Complete dialog boxes, and the one that is appropriate to the installation status is displayed.

- When the status is normal

Figure 2–33: Installation Complete dialog box (when the status is normal)



Software Distribution Manager Setup

Installation Complete

Select the operation to be carried out after completion of the installation, and then click the Finish button.

If you want to execute the program, click the icon in the program folder registered in the Start menu.

☑ Start Database Manager

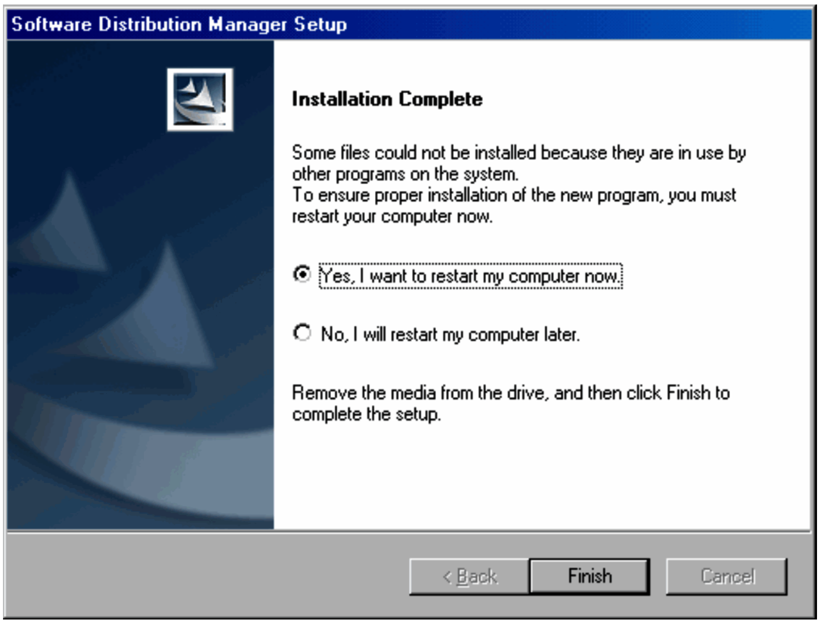
☑ Start Asset Information Manager Subset Setup

☑ Start Remote Control Agent Setup

Select the **Start Database Manager**, **Start Asset Information Manager Subset Setup**, or **Start Remote Control Agent Setup** check box, as appropriate, for the next processing you wish to execute, and then click the **Finish** button.

- When restart is required

Figure 2–34: Installation Complete dialog box (when restart is required)



Software Distribution Manager Setup

Installation Complete

Some files could not be installed because they are in use by other programs on the system.
To ensure proper installation of the new program, you must restart your computer now.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

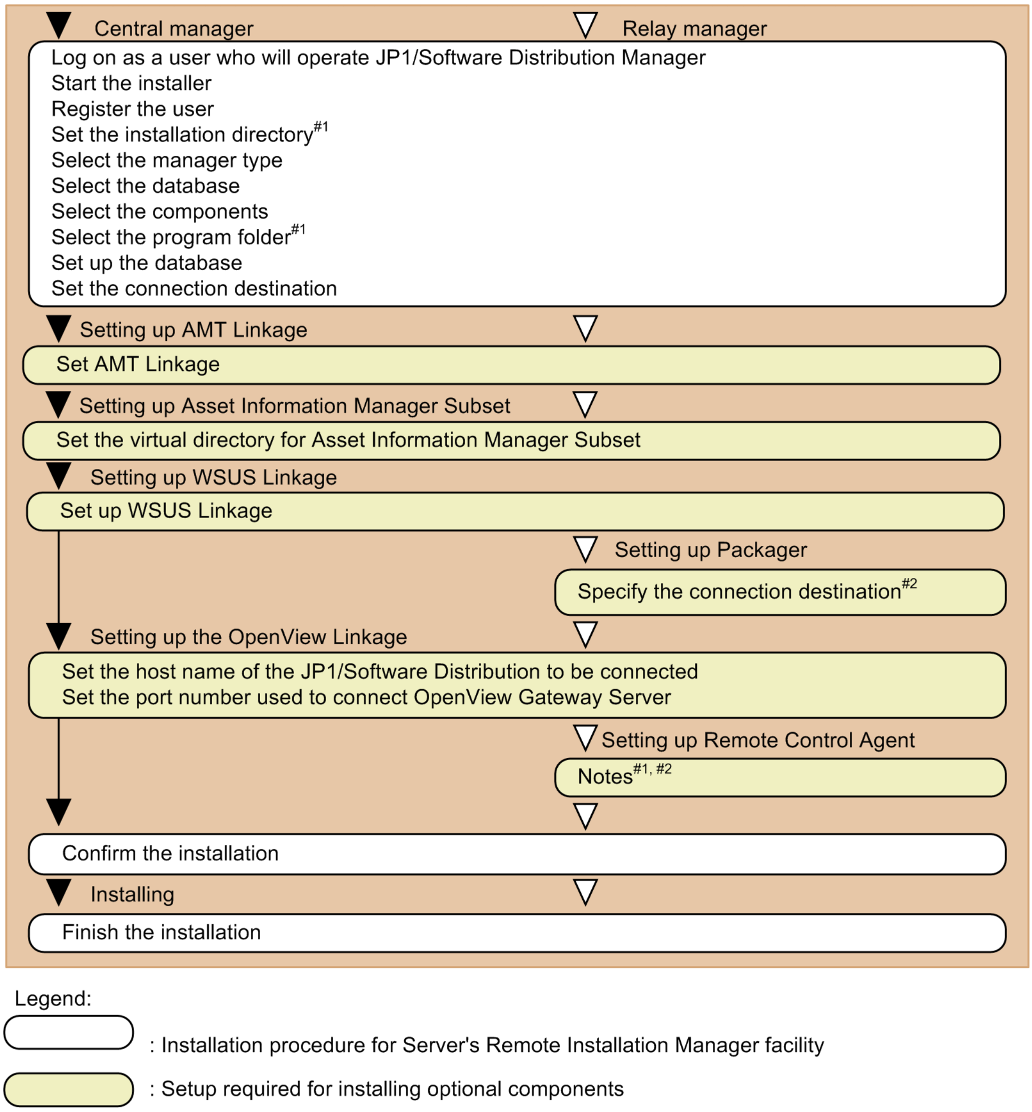
Remove the media from the drive, and then click Finish to complete the setup.

If system restart is required after installation, this dialog box appears. Select whether you wish to restart now or later, remove the CD-ROM from the CD-ROM drive, and then click the **Finish** button.

2.2 Installing Remote Installation Manager

The figure below shows the procedure for installing only Remote Installation Manager of the Server on a separate PC from the one where the Server is installed. In this case, the Server core facility of the Server is not installed. Make sure that the version of the server to be connected matches the version of the Remote Installation Manager.

Figure 2–35: Remote Installation Manager installation procedure


Central manager
Relay manager
Log on as a user who will operate JP1/Software Distribution Manager
Start the installer
Register the user
Set the installation directory#1
Select the manager type
Select the database
Select the components
Select the program folder#1
Set up the database
Set the connection destination
Setting up AMT Linkage
Set AMT Linkage
Setting up Asset Information Manager Subset
Set the virtual directory for Asset Information Manager Subset
Setting up WSUS Linkage
Set up WSUS Linkage
Setting up Packager
Specify the connection destination#2
Setting up the OpenView Linkage
Set the host name of the JP1/Software Distribution to be connected
Set the port number used to connect OpenView Gateway Server
Setting up Remote Control Agent
Notes#1, #2
Confirm the installation
Installing
Finish the installation
Legend:
: Installation procedure for Server's Remote Installation Manager facility
: Setup required for installing optional components

#1: This information is displayed only when a JP1/Software Distribution Manager program folder has not been created.

#2: This information is displayed only when Packager or Remote Control Agent was selected.

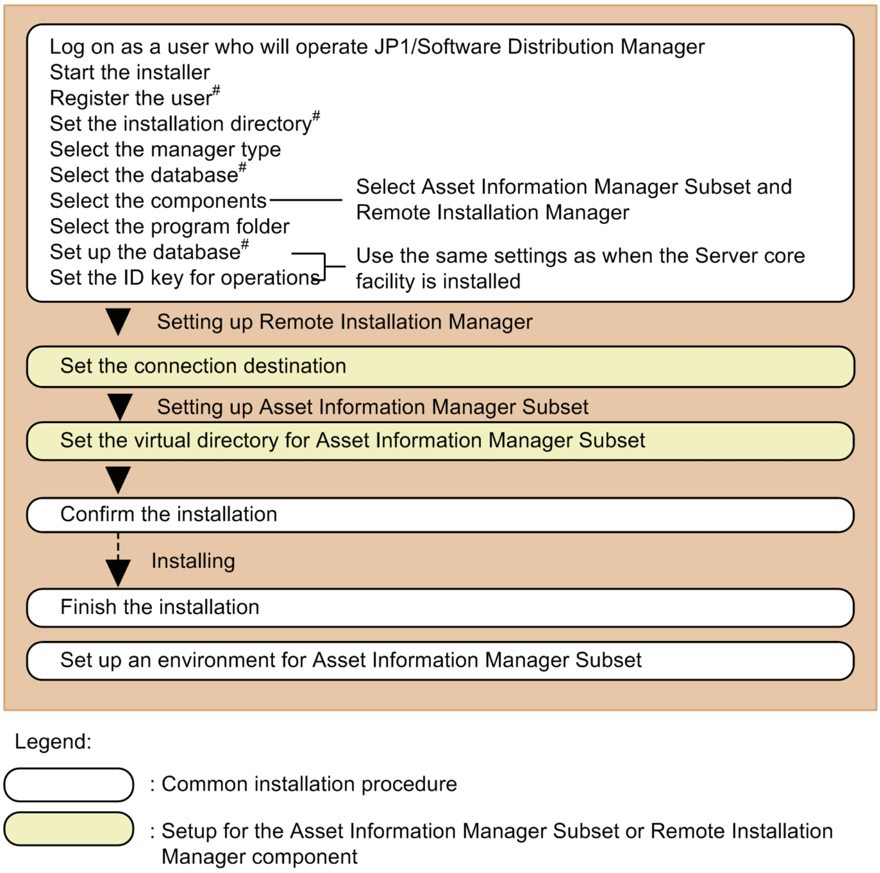
If you select Packager or Remote Control Agent as an installation component in addition to Server, you must also set it up during installation.

For details about each procedure, see *2.1 How to install JP1/Software Distribution Manager*.

2.3 Installing Asset Information Manager Subset

The following figure shows the procedure for installing Asset Information Manager Subset on a separate PC from Server.

Figure 2–36: Asset Information Manager Subset installation procedure


Log on as a user who will operate JP1/Software Distribution Manager
Start the installer
Register the user#
Set the installation directory#
Select the manager type
Select the database#
Select the components
Select the program folder
Set up the database#
Set the ID key for operations
Select Asset Information Manager Subset and Remote Installation Manager
Use the same settings as when the Server core facility is installed
Setting up Remote Installation Manager
Set the connection destination
Setting up Asset Information Manager Subset
Set the virtual directory for Asset Information Manager Subset
Confirm the installation
Installing
Finish the installation
Set up an environment for Asset Information Manager Subset
Legend:
: Common installation procedure
: Setup for the Asset Information Manager Subset or Remote Installation Manager component

#: This information is displayed only during a new installation.

For details about setting the virtual directory for Asset Information Manager Subset, see *2.1.20 Setting the virtual directory for Asset Information Manager Subset*.

Asset Information Manager Subset cannot be installed on a computer on which JP1/Asset Information Manager has been installed.

(1) Notes on installation

- If you select Embedded RDB as the Asset Information Manager Subset database, a `tmp` folder is created at the root of the drive where the software is being installed. The `tmp` folder is required when using Embedded RDB, so do not delete it.
- When you select Embedded RDB as the Asset Information Manager Subset database, restoring a backup database after installing the software is impossible if the name of the drive being used or the installation target folder has been changed. To use a database that was backed up onto another drive, make sure the current installation uses the same path that was used when the backup was made.
- When installing Asset Information Manager in Windows XP Professional SP2, Windows Firewall may display a security warning message. Should a warning message be displayed, reduce the security level or take other action to allow the installation to proceed.
- Asset Information Manager Subset cannot be installed on a machine that runs software that uses 64-bit Microsoft Internet Information Services.

(2) Procedure before installation

Before installing Asset Information Manager Subset, perform the following:

If you are installing Asset Information Manager Subset on a 64-bit OS, make sure that 32-bit applications can run. For information on how to do this, see *10.11(1) Notes on installing Asset Information Manager Subset on a 64-bit OS*.

- Install Remote Installation Manager.

  Remote Installation Manager is required in order to install Asset Information Manager Subset on a separate PC from Server.
- Install Microsoft Internet Information Services.
- Start the Task Scheduler service.
- Stop the services, commands, and tasks of Asset Information Manager Subset.

  Before you perform a new installation of Asset Information Manager Subset-related services, stop *World Wide Web Publishing Service* or *World Wide Web Publishing*.

  Before you perform an overwrite installation of Asset Information Manager Subset, stop the services, commands, and tasks in the following order:

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (when JP1/CSC is linked)

  To use Asset Information Manager Subset after you have performed the operation, start the services in the reverse order from which they were stopped.
- If you use Microsoft Internet Information Services 7.0, it is recommended that you install the required role services before you install Asset Information Manager Subset; this way, the virtual directory will be created automatically (if you install the role services after you have installed Asset Information Manager Subset, the virtual directory will not be created automatically). For details about how to install the role services, see *10.6.2(1) Installing the role services*.

(3) Setting up an environment for Asset Information Manager Subset

To use Asset Information Manager Subset to manage the software operation status, you must set up an environment for Asset Information Manager Subset after its installation.

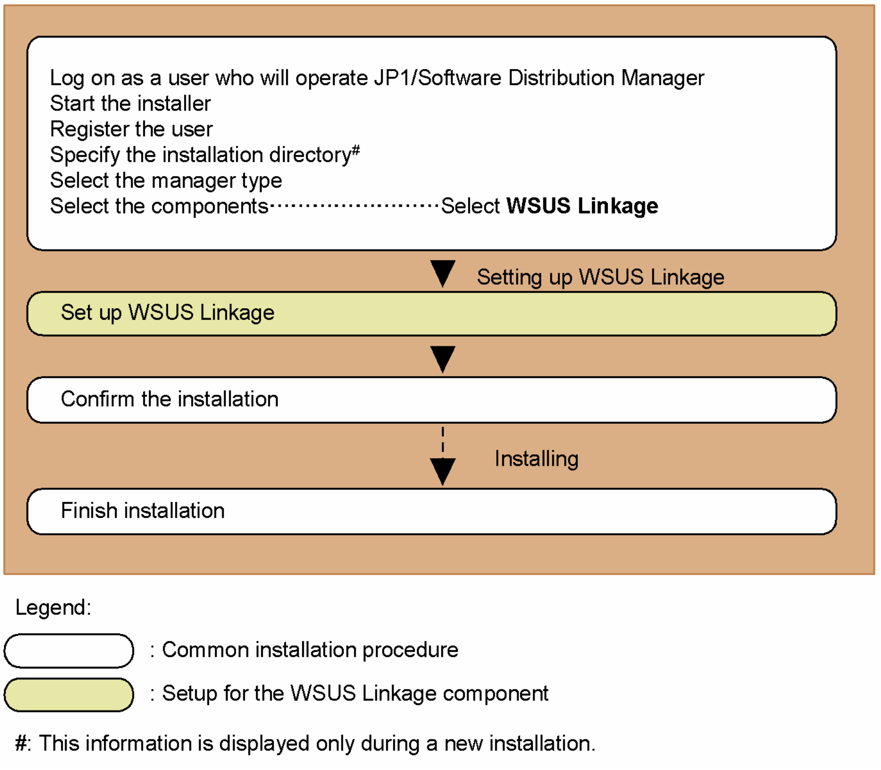
For details about the environment set up for Asset Information Manager Subset, see *10.1 Setting up Asset Information Manager Subset*.

2.4 Installing JP1/Software Distribution on a WSUS server

This section describes how to install WSUS Linkage on a WSUS server.

The figure below shows the procedure for installing WSUS Linkage from the JP1/Software Distribution installation medium. This figure assumes that only **WSUS Linkage** was selected in the Select Components dialog box.

Figure 2–37: WSUS Linkage installation procedure



#: This information is displayed only during a new installation.

For details about the settings for WSUS Linkage, see *2.1.21 Setting up WSUS Linkage*.

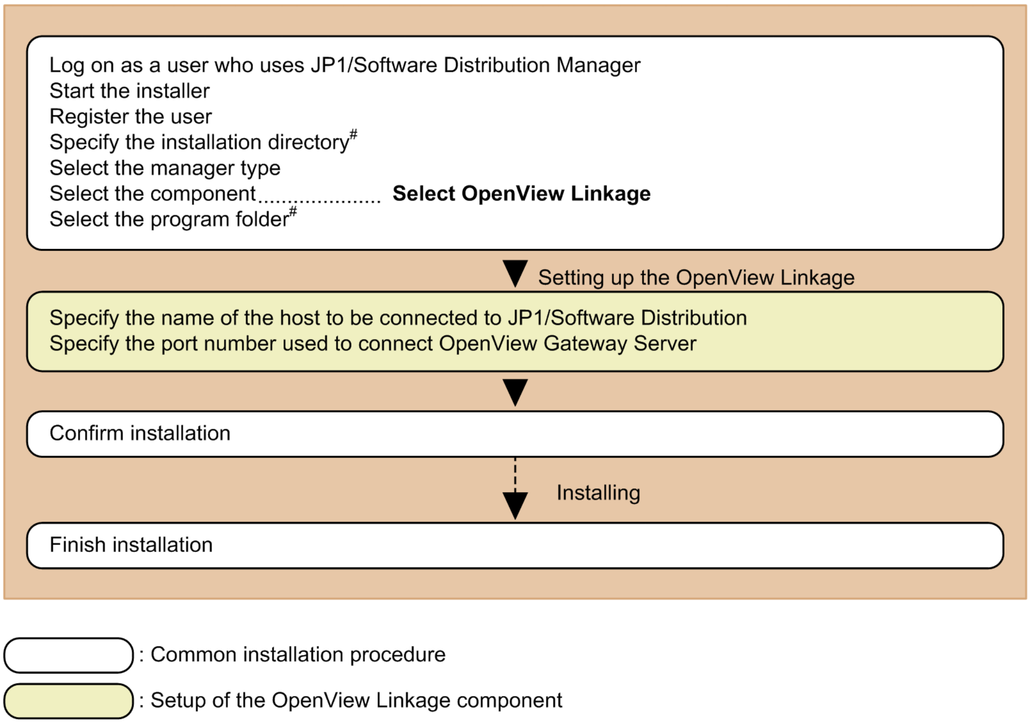
WSUS Linkage is a component common to JP1/Software Distribution and JP1/Asset Information Manager. If JP1/Asset Information Manager's WSUS Linkage component has already been installed on the WSUS server, installation of JP1/Software Distribution's WSUS Linkage component is not necessary.

2.5 Installing JP1/Software Distribution Manager in HP Network Node Manager

This section describes how to install OpenView Linkage in HP Network Node Manager. Before you can install OpenView Linkage, you must start the services provided by HP NNM version 7.5 or earlier.

The figure below shows the procedure for installing OpenView Linkage from the JP1/Software Distribution Manager installation medium. This figure shows the installation procedure when only **OpenView Linkage** is selected from the Select Components dialog box.

Figure 2–38: OpenView Linkage installation procedure


Log on as a user who uses JP1/Software Distribution Manager
Start the installer
Register the user
Specify the installation directory#
Select the manager type
Select the component.................... Select OpenView Linkage
Select the program folder#
Setting up the OpenView Linkage
Specify the name of the host to be connected to JP1/Software Distribution
Specify the port number used to connect OpenView Gateway Server
Confirm installation
Installing
Finish installation
: Common installation procedure
: Setup of the OpenView Linkage component

This is applicable during new installation only.

When installing OpenView Linkage on a PC whose `NtfsDisable8dot3NameCreation` is set to `1` in the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem`, do not include any spaces in the installation target directory. If a space is included, OpenView Linkage cannot be used.

For details about the settings, see *2.1.23 Setting up OpenView Linkage*.

3 Installing JP1/Software Distribution Client

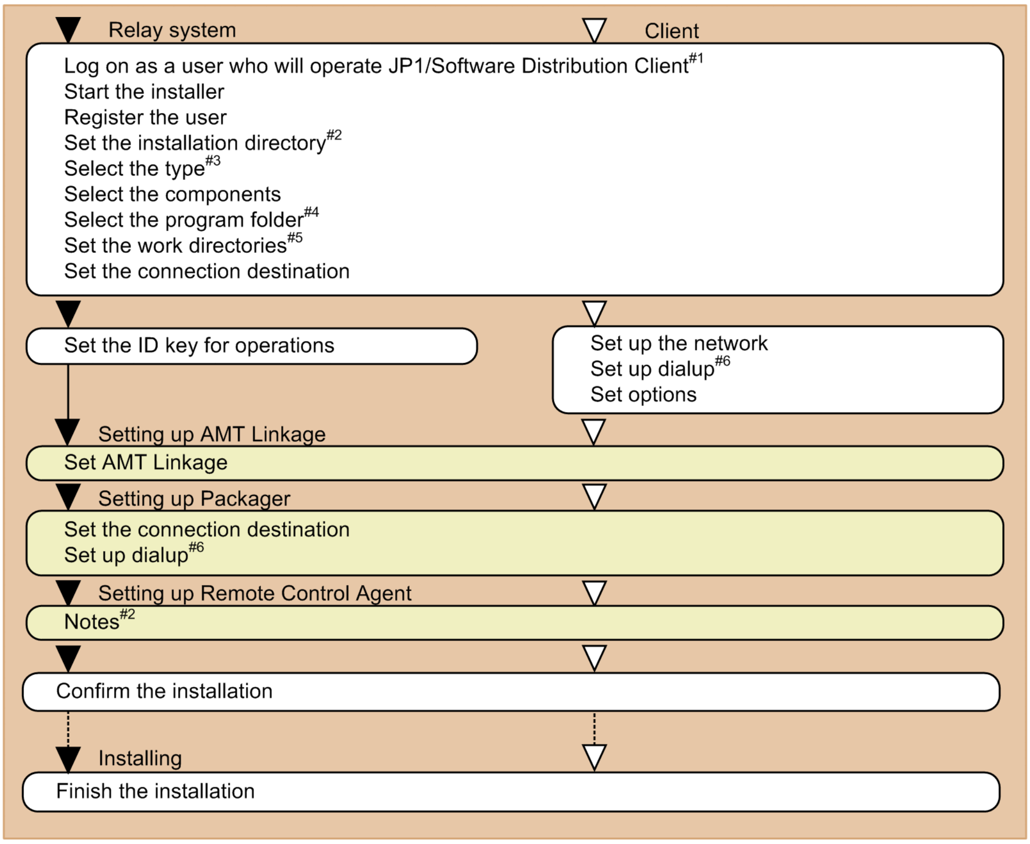
This chapter explains how to install JP1/Software Distribution Client as a relay system or as a client.

3.1 How to install JP1/Software Distribution Client

When you install JP1/Software Distribution Client, you choose whether it will be used as a relay system or as a client.

The following figure shows the procedure for installing JP1/Software Distribution Client as a relay system or client.

Figure 3–1: JP1/Software Distribution Client installation procedure


Relay system
Client
Log on as a user who will operate JP1/Software Distribution Client[#1]
Start the installer
Register the user
Set the installation directory[#2]
Select the type[#3]
Select the components
Select the program folder[#4]
Set the work directories[#5]
Set the connection destination
Set the ID key for operations
Set up the network
Set up dialup[#6]
Set options
Setting up AMT Linkage
Set AMT Linkage
Setting up Packager
Set the connection destination
Set up dialup[#6]
Setting up Remote Control Agent
Notes[#2]
Confirm the installation
Installing
Finish the installation

Legend:

▭ : Installation procedure for Relay system and Client components

🟨 : Setup required for installing optional components

#1: With Windows NT, the facility for installation with non-Administrator user permissions enables a user to use JP1/Software Distribution Client whether or not the user has installed JP1/Software Distribution Client. With Windows Me and Windows 98, there are no restrictions on operations based on user permissions.
#2: This information is displayed only during a new installation.
#3: With Windows Me and Windows 98, a relay system cannot be installed.
#4: This information is displayed only during a new installation or when overwriting the program in an environment in which no program folder is created.
#5: This information is displayed only when Relay system or Client is selected.
#6: This information is displayed only when Dial-up connection is selected in the previous dialog box.

If you select **Packager** or **Remote Control Agent** as an installation component in addition to **Relay system** or **Client**, you must also set up the selected component during installation.

When the pre-installation facility is used, you can install JP1/Software Distribution Client in one computer and then copy its hard disk. For details about how to install JP1/Software Distribution Client using the pre-installation facility, see *1.2.3 Using the pre-installation facility to install JP1/Software Distribution Client (client)*.

The steps in the installation procedure are explained below.

3.1.1 Logging on

In Windows NT, log on using a user name with Administrator permissions. This is the user who will operate JP1/Software Distribution Client. If you enabled the **Run the client with non-Administrator user permissions** option at the setup after installation, any user will be able to use JP1/Software Distribution Client whether or not the user has installed JP1/Software Distribution Client.

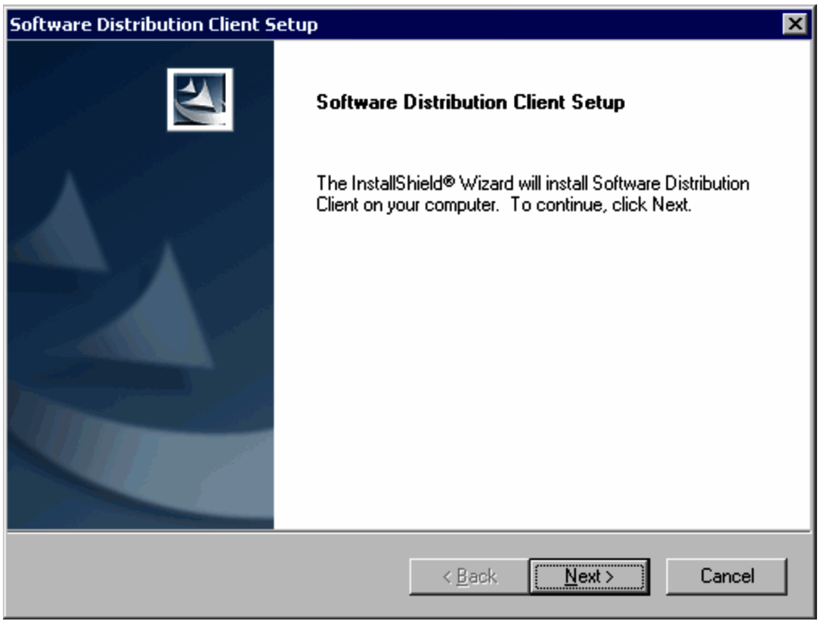
With Windows Me or Windows 98, you can log on and install with any permissions. Any user can use JP1/Software Distribution Client whether or not the user has installed JP1/Software Distribution Client.

3.1.2 Starting the installer

Insert the provided medium into the CD-ROM drive and install the program following the instructions of the installer.

When the installer starts, the JP1/Software Distribution Client installation program starts, and the Software Distribution Client Setup dialog box is displayed.

Figure 3–2: Software Distribution Client Setup dialog box



Software Distribution Client Setup

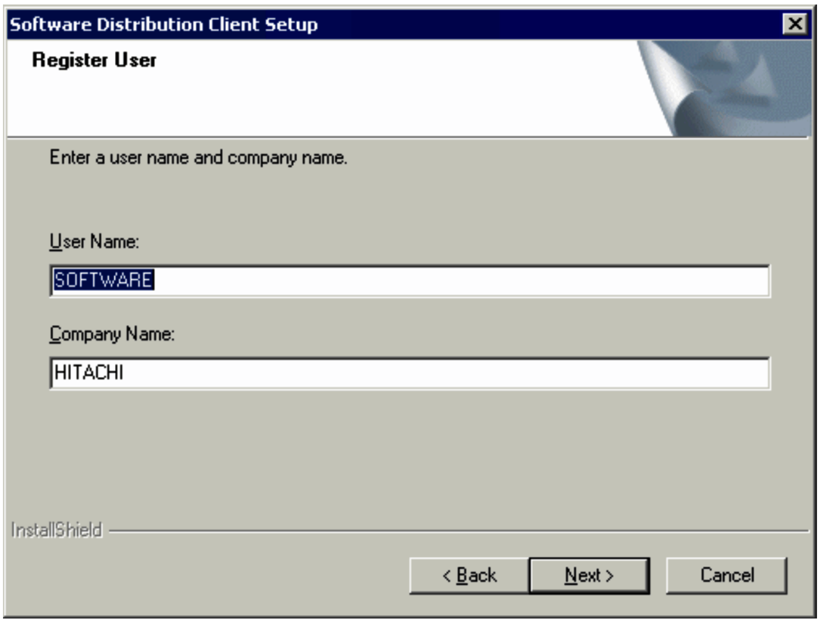
The InstallShield® Wizard will install Software Distribution Client on your computer. To continue, click Next.

Click the **Next** button to continue with installation. To stop installation, click the **Cancel** button. In the subsequent dialog boxes, clicking the **Back** button displays the immediately preceding dialog box.

3.1.3 Registering the user

Register the user name and company name in the Register User dialog box.

Figure 3–3: Register User dialog box



Software Distribution Client Setup

Register User

Enter a user name and company name.

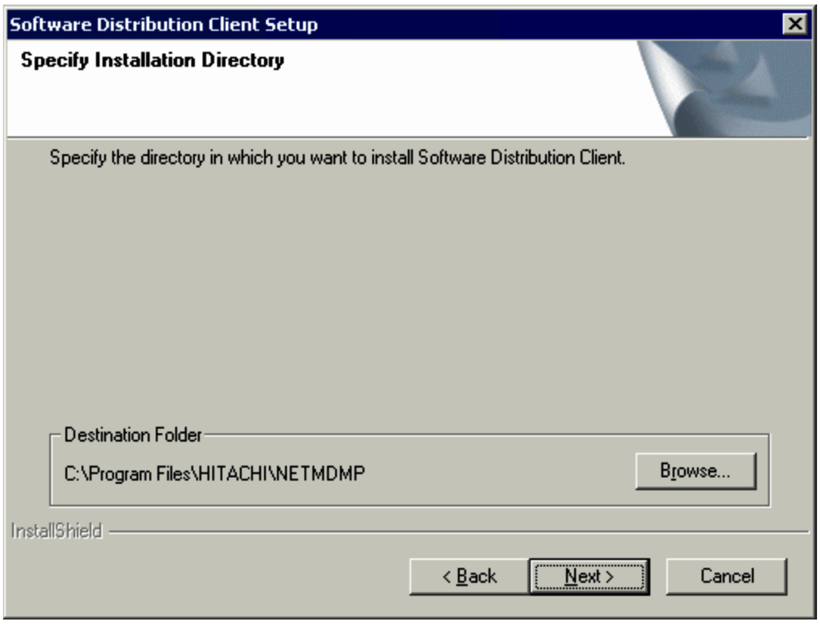
User Name: SOFTWARE

Company Name: HITACHI

3.1.4 Specifying the installation directory

Specify the directory in which JP1/Software Distribution Client is to be installed. This dialog box is displayed only during a new installation. In an upgrade, JP1/Software Distribution Client is installed automatically in the existing installation directory.

Figure 3–4: Specify Installation Directory dialog box



Software Distribution Client Setup

Specify Installation Directory

Specify the directory in which you want to install Software Distribution Client.

Destination Folder: C:\Program Files\HITACHI\NETMDMP

The default installation target is `C:\Program Files\Hitachi\NETMDM` (`C:` indicates the drive on which the OS has been installed). If JP1/Software Distribution Client is to be installed on a computer that is running a 64-bit version of Windows Server 2012, Windows Server 2008 or Windows Server 2003 (x64), the default installation directory is `C:\Program Files (x86)\HITACHI\NETMDMP`. In this case, replace references in the manual to *Program Files* with *Program Files (x86)*.

To change the default installation target directory, click the **Browse** button and specify a desired directory. The following notes apply to changing the installation target directory:

- Do not specify a network drive as the installation target directory. If a network drive is specified, JP1/Software Distribution Client operation cannot be guaranteed.
- Specify the installation target directory using alphanumeric characters, spaces, and the following special characters:
  `_ \ . : ( )`
- Make sure that the installation target directory does not end with `\`. For example, do not specify `C:\NETMDM\`.
- Do not specify a drive name only as the installation target directory. For example, do not specify `C:`.
- If you are installing JP1/Software Distribution Client on a multiboot PC (one that can boot to different OSs), use a different installation target directory for each OS. Sharing the same installation target directory among multiple OSes may result in abnormal operation.

3.1.5 Selecting the type

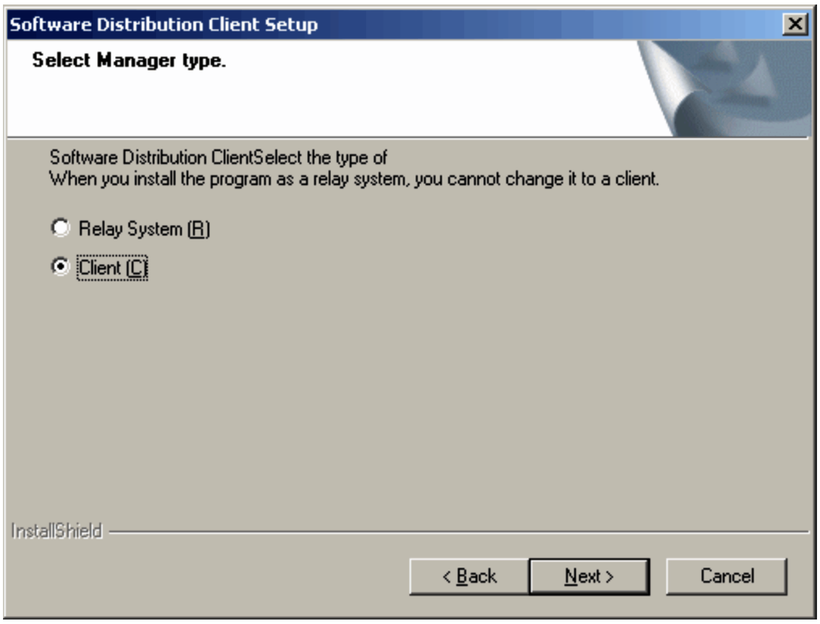
Select the type of JP1/Software Distribution Client. To use it as a relay system, select **Relay System**; to use it as a client, select **Client**.

Note that a relay system cannot be installed in the following cases.

- If the OS is Windows Me or Windows 98
- If JP1/Software Distribution Manager has been installed

In these instances, only JP1/Software Distribution Client (client) can be installed, so the Select Manager type dialog box is not displayed.

Figure 3–5: Select Manager type dialog box



Software Distribution Client Setup

Select Manager type.

Software Distribution ClientSelect the type of
When you install the program as a relay system, you cannot change it to a client.

○ Relay System (R)

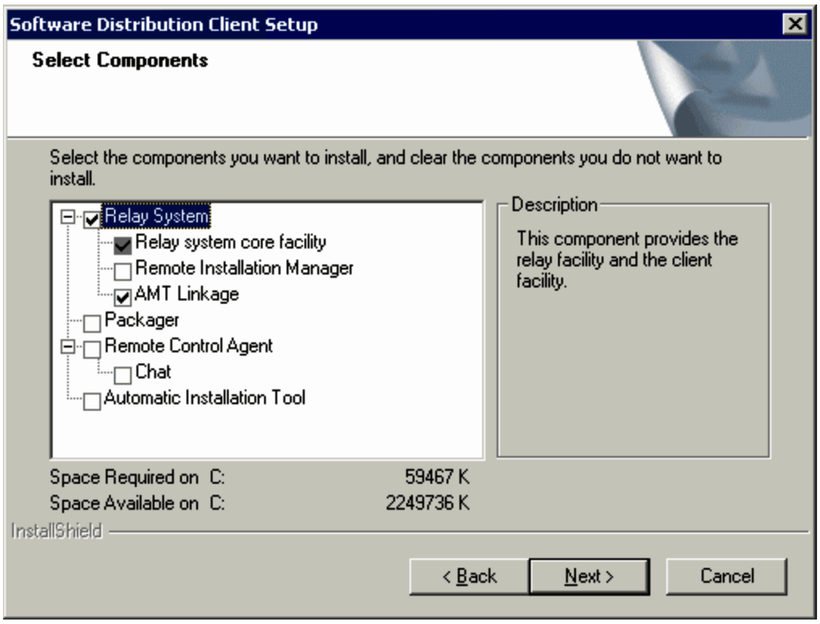
● Client (C)

3.1.6 Selecting the components

Select the components or subcomponents you wish to install. In the case of an upgrade, you can add components or subcomponents, but you cannot delete any installed components or subcomponents. The components displayed for **Relay System** are different from those for **Client**.

(1) Components displayed for Relay system

Figure 3–6: Select Components dialog box (for relay system)



Software Distribution Client Setup

Select Components

Select the components you want to install, and clear the components you do not want to install.

- ☑ Relay System
  - ☑ Relay system core facility
  - □ Remote Installation Manager
  - ☑ AMT Linkage
- □ Packager
- □ Remote Control Agent
  - □ Chat
- □ Automatic Installation Tool

Description

This component provides the relay facility and the client facility.

Space Required on C: 59467 K

Space Available on C: 2249736 K

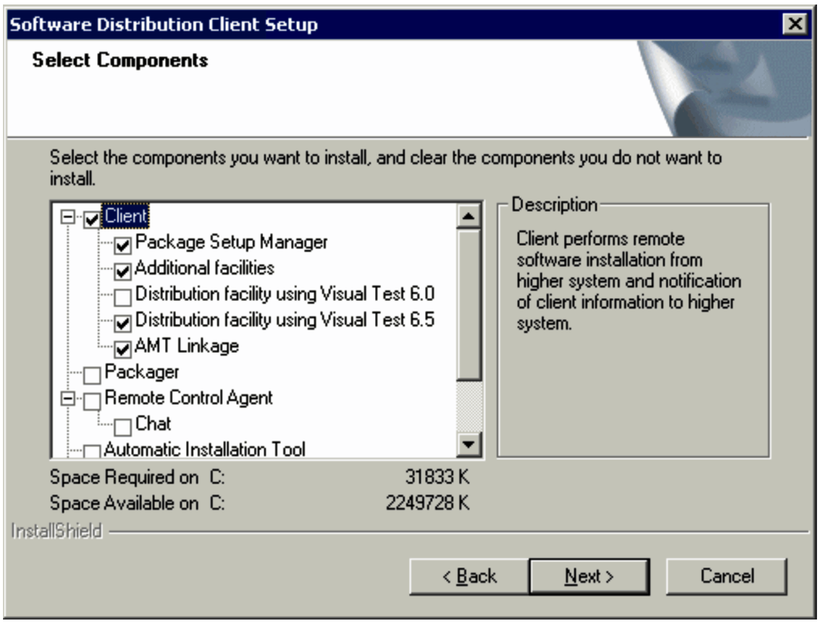
The subcomponents are displayed in a tree hierarchy under the component name.

You should note the following about selecting components:

- If you select **Relay system core facility**, **Client** is installed unconditionally.
- To select **Remote Installation Manager** under **Relay System**, you must select **Relay System**.

(2) Components displayed for Client

Figure 3–7: Select Components dialog box (for client)



Software Distribution Client Setup

Select Components

Select the components you want to install, and clear the components you do not want to install.

- ☑ Client
  - ☑ Package Setup Manager
  - ☑ Additional facilities
  - □ Distribution facility using Visual Test 6.0
  - ☑ Distribution facility using Visual Test 6.5
  - ☑ AMT Linkage
- □ Packager
- □ Remote Control Agent
  - □ Chat
- □ Automatic Installation Tool

Description

Client performs remote software installation from higher system and notification of client information to higher system.

Space Required on C: 31833 K

Space Available on C: 2249728 K

The subcomponents are displayed in a tree hierarchy under the component name.

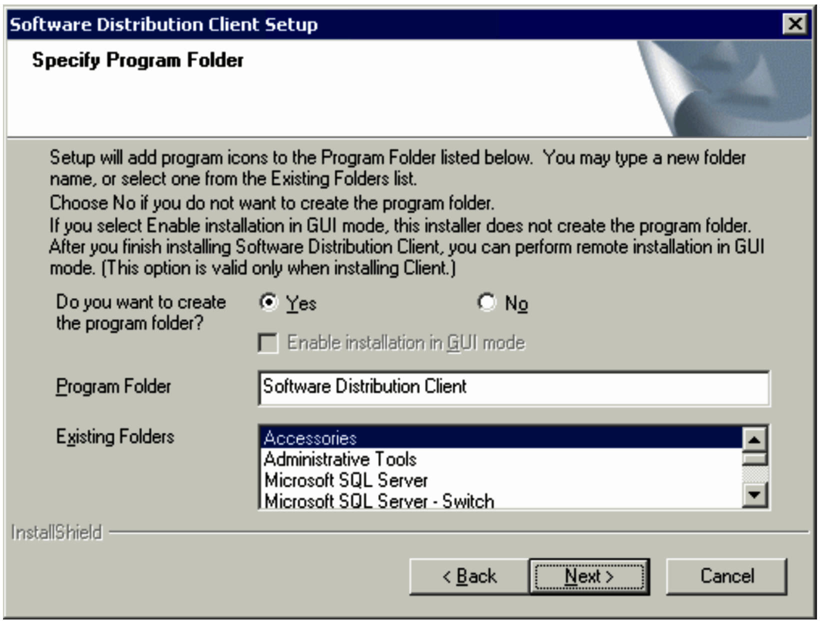
You should note the following about selecting components:

- To select the subcomponents of Client, you must select **Client**.
- You cannot install only online Help.
- You cannot install the Remote Control Agent of JP1/Software Distribution Client on a PC where JP1/Remote Control Agent has been installed. If you wish to install the Remote Control Agent of JP1/Software Distribution Client, you must uninstall JP1/Remote Control Agent and then install the Remote Control Agent.
- You can install only one of the following: **Distribution facility using Visual Test 6.0** or **Distribution facility using Visual Test 6.5**. Select the facility that corresponds to the version of Visual Test used in the environment in which you want to install JP1/Software Distribution Client.
- If you are installing JP1/Software Distribution Client (client) in a Windows XP Mode environment, some components will not be available. For more information about components that can be used, see *C.1 Notes on installation and setup of JP1/Software Distribution Client (client) in a Windows XP Mode environment*.

3.1.7 Selecting the program folder

Select the program folder in which the JP1/Software Distribution Client icon is to be registered. The Specify Program Folder dialog box appears only during new installation or if you are overwriting the program in an environment in which no program folder has been created. In the case of program overwriting, the existing program folder is used automatically.

Figure 3–8: Specify Program Folder dialog box



Software Distribution Client Setup

Specify Program Folder

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the Existing Folders list.
Choose No if you do not want to create the program folder.
If you select Enable installation in GUI mode, this installer does not create the program folder.
After you finish installing Software Distribution Client, you can perform remote installation in GUI mode. (This option is valid only when installing Client.)

Do you want to create the program folder? ● Yes ○ No

□ Enable installation in GUI mode

Program Folder: Software Distribution Client

Existing Folders:
Accessories
Administrative Tools
Microsoft SQL Server
Microsoft SQL Server - Switch

The default is that **Yes** is selected and the icon is registered in the **Software Distribution Client** group. You can select an existing program folder or you can create a new program folder. Note that you cannot specify a program folder name that includes a backslash (\).

If you select **No** when installing Client, packages in the GUI installation mode can no longer be installed. To install packages in the GUI installation mode without creating a program folder, take one of the following actions:

- Select the **Enable installation in GUI mode** check box.

  If you select this option, you will be able to use the GUI installation mode. Note that you can select the **Enable installation in GUI mode** option only when **Client** is being installed. When you are installing **Relay system**, this check box is not displayed.

  When you select the **Enable installation in GUI mode** option, no program folder is created, but the Software Distribution Client Startup folder is created. For details about the Software Distribution Client Startup folder, see *3.1.13 Specifying options*.
- After installation has been completed, execute `dmpsetup.exe` in *JP1/Software-Distribution-Client-installation-directory*`\BIN`.

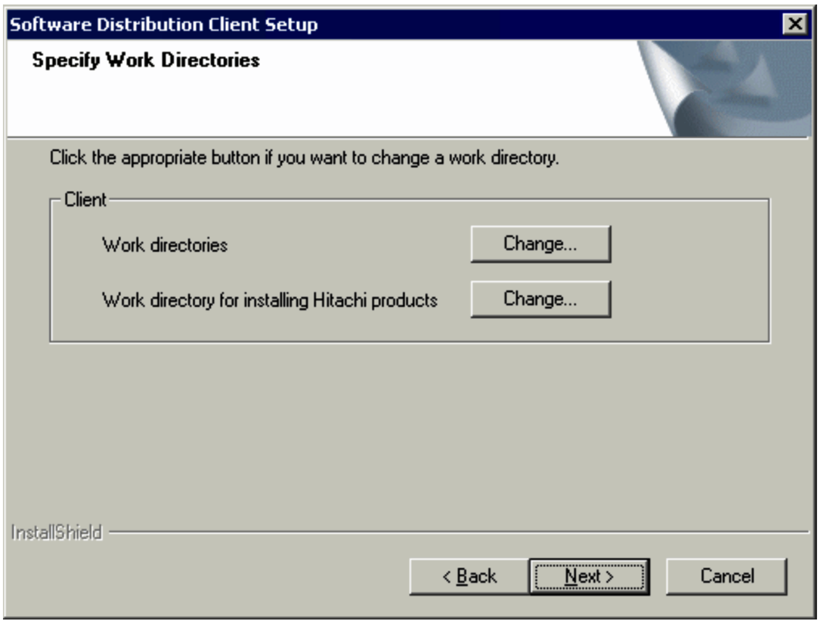
3.1.8 Specifying work directories

When **Relay System** or **Client** is being installed, the Specify Work Directories dialog box appears. Depending on the component to be installed, **Relay system** or **Client** is displayed.

Clicking the **Change** button to the right of each item lets you change that work directory. Express a work directory as alphanumeric characters, spaces, and the following special characters:

`_ \ . : ( )`

Figure 3–9: Specify Work Directories dialog box



Software Distribution Client Setup

Specify Work Directories

Click the appropriate button if you want to change a work directory.

Client

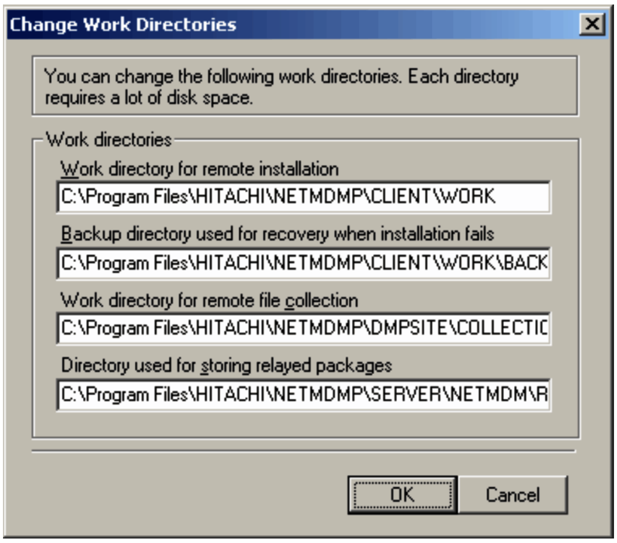
Work directories

Work directory for installing Hitachi products

(1) Change Work Directories

This dialog box displays each default work directory that is used during remote installation of the relay system or client. Changing a directory and then clicking the **OK** button displays the Specify Work Directories dialog box again. If you change these default work directories, set a directory for each purpose. Do not use those directories for any other purposes.

Figure 3–10: Change Work Directories dialog box



Change Work Directories

You can change the following work directories. Each directory requires a lot of disk space.

Work directories

Work directory for remote installation: C:\Program Files\HITACHI\NETMDMP\CLIENT\WORK

Backup directory used for recovery when installation fails: C:\Program Files\HITACHI\NETMDMP\CLIENT\WORK\BACK

Work directory for remote file collection: C:\Program Files\HITACHI\NETMDMP\DMPSITE\COLLECTIC

Directory used for storing relayed packages: C:\Program Files\HITACHI\NETMDMP\SERVER\NETMDM\R

Work directory for remote installation

This directory is used by the relay system or client for installing packages. It requires the same amount of space as any package that is to be installed. Normally, you should specify a directory with at least 50 MB of free space.

Backup directory used for recovery when installation fails

This directory is used for saving a backup of software to be remote-installed by the relay system or client.

Work directory for remote file collection

This directory retains the collected files that are collected by executing a *Collect files from client to relay system* job until the managing server executes an *Acquire collected files from relay system* job or a *Delete collected files from relay system* job. This information is not displayed for Client.

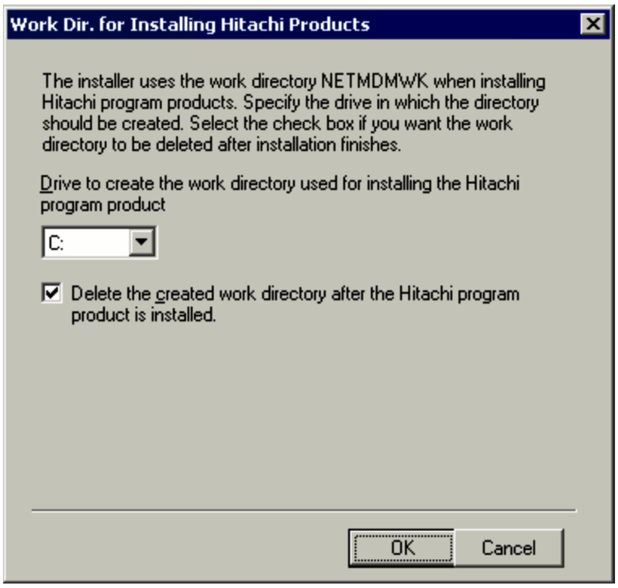
Directory used for storing relayed packages

This directory is used by the relay system to store packages. This directory retains packages that are transferred from the managing server until they are automatically deleted due to the **Package expiration at the relay system**. This information is not displayed for Client.

(2) Work Dir. for Installing Hitachi Products

You can change the drive of the work directory for installing Hitachi program products (`NETMDMWK` directory). Clicking the **OK** button after specifying the settings displays the Specify Work Directories dialog box again.

Figure 3–11: Work Dir. for Installing Hitachi Products dialog box



Work Dir. for Installing Hitachi Products

The installer uses the work directory NETMDMWK when installing Hitachi program products. Specify the drive in which the directory should be created. Select the check box if you want the work directory to be deleted after installation finishes.

Drive to create the work directory used for installing the Hitachi program product

C:

☑ Delete the created work directory after the Hitachi program product is installed.

Drive to create the work directory used for installing the Hitachi program product

Select the drive in which you wish to create the directory used for installing Hitachi program products. The `NETMDMWK` directory is created directly under the selected drive. Do not specify a network drive; if a network drive is specified, operations cannot be guaranteed.

Delete the created work directory after the Hitachi program product is installed.

You can choose whether or not to delete the directory after the Hitachi program product has been installed. To delete the directory, select the **Delete the created work directory after the Hitachi program product is installed** check box. This option is selected as the default. The following points should be noted about selecting the **Delete the created work directory after the Hitachi program product is installed** check box:

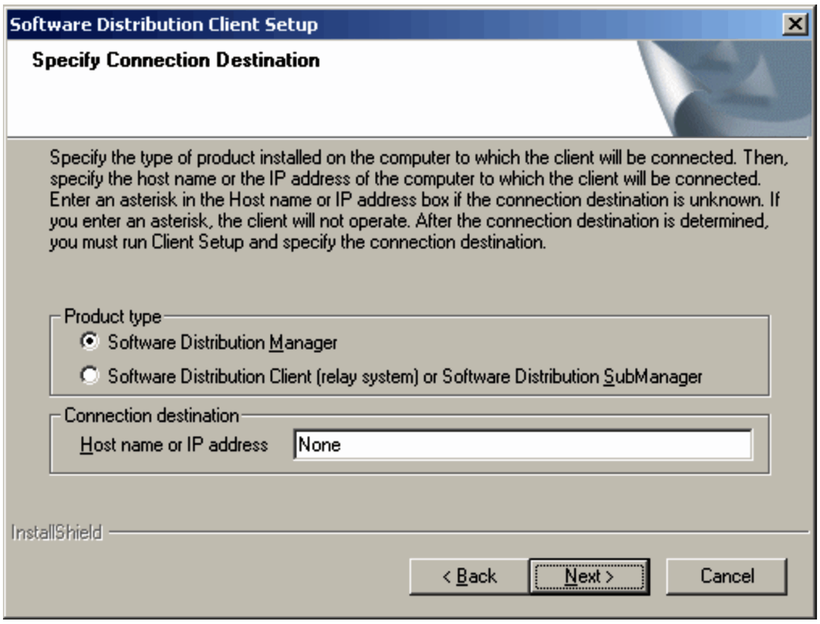
- In Windows NT, you must have the appropriate permissions to read, write, and delete the created drive in order to select the **Delete the created work directory after the Hitachi program product is installed** check box. If these permissions have not been granted, installation of a Hitachi program product will fail.
- Even though the **Delete the created work directory after the Hitachi program product is installed** check box has been selected, the `NETMDMWK` directory may remain after installation. In such a case, the directory will be deleted when the computer is restarted or during polling.

3.1.9 Specifying the connection destination

Specify the higher system to which the relay system or client is to be connected. The Specify Connection Destination dialog box is displayed when **Relay System** or **Client** is being installed.

You can change this connection destination during setup.

Figure 3–12: Specify Connection Destination dialog box



Software Distribution Client Setup

Specify Connection Destination

Specify the type of product installed on the computer to which the client will be connected. Then, specify the host name or the IP address of the computer to which the client will be connected. Enter an asterisk in the Host name or IP address box if the connection destination is unknown. If you enter an asterisk, the client will not operate. After the connection destination is determined, you must run Client Setup and specify the connection destination.

Product type

● Software Distribution Manager

○ Software Distribution Client (relay system) or Software Distribution SubManager

Connection destination

Host name or IP address: None

Product type

Specify either **Software Distribution Manager**, **Software Distribution Client (relay system) or Software Distribution SubManager** as the product type of the higher system to which the relay system or client is to be connected. The default is **Software Distribution Manager**.

Connection destination

The available settings for a relay system differ from those for a client.

For a relay system

Specify the name of the higher system to which the relay system connects, expressed as a node identification key used by the higher system (**Host name or IP address**). The default is **None**. A local host name cannot be specified for the connection destination.

For a client

Specify the host name or IP address of the connection destination for the client. The default is **None**. If the client's connection destination is undetermined, or to use the client as an offline machine for inventory management, specify `?`. A client with `?` specified for **Connection destination** supports only the Local System Viewer and the system monitoring facility. To use other facilities, the client must connect to a higher system.

To create a PC environment that is to be the source of a hard disk copying operation for installation of JP1/Software Distribution Client using the pre-installation facility, specify `*` as the connection destination, in which case the client will not actually operate.

If you specify any value other than `*` as the connection destination and you use the host ID, only the last client is recognized during automatic registration of the system configuration; no other clients will be recognized.

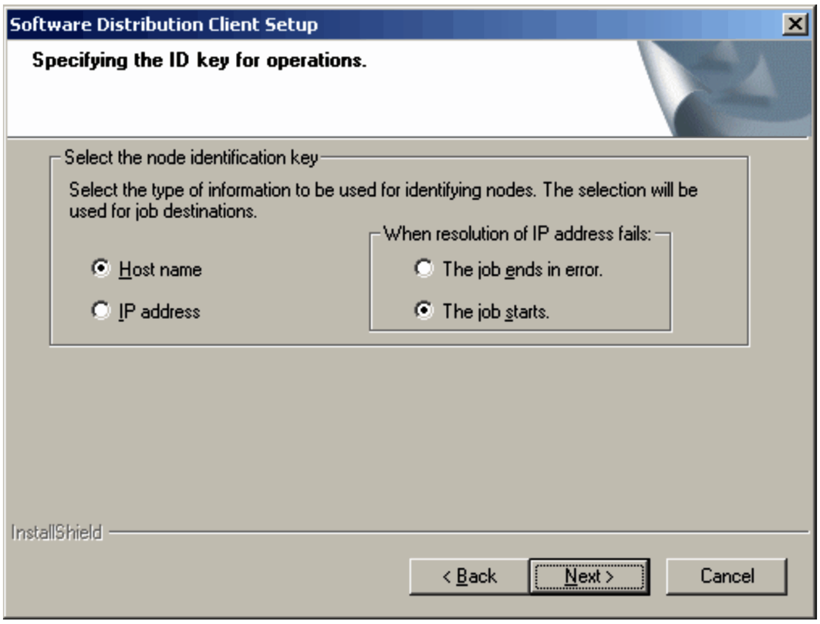
If you specified a connection destination once and are now installing the client by overwriting the setting, you can specify `?`, but you cannot specify `*`. To specify `*`, you must either uninstall the client and then install it again, or change the connection destination to `*` during setup and then install the client again.

3.1.10 Specifying the ID key for operations

Specify the key (ID key for operations) used to manage hosts on the network and identify the destination. This dialog box is displayed when Relay system is installed.

You can change these settings during setup.

Figure 3–13: Specify ID Key for Operations dialog box



Software Distribution Client Setup

Specifying the ID key for operations.

Select the node identification key

Select the type of information to be used for identifying nodes. The selection will be used for job destinations.

● Host name

○ IP address

When resolution of IP address fails:

○ The job ends in error.

● The job starts.

The two types of ID key for operations are node identification keys and host IDs. In **Select the node identification key**, select the node identification key.

Select the node identification key

Select **Host name** or **IP address** as the type of information that terminates the communication target during host-to-host communication. This specification must be appropriate to the ID key settings of the target host. The default is **Host name**. If you select **Host name**, set **When resolution of IP address fails**.

When resolution of IP address fails

Select whether or not a job is to result in an error if a destination address cannot be resolved during job execution. The default is **The job starts**. If **The job starts** is selected, the execution status of a job that cannot resolve an address will be set to `Waiting for transmission`. The status of a job with a nonexistent destination also remains as `Waiting for transmission`.

If the client PC's power is off during job execution in an environment in which a WINS server is used, the destination address cannot be resolved. The **The job ends in error** setting does not support installation that involves polling at system startup when a job is executed on holidays and at night. In such a case, select **The job starts.**

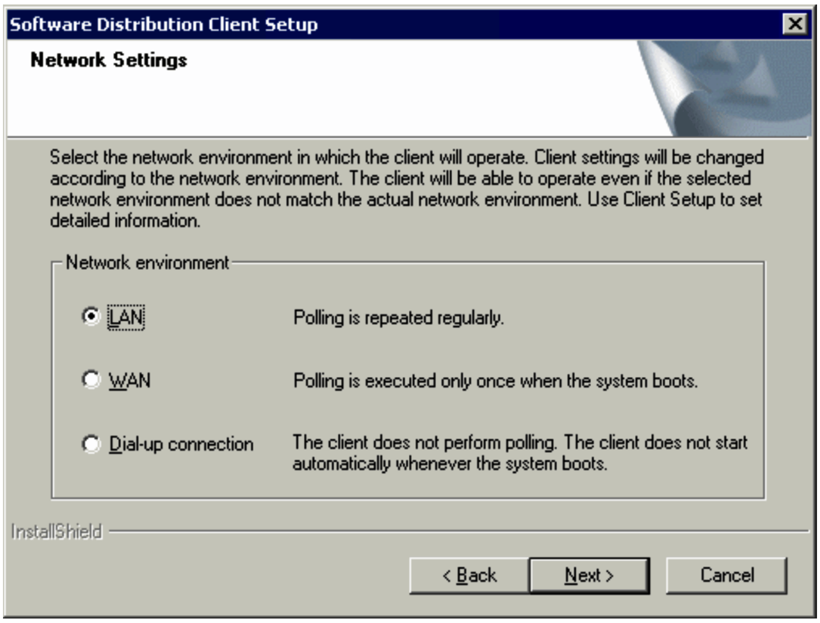
If **The job starts.** is selected and the executed job contains a destination whose address cannot be resolved, system operation may be affected adversely, such as operation of Remote Installation Manager slows down.

3.1.11 Setting the network

Select the network environment in which the client will operate. The timing for polling a higher system is set according to the selected network environment. The Network Settings dialog box is displayed when **Client** is installed.

You can change the polling timing settings during setup.

Figure 3–14: Network Settings dialog box



Software Distribution Client Setup

Network Settings

Select the network environment in which the client will operate. Client settings will be changed according to the network environment. The client will be able to operate even if the selected network environment does not match the actual network environment. Use Client Setup to set detailed information.

Network environment

● LAN	Polling is repeated regularly.
○ WAN	Polling is executed only once when the system boots.
○ Dial-up connection	The client does not perform polling. The client does not start automatically whenever the system boots.

LAN

Sets polling to every 30 minutes.

WAN

Sets polling to only when the client starts.

Dial-up connection

Sets that polling is not to be performed.

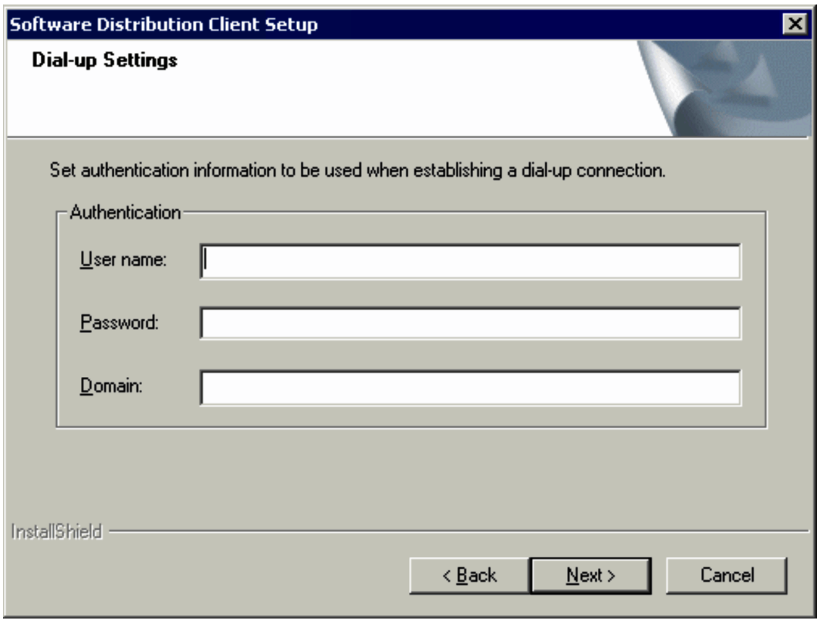
If you select **Dial-up connection**, clicking the **Next** button displays the Dial-up Settings dialog box. If you select **LAN** or **WAN**, clicking the **Next** button displays the Set Options dialog box.

3.1.12 Specifying the dial-up settings

Specify authentication information that is to be used by the client for dial-up connection.

You can change these settings during setup.

Figure 3–15: Dial-up Settings dialog box



Software Distribution Client Setup

Dial-up Settings

Set authentication information to be used when establishing a dial-up connection.

Authentication

User name:

Password:

Domain:

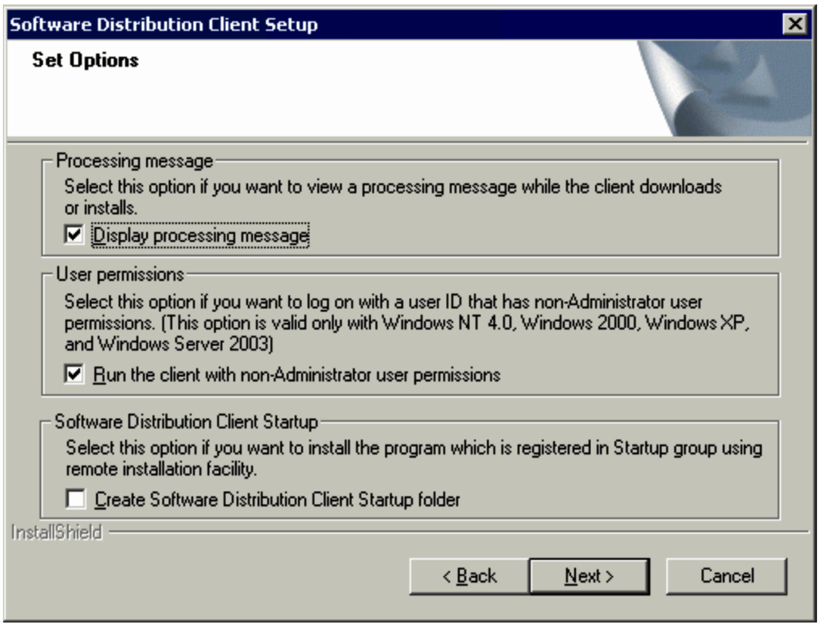
Specify **User name**, **Password**, and **Domain**.

3.1.13 Specifying options

Specify whether or not processing messages are to be displayed and whether or not user permissions (non-Administrator user permissions) are to be used with the client. The Set Options dialog box is displayed when **Client** is being installed.

You can change these settings during setup.

Figure 3–16: Set Options dialog box



Software Distribution Client Setup

Set Options

Processing message

Select this option if you want to view a processing message while the client downloads or installs.

☑ Display processing message

User permissions

Select this option if you want to log on with a user ID that has non-Administrator user permissions. (This option is valid only with Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003)

☑ Run the client with non-Administrator user permissions

Software Distribution Client Startup

Select this option if you want to install the program which is registered in Startup group using remote installation facility.

☐ Create Software Distribution Client Startup folder

Processing message

Specify whether or not the client is to display processing messages during operations such as downloading and installation. The default is for the **Display processing message** check box to be selected.

User permissions

In the case of a Windows NT client, you can specify settings so that any user can install packages whether or not the user has installed the client.

If you select the **Run the client with non-Administrator user permissions** check box, packages can be installed in the GUI installation mode even when the user who installed the client is not logged on. This means that a user without Administrator permissions (non-Administrator user) can install packages. The default is for the **Run the client with non-Administrator user permissions** check box to be selected.

For details about installation with non-Administrator user permissions, see *11.2.3 Installing software using non-Administrator user permissions under Windows NT* in the manual *Administrator's Guide Volume 1*.

In the case of a Windows Me or Windows 98 client, this setting is disabled. The client is available regardless of the login user's permissions.

Software Distribution Client Startup

Specify whether or not the `Software Distribution Client Startup` folder is to be created.

You can move programs registered in the Windows **Startup** group to the `Software Distribution Client Startup` folder. By moving the programs, you can avoid a remote installation error that may result from duplication of programs registered in the **Startup** group and programs for which installation at system startup is specified with JP1/Software Distribution.

To create the `Software Distribution Client Startup` folder, select the **Create Software Distribution Client Startup folder** check box. The default is for this operation to not be selected.

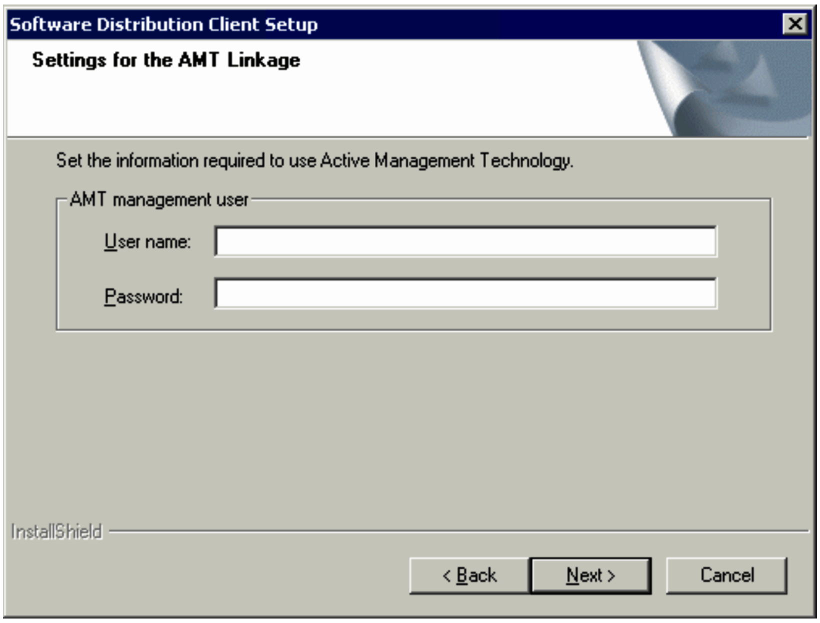
For details about moving startup programs, see *11.2.2 Preparing to install software during system startup* in the manual *Administrator's Guide Volume 1*.

If you select **No** in the Specify Program Folder dialog box and do not select the **Enable installation in GUI mode** option, you cannot create the `Software Distribution Client Startup` folder.

3.1.14 Setting up AMT Linkage

Set information that is needed for controlling the client using AMT Linkage.

Figure 3–17: Settings for the AMT Linkage dialog box



Software Distribution Client Setup

Settings for the AMT Linkage

Set the information required to use Active Management Technology.

AMT management user

User name:

Password:

AMT management user

Sets the information needed to access the client's AMT. The user name and password must match the client's settings.

User name

Specifies the user name used to access the client's AMT, expressed as up to 60 characters.

Password

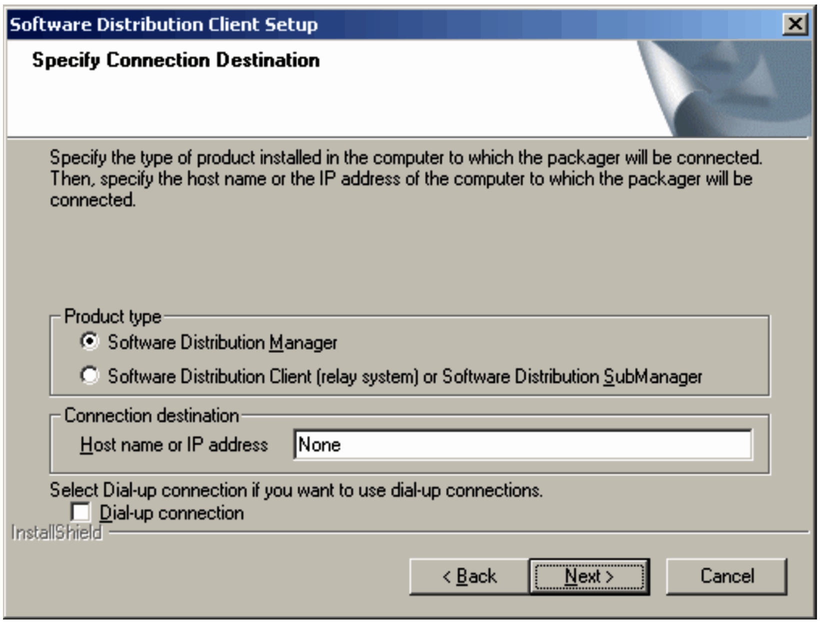
Specifies the password used to access the client's AMT, expressed as up to 60 characters.

3.1.15 Specifying the connection destination (Packager)

Specify the connection destination of the Packager. The Specify Connection Destination dialog box is displayed when the Packager is being installed.

You can change these settings in the Software Distribution Manager Logon dialog box of the Software Distribution Packager window.

Figure 3–18: Specify Connection Destination dialog box



Software Distribution Client Setup

Specify Connection Destination

Specify the type of product installed in the computer to which the packager will be connected. Then, specify the host name or the IP address of the computer to which the packager will be connected.

Product type

● Software Distribution Manager

○ Software Distribution Client (relay system) or Software Distribution SubManager

Connection destination

Host name or IP address: None

Select Dial-up connection if you want to use dial-up connections.

□ Dial-up connection

Product type

Select either **Software Distribution Manager**, **Software Distribution Client (relay system) or Software Distribution SubManager** as the connection destination of the Packager. The default is **Software Distribution Manager**.

Connection destination

Specify the host name or IP address of the connection destination of the Packager. The default is **None**.

Dial-up connection

If the Packager is to use dial-up connection to connect to the higher system, select this check box. The default is that the check box is not selected.

This check box is displayed only for a client; it is not displayed for a relay system.

Click the **Next** button to continue with installation. If you selected **Dial-up connection**, the Dial-up Settings dialog box appears; the settings are the same as when **Client** uses dial-up connection. For details, see *3.1.12 Specifying the dial-up settings*. You must set up the dial-up connection for the Packager separately from the dial-up connection for the client. You can use dial-up connection for only one of them.

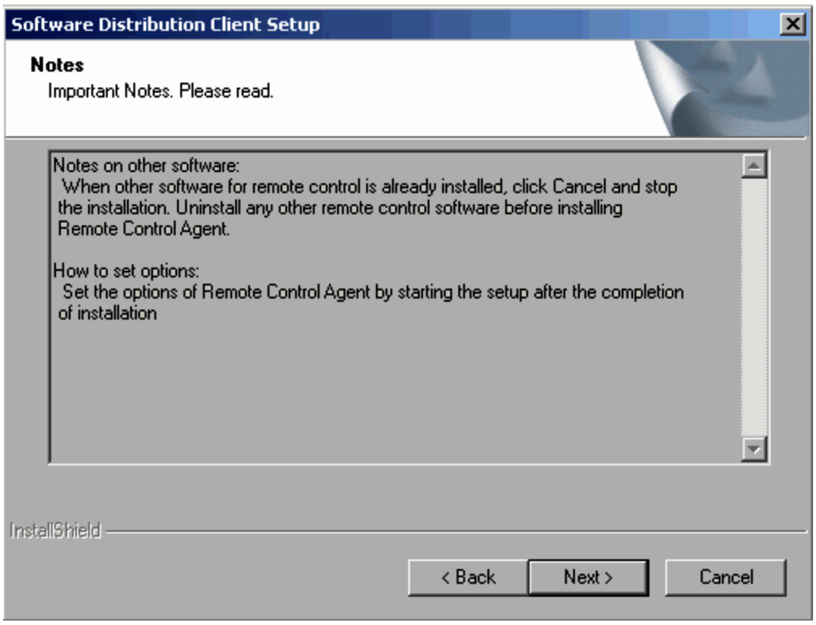
3.1.16 Checking the Notes for the Remote Control Agent

When you install a new Remote Control Agent, the Notes dialog box appears.

The contents of this dialog box depend on whether Remote Control Agent is installed on a Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP, or Windows 2000 system or on a Windows NT 4.0, Windows Me, or Windows 98 system.

- Installing Remote Control Agent on Windows 8, Windows Server 2012, Windows 7, Wndows Server 2008, Windows Vista, Windows Server 2003, Windows XP, or Windows 2000

Figure 3–19: Notes dialog box (for installation on Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP, or Windows 2000)



Software Distribution Client Setup

Notes

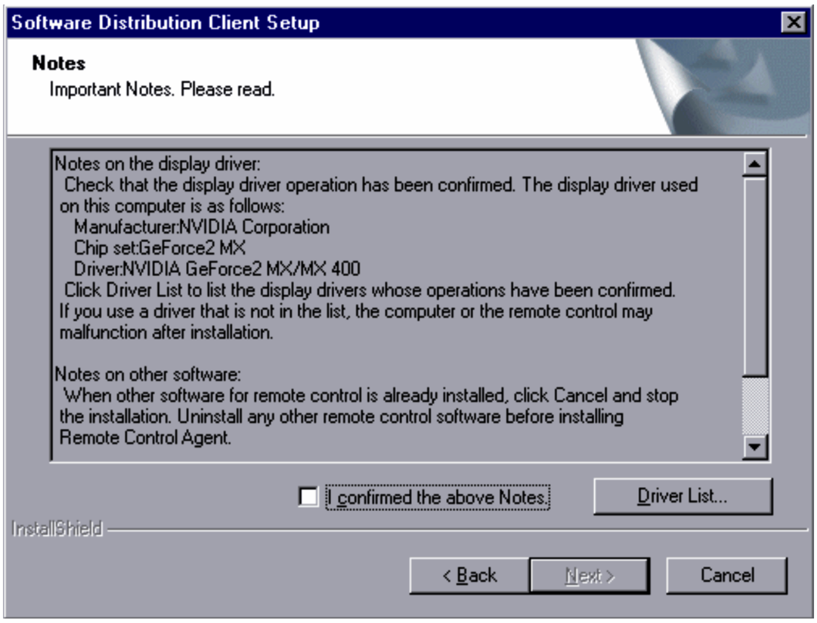
Important Notes. Please read.

Notes on other software:
When other software for remote control is already installed, click Cancel and stop the installation. Uninstall any other remote control software before installing Remote Control Agent.

How to set options:
Set the options of Remote Control Agent by starting the setup after the completion of installation

- Installing Remote Control Agent on Windows NT 4.0, Windows Me, or Windows 98

Figure 3–20: Notes dialog box (for installation on Windows NT 4.0, Windows Me, or Windows 98)



Software Distribution Client Setup

Notes

Important Notes. Please read.

Notes on the display driver:
Check that the display driver operation has been confirmed. The display driver used on this computer is as follows:
Manufacturer:NVIDIA Corporation
Chip set:GeForce2 MX
Driver:NVIDIA GeForce2 MX/MX 400
Click Driver List to list the display drivers whose operations have been confirmed.
If you use a driver that is not in the list, the computer or the remote control may malfunction after installation.

Notes on other software:
When other software for remote control is already installed, click Cancel and stop the installation. Uninstall any other remote control software before installing Remote Control Agent.

□ I confirmed the above Notes.

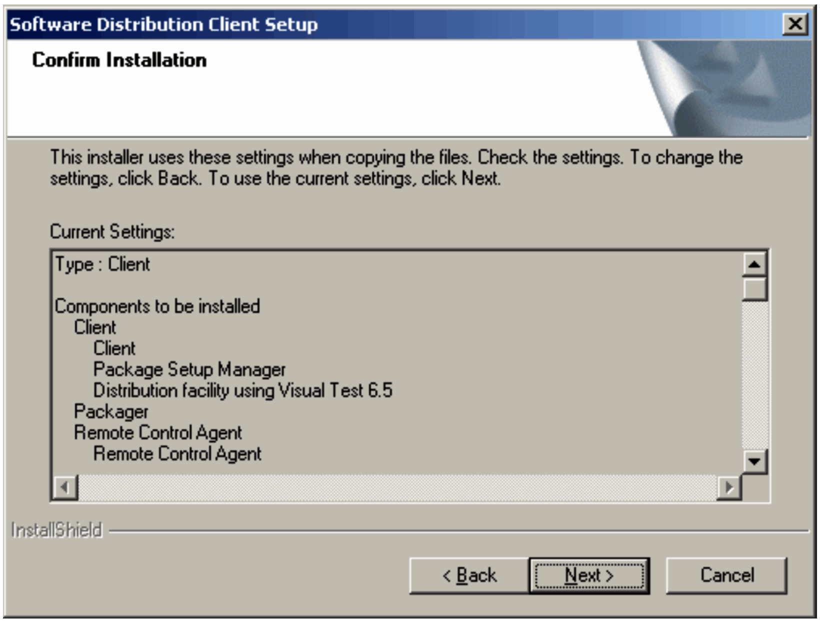
For details about the notes, see the *Job Management Partner 1/Remote Control Description and Operator's Guide*.

For Windows NT 4.0, Windows Me, or Windows 98, after checking the notes, select the **I confirmed the above Notes** check box.

3.1.17 Confirming the installation

The Confirm Installation dialog box displays the specified component settings. Check the displayed information.

Figure 3–21: Confirm Installation dialog box



Software Distribution Client Setup

Confirm Installation

This installer uses these settings when copying the files. Check the settings. To change the settings, click Back. To use the current settings, click Next.

Current Settings:

```
Type : Client

Components to be installed
  Client
    Client
    Package Setup Manager
    Distribution facility using Visual Test 6.5
  Packager
  Remote Control Agent
    Remote Control Agent
```

If you need to change a setting, click the **Back** button to display the corresponding dialog box and make the change.

If no changes are needed, click the **Next** button. The system starts installation.

If the installation fails, the system attempts reinstallation automatically. When the Software Distribution Client Setup dialog box appears, start over from *3.1.3 Registering the user*. If installation still fails, execute the InstallShield environment deletion tool and then reinstall JP1/Software Distribution Client.

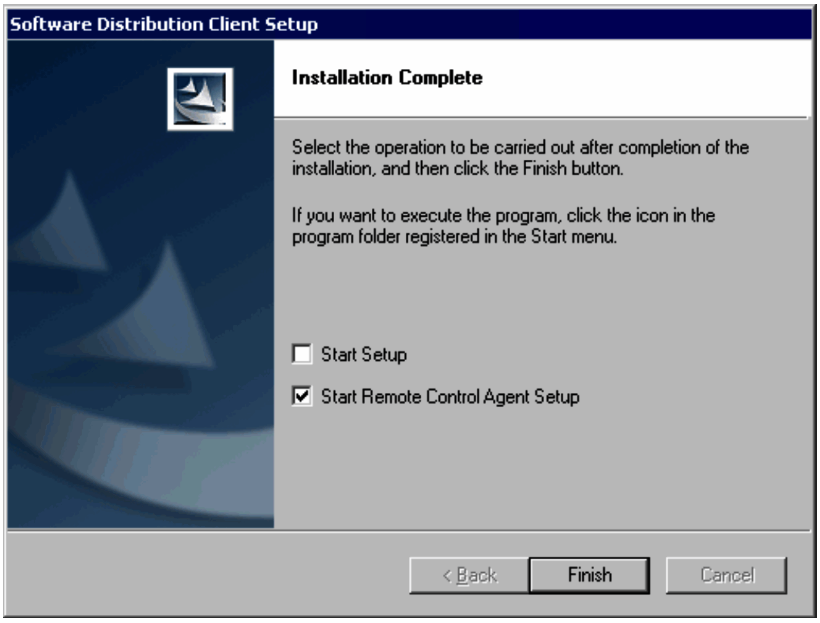
For details about how to reinstall JP1/Software Distribution Client, see *3.2 Handling JP1/Software Distribution Client installation errors*.

3.1.18 Finishing the installation

When installation is complete, the Installation Complete dialog box appears. There are two Installation Complete dialog boxes, and the one that is appropriate to the installation status is displayed.

- When the status is normal

Figure 3–22: Installation Complete dialog box (for normal operation)



Select the operation to be carried out after completion of the installation, and then click the Finish button.

If you want to execute the program, click the icon in the program folder registered in the Start menu.

□ Start Setup

☑ Start Remote Control Agent Setup

Select the **Start Setup** or **Start Remote Control Agent Setup** check box as the operation to be performed after installation is completed, and then click the **Finish** button.

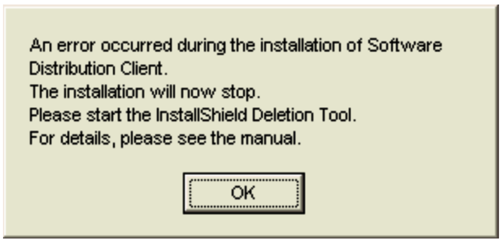
- When restart is required

  If system restart is required after installation, a dialog box appears that lets you select whether you wish to restart now or later. The displayed information is the same as for JP1/Software Distribution Manager. Select whether you wish to restart now or later, remove the CD-ROM from the CD-ROM drive, and then click the **Finish** button.

3.2 Handling JP1/Software Distribution Client installation errors

If a new installation of JP1/Software Distribution Client fails, the system attempts reinstallation automatically. If an error occurs during reinstallation, installation processing is cancelled. When reinstallation fails, the following dialog box appears:

Figure 3–23: Dialog box that is displayed when reinstallation fails



An error occurred during the installation of Software Distribution Client.
The installation will now stop.
Please start the InstallShield Deletion Tool.
For details, please see the manual.

To reinstall JP1/Software Distribution Client, click the **OK** button and then execute the InstallShield environment deletion tool. The InstallShield environment deletion tool is stored under the `disk1` folder in the installation medium.

- JP1/Software Distribution Client tool: `delisclt.exe`

When execution of the InstallShield environment deletion tool is completed, reinstall JP1/Software Distribution Client.

4 Setting Up JP1/Software Distribution Manager

This chapter explains how to set up JP1/Software Distribution Manager.

Only a user with Administrator permissions can set up JP1/Software Distribution Manager.

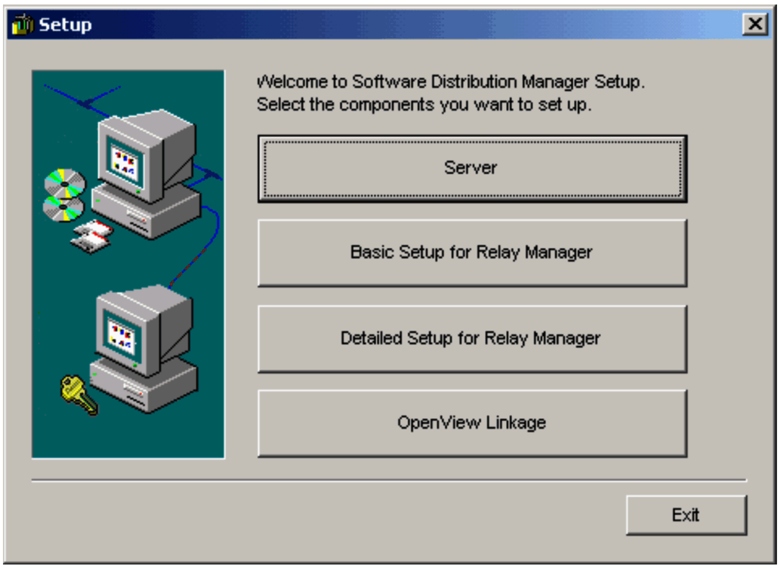
4.1 JP1/Software Distribution Manager setup procedure

This section describes the setup procedure for JP1/Software Distribution Manager.

To set up JP1/Software Distribution Manager:

1. From the **Start** menu, choose **Software Distribution Manager**, and then **Setup**.
   The Setup dialog box appears:

   Figure 4–1: Setup dialog box



Setup

Welcome to Software Distribution Manager Setup.
Select the components you want to set up.

Server
Basic Setup for Relay Manager
Detailed Setup for Relay Manager
OpenView Linkage
Exit

2. Click the button of the component you wish to set up.
   The setup program for the selected component starts. At the central manager, you can set up the Server component. At a relay manager, you can set up the Server, Basic Setup for Relay Manager, and Detailed Setup for Relay Manager components.
3. When you finish with the setup, click the **Exit** button.
   The setup is complete.

The following sections describe how to set up each component.

For details about the setup of Asset Information Manager Subset, see *10. Settings Required for Using Asset Information Manager Subset*.

4.2 Setting up the server

Specify necessary information on each page of the Server Setup dialog box. When you finish, click the **OK** button. The Setup dialog box is displayed again.

To update Server settings, after you finish with the JP1/Software Distribution Manager setup, open **Control Panel**, choose **Administrative Tools**, and then choose **Services** to restart the Remote Install Server service.

The table below describes the Server setup items. If you have installed only Remote Installation Manager, the only pages that are displayed at setup are **Database Environment**, **Communication**, **WSUS Linkage**, and **Audit Log**.

Table 4–1: Server setup items

Classification	Item
Database Environment	Relational database settings (host name of database server, database name, administrator ID, and password)
Communication	Port numbers, startup protocol, interval transfer
Dial-up[#1]	Authentication (user name, password, and domain)
Server Customization	Number of subsystems that can be connected at one time
	Maximum number of subsystems in which jobs can execute concurrently
	When jobs will be deleted
	Monitor startup of subsystems
	Monitor file transfer errors of subsystems
	Accept suspended/resumed file transfer jobs from sources other than the connection destination
Multicast Distribution	Port numbers for multicast distribution and settings for sending jobs by multicast distribution (multicast address and packet size)
Log Options	Record the results of jobs
	Record the results of ID group jobs
	Record the results of all-lower-clients jobs
System Configuration	Apply system configuration information automatically
	Linkage when system configuration is changed
	Deletion history of system configuration information
ID Key for Operations	Select the node identification key
	Resolving IP addresses
	When resolution of IP address fails
	Use host IDs
Cluster Settings[#2]	Enable the cluster system
HP OpenView Linkage[#3]	Activate OpenView Linkage
	Host name or IP address and port number of HP NNM
	Update the system configuration of HP NNM
Event Service	Enable the event service
Error Handling	Generations of log file to be saved
	Maximum lines in a log file

Classification	Item
Error Handling	Type of Event Viewer message
Client Alert[#4]	Relay client alert information to higher system
	Output of client alert information (to CSV file or Event Viewer)
Operation Monitoring	Saving operation monitoring logs
	Backing up operation histories
	Storing operating information in the JP1/Software Distribution relational database
	Timing of automatic storage of operating information in the JP1/Software Distribution relational database
	Outputting status of operation history storage in database
Network connection	Authentication information (login ID, password, domain name)
CSC Linkage	Deletion of *Report message* jobs that were executed from JP1/Client Security Control
WSUS Linkage[#5]	Use of WSUS Linkage
Directory Linkage	Linkage with Active Directory
AIM	URL of Asset Information Manager Subset or JP1/Asset Information Manager to be connected
AMT Linkage[#6]	AMT management user's user ID and password
Audit log	Output of audit logs

Y: Can be set. N: Cannot be set.

#1

This item is displayed when the remote access service is installed.

#2

This item is not displayed at relay managers.

#3

This item is displayed when OpenView Gateway Server has been installed.

#4

This item is available only on relay managers.

#5

This item is displayed only when the server's subcomponent Remote Installation Manager has been installed.

#6

This item is displayed if AMT Linkage has been installed.

4.2.1 Database Environment page

Use the **Database Environment** page to change relational database settings, if necessary.

The settings displayed on the **Database Environment** page depend on the relational database in use.

When you are using Asset Information Manager Subset, in order to change the relational database settings from the **Database Environment** page, you must reset **Create Data Source/Net Service** for Asset Information Manager Subset. For details about the creation of a data source/net service, see *10.3.8 Creating a data source or a net service*.

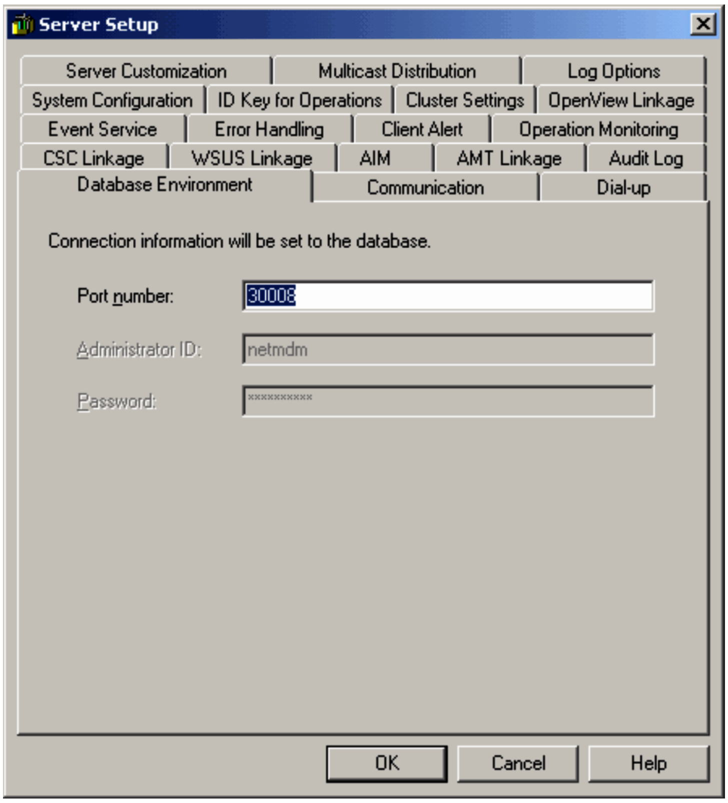
(1) Database Environment page (for Embedded RDB)

This subsection describes how to specify the settings on the **Database Environment** page when Embedded RDB is used.

The settings available on the **Database Environment** page when Server core facility has been installed differ from when only Remote Installation Manager has been installed.

Figures 4-2 and 4-3 show the **Database Environment** page when Server core facility has been installed and when only Remote Installation Manager has been installed, respectively.

Figure 4–2: Database Environment page (when Server core facility has been installed)



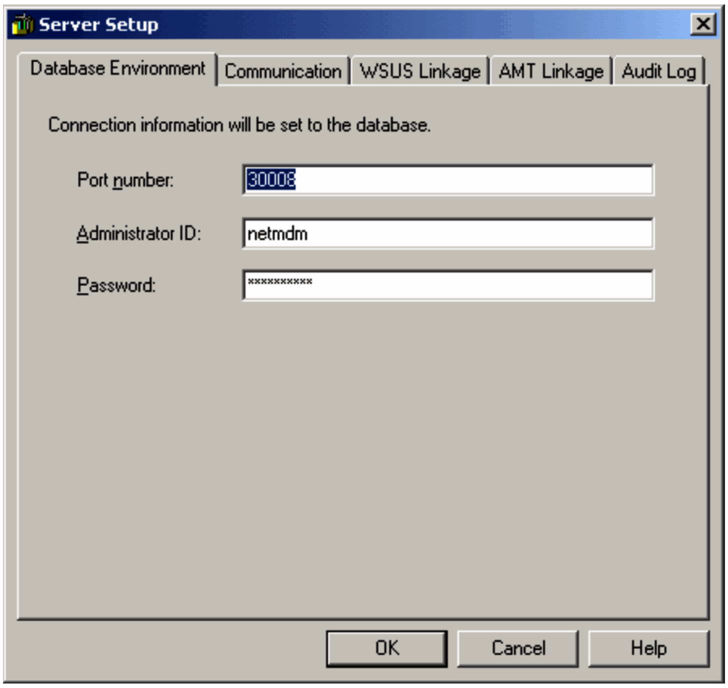
Connection information will be set to the database.

Port number: 30008

Administrator ID: netmdm

Password: **********

Figure 4–3: Database Environment page (when only Remote Installation Manager has been installed)



Connection information will be set to the database.

Port number: 30008

Administrator ID: netmdm

Password: **********

Port number

Specify the port number to be used for connecting the database, in the range from 5001 to 65535. The default is the port number specified in the Database Settings dialog box.

If you have changed the port number from the default setting, you must perform the following operations after completion of setup in order to apply the new settings:

1. Stop the Remote Install Server service.
2. Execute the `netmdb_setup.bat` command that is stored in *JP1/Software-Distribution-installation-directory*`\BIN`.

   Normally, when the `netmdb_setup.bat` command terminates, it waits for an entry from the keyboard. To enable the command to terminate without receiving an entry from the keyboard, execute the command with the `/nopause` option specified.
3. Start the Remote Install Server service.

Administrator ID

Specify the administrator ID to be used to log on to the database. The default is the administrator ID that was specified during installation.

This item is enabled when only Remote Installation Manager has been installed.

Password

Specify the password to be used to log on to the database. The default is the password specified during installation.

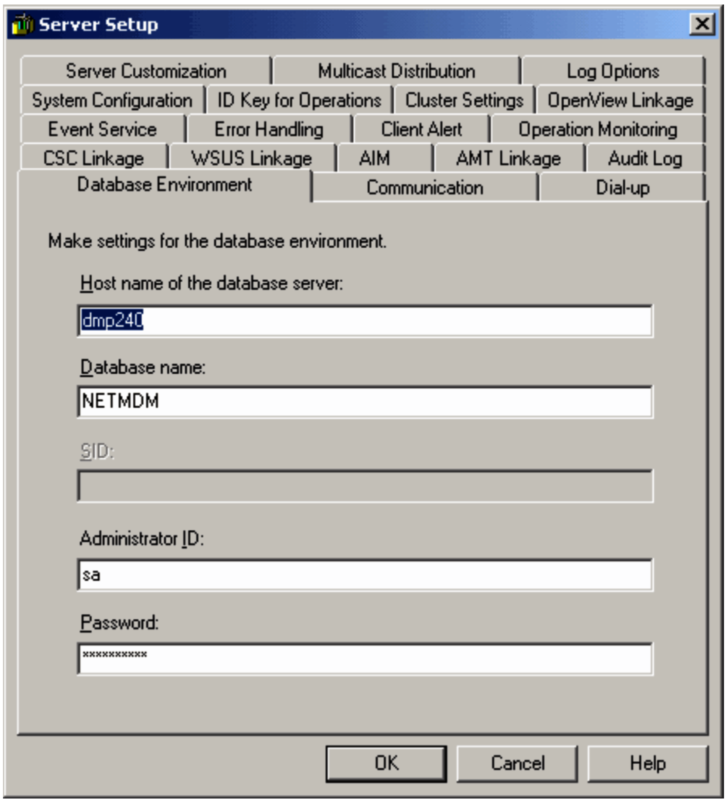
This item is enabled when only Remote Installation Manager has been installed.

(2) Database Environment page (for Microsoft SQL Server or Oracle)

This subsection describes how to specify the settings on the **Database Environment** page when Microsoft SQL Server or Oracle is used.

The settings on this page are not applicable to a PC on which only Remote Installation Manager has been installed. The system assumes for the connection-target PC the settings on the **Database Environment** page that were specified when the Remote Installation Manager was installed or started.

Figure 4–4: Database Environment page (for Microsoft SQL Server or Oracle)



Server Setup

Make settings for the database environment.

Host name of the database server:
dmp240

Database name:
NETMDM

SID:

Administrator ID:
sa

Password:
****

Host name of the database server

Specify the name of the host that will function as the database server.

If named instances are used, specify the host name in the following format:

*database-server's-host-name**instance-name*

Database name

Specify the name of the database. This must be the same name you specified in Database Manager. Specify this item only when Microsoft SQL Server is used for the relational database.

SID

Specify four alphanumeric characters as the database system identifier (*SID*) that indicates an Oracle database instance. The default is NETM. Specify this item only when Oracle is used for the relational database.

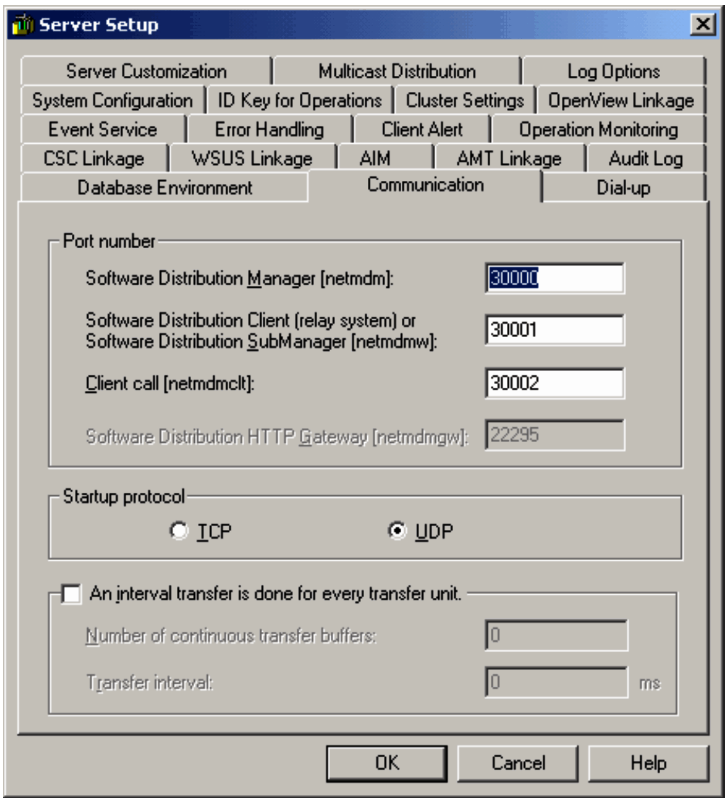
Administrator ID and **Password**

Enter the user ID and password of the user who has access permission to the JP1/Software Distribution database. The system uses the administrator ID that you enter here when it connects to a Packager and to clients. If you will be using Oracle as the relational database, UNLIMITED TABLESPACE permission must be granted as the system permission for this Administrator ID.

4.2.2 Communication page

Set the port numbers and the startup protocol.

Figure 4–5: Communication page



Port number

Software Distribution Manager [netmdm]: 30000

Software Distribution Client (relay system) or Software Distribution SubManager [netmdmw]: 30001

Client call [netmdmclt]: 30002

Software Distribution HTTP Gateway [netmdmgw]: 22295

Startup protocol

○ TCP ● UDP

□ An interval transfer is done for every transfer unit.

Number of continuous transfer buffers: 0

Transfer interval: 0 ms

(1) Port number

Specify the following four port numbers, which JP1/Software Distribution will use for communications:

- **Software Distribution Manager** (default: 30000)
- **Software Distribution Client (relay system) or Software Distribution SubManager** (default: 30001)
- **Client call** (default: 30002)
- **Software Distribution HTTP Gateway** (default: 22295)

Normally, you should use the default port numbers. However, you must change a port number if some other program is using that port. If a port number is set in the `services` file of TCP/IP, the `services` file setting takes precedence.

If you have installed Server core facility and Remote Installation Manager on separate PCs, make sure that the port numbers of Software Distribution Manager and Software Distribution Client (Relay system) or Software Distribution SubManager match in both PCs. If the port numbers do not match, the Remote Installation Manager cannot connect to the server.

The port number for JP1/Software Distribution HTTP Gateway is used only when JP1/Software Distribution HTTP Gateway is used. For details, see *E. Using Internet Options to Install JP1/Software Distribution*.

(2) Startup protocol

If you are not using dial-up connection, select **UDP** or **TCP** as the protocol to be used when the local system is started. The default is **UDP**.

If you select **TCP** and set a port number in the `services` file, also add the following entry to the `services` file: `netmdm` *xxxxx*`/tcp` (where *xxxxx* is the port number).

Note that programs may not start in a WAN environment if you select **UDP**.

(3) An interval transfer is done for every transfer unit.

When a file transfer to subsystems occurs, the file can be divided into specified units and the divided file segments are transferred at regular intervals. This transfer method can reduce the load on the network during file transfer. The default is that this check box is not selected.

Interval transfer is not performed from a subsystem to its higher system.

Number of continuous transfer buffers

File transfer buffer size specified during setup at the destination system determines the buffer's unit size. For example, if **File transfer buffer size** is 4,096 bytes and **Number of continuous transfer buffers** is set to `2`, the job is divided into units of 8,192 bytes.

You can specify a value in the range from 0 to 4,294,967,295 in **Number of continuous transfer buffers**. The default is `1`. If you specify `0`, interval transfer is not performed.

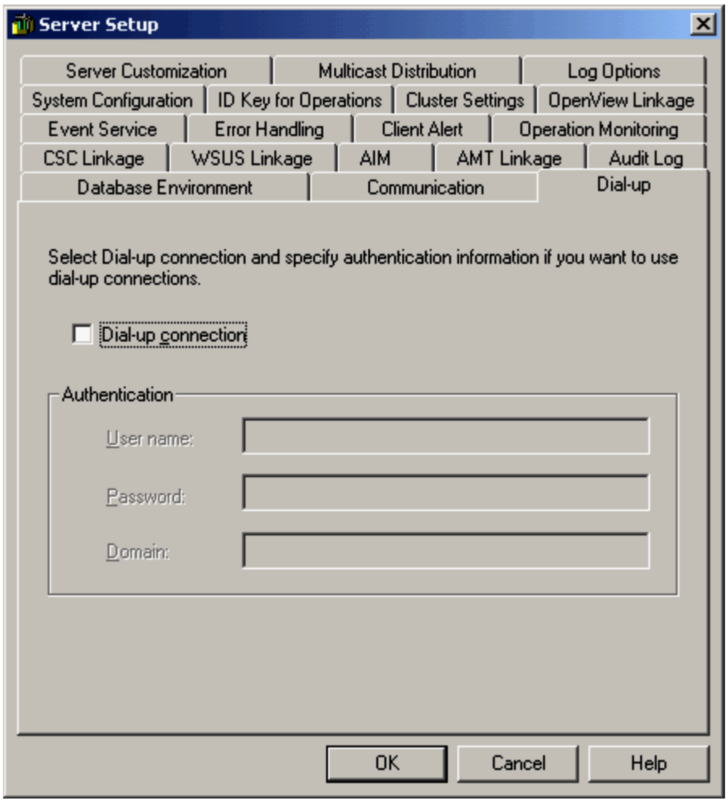
Transfer interval

Specifies the interval time between transfers when interval transfer is performed. You can specify a value in the range from 0 to 4,294,967,295 milliseconds. The default is 1,000 milliseconds. If you specify `0`, interval transfer is not performed.

4.2.3 Dial-up page

To use dial-up connections, select the **Dial-up connection** check box and specify the user name, password, and domain to be used during dialing. This page is displayed only when you install Remote Access Service.

Figure 4–6: Dial-up page



Select Dial-up connection and specify authentication information if you want to use dial-up connections.

□ Dial-up connection

Authentication

User name:

Password:

Domain:

Dial-up connection

Select this check box if you use a dial-up connection. The default is that this check box is not selected.

Authentication

Set the user name, password, and domain that are used during dial-up connection.

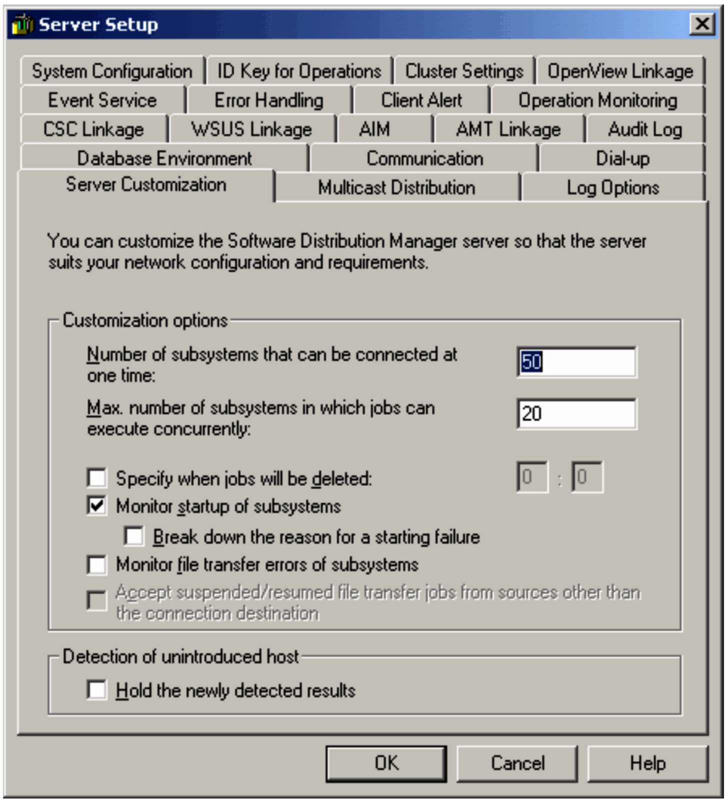
For details about a dial-up connection, see *6.6 Settings for dial-up connections* in the *Description and Planning Guide*.

4.2.4 Server Customization page

Set items here for tuning the CPU, memory, and networks. This page is displayed only at the host where the managing server is installed. You should take into account the performance, network configuration, and operating environment of the PC in which the managing server operates, and then set the necessary items. For an overview of tuning, see *6.1.7(2) Adjusting the maximum number of hosts that can be connected concurrently* in the *Description and Planning Guide*. For details about how jobs are executed on the basis of the settings of **Number of subsystems that can be connected at one time** and **Max. number of subsystems in which jobs can execute concurrently**, see *2.9.6 Flow of job execution* in the *Description and Planning Guide*.

On this page you can also set the method for managing the results from a function that detects hosts on which JP1/Software Distribution is not installed (hosts without a JP1/Software Distribution installed). For details about the function for detecting hosts without a JP1/Software Distribution installed, see *9.7 Detecting hosts on which JP1/Software Distribution is not installed*.

Figure 4–7: Server Customization page



You can customize the Software Distribution Manager server so that the server suits your network configuration and requirements.

Customization options

Number of subsystems that can be connected at one time: 50

Max. number of subsystems in which jobs can execute concurrently: 20

□ Specify when jobs will be deleted: 0 : 0

☑ Monitor startup of subsystems

□ Break down the reason for a starting failure

□ Monitor file transfer errors of subsystems

□ Accept suspended/resumed file transfer jobs from sources other than the connection destination

Detection of unintroduced host

□ Hold the newly detected results

Number of subsystems that can be connected at one time

You can limit the number of subsystems that can be connected at one time. Specifically, this value becomes the number of socket connections. Each socket connection is counted from the time it is established until the time it is released.

Use the formula below to determine the value.

If Embedded RDB is used, the minimum value is 4, the maximum value is 100, and the default value is 30.

If Microsoft SQL Server or Oracle is used, the minimum value is 4, the maximum value is 256, and the default value is 50.

Number of subsystems that can be connected at one time = number of systems that are connected directly + number of Packagers to be connected **x** 2

If the network traffic is heavy, resulting in many packet collisions, you can reduce the traffic by reducing this value, thereby reducing the number of subsystems that can be connected at one time.

A connection request from a subsystem that exceeds this value will be denied, but once there is room in the number of connections, execution requests are sent again.

If you are using Embedded RDB, you must perform the following operations after completion of setup in order to apply the new settings:

1. Stop the Remote Install Server service.
2. Execute the `netmdb_setup.bat` command that is stored in *JP1/Software-Distribution-installation-directory*`\BIN`.

   Normally, when the `netmdb_setup.bat` command terminates, it waits for an entry from the keyboard. To enable the command to terminate without receiving an entry from the keyboard, execute the command with the `/nopause` option specified.
3. Start the Remote Install Server service.

Max. number of subsystems in which jobs can execute concurrently

Specify the maximum number of subsystems that can process jobs concurrently. Specifically, this value becomes the number of startup messages the managing server sends at one time to subsystems (in other words, the number of clients that can execute jobs concurrently). If users execute jobs for more clients than the value specified in this field, the system splits the jobs on the basis of the specified value and executes them.

The minimum value is `0`, the maximum is `100`, and the default is `20`. If you specify `0`, the managing server no longer sends startup messages to the lower systems, disabling job execution initiated by higher systems as well as startup of target systems using the client control facility. If the size of the files to be distributed is large (10 MB or greater), the LAN load may become high even when only a few clients are connected. Therefore, specify a value that matches the network performance. The result of *maximum number of subsystems in which jobs can execute concurrently* **x** *package size* becomes the amount of data that flows over the network at one time.

Specify a value that does not exceed the value specified in **Number of subsystems that can be connected at one time**. If the subsystems are connected via a circuit-switched network, specifying a number greater than the number of agreement lines serves no purpose.

Specify when jobs will be deleted

When you delete a job definition or job execution status, the definition or execution status is not deleted immediately; rather, it is deleted at the time you specify for this item. Specify a value in the range from 00:00 to 23:59.

This setting is valid only for completed jobs, jobs that are running, and jobs in which an error occurred. Jobs that are waiting for transmission are deleted as soon as the user specifies deletion, even if a delayed execution time for jobs has been set.

The default setting is that this check box is not selected.

The managing server usually manages multiple clients. Therefore, when job definitions and execution status information are deleted, database deletion takes time, which may affect adversely other operations or place a load on the core jobs. By specifying a delayed execution time, you can avoid such problems, because the system will execute the deletions in batch processing at the specified time.

Monitor startup of subsystems

This check box determines whether or not you wish to change the job execution status to *Client not started* and to report the status to the managing server when a job cannot be executed because the lower system is not active. The default is for this check box to be selected. A job in *Client not started* status will be executed during the next polling from the client.

Break down the reason for a starting failure

This option specifies whether or not you wish to break down the cause of an error and report it to the managing server when a lower system results in a startup failure. The default is that this check box is not selected. If you select this check box, the *Client not started* job execution status is broken down as follows:

Job execution status	Description
Client not started (JP1/Software Distribution is not running)	Startup failure occurred because JP1/Software Distribution was not running.
Client not started (power is off)	Startup failure occurred because the PC power was off.
Client not started	Startup failure occurred for a reason other than the above.

To break down the reason for a startup failure, the **Monitor startup of subsystems** and **Break down the reason for a starting failure** check boxes must both be selected.

Monitor file transfer errors of subsystems

This check box determines whether or not you wish to change the job execution status to *Communication error* and to report the status to the managing server when a communication error occurs while one of the following jobs is transferring files. The default is that this check box is not selected.

- *Install package* job
- *Send package, allow client to choose* job
- *Transfer package to relay system* job
- *Transfer registry collection definition* job
- *Get system information from client* job
- *Acquire collected files from relay system* job
- *Get system configuration information* job
- *Hold report* job
- *Hold-report release* job
- *Report message* job

This facility monitors transfer only between the managing server specified in the setup and relay systems or clients connected directly under the managing server. If you want to monitor transfers for communication errors in the hierarchy from those relay systems or clients, you must configure them during setup at the relay managers or relay systems. In this manner, you can change the scope of monitoring jobs according to the quality of the communication lines.

Accept suspended/resumed file transfer jobs from sources other than the connection destination

If multiple higher systems are defined as connection destinations, this option determines whether or not you wish to accept *Suspend file transfer* and *Resume file transfer* jobs from a system other than the higher system defined as the default connection destination. The default is that this option is not selected.

If you select this option, you can restart file transfer from a different higher system than the one that instructed the suspension. Note that in such a case, at the Remote Installation Manager of the higher system that instructed the suspension, the *Suspend file transfer* attribute of the lower system remains as being suspended even after the file transfer is restarted.

Hold the newly detected results

The function for detecting hosts at which JP1/Software Distribution has not been installed normally detects any computer on which JP1/Software Distribution has not been installed as a *host without a JP1/Software Distribution installed*.

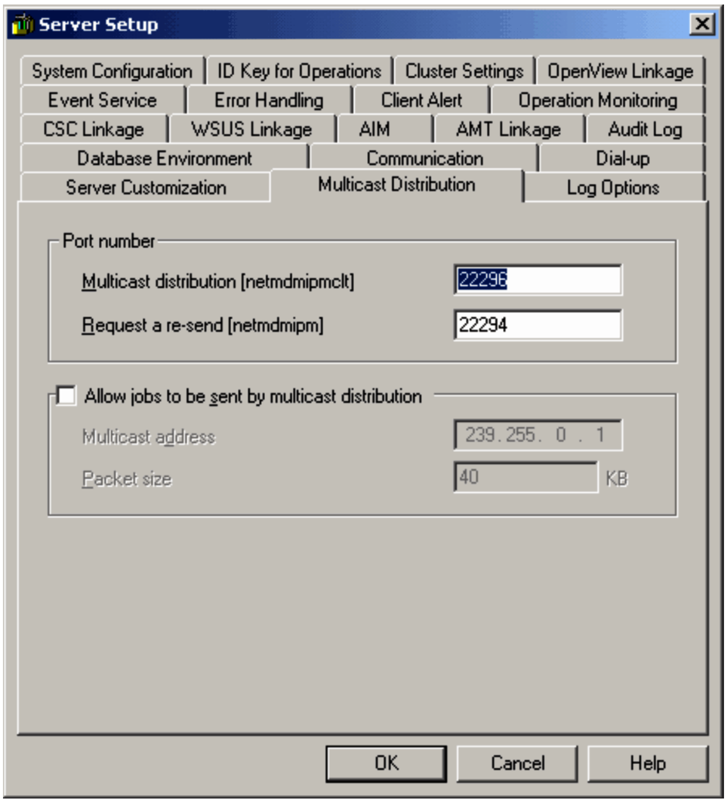
If you select this check box and execute detection of hosts without a JP1/Software Distribution installed, a computer on which JP1/Software Distribution has not been installed is detected as being on *hold*. The default is that this check box is not selected.

You can manually specify any of the detected computers as a host without a JP1/Software Distribution installed. In an environment where Windows computers are mixed with UNIX computers, this enables you to manage them separately, such as by treating only the Windows computers as hosts without a JP1/Software Distribution installed.

4.2.5 Multicast Distribution page

These settings are for distributing jobs to lower systems using multicast distribution. The settings on this page apply to jobs for which you specify multicast distribution.

Figure 4–8: Multicast Distribution page



Port number

Multicast distribution [netmdmipmclt] 22296

Request a re-send [netmdmipm] 22294

☐ Allow jobs to be sent by multicast distribution

Multicast address 239.255. 0 . 1

Packet size 40 KB

(1) Port number

Specify the following two port numbers for multicast distribution of jobs:

- **Multicast distribution** (default: `22296`)
- **Request a re-send** (default: `22294`)

Normally, you should use the displayed default port numbers. However, you must change a port number if some other program is using that port. It is important that you set a port number for **Request a re-send**, because multicast distribution uses the UDP protocol and packets may be resent during distribution.

If a port number is set in the `services` file of TCP/IP, the `services` file setting takes precedence.

(2) Allow jobs to be sent by multicast distribution

Select this option and specify the multicast address and packet size for using the multicast method to send to lower systems jobs for which you have specified multicast distribution. The default is that this check box is not selected.

When this check box is not selected, jobs for which multicast distribution is specified are distributed by unicast distribution. Conversely, even if you select this check box, jobs for which unicast distribution is specified are sent by unicast distribution.

You should clear the **Allow jobs to be sent by multicast distribution** check box if there is a router in the network that is not compatible with IP multicasting. If the network includes routers that are not compatible with IP multicasting, unicast distribution is used; you cannot use multicast distribution. If you do select **Allow jobs to be sent by multicast distribution**, the system will require a long time to switch to unicast distribution in order to send a job.

Multicast address

Specify the multicast address assigned to the multicast group to which jobs are to be distributed. Specify a value in the range from 224.0.1.0 to 239.255.255.255. Do not specify an address already assigned to another multicast group. The default address is 239.255.0.1.

A multicast group is a group of lower systems connected directly to this JP1/Software Distribution Manager. If the multicast address of the lower systems to which a job is to be distributed does not match the multicast address you specify here, the job will be distributed to those lower systems using unicast distribution.

For details about multicast groups and multicast addresses, see *6.2.1 Unicast distribution and multicast distribution* and *6.2.3 System configuration for multicast distribution* in the *Description and Planning Guide*.

Packet size

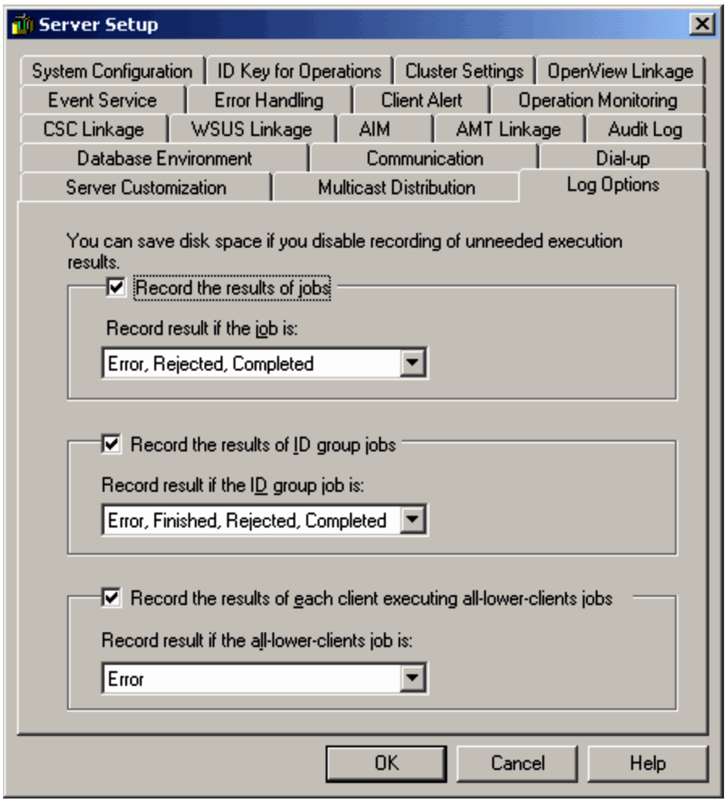
Specify the packet size to be used for distributing a job. Specify a value in the range 1-60 KB. The default is 40 KB.

40 KB is an efficient value for communications lines for 100BASE. For communications lines for 10BASE, you should specify 4 KB. If you specify a packet size that is too large, multicast distribution will fail and the system will continue distribution using unicast distribution.

4.2.6 Log Options page

These settings are for saving job execution results. You can save disk space if you disable the recording of unnecessary execution results. If the volume of recorded execution results for completed jobs becomes too large, operation of the Remote Installation Manager may slow down. You should therefore record only jobs with execution results that may require checking.

Figure 4–9: Log Options page



You can save disk space if you disable recording of unneeded execution results.

☑ Record the results of jobs

Record result if the job is: Error, Rejected, Completed

☑ Record the results of ID group jobs

Record result if the ID group job is: Error, Finished, Rejected, Completed

☑ Record the results of each client executing all-lower-clients jobs

Record result if the all-lower-clients job is: Error

(1) Record the results of jobs

Select this check box to record in the Remote Installation Manager the execution results of jobs without an ID specification. The default is that this check box is selected. To record, you must also select the execution status of the job subject to recording.

Error

A job is recorded in the Remote Installation Manager only if the execution result is Error.

Error, **Rejected**

A job is recorded in the Remote Installation Manager only if the execution result is Error or Rejected.

Error, **Rejected**, **Completed** (default)

A job is recorded in the Remote Installation Manager if the execution result is Error, Rejected, or Completed.

For the following jobs, the execution status cannot be deleted automatically even after the job is completed:

- *Send package, allow client to choose* jobs
- *Get system information from client* jobs when the execution time at the client is specified
- *Get software information from client* jobs when the execution time at the client is specified

(2) Record the results of ID group jobs

Select this check box to record in the Remote Installation Manager for each client the execution results of jobs with an ID group specified. The default is that this check box is selected. When this check box is selected, you must select the execution status of the jobs that are to be recorded:

Error, **Finished**

A job is recorded in the Remote Installation Manager if the execution result is Error or Finished.

Error, **Finished**, **Rejected**

A job is recorded in the Remote Installation Manager if the execution status is Error, Finished, or Rejected.

Error, **Finished**, **Rejected**, **Completed** (default)

A job is recorded in the Remote Installation Manager if the execution status is Error, Finished, Rejected, or Completed.

For clients that belong to an ID group managed by a relay system, this setting is enabled for all job types. For clients that belong to an ID group managed by the managing server, this setting is disabled for the following jobs, and all execution results information for such jobs is recorded in the managing server:

- *Send package, allow client to choose* jobs
- *Get system information from client* jobs when the execution time at the client is specified
- *Get software information from client* jobs when the execution time at the client is specified

(3) Record the results of each client executing all-lower-clients jobs

Select this check box to record in the Remote Installation Manager of the relay manager the execution results of all-lower-clients jobs that each client executes. The default is that this check box is selected. When this check box is selected, you must select the execution status of the jobs to be recorded.

Error (default)

A job is recorded in the Remote Installation Manager only if the execution result is Error.

Error, **Rejected**

A job is recorded in the Remote Installation Manager only if the execution result is Error or Rejected.

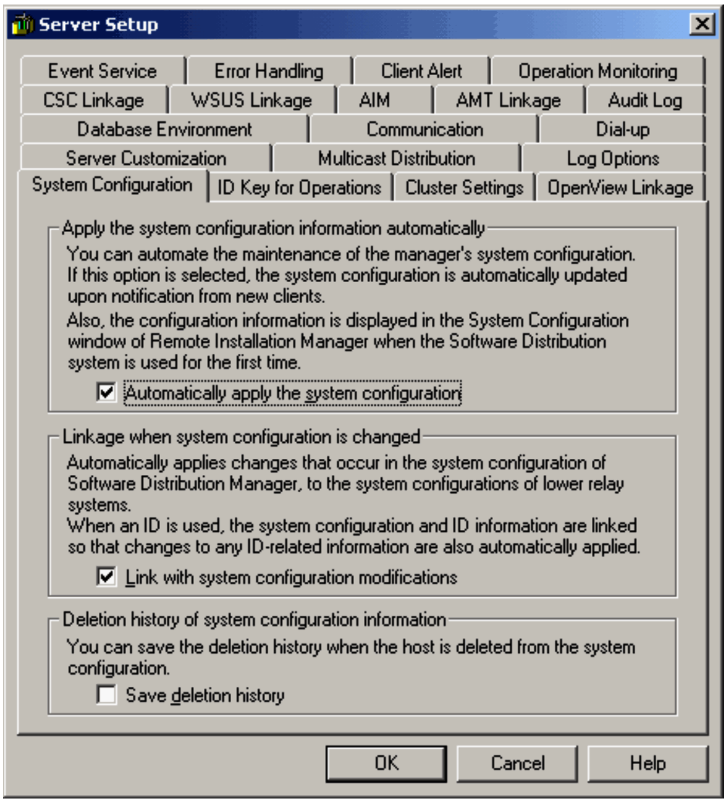
Error, **Rejected**, **Completed**

A job is recorded in the Remote Installation Manager if the execution result is Error, Rejected, or Completed.

4.2.7 System Configuration page

Specify system configuration settings. These items enable automatic change of required information whenever the system configuration changes. They also make it possible for you to manage the deletion history when hosts are removed from the system configuration.

Figure 4–10: System Configuration page



Apply the system configuration information automatically

You can automate the maintenance of the manager's system configuration. If this option is selected, the system configuration is automatically updated upon notification from new clients.
Also, the configuration information is displayed in the System Configuration window of Remote Installation Manager when the Software Distribution system is used for the first time.

☑ Automatically apply the system configuration

Linkage when system configuration is changed

Automatically applies changes that occur in the system configuration of Software Distribution Manager, to the system configurations of lower relay systems.
When an ID is used, the system configuration and ID information are linked so that changes to any ID-related information are also automatically applied.

☑ Link with system configuration modifications

Deletion history of system configuration information

You can save the deletion history when the host is deleted from the system configuration.

□ Save deletion history

(1) Apply the system configuration information automatically

Specify whether or not system configuration information reported from subsystems is to be applied automatically to the system configuration database. The default is that this check box is selected. If you clear this check box, you will have to define system configuration changes manually.

When you first install JP1/Software Distribution, select this check box. This reduces the workload because you will not need to define the system configuration in managing servers.

Note that when this check box is selected, the system automatically changes existing configuration definition information.

(2) Linkage when the system configuration is changed

When the system configuration information for JP1/Software Distribution Manager is changed, you can have the changes in the system configuration information applied automatically to the lower systems. You can also automatically edit ID group information according to the changes in the system configuration information. Therefore, if this check box is selected, there is no need for the system administrator to change ID groups according to the system configuration information from the managing server or the relay managing ID groups. If this check box is not selected, the system administrator must manually edit the ID group information.

This setting takes effect only when **Automatically apply the system configuration** is selected. The default is that this check box is selected. However, if the check box was not selected in the previous version and a new version is installed over the previous one, the check box will not be selected in the default setting.

When you select this check box, you must ensure that all JP1/Software Distribution Managers and JP1/Software Distribution SubManagers in the system have been upgraded to version 05-21 or later. Therefore, clear this check box if your system contains any JP1/Software Distribution Manager or JP1/Software Distribution SubManager whose version is earlier than 05-21.

For details about the operation for linking system configuration information and ID groups, see *8.4 Linking system configuration information and ID group information*.

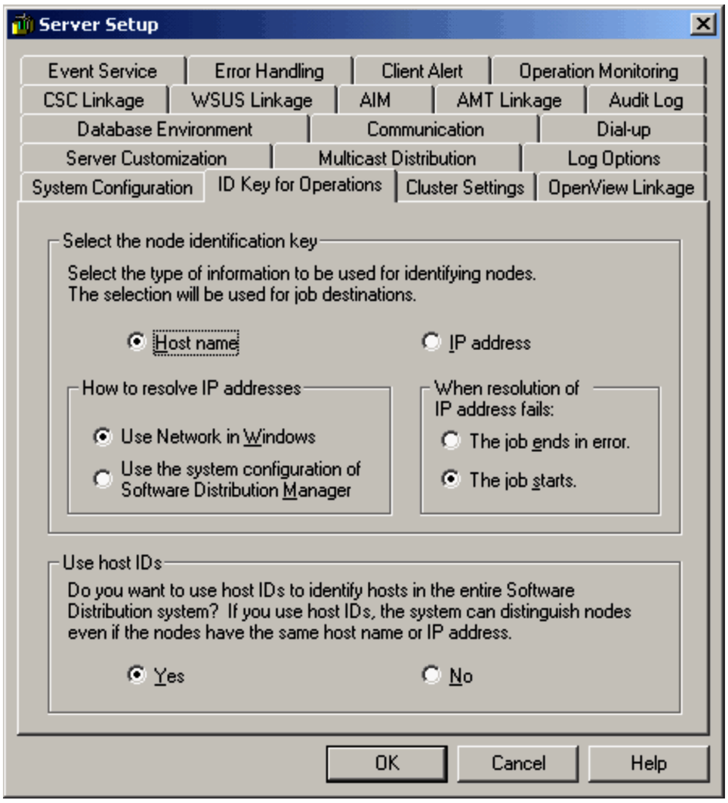
(3) Deletion history of system configuration information

When a host is removed from the system configuration, you can retain its history. When this check box is selected, the system retains host deletion history, such as when a host was deleted. You can use this historical data as management information. You can also restore deleted hosts in the system configuration information on the basis of the applicable deletion history. The default is that this check box is not selected, in which case deletion history is not stored.

4.2.8 ID Key for Operations page

Specify the key for managing hosts in the network and identifying destinations. Also, set the use of host IDs.

Figure 4–11: ID Key for Operations page



Select the node identification key

Select the type of information to be used for identifying nodes.
The selection will be used for job destinations.

● Host name ○ IP address

How to resolve IP addresses

● Use Network in Windows

○ Use the system configuration of Software Distribution Manager

When resolution of IP address fails:

○ The job ends in error.

● The job starts.

Use host IDs

Do you want to use host IDs to identify hosts in the entire Software Distribution system? If you use host IDs, the system can distinguish nodes even if the nodes have the same host name or IP address.

● Yes ○ No

(1) Select the node identification key

Select **Host name** or **IP address** as the information type for determining communication destination hosts during host-to-host communication. Select **Host name** or **IP address** according to the ID key for operations setting in the destination hosts. The default is **Host name**. If you select **Host name** as the node identification key, specify **How to resolve IP addresses** and **When resolution of IP address fails**. You can set the ID key for operations only for the relay manager, regardless of the ID key settings on the higher system.

How to resolve IP addresses

For the method to be used to resolve addresses in creating or starting jobs, select **Use Network in Windows** or **Use the system configuration of Software Distribution Manager**. The default is **Use Network in Windows**.

Use Network in Windows

Obtains an IP address from the Windows network when a job is created or started. The `hosts` file or name server is used for name resolution. If name resolution fails, the IP address is obtained from the system configuration of JP1/Software Distribution.

Use the system configuration of Software Distribution Manager

Obtains an IP address only from the system configuration of JP1/Software Distribution when a job is created or started. In such a case, you must ensure that the IP addresses of the system configuration are always correct.

In some environments in which IP addresses are changed dynamically (e.g., DHCP), you can keep system configuration IP addresses correct by using the facility for automatically registering the system configuration.

In an environment in which jobs are created or started when the name server is turned off (such as at night), address resolution may fail and jobs will not be created even if you choose **Use Network in Windows**. However, choosing **Use the system configuration of Software Distribution Manager** has the benefit of reducing the time it takes until name resolution fails.

This setting, without resolving addresses, determines the destination of jobs by obtaining the IP address from the system configuration information. This means that jobs may not be executable in the following cases.

- Using Host ID

  For details, see *8.2.4(4) Notes on specifying destinations* in the manual *Administrator's Guide Volume 1* and *4.26.9 JOB_DESTINATION (specifying a job destination)* in the manual *Administrator's Guide Volume 2*.

- Using the NAT function

  Job execution requests for a destination cannot be sent when the NAT function is being used. However, jobs can be executed by polling from the destination. For information on how to poll, see *2.13.1(2)(b) Executing a job at an arbitrary time* in the manual *Description and Planning Guide*.

When resolution of IP address fails

Select the processing to be performed when the system cannot resolve a destination address during job execution. The default is **The job starts**. When **The job starts** is selected, the execution status of the job becomes **Waiting for transmission** in the event IP address resolution fails. The execution status of a job addressed to a nonexistent destination becomes **Waiting for transmission** and does not change.

In environments that use a WINS server, the destination address cannot be resolved if the destination client PC is turned off when a job is executed. Thus, if you select **The job ends in error**, you will not be able to set up an operation that executes jobs on holidays or at night or that automatically starts the client by polling when the system starts. If you wish to set up this type of operation, select **The job starts**.

When you select **The job starts**, operation of the Remote Installation Manager may be delayed if an executed job contains a destination whose address cannot be resolved.

(2) Notes on changing the node identification key

If you wish to change the node identification key during operation, delete the following information items from Remote Installation Manager:

- System configuration information
- Destination information
- Job definitions
- Job execution status information

You do not have to delete package information, because that information can be inherited.

You should save the system configuration information in a file before deleting it. You can set the system configuration information by changing the node identification key, editing the output system configuration information, and then importing the file. When you import the system configuration information file that has been output, check to see if the correct host name or IP address is specified for each host. For example, to change the node identification key from host name to IP address, the correct IP address must be specified in the system configuration information file that was output. If you need to edit the file contents, use a program such as a text editor. For details about the contents and output of the system configuration information file, see *8.1.4 Creating the system configuration information from a file*.

(3) Use host IDs

Select whether or not the entire JP1/Software Distribution system is to use host IDs as the information for managing hosts uniquely. The default is **Yes**.

When you are using Asset Information Manager Subset, in order to change the **Use host IDs** setting, you must change the **Working key** settings for Asset Information Manager Subset. For details about the working key settings, see *10.2.5 Setting the link with JP1/SD*.

(4) Notes on using host IDs

The following points should be noted when you change the ID key after the system has been operating:

- If you change from not using host IDs to using host IDs
  Check the following two items if you will be using host IDs:

  The database has been backed up

  If you begin operation with the **Use host IDs** setting set to **Yes** and then change the setting to **No**, you will not be able to use any information that was registered in the database, except for package information. Therefore, if the system contains a database that was recorded without using host IDs, be sure to make a backup of that database.

  The Use host IDs setting has been set to Yes in the higher manager

  If the relay manager uses host IDs, the JP1/Software Distribution Manager version installed in the higher manager to which the relay manager connects must support host IDs. JP1/Software Distribution Manager version 05-21 or higher satisfies this condition. In addition, the **Use host IDs** setting must be set to **Yes**.

  Do not use host IDs in a relay manager if the JP1/Software Distribution Manager version installed in the connection-destination higher server does not support host IDs or if its **Use host IDs** setting was set to **No** in the JP1/Software Distribution Manager setup.

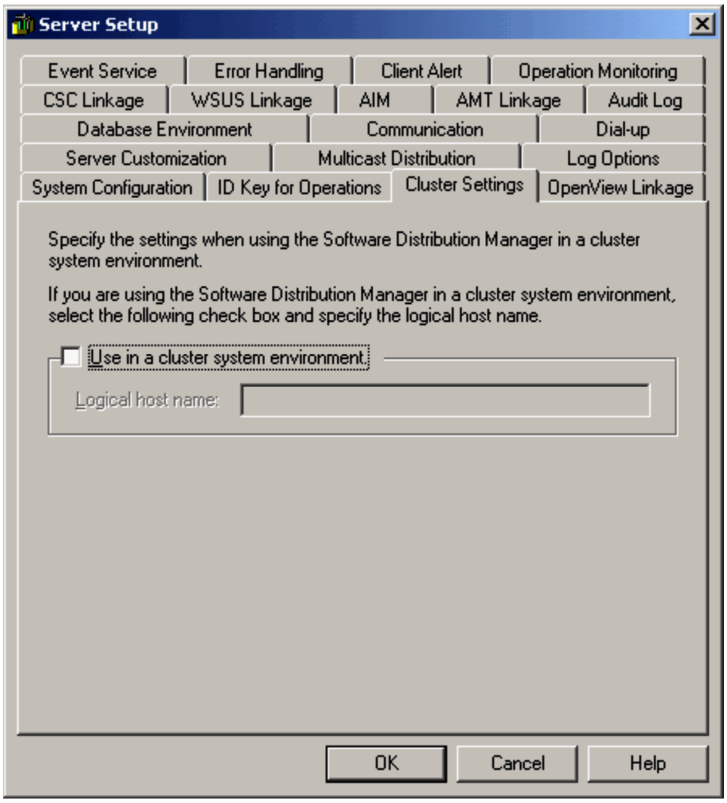
- If you change from using host IDs to not using host IDs
  If you change the **Use host IDs** setting from **Yes** to **No**, you will not be able to use any database information that was recorded while the setting was set to **Yes**, except for package information. You can avoid this problem by doing one of the following:

  - Before changing the setting to **No**, delete all the database information.
  - If you previously backed up the database that was recorded without using host IDs, restore the database from the backup.

4.2.9 Cluster Settings page

Specify this page if you are using JP1/Software Distribution Manager in a cluster system. Select the check box on this page and specify the logical host name (with domain names) of the cluster system.

Figure 4–12: Cluster Settings page



Specify the settings when using the Software Distribution Manager in a cluster system environment.

If you are using the Software Distribution Manager in a cluster system environment, select the following check box and specify the logical host name.

□ Use in a cluster system environment.

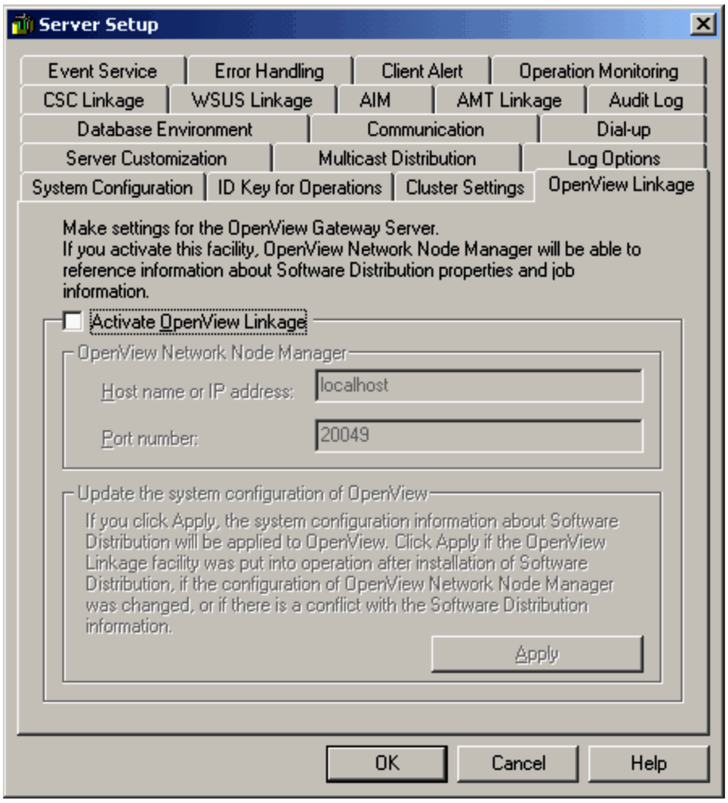
Logical host name:

4.2.10 OpenView Linkage page

Set up the OpenView gateway server that is needed in order to use OpenView Linkage. OpenView Linkage enables you to view JP1/Software Distribution inventory from HP NNM version 7.5 or earlier.

To update the settings on the **OpenView Linkage** page, after completing setup of JP1/Software Distribution Manager, open **Control Panel**, choose **Administrative Tools**, **Services**, and then restart the Remote Installation Gateway Server service in addition to the Remote Install Server service.

Figure 4–13: OpenView Linkage page



Make settings for the OpenView Gateway Server.
If you activate this facility, OpenView Network Node Manager will be able to reference information about Software Distribution properties and job information.

□ Activate OpenView Linkage

OpenView Network Node Manager

Host name or IP address: localhost

Port number: 20049

Update the system configuration of OpenView

If you click Apply, the system configuration information about Software Distribution will be applied to OpenView. Click Apply if the OpenView Linkage facility was put into operation after installation of Software Distribution, if the configuration of OpenView Network Node Manager was changed, or if there is a conflict with the Software Distribution information.

(1) Activate OpenView Linkage

Select whether or not you wish to use OpenView Linkage. The default is that this check box is not selected. To use OpenView Linkage, specify the host name or IP address of HP NNM, and the port number.

(2) Update the system configuration of OpenView

Specify whether or not system configuration information about JP1/Software Distribution is to be applied to HP NNM in batch processing. Click the **Apply** button if you wish to add OpenView Linkage to the existing JP1/Software Distribution environment after starting JP1/Software Distribution operation or if you wish to add the system configuration information of the hierarchy structure from a relay manager in JP1/Software Distribution 06-53 or a later version.

4.2.11 Event Service page

This page is used to specify information about the events that are sent to JP1/IM using JP1/Base's event service facility. If you select the **Enable the event service** check box, the results of jobs executed in JP1/Software Distribution and errors that occur in JP1/Software Distribution Manager are reported to JP1/IM as JP1 events. You can also report alert information sent from clients to JP1/IM as JP1 events. The default is that this check box is not selected.

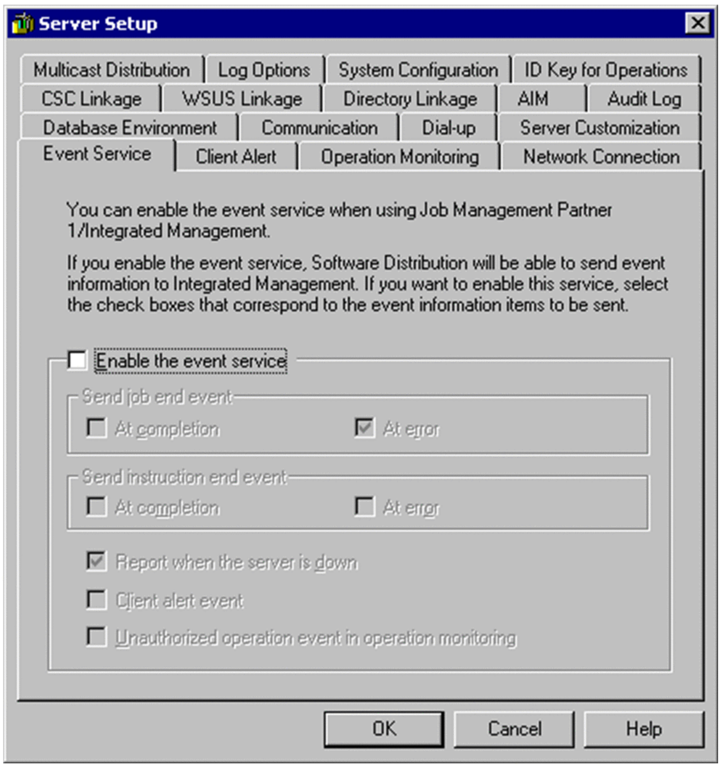
JP1/Software Distribution Manager can report execution results to JP1/IM for the following jobs:

- *Install package* jobs
- *Transfer package to relay system* jobs
- *Collect files from client* jobs
- *Collect files from client to relay system* jobs
- *Acquire collected files from relay system* jobs
- *Send package, allow client to choose* jobs

For these jobs, JP1 Software Distribution Manager can also report the job execution results in detailed units called *instructions*. An instruction is the smallest unit of a job created in JP1/Software Distribution Manager and is created for each destination or distributed software. For example, if you have a job that distributes two software programs to two destinations, four instructions are created for the job.

When JP1/Software Distribution Manager is used with a cluster configuration, events are transferred to the physical host's event service.

Figure 4–14: Event Service page



You can enable the event service when using Job Management Partner 1/Integrated Management.

If you enable the event service, Software Distribution will be able to send event information to Integrated Management. If you want to enable this service, select the check boxes that correspond to the event information items to be sent.

□ Enable the event service

Send job end event

□ At completion ☑ At error

Send instruction end event

□ At completion □ At error

☑ Report when the server is down

□ Client alert event

□ Unauthorized operation event in operation monitoring

Send job end event

Select one of the following check boxes to report job execution results to JP1/IM:

At completion

JP1/Software Distribution Manager reports job execution results when all jobs to all destinations are completed.

At error

JP1/Software Distribution Manager reports job execution results only if an error occurs.

Send instruction end event

Select one of the following check boxes to report job execution results in instruction units for jobs executed in JP1/Software Distribution:

At completion

JP1/Software Distribution Manager reports job execution results when all instructions are completed.

At error

JP1/Software Distribution Manager reports job execution results only if an instruction error occurs.

Report when the server is down

JP1/Software Distribution Manager sends this event when an error occurs in JP1/Software Distribution Manager.

Client alert event

JP1/Software Distribution Manager sends this event to JP1/IM when alert information is sent from clients.

Unauthorized operation event in operation monitoring

If the client performs one of the following unauthorized operations, JP1/Software Distribution Manager notifies JP1/IM.

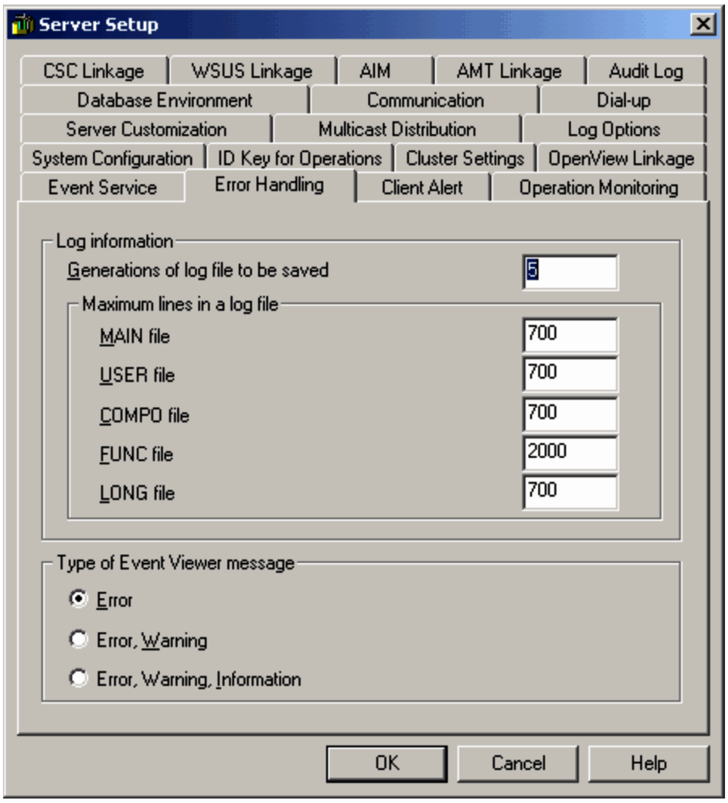
- Connecting to a device whose operation is suppressed
- Starting suppressed software
- Performing a print operation from a client where print operations are suppressed

4.2.12 Error Handling page

Specify the number of generations and number of log entries to be managed and the type of messages to be output to the Event Viewer.

For detailed settings, see *6.2 Setting up Client*.

Figure 4–15: Error Handling page



Log information

Generations of log file to be saved	5

Maximum lines in a log file

MAIN file	700
USER file	700
COMPO file	700
FUNC file	2000
LONG file	700

Type of Event Viewer message

● Error

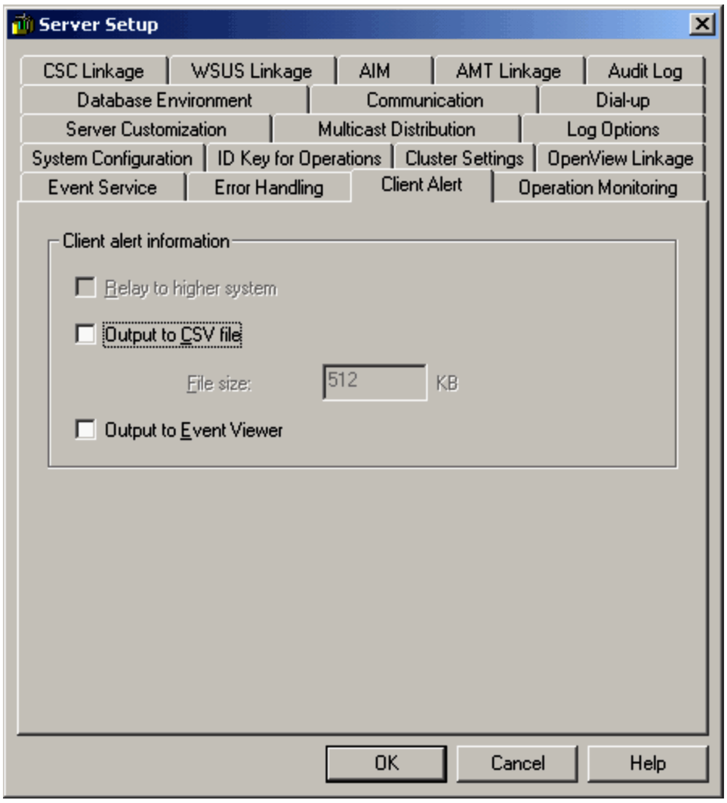
○ Error, Warning

○ Error, Warning, Information

4.2.13 Client Alert page

Specify information about output of and relaying alert information that is sent from clients.

Figure 4–16: Client Alert page



Client alert information

☐ Relay to higher system

☐ Output to CSV file

File size: 512 KB

☐ Output to Event Viewer

Relay to higher system

JP1/Software Distribution Manager relays alert information sent from clients to the higher system. This option is available for relay managers. The default is that this check box is selected. For the central manager, this check box is disabled.

Output to CSV file

JP1/Software Distribution Manager outputs the history of alert information sent from clients to a CSV file. The default is that this check box is not selected. If you select this check box, specify **File size**.

File size

Specifies the size of the CSV file to which the history of alert information is to be saved, in the range from 100 to 2,500 kilobytes. The default is 512 kilobytes. 100 kilobytes of space can accommodate approximately 400 alert information items.

If the amount of alert information exceeds the specified file size, the oldest alert information is overwritten.

Output to Event Viewer

JP1/Software Distribution Manager outputs alert information sent from clients to Windows NT Event Viewer. The default is that this check box is not selected.

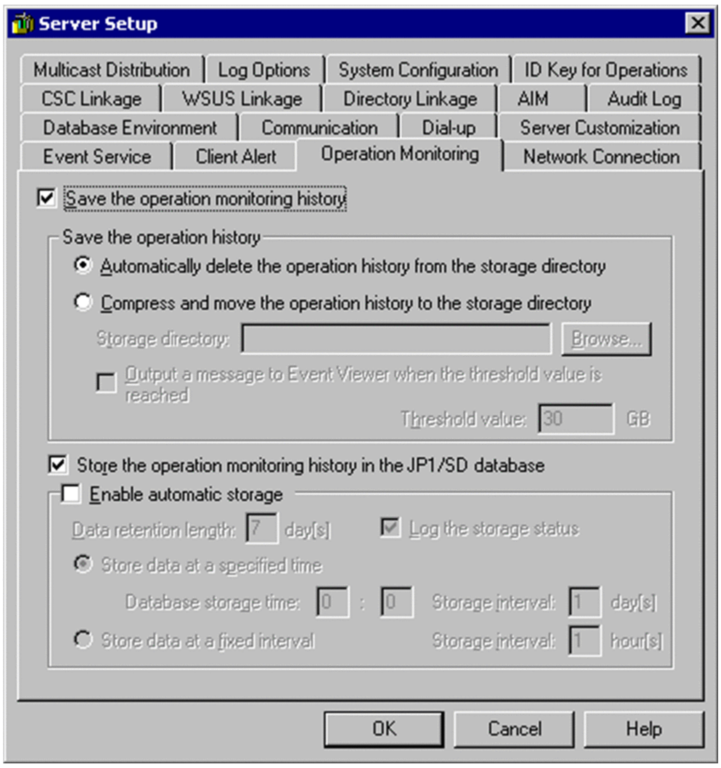
If you select **Output to Event Viewer** check box, all alert information is output to the Event Viewer regardless of the **Type of Event Viewer message** setting on the **Error Handling** page. When the type of alert event is **Critical** or **Warning**, the message type displayed on the Event Viewer is warning messages; when the type of alert event is **Normal**, the message type is information messages.

4.2.14 Operation Monitoring page

This page is used to set how to store operation history that is reported to the managing server when software operation status is monitored. Specify these settings taking into account the number of clients to be monitored and the disk capacity available to the managing server.

See *2.6.5 Examples of managing operation information* in the manual *Description and Planning Guide* for examples of using operation histories.

Figure 4–17: Operation Monitoring page



☑ Save the operation monitoring history

Save the operation history

● Automatically delete the operation history from the storage directory

○ Compress and move the operation history to the storage directory

Storage directory:

□ Output a message to Event Viewer when the threshold value is reached

Threshold value: 30 GB

☑ Store the operation monitoring history in the JP1/SD database

□ Enable automatic storage

Data retention length: 7 day[s] ☑ Log the storage status

● Store data at a specified time

Database storage time: 0 : 0 Storage interval: 1 day[s]

○ Store data at a fixed interval Storage interval: 1 hour[s]

Save the operation monitoring history

Specifies whether to retain operation histories, suppression histories and operating times reported from lower systems. The default is that this check box is selected.

Operation histories are retained in the directory specified for storing operation histories when the product was installed.

Suppression histories and operating times are retained in the JP1/Software Distribution relational database.

Up to 10,000 suppression histories can be stored. If that number is exceeded, the oldest items are deleted.

Up to 220 days of operating time information are retained for each client. If that number of days is exceeded, the oldest operating times are deleted.

If you clear this check box, log information reported from subsystems is not stored. Note that when log information is reported, the following information is updated on the **Attributes** page in Remote Installation Manager's System Configuration, Destination, or Directory Information window:

- Final update date/time of software operation information
- Applied software operation monitoring policy
- Applied software operation monitoring policy version

Log information that has already been stored is retained even if this check box is not selected.

If you use Embedded RDB and have changed the settings, you must perform the following procedure after the setup is completed in order to apply the new settings:

1. Stop the Remote Install Server service.
2. Execute the `netmdb_setup.bat` command that is stored in *JP1/Software-Distribution-installation-directory*`\BIN`.

   When the `netmdb_setup.bat` command terminates, the system is placed in key entry wait status. If you wish to have the command terminate without setting a wait for a key entry, specify the `/nopause` option before executing the command.
3. Start the Remote Install Server service.

(1) Saving operation histories

Automatically delete the operation history from the storage directory

Select to delete operating information from the operation history storage directory if the threshold is exceeded. The default is to automatically delete.

See *Table 4-2* for the thresholds and deletion sizes.

Compress and move the operation history to the storage directory

Select to compress operating information in the operation history storage directory and back it up to another directory when the threshold is exceeded.

See *Table 4-2* for the thresholds.

Storage directory

Specifies the target backup directory when the **Compress and move the operation history to the storage directory** radio button is selected. Specify an existing directory as the backup directory.

You can specify up to 127 single-byte characters (63 double-byte characters) for a local disk directory or a shared directory. Specify shared directories using the `UNC` path.

You can specify the following single-byte characters: `- _ \ . : ( )`. However, you cannot specify to back up operation history directly under a drive (for example, `D:\`) or use network drives whose drive characters are already assigned (for example, `G:\NETM\MONITORING`). Moreover, you cannot specify the directory used as the operation history storage directory.

Do not manually create files or directories under the operation history backup directory.

For each client, the archived operation history is saved in the `OPERATION` directory that is created under the operation history backup directory specified here.

Archived operation histories are not automatically deleted. Check the size of the operation history backup directory periodically and delete operation histories.

Output a message to Event Viewer when the threshold value is reached

Select this box to output a message to the Event Viewer when the size of the operating information in the operation history backup directory exceeds the threshold. The default is `OFF`.

Threshold value

Specifies the threshold (1 to 1,000 GB) for the size of operating information in the operation history backup directory when the **Output a message to the Event Viewer when the threshold value is reached** check box is selected. The default is 30 GB.

When the **Enable automatic storage** check box is selected, operating information in the operation history storage directory is backed up to the operation history backup directory.

The threshold value and deletion size when operating information is automatically backed up to the operation history backup directory vary depending on the new installation values and the setting for timing of storage to the database. The following table shows the threshold values and deletion sizes when operation history is being automatically backed up to the operation history backup directory.

Table 4–2: Threshold values and deletion sizes for saving to the operation history backup directory

Timing	Item	Value
At a new installation (default)	Threshold	3 MB
	Deletion size	1 MB
When upgrading the version	Threshold	Inherits the setting from the previous version
	Deletion size	Inherits the setting from the previous version
When **Storage interval** is changed in setup	Threshold	2 MB **x** {*storage-interval* (days) + *storage-interval* (days) ÷ 2}#
	Deletion size	2 MB **x** {*storage-interval* (days) ÷ 2}#

#

Storage intervals of 1 to 24 hours are counted as one day.

If the **Enable automatic storage** check box is not selected, operating information is backed up to the operation history backup directory only when the `dcmmonrst` command is executed.

Since an event log is output when the operation history storage directory size exceeds 20 MB, you can treat this event log as a reminder for you to execute the `dcmmonrst` command to back up the currently stored operating information to the operation history backup directory.

(2) Store the operation monitoring history in the JP1/SD database

Select this check box to automatically store operating information in the JP1/Software Distribution relational database or when you manually execute a `dcmmonrst` command to store operating information.

For details about the `dcmmonrst` command, see *4.13 dcmmonrst.exe (storing operating information in a database)* in the manual *Administrator's Guide Volume 2*.

(3) Enable automatic storage

Select this check box to automatically store operating information in the JP1/Software Distribution relational database when managing operating information (suppression history and operation history) in the Operation Log List window. The default is not selected.

To manage operating information using the Operation Log List window, operating information must be stored in the JP1/Software Distribution relational database.

! Important note

When operating information is acquired from clients in a virtualized environment, the amount of operating information increases proportionally to the number of users logged on. Therefore, we recommend that you deselect the **Enable automatic storage** check box and manually execute the `dcmmonrst` command as needed to back up operating information to the operation history backup directory.

Data retention length

For each client, specifies the number of days to hold the stored operating information.

Operating information that has aged the specified number of days is deleted, using the latest operating information for each client as the reference point.

Specify 1 to 31 days. The default is 7 days.

Log the storage status

Select this check box to log when operating information is stored in the database to `MONRST.LOG`. The default is that this check box is selected.

For details about `MONRST.LOG`, see *6.3.1 Checking log files* in the manual *Administrator's Guide Volume 2*.

Store data at a specified time

Operating information is stored at the time specified in **Database storage time** after the number of days specified in **Storage interval** have elapsed since information was last stored. The default is to select this item.

The initial operating information is stored at the time specified in the **Database storage time** after Remote Install Server service has started.

Specify **Database storage time** between 0:00 and 23:59. The default is 0:00.

Specify **Storage interval** between 1 and 30 days. The default is 1 day.

Store data at a fixed interval

Stores new operating information after the time specified in **Storage interval** has elapsed since the previous storage operation was completed.

The initial operating information is stored when the time specified in **Storage interval** has elapsed since the Remote Install Server service has started.

Specify **Storage interval** between 1 and 24 hours. The default is 1 hour.

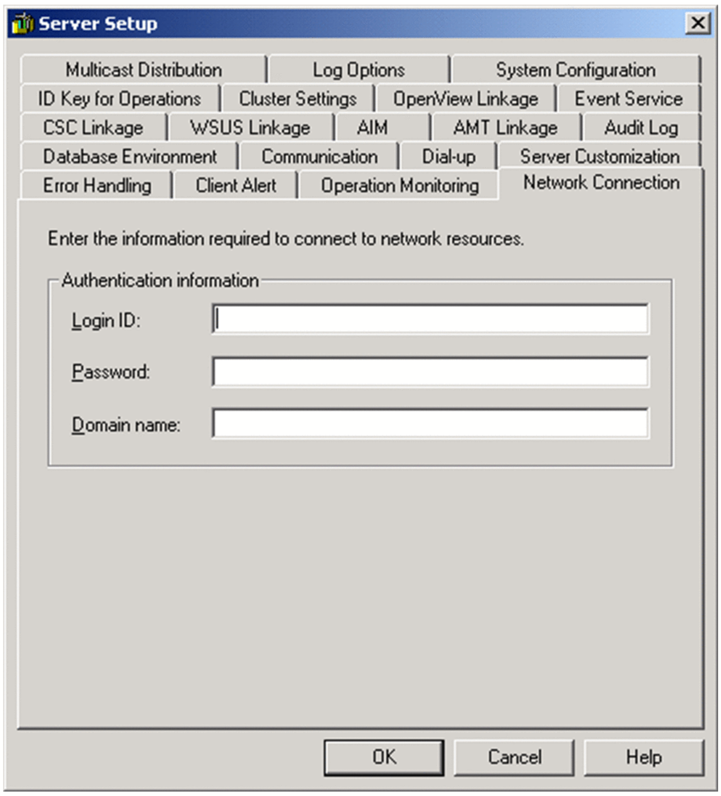
(a) Notes

- If reception of operating information from the client and storage of operating information in the JP1/Software Distribution relational database are scheduled for the same time, each will require processing time. Therefore, set these two processes to execute at different times.
- When the data retention length specifies that the operating information is to be retained for a long time, the initial fixed interval storage of operating information after this setting is changed may execute for a long time.
- Storage of operating information into the database may take a long time depending on the volume of information. While this depends on the nature of the history acquired and the system environment, as a guideline assume 10 seconds to store a day's worth of operating information per client machine.

4.2.15 Network Connection page

If you use a network drive for the operation history storage directory or the operation history backup directory, you use this page to set authentication information for connecting to the network drive. If you set authentication information in the Network Connection Settings dialog box during installation, you can use this page to change that authentication information.

Figure 4–18: Network Connection page



Enter the information required to connect to network resources.

Authentication information

Login ID:

Password:

Domain name:

Login ID

Specifies the login ID used to connect to the network drive, expressed as 1 to 30 alphanumeric characters and symbols. The following symbols cannot be used:

`\ / * : ; , + < = > ? | [ ]`

If you specify a network drive for the operation history storage directory and operation history backup directory, make sure that you also specify the password and domain name.

Password

Specifies the password used to connect to the network drive, expressed as 1 to 30 alphanumeric characters and symbols. Spaces cannot be specified.

Domain name

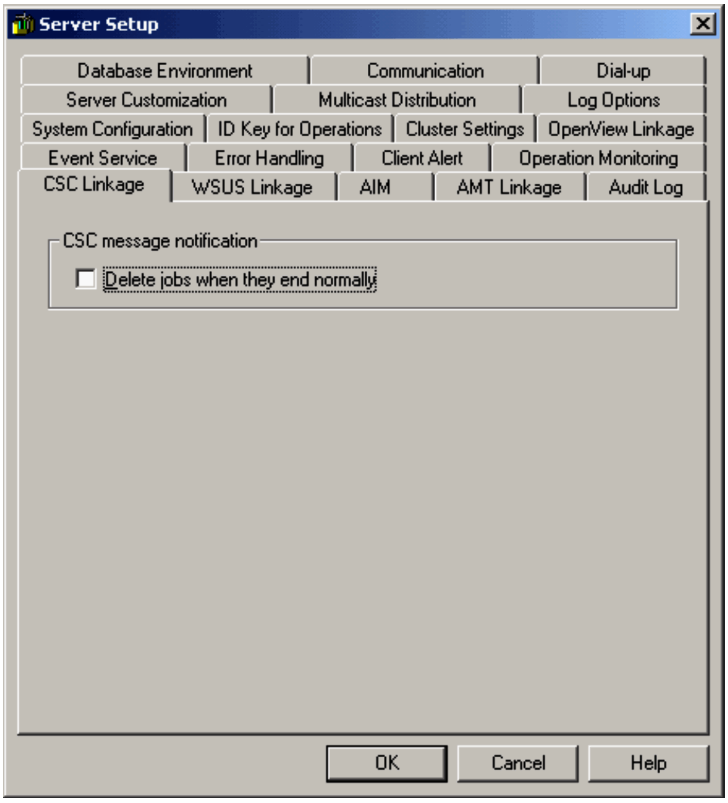
Specifies the domain name used to connect to the network drive, expressed as 1 to 127 alphanumeric characters and symbols. The following symbols cannot be used:

```
\ / * : ; , + < = > ? | [ ]
```

4.2.16 CSC Linkage page

When you send messages from JP1/Client Security Control to clients, the *Report message* jobs executed from JP1/Client Security Control are displayed under the `CSCSendMessage` folder in the Job Status window of Remote Installation Manager. You use this page to set the handling of such *Report message* jobs.

Figure 4–19: CSC Linkage page



CSC message notification

□ Delete jobs when they end normally

Delete jobs when they end normally

Specifies that *Report message* jobs that terminate normally (among all *Report message* jobs executed from JP1/Client Security Control) are to be deleted automatically from the Job Status window. The default is that this check box is not selected (the jobs are not deleted automatically).

On the **Log Options** page for the server setup, you can also specify whether or not the results of normally terminated jobs are to be recorded. The following describes the settings depending on whether the normally terminated *Report message* jobs are to be recorded or deleted:

- When normally terminated *Report message* jobs are to be recorded

  Clear the check box for **Delete jobs when they end normally**, and on the **Log Options** page select the **Error, Rejected, Completed** option. If you select any other option, the normally terminated *Report message* jobs will be deleted.

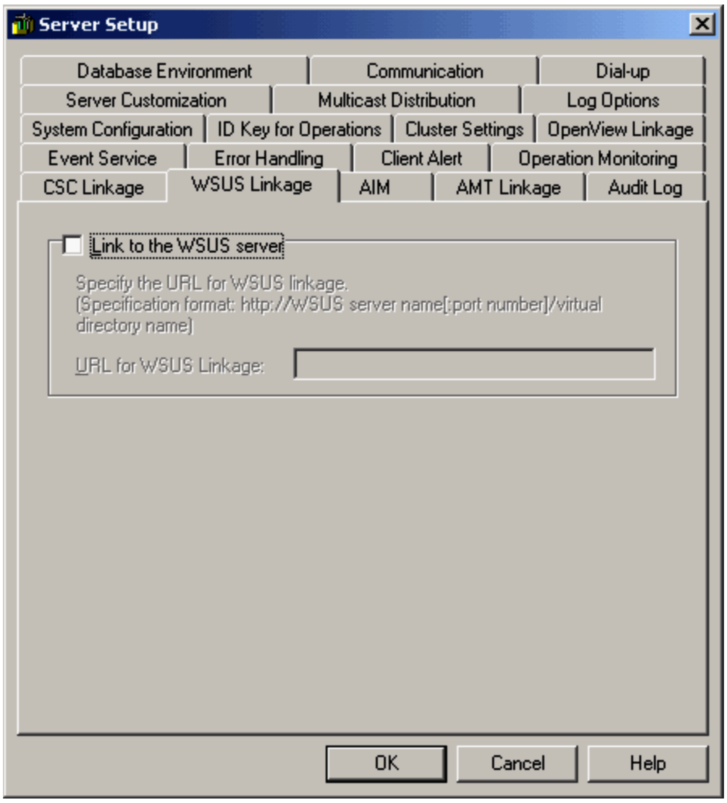
- When normally terminated *Report message* jobs are to be deleted

  Select the check box for **Delete jobs when they end normally**. The normally terminated *Report message* jobs will be deleted regardless of the settings on the **Log Options** page.

4.2.17 WSUS Linkage page

This page specifies the URL of WSUS Linkage to which JP1/Software Distribution is to connect in order to establish linkage with WSUS.

Figure 4–20: WSUS Linkage page



☐ Link to the WSUS server

Specify the URL for WSUS linkage.
(Specification format: http://WSUS server name[:port number]/virtual directory name)

URL for WSUS Linkage:

Link to the WSUS server

To link to WSUS, select this check box. The default is that this check box is not selected.

URL for WSUS Linkage

Specifies the URL of WSUS Linkage to which JP1/Software Distribution is to connect, expressed as up to 127 characters. The following shows the format of the URL that is specified:

`http://`*`WSUS-server-name`*`[:`*`port-number`*` ]/`*`virtual-directory-name`*

WSUS Server name

Specifies the host name of the WSUS server on which WSUS Linkage has been installed.

Port number

Specifies the port number of the Web server on the WSUS server. This item is optional; when it is omitted, 80 is set.

Virtual directory name

Specifies the virtual directory that was created when WSUS Linkage was installed.

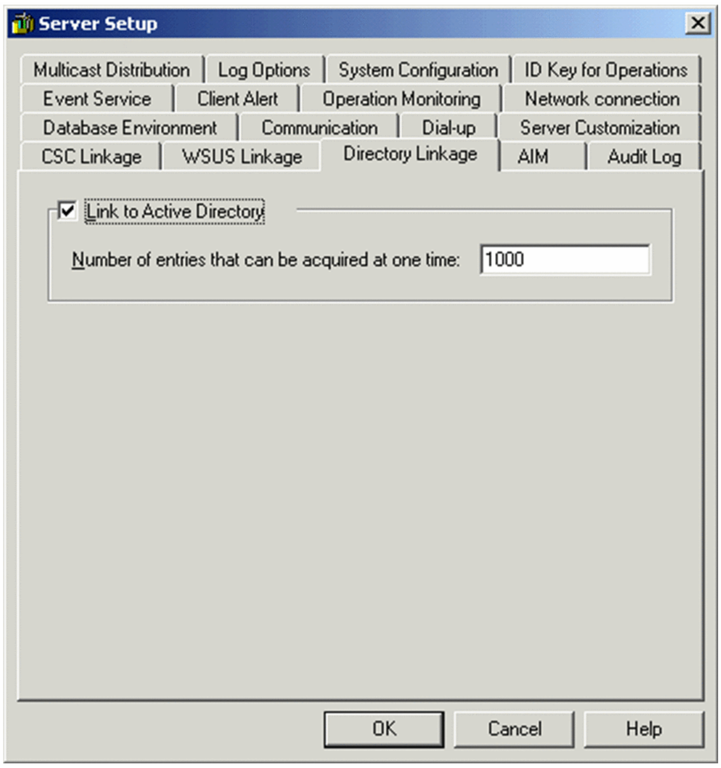
The following example specifies the WSUS server name `wssrv001`, port number `80`, and virtual directory name `netmWS`:

```
http://wssrv001:80/netmWS
```

4.2.18 Directory Linkage page

If you link Active Directory in order to use the directory information managed by Active Directory at the managing server, you must specify the Directory Linkage page.

Figure 4–21: Directory Linkage page



☑ Link to Active Directory

Number of entries that can be acquired at one time: 1000

Link to Active Directory

Select this check box to link to Active Directory. The default is that this check box is not selected.

Number of entries that can be acquired at one time

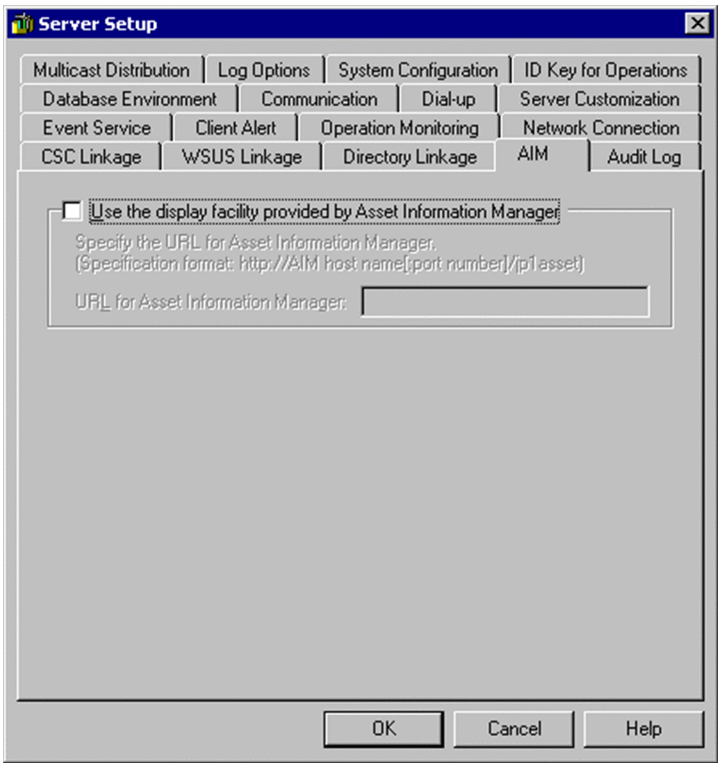
Specifies the number of entries that can be acquired at one time when directory information is acquired from Active Directory. This value must match the setting for Active Directory's page size (the default is 1,000).

You can use the Windows `Ntdsutil` command to check Active Directory's page size.

4.2.19 AIM page

If the software operation status is to be monitored, this page sets the URL of Asset Information Manager Subset so that the Operation Log List, Operation Log Total, and Software Operation Status windows can be used.

Figure 4–22: AIM page



□ Use the display facility provided by Asset Information Manager

Specify the URL for Asset Information Manager.
(Specification format: http://AIM host name[:port number]/jp1asset)

URL for Asset Information Manager:

(1) Use the display facility provided by Asset Information Manager

To start the Operation Log List, Operation Log Total, and Software Operation Status windows, select this check box.

If Asset Information Manager Subset is installed on the computer running the managing server, this check box is selected by default; otherwise, this check box is not selected by default.

URL of Asset Information Manager

Specifies the URL of the Web site for Asset Information Manager Subset or JP1/Asset Information Manager in the following format (if the Web site employs SSL, replace `http` with `https`):

`http://`*`host-name`*`[:`*`port-number`*`]/jp1asset`

If Asset Information Manager Subset is installed on the computer running the managing server, the following URL is set by default:

`http://`*`local-host-name`*`/jp1asset`

host-name

Specifies the host name or IP address of the host on which Asset Information Manager Subset or JP1/Asset Information Manager is installed.

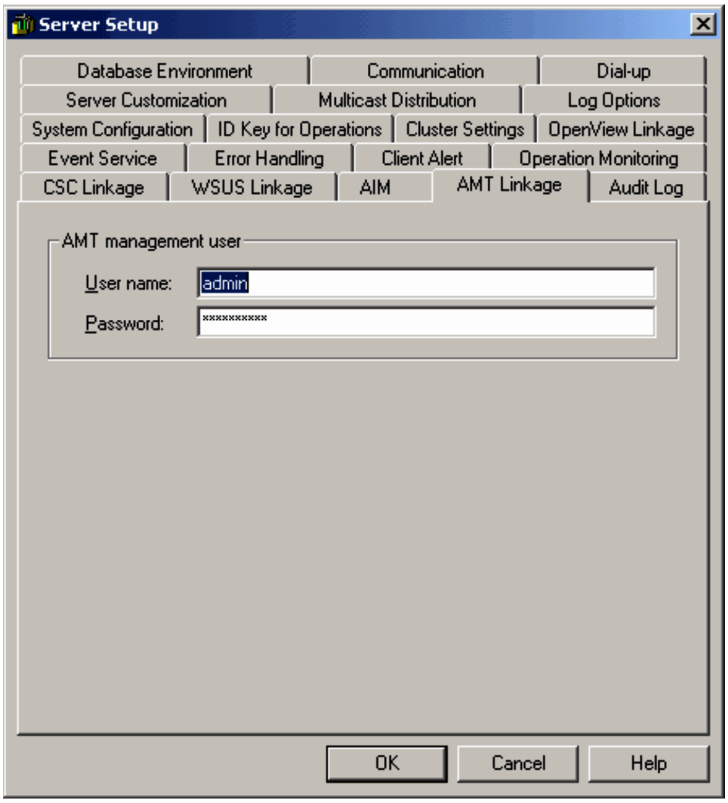
port-number

Specifies the port number of the Web site for Asset Information Manager Subset or JP1/Asset Information Manager.

4.2.20 AMT Linkage page

This page sets the information required in order to control clients using AMT Linkage. By default, the settings specified in the Settings for the AMT Linkage dialog box have been set during installation.

Figure 4–23: AMT Linkage page



AMT management user

User name: admin

Password: ***********

AMT management user

Sets the information needed to access the client's AMT. The user name and password must match the client's settings.

User name

Specifies the user name used to access the client's AMT, expressed as up to 60 characters.

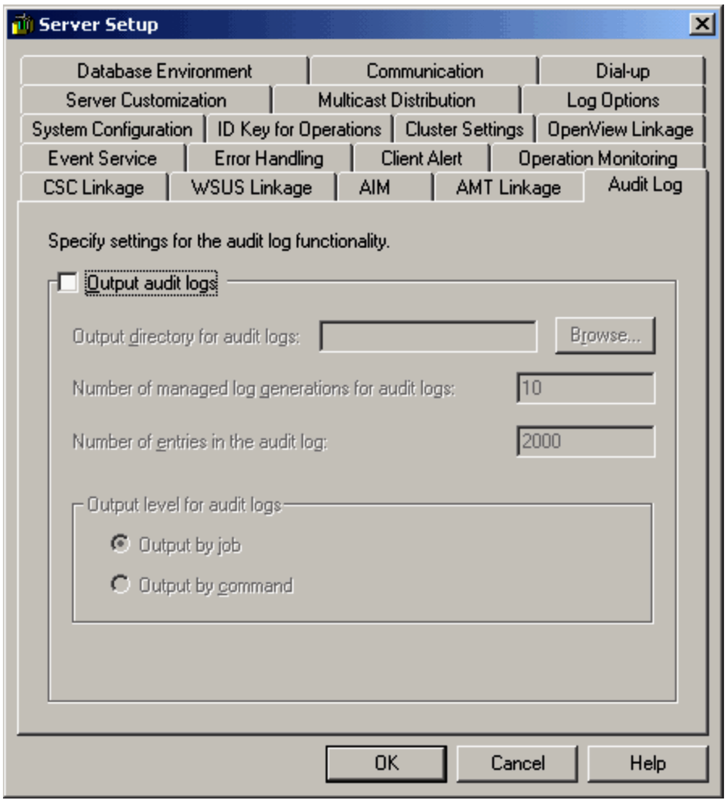
Password

Specifies the password used to access the client's AMT, expressed as up to 60 characters.

4.2.21 Audit Log page

This page sets whether or not audit logs are to be output. If you set to output audit logs, you can also set information such as the output destination and output level of audit logs.

Figure 4–24: Audit Log page



Specify settings for the audit log functionality.

☐ Output audit logs

Output directory for audit logs:

Number of managed log generations for audit logs: 10

Number of entries in the audit log: 2000

Output level for audit logs

● Output by job

○ Output by command

Output audit logs

Select this check box to output audit logs. By default, this option is not set. When this option is selected, the audit log-related settings are enabled.

Output directory for audit logs

Specifies the directory to which audit logs are to be output, expressed as 4 to 127 bytes of characters and the symbols _, \, ., :, (, and).

By default, no output-target directory is specified. For the specified output-target directory, you must grant write permission to the JP1/Software Distribution user.

The audit logs are output to the `NETMAuditManager`*n*`.LOG` file created directly under the directory that is specified here, where *n* indicates the generation number of the log file.

If the JP1/Software Distribution installation directory is specified as the audit log output directory, uninstalling JP1/Software Distribution will delete the audit logs. Specify the output directory that is appropriate to the audit log handling method that you use.

Number of managed log generations for audit logs

Specifies the number of generations in the range from 1 to 999 for the log file to which audit logs are output. The default is `10`.

If the number of audit log entries to be output exceeds the value specified in **Number of entries in the audit log**, a new log file `NETMAuditManager1.LOG` is created and the old log file is renamed `NETMAuditManager2.LOG`. Thereafter, each time a new log file is created, the generation number of the old log file is incremented by 1. When the number of generations exceeds the set value, the oldest log file is deleted.

Number of entries in the audit log

Specifies the number of audit log entries to be output per file in the range from 500 to 9,999. The default is 2,000 entries.

Output level for audit logs

Selects the output level of audit logs. By default, **Output by job** is selected.

When **Output by job** is selected, the audit logs of job execution results are output for each job. Note that the following jobs and operations are not monitored from JP1/NETM/Audit - Manager:

- ID group jobs
- Periodic jobs
- Installation operation by Package Setup Manager

When **Output by command** is selected, the detailed audit logs of job execution results are output for each destination and each package.

If JP1/Software Distribution manages many clients and **Output by command** is selected, output of a large number of audit logs may result in a shortage of disk space.

4.3 Specifying the basic settings for relay managers

Basic setup of a relay manager is required in order for the relay manager to function as a managing server or relay system. When the basic setup is completed, clicking the **OK** button displays the Setup dialog box again.

To immediately move on to detailed setup of the relay manager, click the **Detailed Setup for Relay Manager** button to display the Detailed Information Setup dialog box. If you click the **Exit** button without performing the detailed setup, the defaults are assumed for all detailed settings. For details about the detailed settings, see *4.4 Specifying the detailed settings for relay managers*.

If you change any of the settings in the relay manager setup, you must restart the relay manager service in order for the changes to take effect. While the relay manager service is running, make the changes to the setup and then click the **OK** button in the Relay Manager Setup dialog box. The relay manager service restarts.

The following table lists the basic setup items for a relay manager.

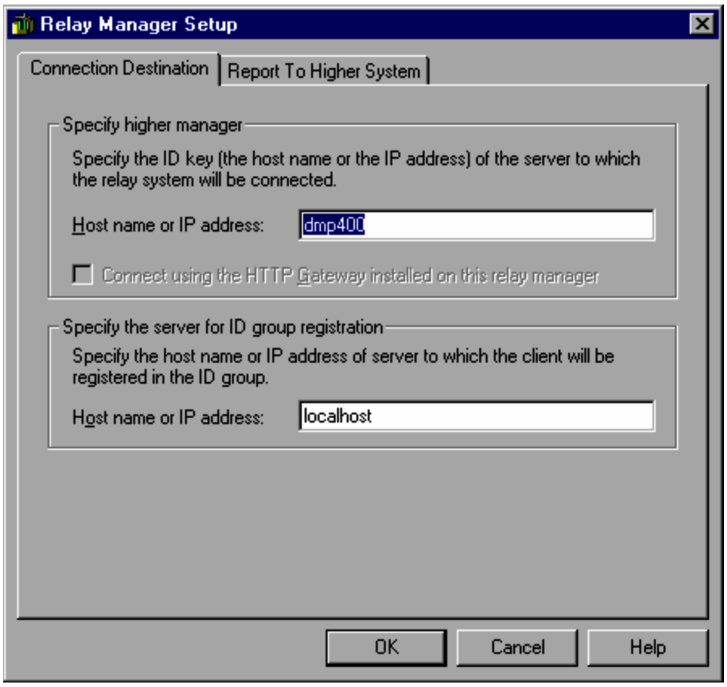
Table 4–3: Basic setup items for a relay manager

Classification	Item
Connection destination	Specify higher manager and Specify the server for ID group registration
Reporting to higher system	Send the result file to the server
	Execute, in parallel, the receiving of jobs from and the sending of result files to the higher system
	Report the split package distribution execution status of the lower system to the higher system
	Specify whether to relay operation monitoring history to the higher system

4.3.1 Connection Destination page

On this page, you set the connection destination of the relay manager.

Figure 4–25: Connection Destination page



Specify higher manager

Specify the ID key (the host name or the IP address) of the server to which the relay system will be connected.

Host name or IP address: dmp400

□ Connect using the HTTP Gateway installed on this relay manager

Specify the server for ID group registration

Specify the host name or IP address of server to which the client will be registered in the ID group.

Host name or IP address: localhost

(1) Specify higher manager

Specify the ID key (host name or IP address) of the higher system to which the relay manager will be connected. If you specify an IP address, do not include leading zeros in the element values. For example, in the case of IP address `10.020.020.010`, you would specify `10.20.20.10`.

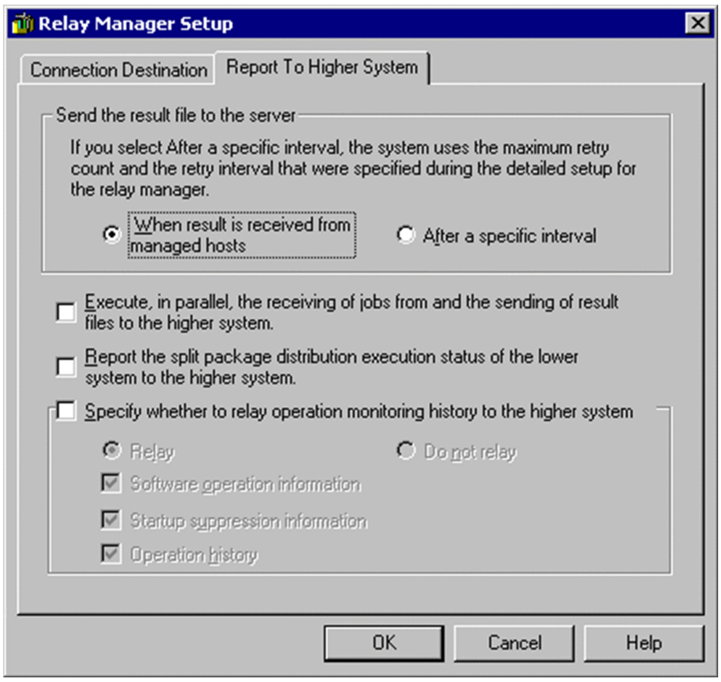
(2) Specify the Server for ID group registration

Specify the ID key (host name or IP address) of the higher system to which the client facilities for the relay manager will be registered in the ID group.

4.3.2 Report To Higher System page

On this page, you set the timing of sending the result files received from lower systems to the managing server.

Figure 4–26: Report To Higher System page



Send the result file to the server

If you select After a specific interval, the system uses the maximum retry count and the retry interval that were specified during the detailed setup for the relay manager.

● When result is received from managed hosts ○ After a specific interval

□ Execute, in parallel, the receiving of jobs from and the sending of result files to the higher system.

□ Report the split package distribution execution status of the lower system to the higher system.

□ Specify whether to relay operation monitoring history to the higher system

● Relay ○ Do not relay

☑ Software operation information

☑ Startup suppression information

☑ Operation history

(1) Send the result file to the server

Set the timing of sending the result files received from lower systems to the managing server. The default selection is **When result is received from managed hosts**.

When result is received from managed hosts

Sends the result file to the higher system whenever the file is received from a lower system. Select this option if you want to check the job execution result immediately.

Selecting this causes JP1 to issue an event when the client performs one of the following unauthorized operations.

- Connecting to a device whose operation is suppressed
- Starting up suppressed software
- Execution of a print operation by a client for which printing operations are suppressed

After a specific interval

Sends the result file received from a lower system to the higher system at specific intervals. The job execution result cannot be checked until the file transmission is executed.

If **When result is received from managed hosts** is selected, transmission costs may increase in network environments in which the number of connections between relay systems and higher systems affects transmission costs. It can also affect how efficiently result files are transmitted.

If 200 or more clients are located under the relay system and large numbers of jobs are executed from higher system targeted at clients, or when notification files are sent frequently from lower systems, select **After a specific interval** so that notification files are sent to higher systems at set intervals.

If you select **After a specific interval**, the relay manager sends result files according to the **Maximum retry count** and **Retry interval** settings you specified for **Resend the remaining installation result files** on the **Retry Communication** page of the Detailed Information Setup dialog box. If you select **After a specific interval** without selecting **Resend the remaining installation result files**, the relay manager sends result files with **Maximum retry count** and **Retry interval** set automatically to the default values.

(2) Execute, in parallel, the receiving of jobs from and the sending of result files to the higher system

Normally, you can establish only one connection from a relay manager to the higher system. This means you can usually not send results files to the higher system while receiving jobs nor receive jobs from the higher system while sending results files.

By enabling this option, you can concurrently receive (download) jobs from the higher system (central manager or relay manager) to which the local system connects and send (upload) results files to it. The default is that this check box is not selected.

When you select this check box, the relay manager is provided with two connections to the higher system. These connections make it possible to perform downloading and uploading concurrently. However, because the number of connections to the higher system increases, the load on the network also increases. In addition, the number of client connections to the relational database also increases. Thus, you should select this option only if the network environment has sufficient capacity.

■ Estimating the number of subsystems that can be connected concurrently

When this option is selected, the relay manager is provided with two connections to the higher system. Therefore, during setup of the higher system (central manager), it is necessary to increase the value of **Number of subsystems that can be connected at one time**. Use the following formula to determine the appropriate value:

Number of subsystems that can be connected at one time
= number of relay systems to be directly connected **x** 2
+ number of clients to be directly connected
+ number of Remote Installation Managers to be concurrently connected
+ number of packagers to be concurrently connected **x** 2

If Microsoft SQL Server or Oracle is used on the higher system, you must also increase the number of clients that can connect to the relational database. The method for determining the number of clients connected to the relational database depends on the database in use (Oracle or Microsoft SQL Server).

For Oracle

For details about how to estimate the value, see *7.3.3(2) Tuning the initialization parameter file*.

Determine the number of clients that can be connected using the *number of concurrent client or relay system connections* as the **Number of subsystems that can be connected at one time**.

For Microsoft SQL Server

For details about how to estimate the value, see *7.3.2(2) Tuning the database environment*.

Determine the number of clients that can be connected using the *number of concurrent client or relay system connections* as the **Number of subsystems that can be connected at one time**.

(3) Report the split package distribution execution status of the lower system to the higher system

If you use split distribution of packages, select this check box to report the distribution progress at the lower systems to the higher system. The default is that this check box is not selected.

When you select this check box, you can use Remote Installation Manager's Job Status window on the higher system to check the status of split distribution that is underway at systems positioned lower than the relay manager/system.

For details about checking the status of split distribution in the Job Status window, see *8.4.3 Items displayed in the Job Status window* in the manual *Administrator's Guide Volume 1*.

Note that when this option is enabled, the network's workload increases due to the increase in the volume of communication associated with reporting the execution status of split distribution from the lower systems to the higher system. This setting is therefore recommended only for a network environment with sufficient capacity. Do not select this check box if the higher system's version is 07-50 or earlier, or if it is UNIX, because the execution status of split distribution in the lower systems cannot be checked even when this option is selected.

(4) Specify whether to relay operation monitoring history to the higher system

The destination of operation information depends on whether the operation monitoring policy is applied via the relay manager, or by executing a job from the relay manager. This option enables you to specify whether the operation information reported from lower systems is to be managed by the relay manager, or also reported to the higher system. The default is that this check box is not selected.

(a) Operation when the check box is selected

The following describes how this operation is handled depending on whether **Relay** or **Do not relay** is selected.

Relay

Operation information that is reported periodically from the client or that is acquired by the *Get software monitoring information from the client* job is always reported to the higher system via the relay manager.

If the policy is applied from the higher system, the operation information is sent to the higher system that applied the policy. If the policy is applied from the relay manager, the operation information is sent to the higher system at the connection destination of the relay manager.

You can also select the information you want reported to the higher system. The following information may be selected:

- Software operating information
- Startup suppression information
- Operation histories

If **Relay** is selected, choose at least one of the above types of information. The default is that all check boxes are selected.

Notes

To issue a JP1 event when the client performs one of the following unauthorized operations, select the **Startup suppression information** check box.

- Connecting to a device whose operation is suppressed
- Starting up suppressed software
- Execution of a print operation by a client for which printing operations are suppressed

If the following check boxes are selected on the **Event Service** page of server setup for both the managing server and the relay manager, a JP1 event with the same content is reported to JP1/IM.

- **Unauthorized operation event in operation monitoring**
- **Startup suppression information**

To prevent this, specify one of the following settings:

- Select **Do not relay**
- Clear the **Startup suppression information** check box
- Clear the **Unauthorized operation event in operation monitoring** check box on the **Event Service** page of the managing server and the relay manager.

Do not relay

Operation information reported from lower systems is not reported to any system above the relay manager that specified this setting.

For example, when a *Get software monitoring information from the client* job is executed from the higher system, the operation information obtained from the lower systems is sent to the relay manager, not to the higher system.

(b) Operation when the check box is not selected

Information that is reported periodically from the client or operation information that is acquired by the *Get software monitoring information from the client* job is sent to the system that applied the operation monitoring policy (the system that executed the *Set the software monitoring policy* job).

For example, if the policy is applied from the higher system, the operation information is sent to the higher system even if the *Get software monitoring information from the client* job is executed from the relay manager.

Note

When this check box is not selected and the **Unauthorized operation event in operation monitoring** check box on the **Event Service** page of server setup is selected in both the managing server and the relay manager, both systems may report identical JP1 events to JP1/IM. To prevent this, make sure the **Unauthorized operation event in operation monitoring** check box in the **Event Service** page of either the managing server or the relay manager is not selected.

4.4 Specifying the detailed settings for relay managers

Detailed setup of a relay manager is required in order for the relay manager to function as a client. When the detailed setup is completed, clicking the **OK** button displays the Setup dialog box again.

If you change any of the settings in the relay manager setup, you must restart the relay manager service in order for the changes to take effect. While the relay manager service is running, make the changes to the setup and then click the **OK** button in the Detailed Information Setup dialog box. The relay manager service restarts.

The following table lists the detailed setup items for a relay manager.

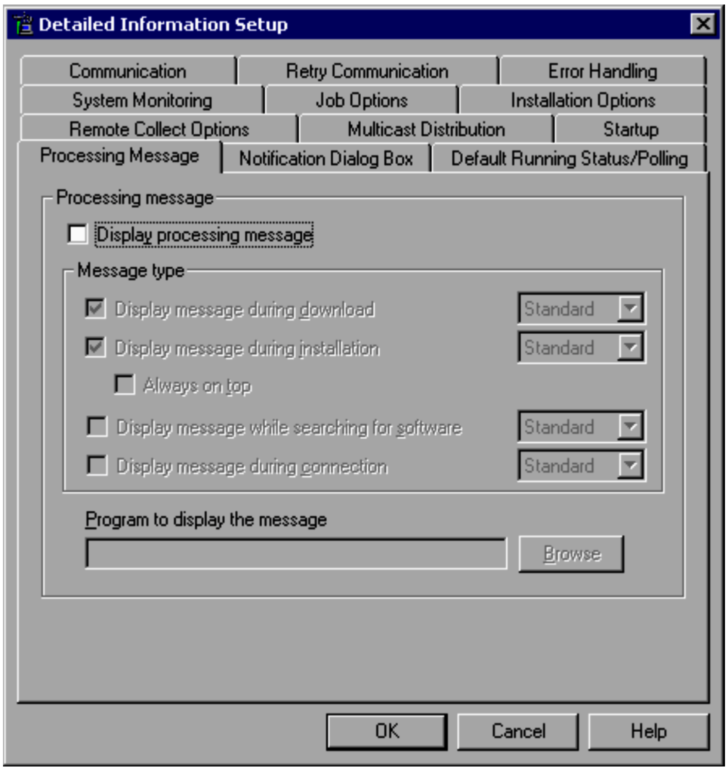
Table 4–4: Detailed setup items for a relay manager

Category	Item
Processing Message	Display processing message
	Program to display the message
Notification Dialog Box	Display Message box at job error
	Prompt users before deletion whenever a shortcut in Software Distribution Client startup fails
	Display the Update User Information dialog box at system startup
	Display the Update User Information dialog box at periodic execution
Default Running Status/Polling	Start client automatically at system startup
	Whether client will poll managing server
	Polling frequency
Communication	Port numbers
	Protocol used by the higher system requesting the client to start a job
	File transfer buffer size
	Wait for response from communications software
	Multiple network adapters
	Automatic registration of this computer in the system configuration
	Also report inventory to the server
Retry Communication	Socket connection (retry count/interval)
	Communication failure (retry count/interval)
	Installation results files failed to transmit to the higher server
Error Handling	Generations of log file to be saved
	Maximum lines in a log file
	Type of Event Viewer message
System Monitoring	System monitoring
	Display the System Monitoring icon
	Display alert messages
	Report alerts to the higher system
	Report inventory to the higher system when the system is changed
Job Options	Automatic inventory update

Category	Item
Job Options	Suppress periodic jobs when the connection destination of the client is changed
	Suppress reports of the job status *Waiting for installing/collecting* to the higher system
	Do not repeat package IDs when collecting software information
Installation Options	Installation/file collection job (retry count/interval)
	Split package distribution
	Check local disk capacity before unpacking software
	Store installation history in the event of an installation error
	Delete the work directory for installing Hitachi program products after installation
	`InstallShield` timeout
Remote Collect Options	Restricting remote collection jobs executed on the client
Multicast Distribution	Port numbers for multicast distribution and allowing jobs to be distributed using multicast distribution (multicast address)
Startup	Create Software Distribution Client Startup folder
	Move programs in Startup group to the Software Distribution Client Startup group
	Select shortcuts to move programs to the Software Distribution Client Startup group

Note that the settings in the Detailed Information Setup dialog box are the same as those in the Client Setup dialog box for JP1/Software Distribution Client (client); for details, see *6.2 Setting up Client*.

Figure 4–27: Detailed Information Setup dialog box



Detailed Information Setup

Processing message

☐ Display processing message

Message type

☑ Display message during download — Standard

☑ Display message during installation — Standard

☐ Always on top

☐ Display message while searching for software — Standard

☐ Display message during connection — Standard

Program to display the message

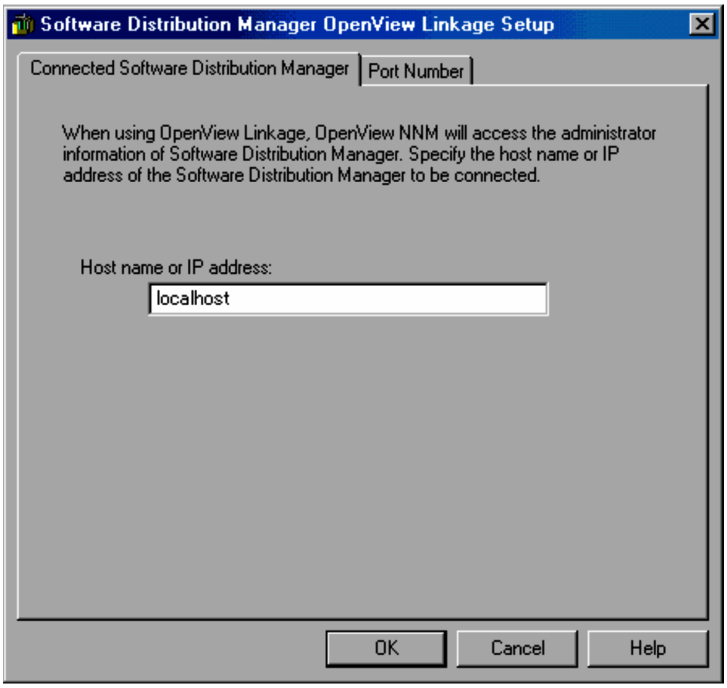
4.5 Setting up hp OpenView Linkage

You use the Software Distribution Manager OpenView Linkage Setup dialog box to set up the operating environment for using OpenView Linkage. When you finish with the settings, click the **OK** button to display the Setup dialog box.

4.5.1 Connected Software Distribution Manager page

Specify the host name or IP address of the JP1/Software Distribution Manager to which OpenView Linkage connects.

Figure 4–28: Connected Software Distribution Manager page



Software Distribution Manager OpenView Linkage Setup
Connected Software Distribution Manager
Port Number
OK
Cancel
Help

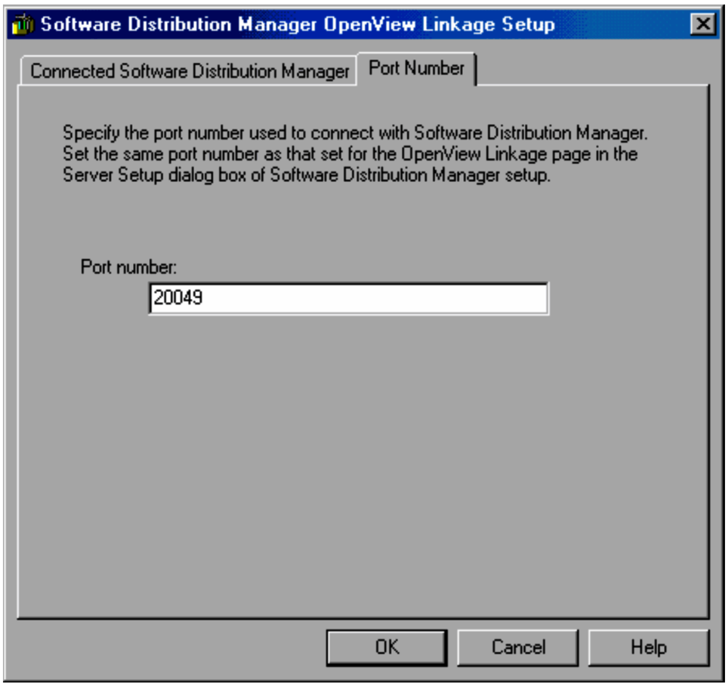
When using OpenView Linkage, OpenView NNM will access the administrator information of Software Distribution Manager. Specify the host name or IP address of the Software Distribution Manager to be connected.

Host name or IP address: localhost

4.5.2 Port Number page

Specify the port number that HP NNM version 7.5 or earlier uses to gain access to JP1/Software Distribution's administrator information.

Figure 4–29: Port Number page



Software Distribution Manager OpenView Linkage Setup
Connected Software Distribution Manager
Port Number

Specify the port number used to connect with Software Distribution Manager. Set the same port number as that set for the OpenView Linkage page in the Server Setup dialog box of Software Distribution Manager setup.

Port number: 20049

This setting must be the same value specified on the **OpenView Linkage** page of the server setup. The default is `20049`.

4.6 Registry settings (JP1/Software Distribution Manager)

You can set items not found in the setup procedure by editing the registry. Those items are described below.

(1) Display OS name

The following OS names can be displayed in the **Selected OSs** of the Condition Settings dialog box shown in the inventory viewer, and under **Comment** in the CSV Output Utility dialog box (specify output constraints) of the CSV output utility.

- Windows Server 2008 Datacenter
- Windows Server 2008 R2 Datacenter

To display these operating systems, create the registry value shown below in registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi\NETM/DM`. For 32-bit operating systems, create the registry value in registry key `HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\NETM/DM`.

Name

`Win2008DeOption`

Type

`REG_SZ`

Data

`YES`

(2) Continue command processing after Windows logoff

If the PC on which JP1/Software Distribution Manager is installed is running any of the operating systems shown below, command processing can be made to continue even after you log off of Windows, when processing commands other than `dcmmonrst.exe` (store operating information in database) or `dcmstdiv.exe` (input offline machine information).

- Windows 2000
- Windows XP
- Windows Server 2003

For the commands that can be executed, see *4.2.1 Command types* in the manual *Administrator's Guide Volume 2*.

To have command processing continue after logging off of Windows, create the registry value shown below in registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi\NETM/DM`. For 32-bit operating systems, create the registry value in registry key `HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\NETM/DM`.

Name

`CmdLogoffContinue`

Type

`REG_SZ`

Data

`YES`

Notes

- To have command processing continue after logging off of Windows, the command must be executed from the service. Processing of commands executed by any other method will not continue after logging off of Windows even if the registry is set up to do so.
- If the OS of the PC where JP1/Software Distribution Manager is installed is Windows Server 2012, Windows 8, Windows Vista, Windows Server 2008, or Windows 7, processing of commands executed from the service will continue after Windows logs off regardless of the registry settings.

  - Operation will vary depending on the combination of registry settings and whether or not the command argument `/LC` was specified. For details, see *4.28 Command operation at logoff that depends on a registry setting and logoff option* in the manual *Administrator's Guide Volume 2*.

(3) Outputting a Unicode file in CSV format

A Unicode CSV file can be output using the CSV output utility or the CSV output command (`dcmcsvu.exe`). To output a Unicode CSV file, all the following conditions must be fulfilled.

- The output request must be executed from JP1/Software Distribution Manager.
- JP1/Software Distribution must be using the following relational database:
  - Microsoft SQL Server 2005 or later
- One of the following templates must be specified when the CSV output utility or CSV output command (`dcmcsvu.exe`) was executed:
  - System information
  - Previously installed package information
  - Registry collection item
  - Microsoft Office products
  - Anti-virus products

To output a Unicode CSV file, create the following registry value in the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi\NETM/DM`. For 32-bit operating systems, create the registry value in registry key `HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\NETM/DM`.

Name

`UnicodeOption`

Type

`REG_SZ`

Data

`YES`

5 Setting Up JP1/Software Distribution Client (relay system)

This chapter explains how to set up JP1/Software Distribution Client (relay system).

Only a user with Administrator permissions can set up JP1/Software Distribution Client (relay system).

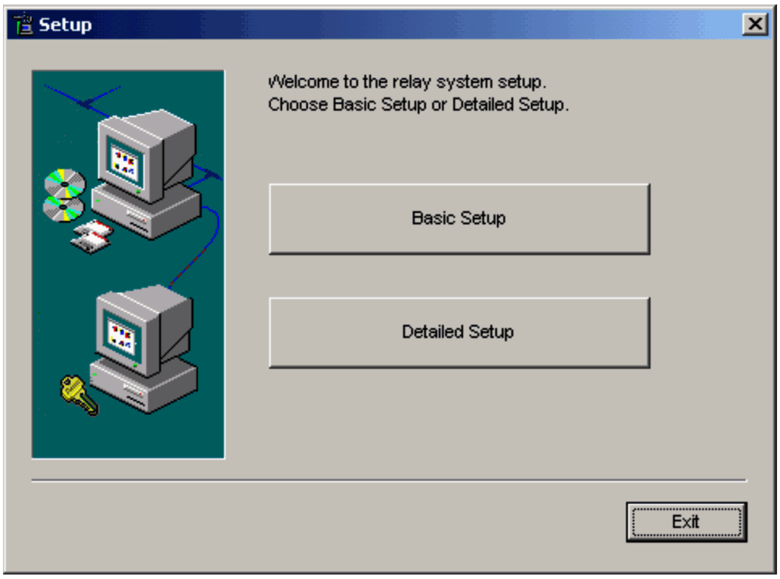
5.1 JP1/Software Distribution Client (relay system) setup procedure

This section describes the setup procedure for JP1/Software Distribution Client (relay system).

To set up JP1/Software Distribution Client (relay system):

1. From the **Start** menu choose **Software Distribution SubManager**, and then **Setup**.
   The Setup dialog box appears:

   Figure 5–1: Setup dialog box

   Welcome to the relay system setup.
   Choose Basic Setup or Detailed Setup.

2. Click the **Basic Setup** button or **Detailed Setup** button.
   The setup program for the selected setup type starts.
3. When you finish with the setup, click the **Exit** button.
   The setup is completed.

The following sections describe the procedures for basic setup and detailed setup for relay systems.

5.2 Specifying the basic settings for relay systems

Basic setup is required when JP1/Software Distribution Client (relay system) serves as a managing server or as a relay system. When you finish setting the basic setup and click the **OK** button, the Setup dialog box appears. If you wish to perform the detailed setup for the relay system, click the **Detailed Setup** button to display the Detailed Information Setup dialog box. If you click the **Exit** button without performing the detailed setup, the defaults are assumed for all detailed settings. For details about the detailed settings, see *5.3 Specifying the detailed settings for relay systems*.

If you change any of the settings in the relay system setup, you must restart the relay system service before the changes will take effect. While the relay system service is running, changing the setup and then clicking the **OK** button in the Relay System Setup dialog box restarts the relay system service.

The following table lists the basic setup items for a relay system.

Table 5–1: Basic setup items for a relay system

Category	Item
Connection Destination	Host name or IP address of the higher system (JP1/Software Distribution Manager, JP1/Software Distribution Client (relay system), or JP1/Software Distribution SubManager)
	Poll multiple higher systems
	Host name or IP address of the system for ID group registration (JP1/Software Distribution Manager, JP1/Software Distribution Client (relay system), or JP1/Software Distribution SubManager)
Communication	Startup protocol (UDP or TCP)
	Interval transfer
Dial-up	Authentication information (user name, password, domain)
Relay System Customization	Number of clients that can be connected at once
	Maximum number of relays or clients in which jobs can execute concurrently
	Record the system/software information answered from the lower clients
	Record the results of ID group jobs
	Monitor startup of subsystems
	Monitor file transfer errors of subsystems
	Accept suspended/resumed file transfer jobs from sources other than the connection destination
Report To Higher System	Timing for sending results files to the server
	Execute in parallel receive of jobs from and send of results files to the higher system
	Report the split package distribution execution status of the lower system to the higher system
Multicast Distribution	Settings for sending jobs by multicast distribution (multicast address and packet size)
System Configuration	Apply system configuration information automatically
	Linkage when system configuration is changed
ID Key for Operations	Select the node identification key (host names/IP addresses)
	Resolving IP address
	When resolution of IP address fails
Event Service	Enable event service
Remote Installation Manager	Report the installation status to the managing server

Category	Item
Remote Installation Manager	Report the ID group job status to the managing server
Client Alert	Relay client alert information to the higher system
	Output client alert information (CSV file or Event Viewer)
AMT Linkage#	AMT management user's user ID and password

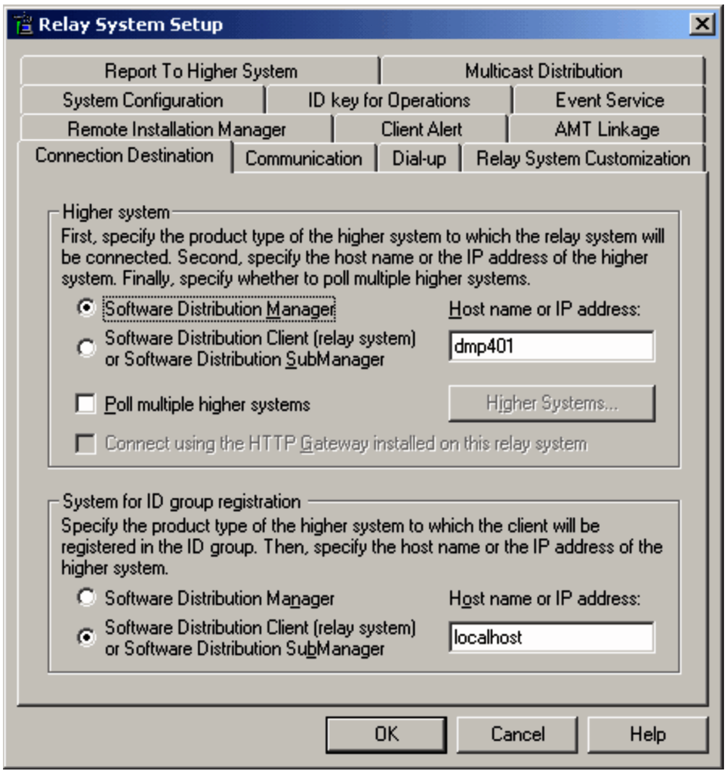
#

This item is displayed if AMT Linkage has been installed.

5.2.1 Connection Destination page

On this page, you set the connection destination of the relay system.

Figure 5–2: Connection Destination page



Higher system

First, specify the product type of the higher system to which the relay system will be connected. Second, specify the host name or the IP address of the higher system. Finally, specify whether to poll multiple higher systems.

● Software Distribution Manager

○ Software Distribution Client (relay system) or Software Distribution SubManager

Host name or IP address: dmp401

□ Poll multiple higher systems

□ Connect using the HTTP Gateway installed on this relay system

System for ID group registration

Specify the product type of the higher system to which the client will be registered in the ID group. Then, specify the host name or the IP address of the higher system.

○ Software Distribution Manager

● Software Distribution Client (relay system) or Software Distribution SubManager

Host name or IP address: localhost

(1) Higher system

Select the local system's higher system. Select JP1/Software Distribution Manager, JP1/Software Distribution Client (relay system), or JP1/Software Distribution SubManager (JP1 Version 7i or earlier for Windows; JP1 Version 8 or earlier for Unix).

The following table shows the supported product types and the corresponding product names:

Product type	Corresponding product name
JP1/Software Distribution Manager	JP1/Software Distribution Manager for Windows Software Distribution Manager for Windows JP1/Software Distribution Manager for UNIX JP1/Software Distribution for UNIX

Product type	Corresponding product name
JP1/Software Distribution Manager	JP1/Software Distribution Workstation Assistant for UNIX Software Distribution for UNIX Software Distribution Workstation Assistant for UNIX
JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager	JP1/Software Distribution Client (relay system) for Windows JP1/Software Distribution SubManager for Windows Software Distribution SubManager for Windows JP1/Software Distribution Client (relay system) for UNIX JP1/Software Distribution SubManager for UNIX JP1/Software Distribution Workstation for UNIX Software Distribution Workstation for UNIX

Host name or IP address

Based on the operation key (host name or IP address) used by the higher system, specify the address of the higher system. Specify it as follows.

- If the operation key is the host name, set the host name of the higher system (full name).
- If the higher system is an environment that uses a DNS server, set the fully qualified domain name (the host name followed by a period and domain name).
- If the higher system has multiple network adapters that are connected to the same segment, set the host name with the highest priority in the bind order set by the higher system OS as the higher connection target of the relay system.

Poll multiple higher systems

Specifies whether multiple higher systems are to be polled (multi-polling) when there are multiple job execution routes from the managing server. The default is that this check box is not selected. When this check box is selected, the **Higher Systems** button is enabled. Click this button to open the Specify Higher Systems dialog box. In this dialog box, specify settings such as the names and priority levels of the higher systems. Note that you must use the ID key for operations (host names or IP addresses) to specify the higher system names.

When a higher system other than the local system is specified as the system for ID group registration, and you change the higher system whose priority level is 1, the system for ID group registration is also changed to the new higher system that has priority level 1.

Note that when you specify the ID key for operations for the higher system names, they must all be either host names or IP addresses.

For details about the multi-polling function, see *6.4.1 Multi-polling environment for a relay system* in the *Description and Planning Guide*.

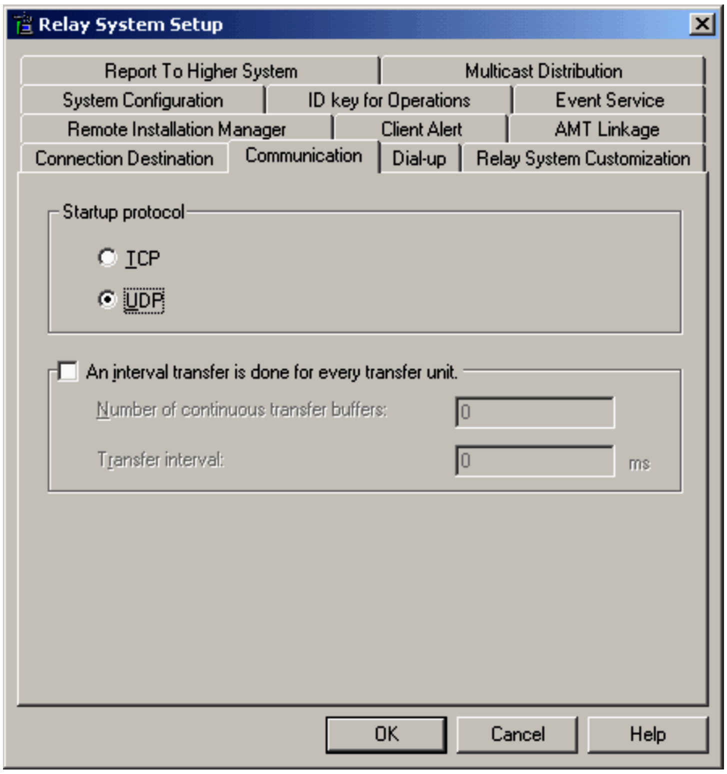
(2) System for ID group registration

Select the higher system that performs ID group registration. Select JP1/Software Distribution Manager, JP1/Software Distribution Client (relay system), or JP1/Software Distribution SubManager (JP1 Version 7i or earlier for Windows; JP1 Version 8 or earlier for Unix). Also specify the address of the higher system with the ID key for operations (host name or IP address) used by the higher system.

5.2.2 Communication page

On this page, you specify the startup protocol and whether or not internal transfer is to be performed.

Figure 5–3: Communication page



Startup protocol

○ TCP

● UDP

□ An interval transfer is done for every transfer unit.

Number of continuous transfer buffers: 0

Transfer interval: 0 ms

(1) Startup protocol

Select **UDP** or **TCP** as the protocol to be used when the local system is started. The default is **UDP**.

If you select **TCP** and set a port number in the `services` file, also add the following entry to the `services` file: `netmdm` *xxxxx*`/tcp` (where *xxxxx* is the port number).

Note that programs may not start in a WAN environment if you select **UDP**.

(2) Interval transfer

When a file transfer to subsystems occurs, the file can be divided into specified units and the divided file segments are transferred at regular intervals. This transfer method can reduce the load on the network during file transfer. The default is that this check box is not selected.

Interval transfer is not performed from a subsystem to its higher system.

Number of continuous transfer buffers

File transfer buffer size specified during setup at the destination system determines the buffer size. For example, if **File transfer buffer size** is 4,096 bytes and **Number of continuous transfer buffers** is set to `2`, the job is divided into units of 8,192 bytes.

You can specify a value in the range from 0 to 4,294,967,295 in **Number of continuous transfer buffers**. The default is `1`. If you specify `0`, interval transfer is not performed.

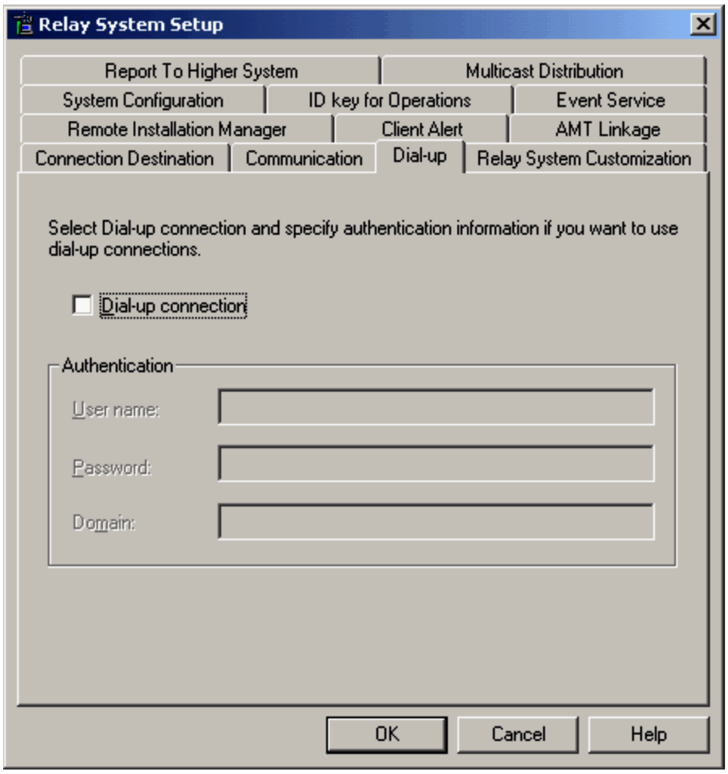
Transfer interval

Specifies the interval time between transfers when interval transfer is performed. You can specify a value in the range from 0 to 4,294,967,295 milliseconds. The default is 1,000 milliseconds. If you specify `0`, interval transfer is not performed.

5.2.3 Dial-up page

To use dial-up connections, select the **Dial-up connection** check box and specify the user name, password, and domain to be used during dialing. This page is displayed only in an environment that supports dial-up connection.

Figure 5–4: Dial-up page



Select Dial-up connection and specify authentication information if you want to use dial-up connections.

□ Dial-up connection

Authentication

User name:

Password:

Domain:

Dial-up connection

Select this check box if you use a dial-up connection. The default is that this check box is not selected.

Authentication

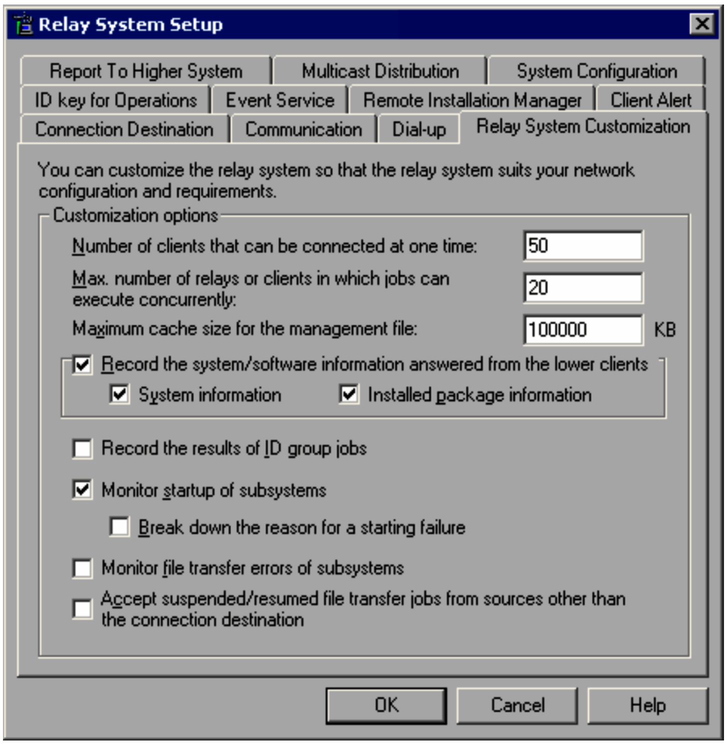
Set the user name, password, and domain that are used during dial-up connection.

For details about a dial-up connection, see *6.6 Settings for dial-up connections* in the *Description and Planning Guide*.

5.2.4 Relay System Customization page

If you will be using the local system as a managing server or a relay system, set items for tuning the CPU, memory, and networks. For an overview of tuning, see *6.1.7(2) Adjusting the maximum number of hosts that can be connected concurrently* in the *Description and Planning Guide*.

Figure 5–5: Relay System Customization page



You can customize the relay system so that the relay system suits your network configuration and requirements.

Customization options

Number of clients that can be connected at one time: 50

Max. number of relays or clients in which jobs can execute concurrently: 20

Maximum cache size for the management file: 100000 KB

☑ Record the system/software information answered from the lower clients

☑ System information ☑ Installed package information

□ Record the results of ID group jobs

☑ Monitor startup of subsystems

□ Break down the reason for a starting failure

□ Monitor file transfer errors of subsystems

□ Accept suspended/resumed file transfer jobs from sources other than the connection destination

The following describes items unique to this page. The other settings are the same as on the **Server Customization** page for the Server setup for JP1/Software Distribution Manager. For details, see *4.2.4 Server Customization page*.

Number of clients that can be connected at one time

You can limit the number of subsystems that can be connected at one time. Specifically, this value becomes the number of socket connections. Each socket connection is counted from the time it is established until the time it is released. Determine the value using the formula shown below:

Number of subsystems that can be connected at any one time =

number of directly connected systems + number of Packagers to be connected **x** 2

The minimum value is 4, the maximum is 9,999, and the default is 50.

If the network traffic is heavy, resulting in many packet collisions, you can reduce the traffic by reducing this value, thereby reducing the number of subsystems that can be connected at one time.

A connection request from a subsystem that exceeds this value will be denied, but once there is room in the number of connections, execution requests are sent again.

Max. number of relays or clients in which jobs can execute concurrently

Specify the maximum number of subsystems that can process jobs concurrently. Specifically, this value becomes the number of startup messages the managing server sends at one time to subsystems (in other words, the number of clients that can execute jobs concurrently). If users execute jobs for more clients than the value specified in this field, the system splits the jobs on the basis of the specified value and executes them.

The minimum value is `0`, the maximum is `9,999`, and the default is `20`. If you specify `0`, the managing server no longer sends startup messages to the lower systems, disabling job execution initiated by higher systems as well as target system startup using the client control facility. If the size of the files to be distributed is large (10 MB or greater), the LAN load may become high even when only a few clients are connected. Therefore, you should specify a value that matches the network performance. The result of *maximum number of relays or clients in which jobs can execute concurrently* **x** *package size* becomes the amount of data that flows over the network at one time.

Specify a value that does not exceed the value specified in **Number of clients that can be connected at one time**. If the subsystems are connected through a circuit-switched network, specifying a number greater than the number of agreement lines serves no purpose.

Maximum cache size for the management file

Specify the maximum size of the information about the jobs executed from the higher system or relay system (management files) that is to be cached in the relay system's memory. The minimum value is 0, the maximum is 1000000 (1 gigabyte), and the default is 100000 (100 megabytes). If you specify 0, the function for caching management files is disabled.

When a job is created, its management file is cached in memory until the job is deleted. If the total size of the cached management files exceeds the maximum size you have specified, job processing throughput will deteriorate. To avoid such deterioration of job processing throughput, you should take care to specify a maximum cache size for the management file that is appropriate to the actual scope of your operations. Determine the value based on the estimated value of each item in the following formula:

Cache size for the management files (kilobytes) =

Number of jobs stored in the relay system and that are executed from the higher system or this relay system

x *number of destinations for each job*

x *number of packages for each job* (applicable to remote installation jobs)

x 1 kilobyte

When the maximum size would be exceeded because of a need to cache another management file, the least frequently referenced management file is deleted so that the new management file can be cached.

Record the system/software information answered from the lower clients

Specify whether or not system information and installed-package information that are sent from a lower system when jobs are executed is to be recorded. By default, this check box is selected.

System information

Records system information that is reported from a lower system when jobs are executed. By default, this check box is selected.

Installed package information

Records installed package information that is reported from a lower system when jobs are executed. By default, this check box is selected.

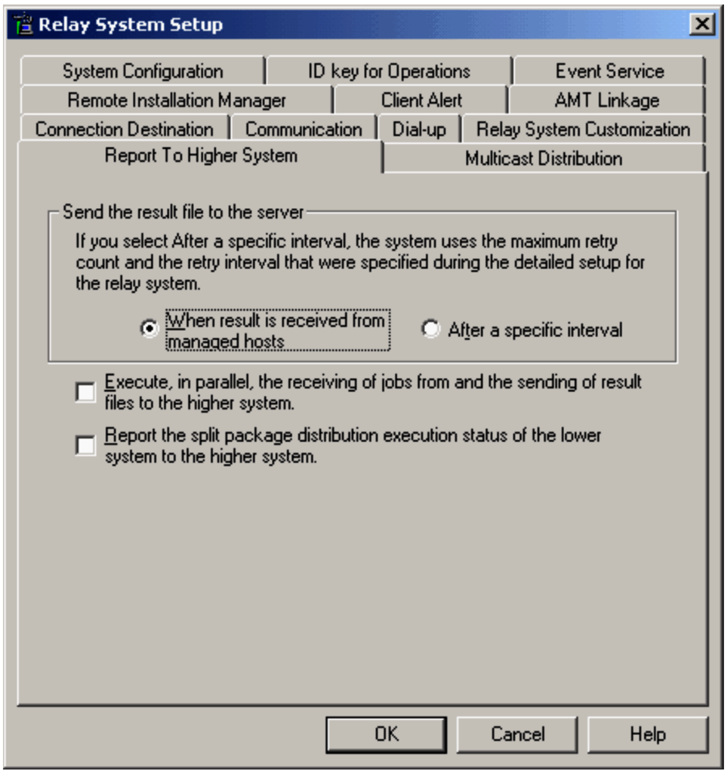
Record the results of ID group jobs

Specify whether or not the results of ID group jobs that are executed by clients and that terminate normally are to be recorded. ID group jobs that result in an error are recorded regardless of this setting. To check the results of ID group jobs in the relay system, the client's execution results must be managed in the relay system that manages the ID group. The results from each client are deleted when the ID group job is invalid or cancelled. The default is that this check box is not selected.

5.2.5 Report To Higher System page

Specify the timing for sending results files received from the subsystems to the managing server.

Figure 5–6: Report To Higher System page



Send the result file to the server

If you select After a specific interval, the system uses the maximum retry count and the retry interval that were specified during the detailed setup for the relay system.

● When result is received from managed hosts ○ After a specific interval

□ Execute, in parallel, the receiving of jobs from and the sending of result files to the higher system.

□ Report the split package distribution execution status of the lower system to the higher system.

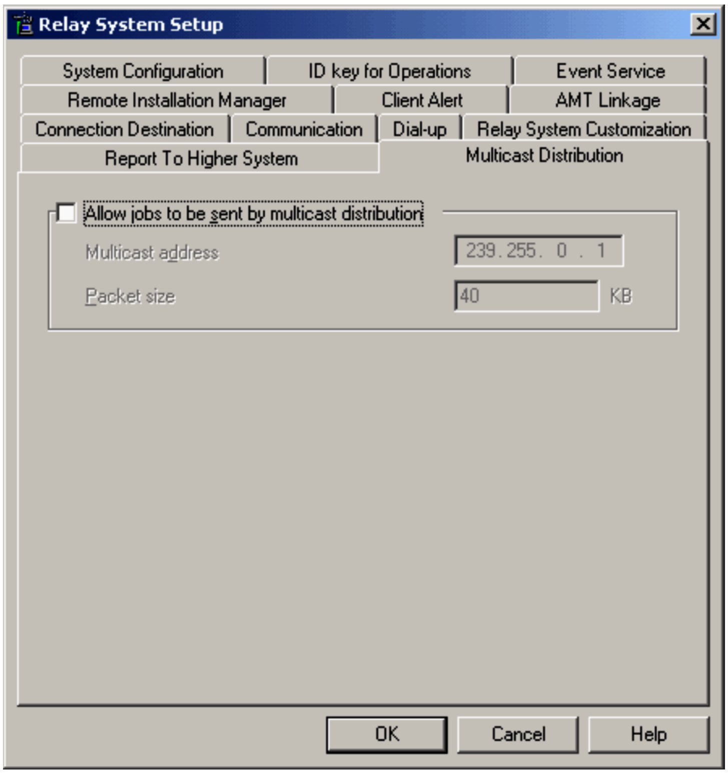
The settings are the same as on the **Report To Higher System** page of the relay manager setup for JP1/Software Distribution Manager. See *4.3.2 Report To Higher System page*.

5.2.6 Multicast Distribution page

These settings are for distributing jobs to lower systems using multicast distribution. The settings on this page apply to jobs for which you specify multicast distribution.

You cannot use this page to specify port number for multicast distribution or the port number for packet resend requests. You must specify these port numbers in the detailed setup for the relay system. A relay system uses the same value for the port number for sending jobs and the port number for receiving jobs.

Figure 5–7: Multicast Distribution page



□ Allow jobs to be sent by multicast distribution

Multicast address 239 . 255 . 0 . 1

Packet size 40 KB

(1) Allow jobs to be sent by multicast distribution

Select this option and specify the multicast address and packet size for using the multicast method to send to lower systems jobs for which you have specified multicast distribution. The default is that this check box is not selected.

When this check box is not selected, jobs for which multicast distribution is specified are distributed by unicast distribution. Conversely, even if you select this check box, jobs for which unicast distribution is specified are sent by unicast distribution.

You should clear the **Allow jobs to be sent by multicast distribution** check box if there is a router in the network that is not compatible with IP multicasting. If the network includes routers that are not compatible with IP multicasting, you cannot use multicast distribution. If you do select **Allow jobs to be sent by multicast distribution**, the system will require a long time to switch to unicast distribution in order to send the job.

Multicast address

Specifies the multicast address assigned to the multicast group to which jobs are to be distributed. Specify a value in the range from 224.0.1.0 to 239.255.255.255. Do not specify an address already assigned to another multicast group. The default address is 239.255.0.1.

A multicast group is a group of lower systems directly connected to this JP1/Software Distribution Client (relay system). If the multicast address of the lower systems to which a job is to be distributed does not match the multicast address you specify here, the job will be distributed to those lower systems using unicast distribution.

For details about multicast groups and multicast addresses, see *6.2.1 Unicast distribution and multicast distribution* and *6.2.3 System configuration for multicast distribution* in the *Description and Planning Guide*.

Packet size

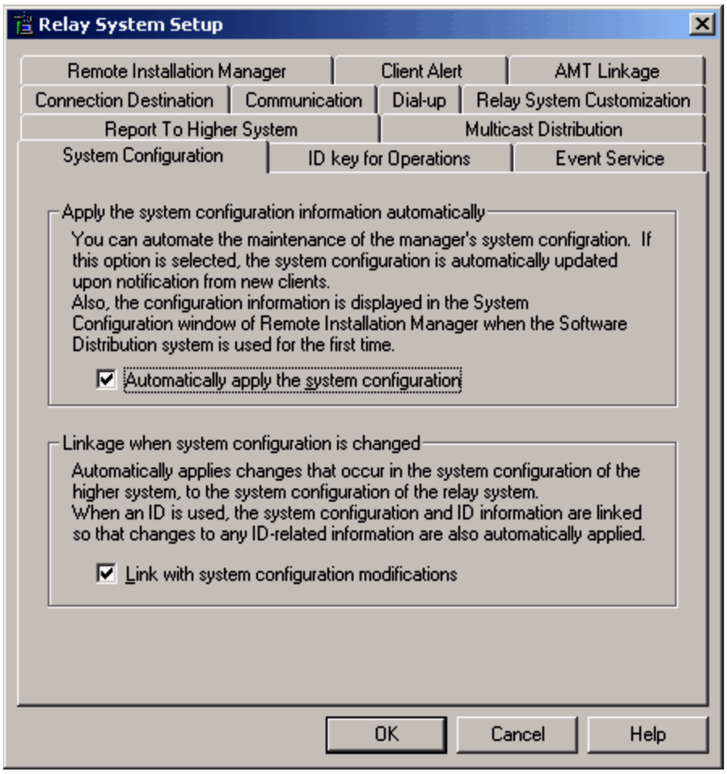
Specify the packet size to be used for distributing a job. Specify a value in the range from 1 to 60 KB. The default is 40 KB.

40 KB is an efficient value for communications lines for 100BASE. For communications lines for 10BASE, you should specify 4 KB. If you specify a packet size that is too large, multicast distribution will fail and the system will continue distribution using unicast distribution.

5.2.7 System Configuration page

If the local system will be used as a relay system, specify settings for reporting various information items to the higher system.

Figure 5–8: System Configuration page



Apply the system configuration information automatically

You can automate the maintenance of the manager's system configration. If this option is selected, the system configuration is automatically updated upon notification from new clients.
Also, the configuration information is displayed in the System Configuration window of Remote Installation Manager when the Software Distribution system is used for the first time.

☑ Automatically apply the system configuration

Linkage when system configuration is changed

Automatically applies changes that occur in the system configuration of the higher system, to the system configuration of the relay system.
When an ID is used, the system configuration and ID information are linked so that changes to any ID-related information are also automatically applied.

☑ Link with system configuration modifications

(1) Apply the system configuration information automatically

Specify whether or not system configuration information reported from subsystems is to be sent (relayed) automatically to the higher system. The default is that this check box is selected.

When you first install JP1/Software Distribution Client (relay system), you should make sure that this check box is selected. This reduces the workload because you will not need to specify configuration definitions in managing servers.

If JP1/Software Distribution Client (relay system) is already installed and you are only upgrading the version, note that selecting this check box will cause the system to change existing configuration definitions automatically. If you clear this check box, you must define the system configuration manually.

(2) Linkage when system configuration is changed

When system configuration information for the higher system is changed, you can have the changes in the system configuration information applied automatically to the relay system. You can also automatically edit ID group information according to the changes in the system configuration information. Therefore, if this check box is selected, there is no need for the system administrator to change ID groups according to the system configuration information from the managing server or the relay managing ID groups. If this check box is not selected, the system administrator must manually edit the ID group information.

This setting takes effect only when **Automatically apply the system configuration** is selected. The default is that this check box is selected. However, if the check box was not selected in the previous version and a new version is installed over the previous one, the check box will not be selected in the default setting.

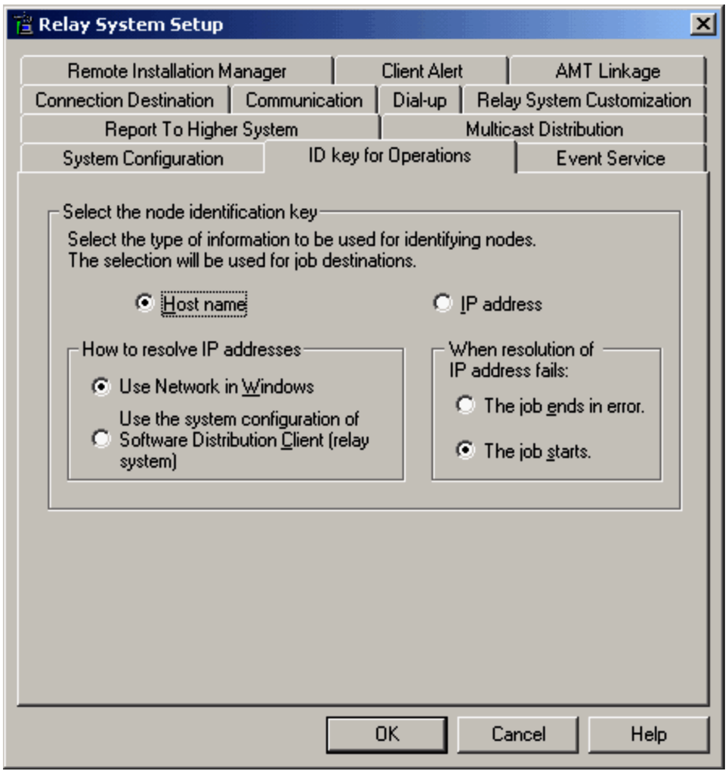
When you select this check box, you must ensure that all JP1/Software Distribution Manager and JP1/Software Distribution SubManager programs in the system have been upgraded to version 05-23 or higher. Therefore, clear this check box if your system contains any JP1/Software Distribution Manager or JP1/Software Distribution SubManager whose version is earlier than 05-23.

For details about the operation for linking system configuration information and ID groups, see *8.4 Linking system configuration information and ID group information*.

5.2.8 ID Key for Operations page

Specify the node identification key, the method used to resolve addresses, and how to handle jobs if the system cannot resolve the IP address of a job destination.

Figure 5–9: ID key for Operations page



Select the node identification key

Select the type of information to be used for identifying nodes.
The selection will be used for job destinations.

● Host name ○ IP address

How to resolve IP addresses

● Use Network in Windows

○ Use the system configuration of Software Distribution Client (relay system)

When resolution of IP address fails:

○ The job ends in error.

● The job starts.

(1) Select the node identification key

Select **Host name** or **IP address** as the information type for node identification. Select **Host name** or **IP address** according to the *ID key for operations* setting on the higher system to be connected. The default is **Host name**. If you select **Host name**, specify **How to resolve IP addresses** and **When resolution of IP address fails**.

Each relay system inherits the ID key for operations from a higher system that is specified as the connection destination. (The relay system receives the key information from the higher system when the relay system establishes a connection with the higher system, and when the relay system's connection is changed to a different higher system.)

(a) How to Resolve IP addresses

For the method to be used to resolve addresses in creating or starting jobs, select **Use Network in Windows** or **Use the system configuration of Software Distribution Manager**. The default is **Use Network in Windows**.

Use Network in Windows

Obtains an IP address from the Windows network when a job is created or started. The `hosts` file or name server is used for name resolution. If name resolution fails, the IP address is obtained from the system configuration of JP1/Software Distribution.

Use the system configuration of Software Distribution Manager

Obtains the IP address only from the system configuration of JP1/Software Distribution when a job is created or started. In such a case, you must ensure that the IP addresses of the system configuration are always correct. In some environments in which IP addresses are changed dynamically (e.g., DHCP), you can keep system configuration IP addresses correct by using the facility for automatically registering the system configuration.

In an environment in which jobs are created or started when the name server is turned off (such as at night), address resolution may fail and jobs will not be created even if you choose **Use Network in Windows**. However, choosing **Use the system configuration of Software Distribution Manager** has the benefit of reducing the time it takes until name resolution fails.

This setting, without resolving addresses, determines the destination of jobs by obtaining the IP address from the system configuration information. That means jobs may not be executable in the following cases:

- When using the host ID

  For details, see *8.2.4(4) Notes on specifying destinations* in the manual *Administrator's Guide Volume 1* and *4.26.9 JOB_DESTINATION (specifying a job destination)* in the manual *Administrator's Guide Volume 2*.

- When using the NAT function

  Job execution requests for a destination cannot be sent when the NAT function is being used. However, jobs can be executed by polling from the destination. For information on how to poll, see *2.13.1(2)(b) Executing a job at an arbitrary time* in the manual *Description and Planning Guide*.

(b) When resolution of IP address fails

Select the processing to be performed when the system cannot resolve a destination address during job execution. The default is **The job starts**. When **The job starts** is selected, the execution status of the job becomes **Waiting for transmission** in the event IP address resolution fails. The execution status of a job addressed to a nonexistent destination becomes **Waiting for transmission** and does not change.

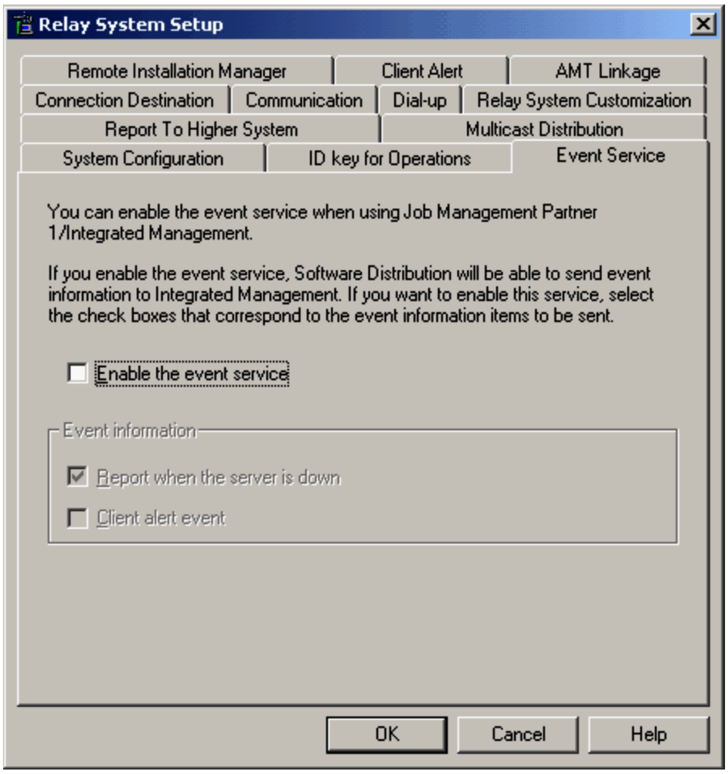
In environments that use a WINS server, the destination address cannot be resolved if the destination client PC is turned off when a job is executed. Thus, if you select **The job ends in error**, you will not be able to set up an operation that executes jobs on holidays or at night or that automatically starts the client by polling when the system starts. If you wish to set up this type of operation, select **The job starts**.

When you select **The job starts**, operation of the Remote Installation Manager may be delayed if an executed job contains a destination whose address cannot be resolved.

5.2.9 Event Service page

This page is used to specify information about the events that are sent to JP1/IM using JP1/Base's event service facility. If you select the **Enable the event service** check box, errors that occur in JP1/Software Distribution Client (relay system) are reported to JP1/IM as JP1 events. You can also report alert information sent from clients to JP1/IM as JP1 events. The default is that this check box is not selected.

Figure 5–10: Event Service page



You can enable the event service when using Job Management Partner 1/Integrated Management.

If you enable the event service, Software Distribution will be able to send event information to Integrated Management. If you want to enable this service, select the check boxes that correspond to the event information items to be sent.

□ Enable the event service

Event information

☑ Report when the server is down

□ Client alert event

Report when the server is down

JP1/Software Distribution Client (relay system) sends this event to JP1/IM when an error occurs in JP1/Software Distribution SubManager.

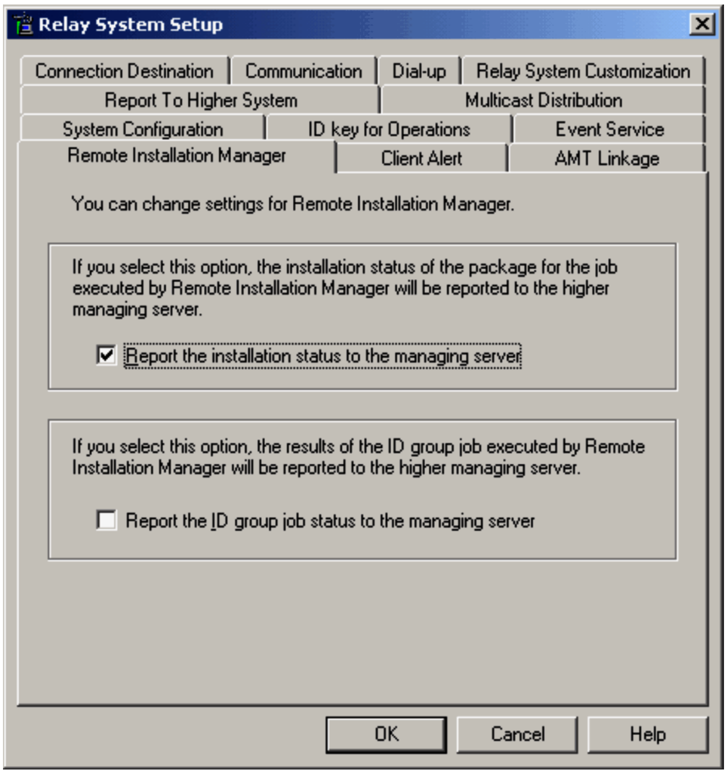
Client alert event

JP1/Software Distribution Client (relay system) sends this event to JP1/IM when alert information is sent from clients.

5.2.10 Remote Installation Manager page

Specify whether or not you wish to report the status of remote installations executed by the Remote Installation Manager of the relay system and the execution results of ID group jobs from the relay system to the higher managing server.

Figure 5–11: Remote Installation Manager page



You can change settings for Remote Installation Manager.

If you select this option, the installation status of the package for the job executed by Remote Installation Manager will be reported to the higher managing server.

☑ Report the installation status to the managing server

If you select this option, the results of the ID group job executed by Remote Installation Manager will be reported to the higher managing server.

□ Report the ID group job status to the managing server

Report the installation status to the managing server

Select this option to report the status of remote installations executed by the Remote Installation Manager to the higher managing server. The default is that this check box is selected.

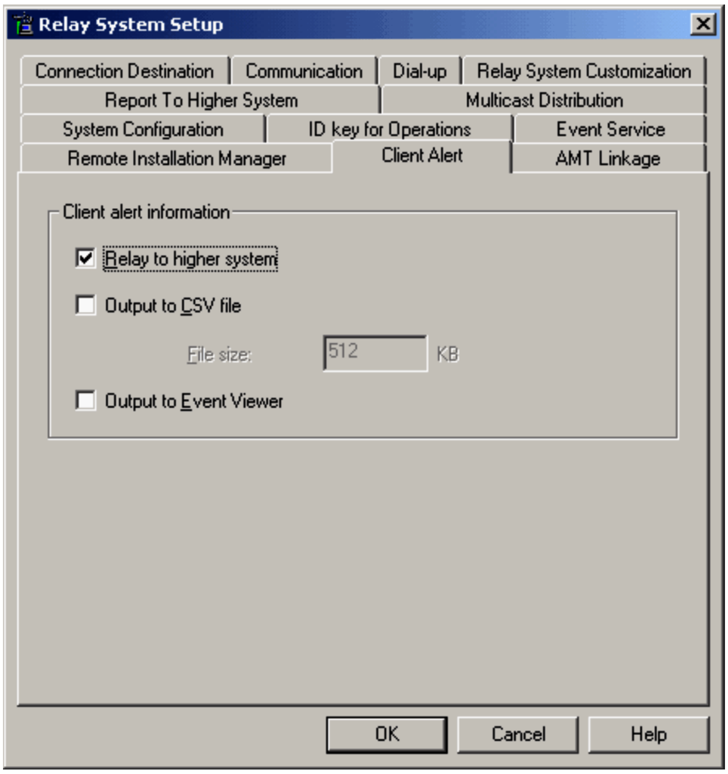
Report the ID group job status to the managing server

Select this option to report the execution results of ID group jobs executed by the Remote Installation Manager to the higher managing server. The default is that this check box is not selected.

5.2.11 Client Alert page

Specify information about output of and relaying alert information that is sent from clients.

Figure 5–12: Client Alert page



Relay System Setup

Client alert information

☑ Relay to higher system

□ Output to CSV file

File size: 512 KB

□ Output to Event Viewer

Relay to higher system

JP1/Software Distribution Client (relay system) relays alert information sent from clients to the higher system. The default is that this check box is selected.

Output to CSV file

JP1/Software Distribution Client (relay system) outputs the history of alert information sent from clients to a CSV file. The default is that this check box is not selected. If you select this check box, specify **File size**.

File size

Specifies the size of the CSV file to which the history of alert information is to be saved, in the range from 100 to 2,500 kilobytes. The default is 512 kilobytes. 100 kilobytes of space can accommodate approximately 400 alert information items.

If the amount of alert information exceeds the specified file size, the oldest alert information is overwritten.

Output to Event Viewer

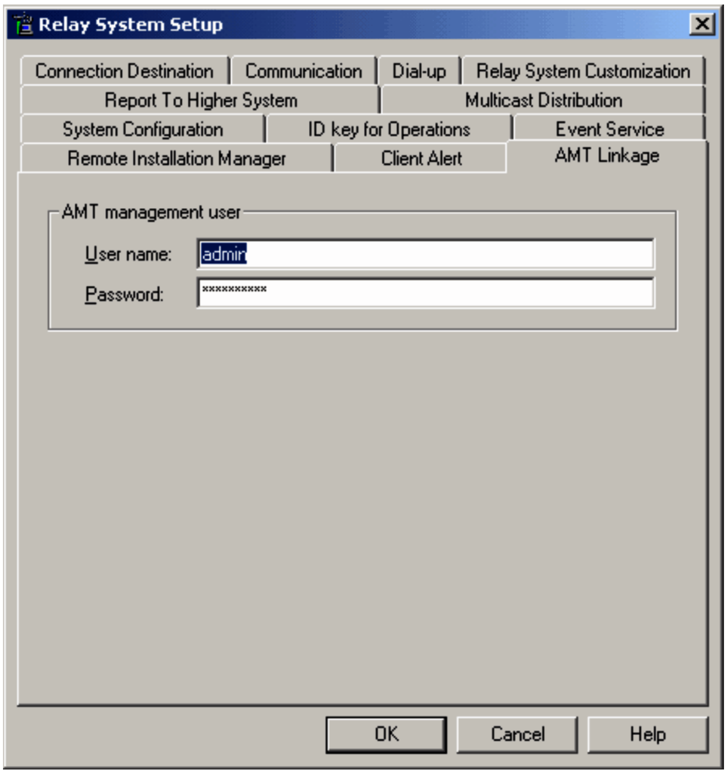
JP1/Software Distribution Client (relay system) outputs alert information sent from clients to Windows NT Event Viewer. The default is that this check box is not selected.

When you select **Output to Event Viewer**, alert information is output to all Event Viewers regardless of the **Type of Event Viewer message** setting on the **Error Handling** page. When the type of alert event is **Critical** or **Warning**, the message type displayed on the Event Viewer is warning messages; when the type of alert event is **Normal**, the message type is information messages.

5.2.12 AMT Linkage page

This page sets the information required in order to control clients using AMT Linkage. By default, the settings specified in the Settings for the AMT Linkage dialog box during installation have been set.

Figure 5–13: AMT Linkage page



AMT management user

User name: admin

Password: ***********

AMT management user

Sets the information needed to access the client's AMT. The user name and password must match the client's settings.

User name

Specifies the user name used to access the client's AMT, expressed as up to 60 characters.

Password

Specifies the password used to access the client's AMT, expressed as up to 60 characters.

5.3 Specifying the detailed settings for relay systems

Detailed setup of relay systems is required in order for a JP1/Software Distribution Client (relay system) to function as a client. When the detailed setup is completed, clicking the **OK** button displays the Setup dialog box again.

If you change any of the settings in the relay system setup, you must restart the relay system service in order for the changes to take effect. While the relay system service is running, make the changes to the setup and then click the **OK** button in the Relay System Setup dialog box or Detailed Information Setup dialog box. The relay system service restarts.

The following table lists the detailed setup items for a relay system.

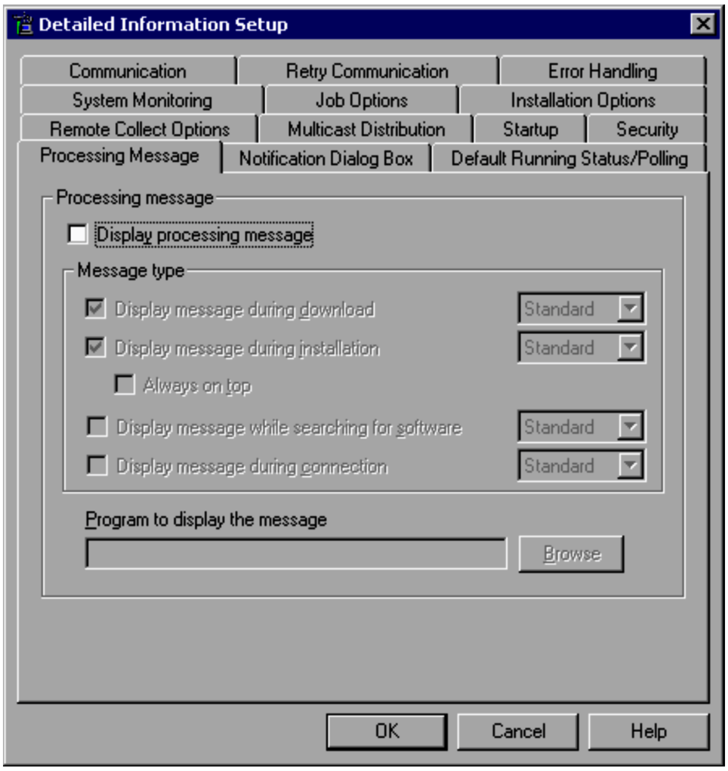
Table 5–2: Detailed setup items for a relay system

Category	Item
Processing Message	Display processing message
	Program to display the message
Notification Dialog Box	Display message box at job error
	Prompt users before deletion whenever a shortcut in Software Distribution Client startup fails
	Display the Update User Information dialog box at system startup
	Display the Update User Information dialog box at periodic execution
Default Running Status/Polling	Start client automatically at system startup
	Whether or not client will poll managing server
	Polling frequency
Communication	Port numbers
	Protocol used by the higher system requesting the client to start a job
	File transfer buffer size
	Wait for response from communications software
	Multiple network adapters
	Automatic registration of this computer in the system configuration
	Also report inventory to the server
Retry Communication	Socket connection (retry count/interval)
	Communication failure (retry count/interval)
	Installation results files failed to transmit to the higher server
	Automatic registration of this computer in the system configuration
Error Handling	Number of log file generations to be saved
	Maximum lines in a log file
	Message displayed in Event Viewer
	Type of Event Viewer message
System Monitoring	System monitoring
	Display the System Monitoring icon
	Display alert messages

Category	Item
System Monitoring	Report alerts to the higher system
	Report inventory to the higher system when the system is changed
Job Options	Automatic inventory update
	Suppress periodic jobs when the connection destination of the client is changed
	Suppress reports of the job status *Waiting for installing/collecting* to the higher system
	Do not repeat package IDs when collecting software information
Installation Options	Installation/file collection job (retry count/interval)
	Split package distribution
	Check local disk capacity before unpacking software
	Store installation history in the event of an installation error
	Delete the work directory for installing Hitachi program products after installation
	`InstallShield` timeout
Remote Collect Options	Restricting remote collection jobs executed on the client
Multicast Distribution	Port numbers for multicast distribution and allowing jobs to be distributed using multicast distribution (multicast address)
Startup	Create Software Distribution Client Startup folder
	Move programs in Startup group to the Software Distribution Client Startup group
	Select shortcuts to move programs to the Software Distribution Client Startup group
Security	Use as `User` permissions

Note that the settings in the Detailed Information Setup dialog box are the same as those in the Client Setup dialog box for JP1/Software Distribution Client (client); for details, see *6.2 Setting up Client*.

Figure 5–14: Detailed Information Setup dialog box



Processing message

□ Display processing message

Message type

☑ Display message during download — Standard

☑ Display message during installation — Standard

□ Always on top

□ Display message while searching for software — Standard

□ Display message during connection — Standard

Program to display the message

5.4 Registry settings (JP1/Software Distribution Client (relay system))

You can set the following item, not found in the setup procedure, by editing the registry. This is described below.

Continue command processing after Windows logoff

If the PC on which JP1/Software Distribution Client (relay system) is installed is running any of the operating systems shown below, command processing can be made to continue even after you log off of Windows.

- Windows NT 4.0
- Windows 2000
- Windows XP
- Windows Server 2003

For the commands that can be executed, see *4.2.1 Command types* in the manual *Administrator's Guide Volume 2*.

To have command processing continue after logging off of Windows, create the registry value shown below in registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi\NETM/DM/P`. For 32-bit operating systems, create the registry value in registry key `HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\NETM/DM/P`.

Name

`CmdLogoffContinue`

Type

`REG_SZ`

Data

`YES`

Notes

- To have command processing continue after logging off of Windows, the command must be executed from the service. Processing of commands executed by any other method will not continue after logging off of Windows even if the registry is set up to do so.
- If the OS of the PC where JP1/Software Distribution Client (relay system) is installed is Windows 8, Windows Server 2012, Windows Vista, Windows Server 2008, or Windows 7, processing of commands executed from the service will continue after logging off of Windows regardless of the registry settings.
- Operation will vary depending on the combination of registry settings and whether the command argument `/LC` was specified. For details, see *4.28 Command operation at logoff that depends on a registry setting and logoff option* in the manual *Administrator's Guide Volume 2*.

6 Setting Up JP1/Software Distribution Client (client)

This chapter explains how to set up JP1/Software Distribution Client (client).

Only a user with Administrator permissions can set up JP1/Software Distribution Client (client).

6.1 JP1/Software Distribution Client (client) setup procedure

This section describes the setup procedure for JP1/Software Distribution Client (client).

To set up JP1/Software Distribution Client (client):

1. From the **Start** menu choose **Software Distribution Client**, and then **Setup**.
   The Client Setup dialog box appears:
2. Choose the tab for the information you wish to set up.
   Specify the appropriate items.
3. When you finish with the setup, click the **OK** button.
   The setup is completed. Note that to apply the specified settings, the client manager must restart the client.

The following sections describe how to set up a client.

6.2 Setting up Client

For JP1/Software Distribution Client (client), you specify the setup items in the Client Setup dialog box. You also need to specify these setup items in the following cases:

- When the client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system) are used.
- When Startup Kit Support Tool is used to create setup information in an installation set.

In these cases, you use the Detailed Information Setup dialog box to specify almost the same settings as in the Client Setup dialog box. However, there are some items that are not displayed in the Detailed Information Setup dialog box.

The following table lists the client setup items.

Table 6–1: Client setup items

Category	Item
Connection Destination#1	Host name or IP address for the product (JP1/Software Distribution Manager, JP1/Software Distribution Client (relay system), or JP1/Software Distribution SubManager)
	Automatically specify the higher system that requested a job execution as the connection destination
	Poll multiple higher systems
	Automatically register this computer in the system configuration
	Also report this computer's inventory to the server
Processing Message	Display processing message
	Program to display the message
Notification Dialog Box	Display Message box at job error
	Prompt users before deletion whenever a shortcut in Software Distribution Client startup fails
	Display the Update User Information dialog box at system startup
	Display the Update User Information dialog box at periodic execution
Default Running Status/Polling	Start client automatically at system startup
	Whether or not client will poll managing server
	Polling frequency
	Method for polling multiple higher systems
Dial-up#1	Dialup connection
	Authentication information (user name, password, domain)
Communication	Port numbers
	Protocol used by the higher system requesting the client to start a job
	File transfer buffer size
	Wait time for response from communications software
	Multiple network adapters
Retry Communication	Socket connection (retry count/interval)
	Communication failure (retry count/interval)
	Installation results files failed to transmit to the higher server

Category	Item
Error Handling	Generations of log file to be saved
	Maximum lines in log file
	Message output to Event Viewer
	Type of Event Viewer message
System Monitoring	System monitoring
	Display the System Monitoring icon
	Display alert messages
	Report alerts to the higher system
	When the system is changed, inventory information is notified to Higher System.
Job Options	Job hold facility
	Allow the administrator to shut down or restart
	Automatic inventory update
	Suppress periodic jobs when the connection destination of the client is changed
	Suppress reports of the job status *Waiting for installing/collecting* to the higher system
	Handling of Hitachi program products included in software information
	Do not repeat package IDs when collecting software information
Installation Options	Installation/file collection job (retry count/interval)
	Split package distribution
	Check local disk capacity before unpacking software
	Delete package information of the system previously connected to the client
	Store installation history in the event of an installation error
	Delete the work directory for installing Hitachi program products after installation
	`InstallShield` timeout
Remote Collect Options	Restricting remote collection jobs executed on the client
Multicast Distribution	Port numbers for multicast distribution and allowing jobs to be received by multicast distribution (multicast address)
Startup	Create Software Distribution Client Startup folder
	Move programs in the Startup group to the Software Distribution Client Startup group
	Select shortcuts to move programs to the Software Distribution Client Startup group
Setup Protection#2	Protect setup information
Security (applicable to Windows NT)#3	Use as `User` permissions

#1

This item is not displayed during setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system). Also, the settings for creating setup information in an installation set are not displayed.

#2

This item is not displayed during setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system).

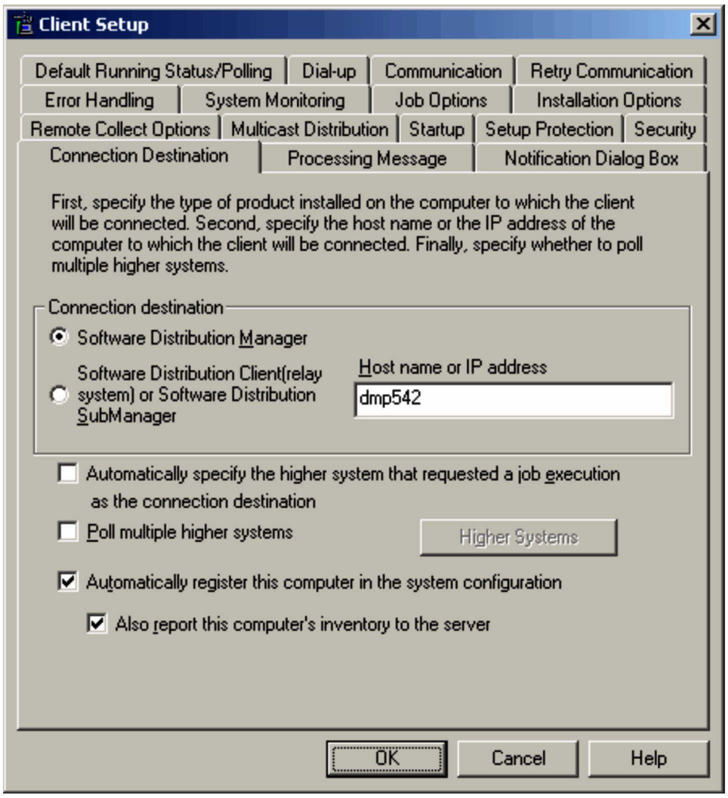
#3

This item is not displayed during setup of client facilities for JP1/Software Distribution Manager.

6.2.1 Connection Destination page

Specify the connection destination of the client. This page is not provided for setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system). Also, the settings for creating setup information in an installation set are not displayed.

Figure 6–1: Connection Destination page



First, specify the type of product installed on the computer to which the client will be connected. Second, specify the host name or the IP address of the computer to which the client will be connected. Finally, specify whether to poll multiple higher systems.

Connection destination

● Software Distribution Manager

○ Software Distribution Client(relay system) or Software Distribution SubManager

Host name or IP address: dmp542

□ Automatically specify the higher system that requested a job execution as the connection destination

□ Poll multiple higher systems

☑ Automatically register this computer in the system configuration

☑ Also report this computer's inventory to the server

(1) Connection destination

Select the client's connection destination (higher system). Select JP1/Software Distribution Manager, JP1/Software Distribution Client (relay system), or JP1/Software Distribution SubManager (JP1 Version 7i or earlier for Windows; JP1 Version 8 or earlier for Unix). Also specify the address of the connection destination using the same ID key for operations (host name or IP address) that is used by the higher system.

- Supported product types and corresponding product names

  The following table shows the supported product types and the corresponding product names:

Product type	Corresponding product name
JP1/Software Distribution Manager	JP1/Software Distribution Manager for Windows Software Distribution Manager for Windows JP1/Software Distribution Manager for UNIX Software Distribution Manager for UNIX JP1/Software Distribution Workstation Assistant for UNIX Software Distribution for UNIX Software Distribution Workstation Assistant for UNIX

Product type	Corresponding product name
JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager	JP1/Software Distribution Client (relay system) for Windows JP1/Software Distribution SubManager for Windows Software Distribution SubManager for Windows JP1/Software Distribution Client (relay system) for UNIX JP1/Software Distribution SubManager for UNIX JP1/Software Distribution Workstation for UNIX Software Distribution Workstation for UNIX

Note

- If the connection destination is undefined or the client is used as an offline machine to manage inventory, specify `?`. If you specify `?`, the client can use only the Local System Viewer and system monitoring facility. To use other facilities, the client must connect to a higher system.
- When you create a PC environment for copying the hard disk in order to use the pre-installation facility to install JP1/Software Distribution Client (client), specify `*`. When `*` is specified, the client is initialized upon completion of setup and stops running.
- Note that you can distribute a file to clients for determining the connection destinations. This file sets the appropriate connection destinations automatically on the basis of the IP address of each client machine. This function is useful because if the IP address is changed when the client machine is moved, for example, the connection destination is updated automatically. For details, see *6.5.4 Automatic Updating of the Client Connection Destination* in the *Description and Planning Guide*.
- We recommend that clients in virtualized environments specify Software Distribution Manager as the connection destination.

(2) Automatic specification of the higher system that requested job execution as the connection destination

When you select the **Automatically specify the higher system that requested a job execution as the connection destination** check box, the connection destination of the client is switched automatically to the higher system that requested job execution if the request for job execution was received from a system other than the higher system that was specified as the connection destination.

By selecting this option, you can automatically change the connection destinations of the client on the basis of the job execution requests from higher systems, without having to change the settings in the client setup or create an information file for higher connection destinations.

Note that you cannot use the following functions when you select this check box:

- Poll multiple higher systems
- Specify multiple network adapters

If `*` or `?` is specified, the connection destination will not be set automatically even if this check box is selected.

(3) Poll multiple higher systems

Specifies whether multiple higher systems are to be polled (multi-polling) when there are multiple job execution routes from the managing server. The default is that this check box is not selected. When this check box is selected, the **Higher Systems** button is enabled. Click this button to open the Specify Higher Systems dialog box. In this dialog box, specify settings such as the names and priority levels of the higher systems. Note that you must use the ID key for operations (host names or IP addresses) to specify the higher system names. You must also specify the polling method on the **Default Running Status/Polling** page of the Client Setup dialog box.

If you select this check box and specify the priority order of network adapters in **Specify multiple network adapters** on the **Communication** page, polling might fail and a delay may occur between a retry and the retry timeout.

For details about the multi-polling function, see *6.5.3 Multi-polling environment for clients* in the *Description and Planning Guide*.

(4) Automatic registration of this computer in the system configuration

When this check box is selected, the local system is registered automatically with the JP1/Software Distribution network managed by the managing server. When you uninstall JP1/Software Distribution Client (client), you can remove the local system from the JP1/Software Distribution network. Registration is performed when setup is completed.

The default is that this check box is selected. Be sure to select this check box if you use a firewall. When the check box is cleared, you must define this client when you define the system configuration for the managing server.

Select this check box also when you use the client facility with JP1/Software Distribution version 06-00 or later, or the facility for detecting hosts on which JP1/Software Distribution has not been installed.

If either of the following occurs, the system configuration is not automatically registered (except for the offline machine).

- The host name, IP address, or host ID of the local system cannot be obtained.
- The IP address of the local system is a loopback address (127.0.0.1).

Also report this computer's inventory to the server

When the **Automatically register this computer in the system configuration** check box is selected, this check box is enabled. Select this check box if you wish to notify the higher system of inventory information as well as of system configuration information. The default is that this check box is selected.

The higher system is notified of the following inventory information:

- System information (system information and registry information)
- Software information listed in **Add/Remove Programs**
- Patch information

The higher system is notified of inventory information at the following times:

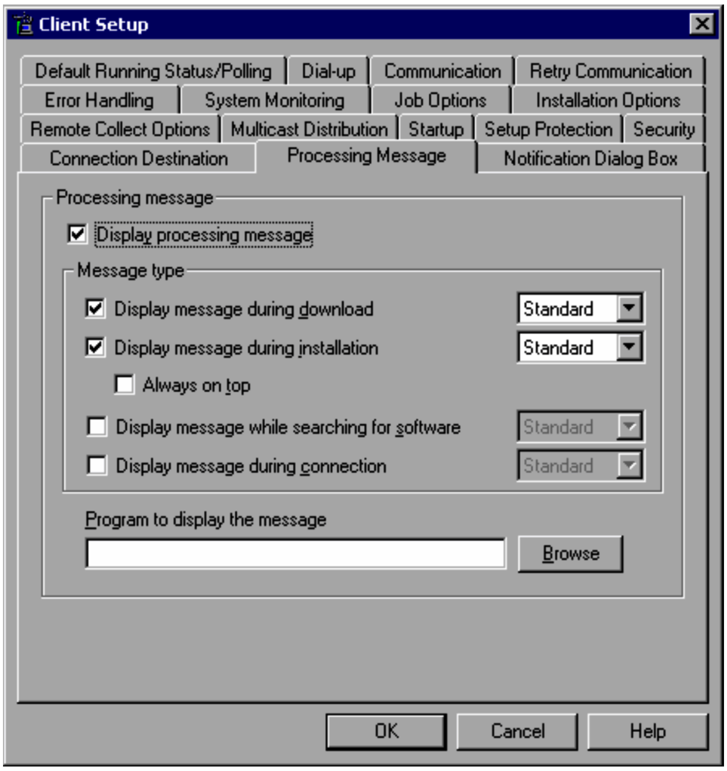
- When a new client is installed
- When the connection destination is changed by the client setup
- When the higher system's operation mode is changed from one in which host IDs are used to one in which host IDs are not used

Select this check box also when you use the facility for detecting hosts on which JP1/Software Distribution has not been installed.

6.2.2 Processing message page

Specify whether or not you wish to display a message dialog box that shows processing progress (processing message) when JP1/Software Distribution Client (client) executes processing automatically on the basis of an instruction from the managing server. You must also specify the format of the dialog box to be displayed.

Figure 6–2: Processing Message page



Processing message

☑ Display processing message

Message type

☑ Display message during download — Standard

☑ Display message during installation — Standard

□ Always on top

□ Display message while searching for software — Standard

□ Display message during connection — Standard

Program to display the message

Browse

To display a processing message while the client is executing an operation, such as downloading or installation, select the **Display processing message** check box. The default is that this check box is selected. However, during setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system), this option is not selected as the default.

If you select the **Display processing message** check box, also select the message types for which a processing message is to be displayed. Also select either **Standard** or **Program to display the message** as the format of the dialog box to be displayed for each message type. If you select **Standard**, the standard dialog box provided by JP1/Software Distribution is used to display the processing message. If you select **Program to display the message**, a user-created dialog box display program is started.

The default is that the standard processing message is displayed during downloading and installation.

(1) Message type

- **Display message during download**
  This option displays the dialog box indicating that the client is downloading a package.
- **Display message during installation**
  This option displays the dialog box indicating that the client is installing a package.

  Always on top

  Select this check box to display the processing message as the topmost window during installation. This prevents the user from mistakenly operating dialog boxes displayed by applications of other companies during distribution. The default is that this check box is not selected.
- **Display message while searching for software**
  This option displays the dialog box indicating that the client is searching for installed software.
- **Display message during connection**
  This option displays the dialog box indicating that the client is connecting to a higher system.

Note

If a distributed package contains the processing message setting, **Display message during download** and **Display message during installation** are forcibly displayed or hidden as specified in the package settings. In such a case, the **Display processing message** setting at the client setup is ignored.

(2) Program to display the message

If you selected **Program to display the message** as the message display method, specify the name of the program to be used to display a dialog box. Specify a user-created dialog box display program (an `.exe` program file), including the path name. Note that the window for displaying the message need not be a dialog box as long as the conditions described below, such as parameters and titles, are met.

If messages are not displayed correctly due to an error in the specified user-created program, such as a setup error, processing continues regardless of the action of the user-created program.

Shown below is the syntax of the arguments (character strings ending with NULL) that are passed to the dialog box display program when each dialog box is displayed. Refer to this syntax when you create a user program.

Format

```
parameter-1△parameter-2△parameter-3△parameter-4
```

△: space

parameter-1

Top window display option (1 byte):

1: Do not display the dialog box as the top window.

2: Display the dialog box as the top window.

parameter-2

Processing message type (1 byte):

1: Dialog box displayed during package downloading

2: Dialog box displayed during package installation

3: Dialog box displayed during software search processing

5: Dialog box displayed during connection to higher system

parameter-3 and *parameter-4*

The contents of *parameter-3* and *parameter-4* depend on the specification of *parameter-2*, as shown below:

parameter-2	parameter-3	parameter-4
1	*package-identification-ID* (1 to 44 bytes)	*package-name* (1 to 50 bytes)
2	*package-identification-ID* (1 to 44 bytes)	*package-name* (1 to 50 bytes)
3	*host-name* or *IP-address* (1 to 256 bytes)	(null)
5	(null)	(null)

Note: *(null)* is a character string (6 characters) that indicates no value.

Example

The following shows examples of the coding to display each type of dialog box:

- **Display message during download**

  `1 1` *package-identification-ID package-name*

- **Display message during installation**

  When not displaying the dialog box as the top window:

  `1 2` *package-identification-ID package-name*

  When displaying the dialog box as the top window:

  `2 2` *package-identification-ID package-name*

- **Display message while searching for software**

```
1 3 host-name (null)
```

- **Display message during connection**

```
1 5 (null) (null)
```

When you create the user program, specify the window names of the dialog boxes to be displayed, as shown below; if any other window names are used, the dialog boxes will not close:

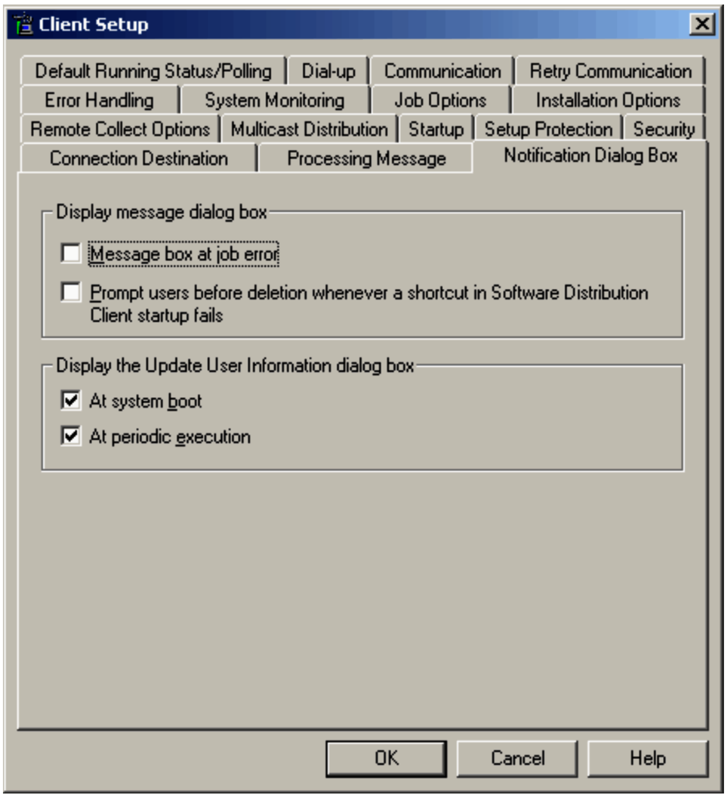
- **Display message during download**: Software Distribution - Download
- **Display message during installation**: Software Distribution - Installing
- **Display message while searching for software**: Software Distribution - Searching installed software
- **Display message during connection**: Software Distribution - Under connection

To close the dialog box display, issue the `PostMessage` function (specifying `WN_CLOSE`) from JP1/Software Distribution to the user-created program. For Windows, issue the `PostMessage` function, and then issue the `TerminateProcess` function to stop the user-created program process.

6.2.3 Notification Dialog box page

Specify whether or not you wish to display various message dialog boxes and the Update User Information dialog box.

Figure 6–3: Notification Dialog Box page



Client Setup

Display message dialog box

□ Message box at job error

□ Prompt users before deletion whenever a shortcut in Software Distribution Client startup fails

Display the Update User Information dialog box

☑ At system boot

☑ At periodic execution

(1) Display Message dialog box

Message box at job error

Specify whether or not the client is to display an error dialog box if a job from the managing server or relay system fails. To display the error dialog box, select this check box. The default is that this check box is not selected.

Prompt users before deletion whenever a shortcut in Software Distribution Client startup fails

If the execution file for an icon or shortcut that exists at Software Distribution Client startup has already been uninstalled, the user may not be able to execute the icon or shortcut.

In such a case, the system can display a dialog box that asks the user to confirm that the system should delete the disabled icon or shortcut. To display this dialog box, select this check box. The default is that this check box is not selected.

(2) Display the Update User Information dialog box

At system boot

Specify whether or not the client is to display the Software Distribution - Update User Information dialog box automatically at system startup when the managing server requests user information (distributes an input item list). The default is that this check box is selected.

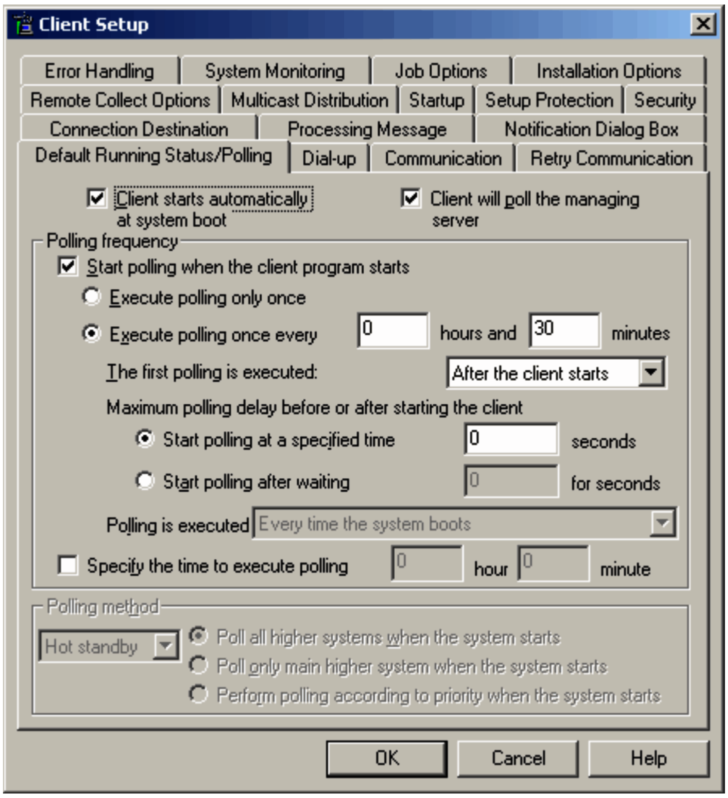
At periodic execution

Specify whether or not the client is to display the Software Distribution - Update User Information dialog box each time a job is executed if the managing server periodically executes *Get system configuration information* jobs. The default is that this check box is selected.

6.2.4 Default Running Status/Polling page

Specify whether or not you wish to make the client resident, and whether or not you wish to perform polling. If polling is to be performed, also specify the polling timing.

Figure 6–4: Default Running Status/Polling page



☑ Client starts automatically at system boot

☑ Client will poll the managing server

Polling frequency

☑ Start polling when the client program starts

○ Execute polling only once

● Execute polling once every 0 hours and 30 minutes

The first polling is executed: After the client starts

Maximum polling delay before or after starting the client

● Start polling at a specified time 0 seconds

○ Start polling after waiting 0 for seconds

Polling is executed Every time the system boots

□ Specify the time to execute polling 0 hour 0 minute

Polling method

Hot standby

● Poll all higher systems when the system starts

○ Poll only main higher system when the system starts

○ Perform polling according to priority when the system starts

Client starts automatically at system boot

Specify whether or not the client is to start automatically whenever the system starts. The default is that this check box is selected; however, the default setting may change depending on the network environment.

In normal operation, the client starts automatically at system startup and executes requested processing on the basis of instructions from the connection destination. However, this means that any job the user is executing will be terminated abnormally if installation of another company's software begins during that job. Also, the system uses memory and CPU resources while the client is active, even when the system is not using the client. You can avoid these problems by clearing the **Client starts automatically at system boot** check box.

Note that if a client is not started automatically at system startup, it can execute automatic polling only when the system is started. If polling is necessary during system startup for a client that is not started automatically, choose the **Execute Job Backlog** icon to execute polling.

This item cannot be specified during setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system).

Client will poll the managing server

Specify whether or not the client is to *poll* (monitor for instructions from the managing server).

Normally, the client executes requested processing on the basis of instructions from the managing server. However, instructions from the managing server may not reach the client in the event of a communications error or if the client PC has not been started. In such cases, the client can execute polling to receive instructions. If you use the client control facility, it is recommended that you perform polling. If the system uses a low-speed WAN, you may want to disable polling to minimize unnecessary data transmissions.

The default is that the **Client will poll the managing server** check box is selected. If you enable polling, you must also specify the polling timing.

(1) Polling timing

Specify the polling timing. The default is **Start polling when the client program starts**.

Start polling when the client program starts

Select this check box to set polling at the time of system startup. Also select either **Execute polling only once** or **Execute polling once every**.

The default is **Execute polling once every**. The default polling interval depends on the program.

- For setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system):

  Polls every two hours.

- For setup of JP1/Software Distribution Client (client) and creation of setup information in an installation set:

  Polls every 30 minutes (however, the default value may change depending on the network environment).

Execute polling only once

The client polls the managing server only once at system startup.

Execute polling once every

The client polls the managing server at a fixed interval. The permitted range of the polling interval is 1 minute to 12 hours. To lighten the network load, specify the largest possible interval.

The client uses this value as a timer value for monitoring failure recovery when a communications error occurs and the client cannot recognize remote installation instructions.

The first polling is executed

Select **Before the client starts** or **After the client starts** as the polling timing during system start. If the client has not started at the time of job execution, this setting can control the installation timing of a package with **Install when system starts** specified. The default is **After the client starts**.

- When **Before the client starts** is selected

  When the client system starts, polling takes place first and then downloaded packages are installed.

  If a package with **Install when system starts** specified is downloaded by polling during system startup, the package is installed immediately after that. Therefore, installation is completed after the first system startup.

- When **After the client starts** is selected

  When the client system starts, downloaded packages are installed and then polling takes place.

  If a package with **Install when system starts** specified is downloaded by polling, which takes place after starting the client system and installing downloaded packages, this package is not installed until the time of the next system startup.

Selecting **Before the client starts** provides the advantage of completing installation at the time of the first system startup. However, if programs are registered in the Software Distribution Client Startup folder, startup of these programs is delayed by installation of packages that are downloaded by polling.

To start the programs in the Software Distribution Client Startup folder sooner, select **After the client starts**. In this case, these programs start without waiting for polling.

For details about the differences in the installation time depending on the polling setting, see *11.2.2 Preparing to install software during system startup* in the manual *Administrator's Guide Volume 1*.

Maximum polling delay before or after starting the client

Specifies the timing and delay before polling begins after system startup.

Start polling at a specified time

Starts polling anytime before the specified amount of time (in seconds) elapses after the client starts. Specify the polling time in the range from 0 to 300 seconds. The default is 0 seconds. If you specify `0`, polling starts at the time of client startup.

This setting prevents multiple PCs from being connected to the higher system at the same time even when they are started at the same time, thereby distributing the load on the network. If system performance is inadequate to keep up with the number of PCs connected to the higher system, or if the load on the network is too high, you can reduce the load by increasing this setting's value.

Start polling after waiting

Starts polling when the specified amount of time (in seconds) has elapsed after the client has started. Specify the amount of time the client stands by in the range from 0 to 7,200 seconds. The default is 0 second. When `0` is specified, polling starts at the same time as startup.

This setting can delay polling in an environment where polling starts after the client establishes connection with the higher system, such as an environment using IEEE802.1X that requires user authentication when the network is connected.

In such an environment, set this value based on the amount of time required for login after OS startup.

Polling is executed

If you select **Execute polling only once** and specify **Before the client starts** for **The first polling is executed**, you can specify either **Every time the system boots** or **When the system boots for the first time each day**. The default is **Every time the system boots**. This setting is not available during setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system).

Specify the time to execute polling

Select this check box to execute polling once a day at a specified time. When you select this check box, you must specify a polling execution time. If you change the pooling execution time after executing polling based on the **When the system boots for the first time each day** setting, no polling takes place on that day when the new polling execution time is reached.

Polling at a specified time cannot be specified during setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system).

(2) Polling method

Specify the polling method the client will use if it cannot connect to the higher system to be polled (due to a relay system error, for example). The default setting is **Hot standby**. This item is not available at setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system).

Specify this item if you set **Poll multiple higher systems** on the **Connection Destination** page.

Hot standby

This method polls the relay systems that were set in the Specify Higher Systems dialog box in order of their priorities, starting with the relay system with the highest priority. The client then recognizes the relay systems that can be connected as the higher systems to be polled.

If connection to a higher system becomes disabled, the client polls the relay systems in sequence, starting each time it polls with the highest-priority relay system. The client thus determines the higher systems to be polled.

However, you can select one of the following three polling methods as the method to be used when the system starts (first polling):

- **Poll all higher systems when the system starts**
- **Poll only main higher system when the system starts**
- **Perform polling according to priority when the system starts**

The default is **Poll all higher systems when the system starts**.

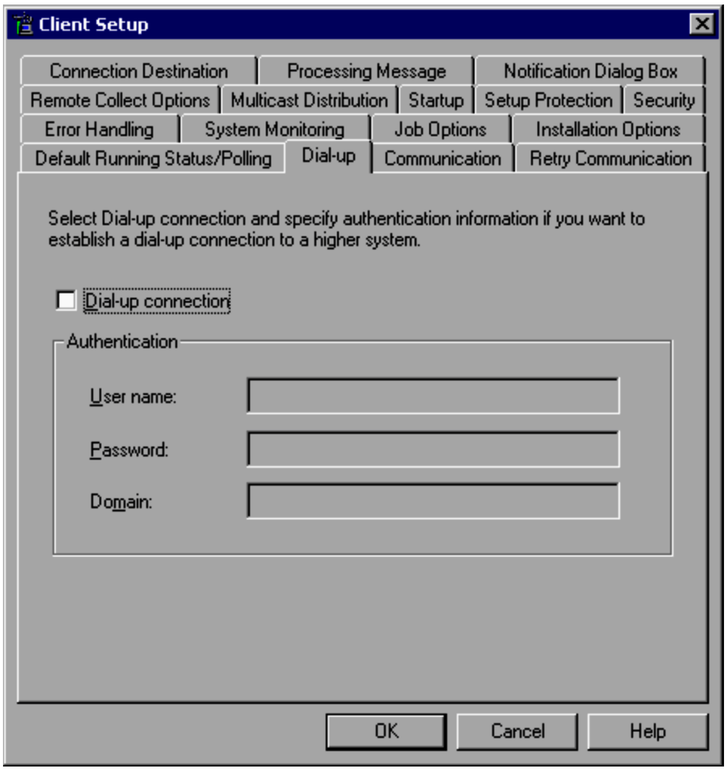
Multiple hosts

This method polls all relay systems that were specified in the Specify Higher Systems dialog box.

6.2.5 Dial-up page

Specify the settings required for dial-up connection. This page is displayed only in an environment that supports dial-up connection. This page is not provided for setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system) nor when setup information is created in an installation set.

Figure 6–5: Dial-up page



Select Dial-up connection and specify authentication information if you want to establish a dial-up connection to a higher system.

□ Dial-up connection

Authentication

User name:

Password:

Domain:

Dial-up connection

To use dial-up connection, select this check box. The default is that this check box is not selected.

Authentication

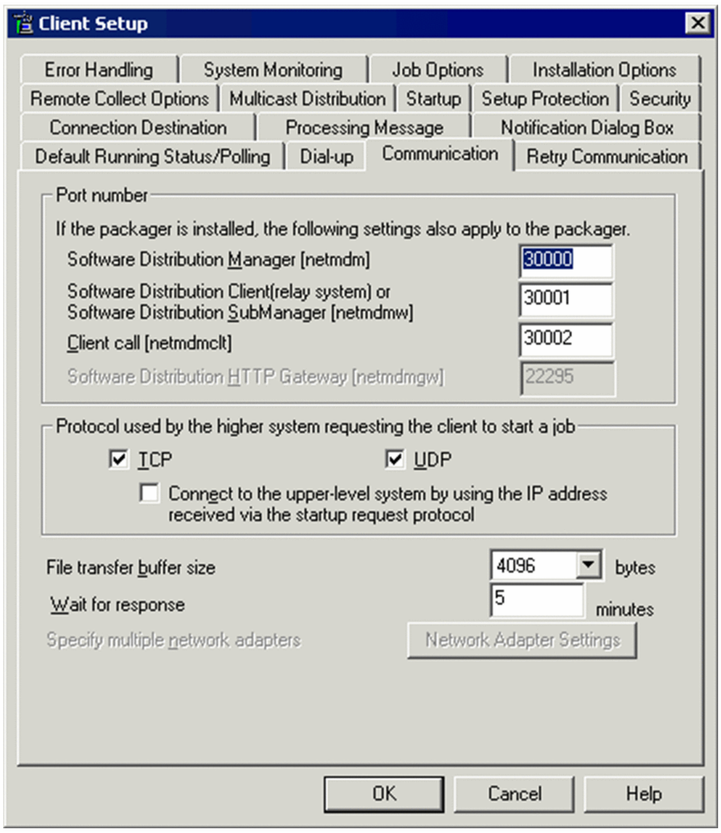
Specify the user name, password, and domain to be used during dial-up connection.

For details about a dial-up connection, see *6.6 Settings for dial-up connections* in the *Description and Planning Guide*.

6.2.6 Communication page

Specify the port number and startup protocol.

Figure 6–6: Communication page



Port number

If the packager is installed, the following settings also apply to the packager.

Software Distribution Manager [netmdm]: 30000

Software Distribution Client(relay system) or Software Distribution SubManager [netmdmw]: 30001

Client call [netmdmclt]: 30002

Software Distribution HTTP Gateway [netmdmgw]: 22295

Protocol used by the higher system requesting the client to start a job

☑ TCP ☑ UDP

□ Connect to the upper-level system by using the IP address received via the startup request protocol

File transfer buffer size: 4096 bytes

Wait for response: 5 minutes

Specify multiple network adapters

(1) Port numbers

Specify the following four port numbers, which the client will use for communications:

- **Software Distribution Manager** (default: `30000`)
- **Software Distribution Client (relay system) or Software Distribution SubManager** (default: `30001`)
- **Client call** (default: `30002`)
- **Software Distribution HTTP Gateway** (default: `22295`)

Normally, you should use the default port numbers. However, you must change a port number if some other program is using that port. If a port number is set in the `services` file of TCP/IP, the `services` file setting takes precedence.

If a Packager is installed, the values that you specify here also apply to the Packager.

You must provide a port number for **Software Distribution HTTP Gateway** only when JP1/Software Distribution HTTP Gateway is used. For details, see *E. Using Internet Options to Install JP1/Software Distribution*.

(2) Protocol used by the higher system requesting the client to start a job

Select the communications protocol for receiving execution requests from the higher system. The following two protocols can be selected:

- **UDP**
- **TCP**

You can select both protocols. If the system uses a firewall, you must select the TCP protocol. The default is that both protocols are selected.

Connect to the upper-level system by using the IP address received via the startup request protocol

Select this check box to enable the higher system to be connected even when the higher system's name cannot be resolved. By default, this check box is not selected.

When a host name is used for an ID key for operations, the client may not be able to resolve the higher system's name in some environments, such as where a quarantine system prohibits the client from connecting to the DNS server or the higher system uses multiple network adapters. If this check box is selected in such cases, the IP address in execution request information is stored at the time the execution request information is received from the higher system, enabling the client to connect to the higher system.

For details about the connection settings applicable when the client cannot resolve the higher system's name, see *6.5.6 Connection settings when the name of the higher system cannot be resolved* in the *Description and Planning Guide*.

This check box is enabled when the **TCP** or **UDP** check box is selected. In the setup of client facilities for a relay manager/system, this check box is always disabled.

Note

- There is no need to set this option if an IP address is used as the ID key for operations.
- If the higher system's version is earlier than 06-71, connection cannot be established correctly even with this check box selected.
- If the higher system is a cluster system, connection may not be established correctly.
- If the communication protocol used for execution request information is UDP, connection may not be established correctly in an environment where the higher system uses multiple network adapters.

(3) File transfer buffer size

Specify the size of the buffer that the local system is to use for file transfer with the higher system. Increasing the buffer size improves transfer efficiency. However, if the buffer size is large, the higher system must have a memory size equal to *buffer size* **x** *number of clients that can be connected concurrently*. Adjust the buffer size according to the memory size of the higher system. Specify the buffer size in the range from 512 to 4,096 bytes. The default is 4,096 bytes.

Note that the file transfer buffer size for UNIX Software Distribution version 01-09 or earlier is fixed at 1,024 bytes; therefore, any value greater than 1,024 bytes that is specified is ignored when connection is established with UNIX Software Distribution version 01-09 or earlier.

(4) Wait for response

Set the amount of time the client is to wait for a response from TCP/IP. When you set this item, the system can monitor when the client downloads files and other operations.

If TCP/IP does not respond within the specified time, the system assumes that a communications error has occurred.

Specify the response wait time in the range from 0 to 120 minutes. The default is 5 minutes. If you specify `0`, the system does not monitor for a response from TCP/IP.

(5) Specify multiple network adapters

Select the **Specify multiple network adapters** check box in you wish to specify a priority order for the communications lines used by JP1/Software Distribution in an environment in which there are multiple network adapters (multiple LAN connections). This item is not displayed when setup information is created in an installation set.

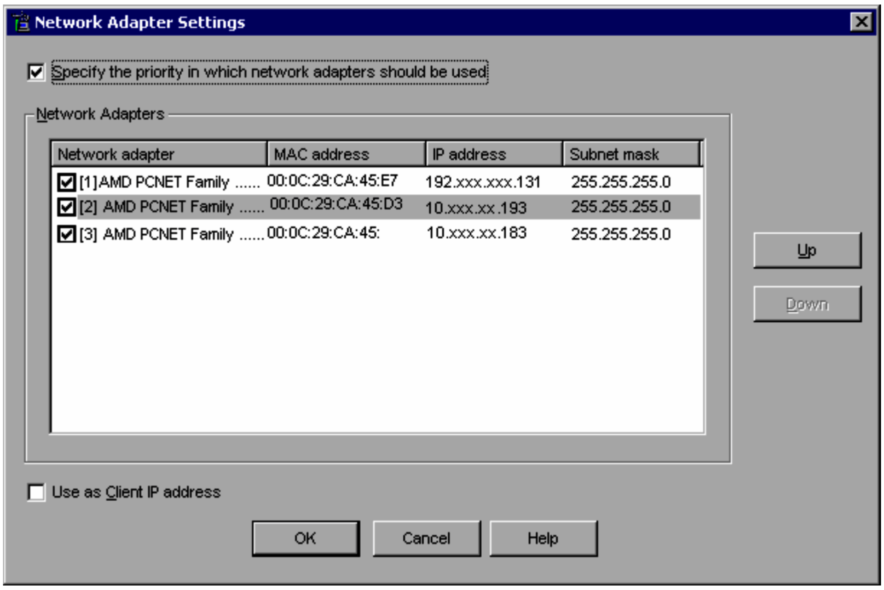
Clicking the **Network Adapter Settings** button displays the Network Adapter Settings dialog box.

Select this option if you normally use one network as your first priority but want to switch to a network with a second or lower priority in the event of a network failure or when the networks used by JP1/Software Distribution are restricted.

The **Network Adapter Settings** button is disabled in the following cases:

- When there is only one network adapter
- When dial-up connection is specified.

Figure 6–7: Network Adapter Settings dialog box



☑ Specify the priority in which network adapters should be used

Network Adapters

Network adapter	MAC address	IP address	Subnet mask
☑ [1] AMD PCNET Family	00:0C:29:CA:45:E7	192.xxx.xxx.131	255.255.255.0
☑ [2] AMD PCNET Family	00:0C:29:CA:45:D3	10.xxx.xx.193	255.255.255.0
☑ [3] AMD PCNET Family	00:0C:29:CA:45:	10.xxx.xx.183	255.255.255.0

☐ Use as Client IP address

Specify the priority in which network adapters should be used

Select this check box to specify priorities for using the network adapters when there are multiple network adapters. The default is that this check box is not selected.

Network Adapters

The following items are listed:

- **Network adapter**#
- **MAC address**
- **IP address**
- **Subnet mask**

#

The number in square brackets is the binding order set by Windows. However, depending on the Windows version, it may not actually be the binding order.

Select the check boxes to specify the network adapters to be used by JP1/Software Distribution. If you select multiple network adapters, they are listed in descending order of priority. If you select only one network adapter check box, it is selected as the network adapter dedicated to JP1/Software Distribution. The system ignores an unsupported network adapter, if selected.

To change the priority order, select the network adapter you wish to change and use the **Up** or **Down** button to move it.

If multiple IP addresses are assigned to one network adapter, only the last assigned IP address is listed under **Network Adapters** and only that address can be used by JP1/Software Distribution.

Use as Client IP address

Select this check box if you wish to send to the higher system the IP address of the network adapter that is used according to the priority settings as the client's IP address. The default is that this check box is cleared, in which case the IP address of the network adapter that has the highest priority order is sent to the higher system in the binding order set by Windows. Note that the system ignores a network adapter whose IP address is `0.0.0.0`.

Note

It is recommended that host names be used as the node identification key when selecting **Specify the priority in which network adapters should be used**. If you use IP addresses as the node identification key, they can be used also with the host IDs, but the IP addresses displayed by the Remote Installation Manager of the higher system may differ from the IP addresses specified in **Network Adapters**. If you select the **Use as Client IP address** check box, the IP addresses specified in **Network Adapters** are sent to the higher system and displayed by the Remote Installation Manager.

(6) Automatic registration of this computer in the system configuration

This item is displayed only at the following times:

- During setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system)
- During creation of setup information in an installation set

For details about the setup method, see *6.2.1 Connection Destination page*.

(7) Also report this computer's inventory to the server

This item is displayed at the following times:

- During setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system)
- During creation of setup information in an installation set

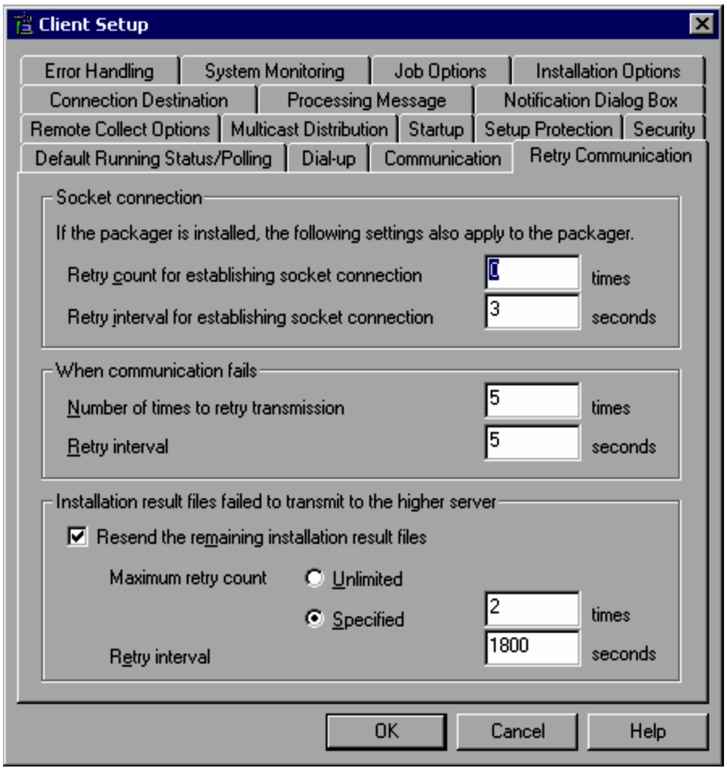
For details about the setup method, see *6.2.1 Connection Destination page*.

6.2.7 Retry Communication page

Specify the retry count in the event of an error.

If communication cannot be established after the specified number of retries, processing is cancelled. The cancelled processing is restarted at an appropriate time, such as during polling to the higher system, job execution on the higher system, and re-execution.

Figure 6–8: Retry Communication page



Socket connection

If the packager is installed, the following settings also apply to the packager.

Retry count for establishing socket connection: 0 times

Retry interval for establishing socket connection: 3 seconds

When communication fails

Number of times to retry transmission: 5 times

Retry interval: 5 seconds

Installation result files failed to transmit to the higher server

☑ Resend the remaining installation result files

Maximum retry count: ○ Unlimited ● Specified 2 times

Retry interval: 1800 seconds

(1) Socket connection

Specify a retry count and interval for establishing socket connection. If Packager is installed, the socket connection values specified on this page also apply to the Packager.

Retry count for establishing socket connection

Specify a retry count for establishing a socket connection that is to be used if an error occurs while the client is trying to establish a socket connection with the higher system. The client executes the number of retries you specify in this setting at the interval you specify for **Retry interval for establishing socket connection**. Specify the retry count in the range from `0` to `100`. The default is `0`. When `0` is specified, no retries are attempted. If you upgrade the program, the retry count for the previous version is inherited as the default value.

Retry interval for establishing socket connection

Specify the retry interval for establishing a socket connection that is to be used if an error occurs while the client is trying to establish a socket connection with the higher system. The client executes the number of retries you specify for **Retry count for establishing socket connection** at the interval you specify here. Specify the retry interval in the range from 1 to 1,800 seconds. The default is 3 seconds.

(2) When communication fails

Specify a retry count and retry interval to be used if a communication error occurs during file transmission from the higher system to the client.

When a retry is executed, the system restarts file transmission from the file that was being transferred when the previous file transmission was interrupted. This item enables you to reduce the volume of unnecessary communication, because the system does not retransmit files that were transmitted before the communication error occurred.

The retry count and interval specified here are applicable to unicast distribution.

Number of times to retry transmission

Specify the number of retries to be executed if a communication error occurs during file transmission. The system executes the number of retries you specify in this setting at the interval you specify for **Retry interval**. Specify the number of retries in the range from 0 to 999. The default is 5 times. The default value may depend on the network environment.

Retry interval

Specify the retry interval for retries to be executed if a communication error occurs during file transmission. The system executes the number of retries you specify for **Number of times to retry transmission** at the interval you specify here. Specify the retry interval in the range from 1 to 7,200 seconds. The default is 5 seconds.

(3) Installation results files failed to transmit to the higher server

Select whether or not the client is to resend results files that could not be sent to the higher system. The default is that the **Resend the remaining installation result files** check box is selected.

Resend the remaining installation result files

When this option is selected, the client monitors whether there are results files that it has not sent to the higher system and sends any that it finds. You can specify a retry count and retry interval.

Maximum retry count

Select the retry count from the following two choices. The client executes the number of retries you specify here at the interval you specify for **Retry interval**.

- **Unlimited**
- **Specified**

The default is **Specified**. When you select **Specified**, you can specify a retry count in the range from 1 to 300. The default is 10 for setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system), and 2 for setup of JP1/Software Distribution Client (client) and creation of setup information in an installation set.

Retry interval

Specify the retry interval. The permitted value range is from 60 to 3,600 seconds. The default is 300 seconds for setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system).

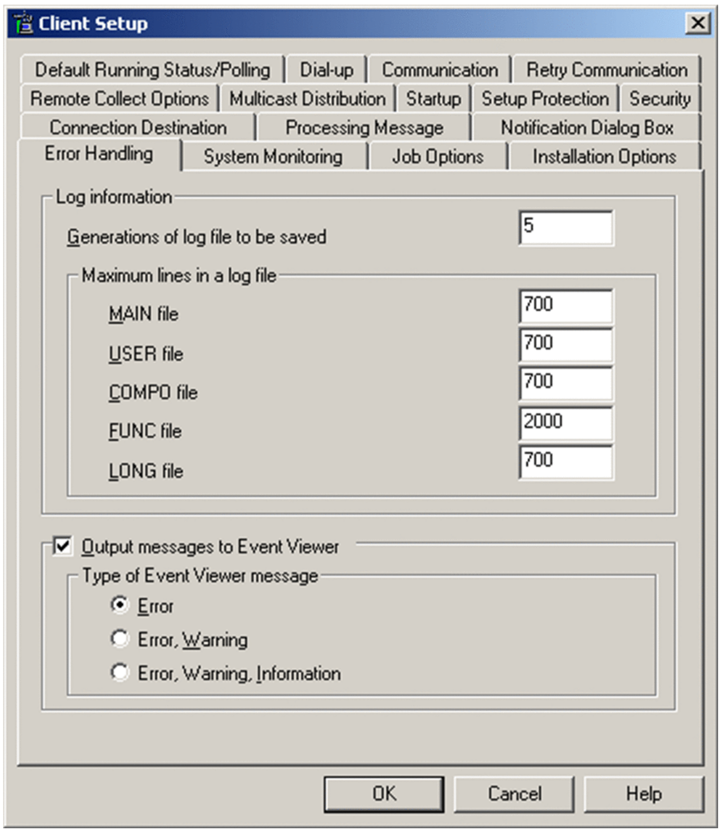
For setup of JP1/Software Distribution Client (client) and the settings in an installation set, the value is 1,800 seconds.

For the retry interval, specify a value based on system requirements. For example, specify a low value for systems that check security, since information from the client is required immediately.

6.2.8 Error Handling page

Specify the number of generations and number of log entries to be managed and the type of messages to be output to the Event Viewer.

Figure 6–9: Error Handling page



Client Setup

Log information

Generations of log file to be saved: 5

Maximum lines in a log file

MAIN file: 700

USER file: 700

COMPO file: 700

FUNC file: 2000

LONG file: 700

☑ Output messages to Event Viewer

Type of Event Viewer message

● Error

○ Error, Warning

○ Error, Warning, Information

(1) Log information

Log files are output to *installation-directory*`\log` for each type of information for error analysis purposes. With normal operation, there is no need to change the default values. If the log information takes up too much space on the disk, you can adjust values.

Generations of log file to be saved

Specify the number of log generations to be saved. Specify the value in the range from 1 to 999. The default is 5.

Maximum lines in a log file

Specify the number of output lines for the log files shown below. Specify the value in the range from 500 to 9,999 lines. The following table shows the default value and file names of each log type.

Item	Default value	File names
MAIN file	`700`	• `MAIN.LOG`
USER file	`700`	• `BUILD.LOG` • `SCRIPT.LOG` • `USER.LOG`
COMPO file	`700`	• `API.LOG` • `ATRFILE.LOG` • `BSAPI.LOG`

Item	Default value	File names
COMPO file	`700`	• `CLTPROTO.LOG` • `DEFAULT.LOG` • `EXCFILE.LOG` • `MNGFILE.LOG` • `RDBMENTE.LOG` • `SERVICE.LOG` • `SRVSOCK.LOG` • `STSFILE.LOG` • `WSH.LOG`
FUNC file	`2000`	• `AMTAPI.LOG` • `CLIENT.LOG` • `CLTDEL.LOG` • `DCMAMT.LOG` • `DISCVRY.LOG` • `DLL.LOG` • `DPT.LOG` • `INVENTRY.LOG` • `MLTPROTO.LOG` • `MONRST.LOG` • `MONTRACE.LOG` • `NDGMENT.LOG` • `PSM.LOG` • `SCHEDULE.LOG` • `SCHTRACE.LOG` • `SERVER.LOG` • `SITE.LOG` • `SRVAPI.LOG` • `SRVLOCK.LOG` • `USER_CLT.LOG` • `WRAPPER.LOG`
LONG file	`700`	• `DUMP.LOG` • `NODE.LOG` • `NODEOPR.LOG` • `RDBSRV.LOG` • `USERINV.LOG`

The number of log generations to be saved or the number of log entries cannot be set for the following types of log files:

- `alerterr.log`
- `alerthis.log`
- `CSVODBC.log`
- `CSVODBCSYS.log`
- `Dmoledb.log`
- `DPTExpt.log`

- `DPTInpt.log`
- `INVODBC.log`
- `rimfind`*`n`*`.log`
- `smart`*`n`*`.log`
- `SMC.LOG`
- `SMCAPP64.LOG`
- `SMCCMDS.LOG`
- `SMCCSAPP.LOG`
- `SMCDEV64.LOG`
- `SMCDEVICECHANGE.LOG`
- `SMCDEVSR.LOG`
- `SMCUAP64.LOG`
- `SMCUSAGE.LOG`
- `SMCUSAPP.LOG`

You can use the following formula to determine the size of each log file:

Size of a log file (bytes) =
(*size of the header* + (*size of 1 entry* **x** *number of entries*)) **x** (*number of generations* + 1)

Size of the header: 17 bytes

Size of 1 entry: 192 bytes (use 300 bytes in the case of a LONG file)

(2) Output message to Event Viewer

You can select whether to output messages to the Windows NT Event Viewer. By default, this check box is selected. Note that you cannot control whether to output messages to Event Viewer during JP1/Software Distribution Manager or relay manager setup. These messages are always output to Event Viewer.

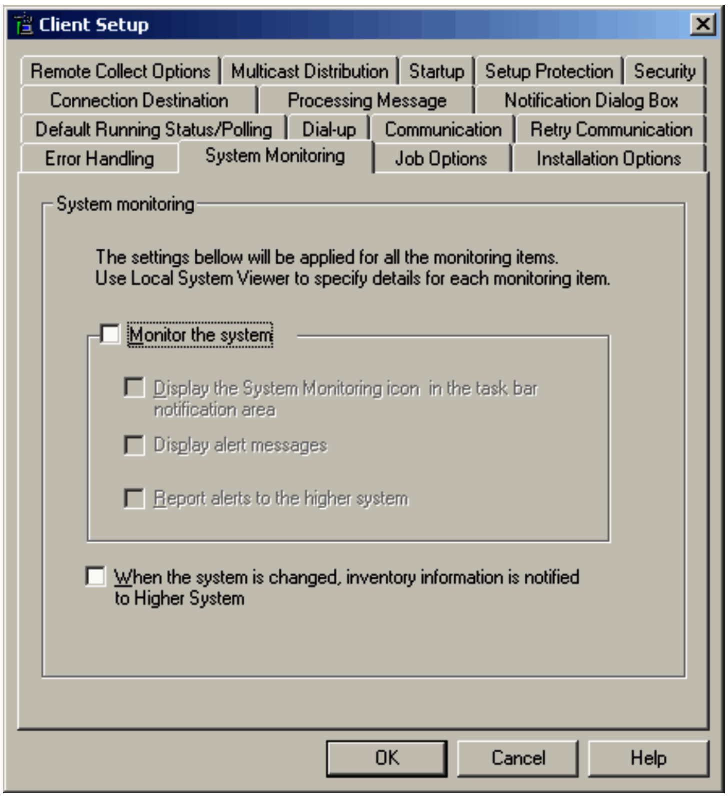
If you are outputting messages to Event Viewer, you can select whether to output the following three sets of messages.

- **Error**
- **Error**, **Warning**
- **Error**, **Warning**, **Information**

6.2.9 System Monitoring page

The client facility for monitoring the hardware of the local PC is called *system monitoring*. This page specifies information about system monitoring for the client.

Figure 6–10: System Monitoring page



Client Setup

System monitoring

The settings bellow will be applied for all the monitoring items.
Use Local System Viewer to specify details for each monitoring item.

□ Monitor the system

□ Display the System Monitoring icon in the task bar notification area

□ Display alert messages

□ Report alerts to the higher system

□ When the system is changed, inventory information is notified to Higher System

System monitoring

Specify whether or not you wish to monitor the hardware status of the local PC. The default is that this check box is not selected.

By selecting this check box, you can display the hard disk and memory status on the **System Conditions** page of Local System Viewer. You can also issue alerts when errors are detected in the hardware being monitored.

In the Conditions Settings for System Monitoring window, specify the details of the items to be monitored and the method for issuing alerts. Note that the settings specified in the Conditions Settings for System Monitoring window take effect only if **Monitor the system** is selected during client setup.

When **Monitor the system** is selected, you can specify the following three settings:

Display the System Monitoring icon in the task bar notification area

Select whether or not you wish to display the **System Monitoring** icon in the task bar notification area. The default is that this check box is not selected.

By displaying the **System Monitoring** icon, you can determine from the icon's status whether or not system monitoring is underway and whether or not an alert has been issued. Double-clicking on the **System Monitoring** icon starts Local System Viewer that enables you to check the item resulting in an alert.

For details about the **System Monitoring** icon, see *11.8.3 Using the System Monitoring icon* in the manual *Administrator's Guide Volume 1*.

Display alert messages

Select whether or not you wish to display a pop-up menu to notify the user in the event of an alert. The default is that this check box is not selected. If you are remote-controlling an unattended PC, you should clear this check box.

Note that you must select this **Display alert messages** check box to apply the **Display alert messages** option to each item being monitored in the Conditions Settings for System Monitoring window.

Report alerts to the higher system

Select whether or not you wish to report alert messages to the higher system in the event of an alert. The default is that this check box is not selected.

This option is applicable only when the client is connected to a higher system. The corresponding higher system can check the alert messages using a CSV file containing historical alert information, Event Viewer of Windows NT, or the Event Console window of JP1/IM - View.

Note that you must select this **Report alerts to the higher system** check box to apply the **Report alerts to the higher system** option to each item being monitored in the Conditions Settings for System Monitoring window.

When the system is changed, inventory information is notified to Higher System

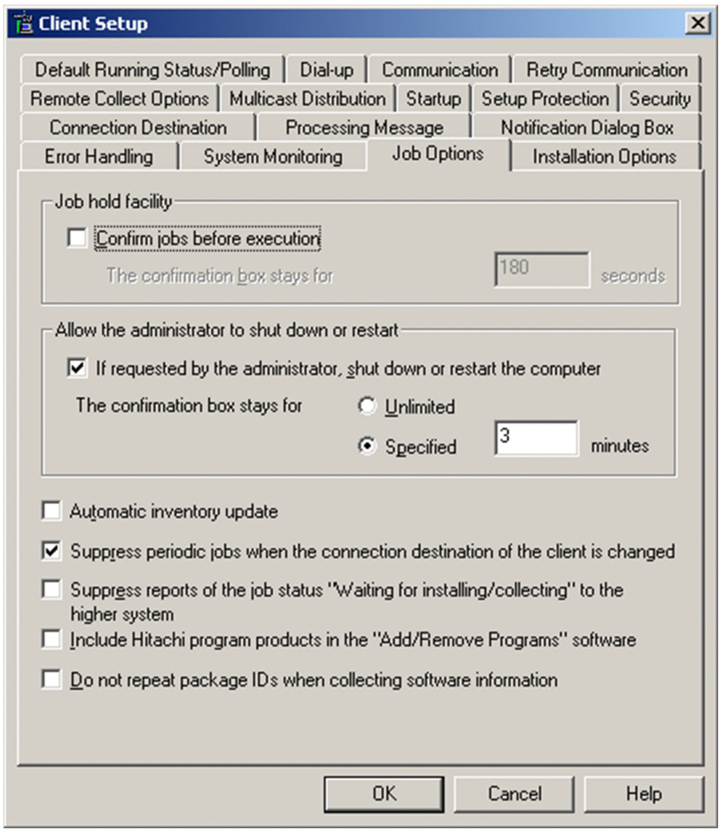
Select whether or not you wish to automatically report inventory to the higher system when system or software information is changed, such as when a host name is changed or software is uninstalled. The default is that this check box is cleared.

For details about the facility for automatically reporting inventory to the higher system and the inventory to be reported, see *2.13.4(3) Automatic reporting of updated inventory information* in the *Description and Planning Guide*.

6.2.10 Job Options page

Specify whether or not you wish to use each job option, such as the job hold facility and the client control facility, during job execution.

Figure 6–11: Job Options page



Job hold facility

□ Confirm jobs before execution

The confirmation box stays for 180 seconds

Allow the administrator to shut down or restart

☑ If requested by the administrator, shut down or restart the computer

The confirmation box stays for ○ Unlimited

● Specified 3 minutes

□ Automatic inventory update

☑ Suppress periodic jobs when the connection destination of the client is changed

□ Suppress reports of the job status "Waiting for installing/collecting" to the higher system

□ Include Hitachi program products in the "Add/Remove Programs" software

□ Do not repeat package IDs when collecting software information

(1) Job hold facility

This item sets the job hold facility. For details about the job hold facility, see *2.13.1(2)(a) Using the job hold and cancellation facility* in the *Description and Planning Guide*. During setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system), this item is displayed but cannot be set.

Confirm jobs before execution

Select this check box to use the job hold facility. The default is that this check box is not selected.

The confirmation box stays for

If you will be using the job hold and cancellation facility, set the display duration for the Hold or Cancel Software Distribution Job dialog box. The dialog box displays the number of seconds remaining until execution.

If the user performs no operations on the dialog box within the specified display duration, when the remaining number of seconds reaches 0, the system executes the displayed operation and closes the dialog box.

Specify the value in the range from 0 to 1,800 seconds. The default is 180 seconds. If you specify `0`, the dialog box remains displayed until the user performs an operation.

(2) Allow the administrator to shut down or restart

The administrator can specify for a job that the computer is to be shut down by client control after a job is executed. The administrator can also specify for a package that the computer is to be restarted automatically after a package has been installed.

This item specifies whether or not it is to be permitted for the computer to be shut down when shutdown after job execution is specified for the job and whether or not it is to be permitted for the computer to be restarted when restart after package installation is specified. It also specifies the settings for the confirmation dialog box when shutdown or restart is enabled.

Note that you cannot specify this item during setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system).

If requested by the administrator, shut down or restart the computer

Specify whether or not it is to be permitted for the client to be shut down or restarted on the basis of an instruction when the administrator specifies shutdown after job execution or restart after package installation. The default is that this check box is selected.

If the administrator uses the client control facility to start the PC to execute jobs when it is unattended, you should select this check box so that the PC can be shut down by an instruction. For a PC that is always running, you do not need to select this check box.

If you want to have the computer restarted automatically after package installation on the basis of an instruction from the administrator, select this check box.

Note that if you select **If requested by the administrator, shut down or restart the computer** check box, a confirmation dialog box is displayed before shutdown or restart takes place.

The confirmation box stays for

If you select this option, specify how long the confirmation dialog box is to be displayed before shutdown or restart takes place. When the dialog box has been displayed at the client for the specified amount of time, shutdown or restarts begins. Specify the value in the range from 1 to 60 minutes. The default is 3 minutes. If you specify **Unlimited**, shutdown or restart does not begin until the user makes an entry. If a job is executed from the Package Setup Manager of the client, shutdown or restart does not begin until the user makes an entry even though the specified display time elapses.

For details about shutting down the computer by the client control facility, see *6.3.3 Notes on shutdown* in the *Description and Planning Guide*. For details about automatic restart of the computer, see *2.2.8 Options page* in the manual *Administrator's Guide Volume 1*.

(3) Automatic inventory update

Specify whether or not the client is to report to the higher system information such as the available disk space in the local system (which changes whenever an installation is executed) together with the installation results. When automatic inventory updating is enabled, the communication volume increases by about 500 bytes for each installation instruction. The default is that this check box is not selected.

(4) Suppress periodic jobs when the connection destination of the client is changed

Among the *Get system information from client* jobs, *Get software information from client* jobs, and *Transfer user inventory schema to client* jobs, jobs that are specified to execute at a client periodically (for example, daily, weekly, or monthly) are referred to as *periodic jobs*.

A periodic job reports periodically the execution results to the connection destination where the job was executed. Therefore, even if a client cannot communicate with the destination (for example, because the client was moved), the job will still try to report the execution results. In such a case, to stop unnecessary communications, select this check box to suppress execution of periodic jobs when the connection destination of the client has changed.

The default is that this check box is selected.

The following table shows the periodic jobs that are executed without being suppressed even though you select this check box:

Product type and setting conditions			Periodic jobs that are not suppressed
Client	Polling of multiple higher systems	No	Jobs at the connection destination after the client is changed
		Yes	Jobs at the connection destination after the client is changed and that have multiple higher systems
Relay system			Jobs at the connection destination after the client is changed and that belong to the relay system itself
Relay manager			Jobs at the connection destination after the client is changed and that belong to the relay manager itself

You should note the following about using this option:

When you want to execute the same job even when the client connection destination is changed

When **Suppress periodic jobs when the connection destination of the client is changed** is selected, periodic jobs cannot be executed at the previous connection destination if you change the destination. If you want to execute the same periodic jobs at the new connection destination, do either of the following:

When you use ID group jobs (you change the destination within the same network by using the same ID group):

- When **Linkage when system configuration is changed** is selected

  The same periodic jobs are executed because the system connects to the ID group even if you change the connection destination of the client.

- When **Linkage when system configuration is changed** is not selected

  After you change the connection destination on the client, register the jobs in the ID group.

When you use host groups:

At the new connection destination system, delete or execute periodic jobs periodically.

Using the client on an offline machine

With an offline machine, if you wish to suppress periodic jobs from a system that is not at the connection destination, and execute periodic jobs that are from the connection destination, set the host name and IP address of the connection destination in the `hosts` file so that the address can be resolved. If the address cannot be resolved, periodic jobs from the connection destination are also suppressed.

If you wish to execute periodic jobs from the connection destination even when the address cannot be resolved, select the check box. In this case, periodic jobs from a system that is not at the connection destination can no longer be suppressed.

When uncompleted jobs are generated

Depending on the timing for suppressing periodic jobs, periodic jobs may be suppressed without being executed at all. In such a case, the execution status of jobs on the managing server stays at 70% and their execution is not completed.

(5) Suppress reports of the job status "Waiting for installing/collecting" to the higher system

When a job is distributed to a client, the higher system may be notified that the job is in the *Waiting for installing/collecting* status. After this notification, the execution status of this job in the Job Status window of the higher system is placed in the *Waiting for installing/collecting* status. Normally, after a job is distributed, it takes some time before completion (or failure) of installation or collection is reported to the higher system. Therefore, the contents of the Job Status window change each time the report is made.

However, the higher system may receive the job results (completion or failure) report immediately after receiving the *Waiting for installing/collecting* status report. If you select this check box for such cases, the *Waiting for installing/collecting* report is suppressed. Every time this report is suppressed, 170 bytes (340 bytes for an ID group job) of network traffic is eliminated. Also, the load on the higher system for updating the job execution status is reduced. In the initial settings, this check box is not selected.

You can suppress the *Waiting for installing/collecting* status report for the following jobs:

- *Install package* job
- *Collect files from client* job
- *Collect files from client to relay system* job
- *Get system information from client* job
- *Get software information from client* job
- *Get user inventory information* job

When any of these jobs is executed with the following settings specified, and all the conditions for suppression are satisfied, the *Waiting for installing/collecting* status report is suppressed. The conditions for suppression depend on the combination of the job settings.

Job settings			Conditions for suppression
Installation date/ time	Install when system starts	GUI installation mode	
Y#1	N	N	• The specified date/time has been reached when the job distribution is completed.
N	Y	N	• At the client, **The first polling is executed: Before the client starts** is set. • The job was distributed at the first polling.
Y	Y	N	• At the client, **The first polling is executed: Before the client starts** is set. • The job was distributed at the first polling. • The specified date/time has been reached when the job distribution is completed.
N	N	Y#2	• The client has logged on when the job distribution is completed.
Y	N	Y#2	• The specified date/time has been reached when the job distribution is completed. • The client has logged on when the job distribution is completed.
N	Y	Y#2	• At the client, **The first polling is executed: Before the client starts** is set. • The job was distributed at the first polling. • The client has logged on when the job distribution is completed.
Y	Y	Y#2	• At the client, **The first polling is executed: Before the client starts** is set. • The job was distributed at the first polling. • The specified date/time has been reached when the job distribution is completed. • The client has logged on when the job distribution is completed.

Legend:

Y: Specified. N: Not specified

#1

Suppression is not performed for *Collect files from client* jobs and *Collect files from client to relay system* jobs.

#2

Suppression is performed for *Install package* jobs only.

(6) Include Hitachi progam products in the "Add/Remove Programs" software

Software information about Hitachi program products is reported to the higher system as installed packages under the type **Hitachi program products**. Therefore, when a *Get software information from client* job is received in which the option **Search software listed in "Add/Remove Programs"** is specified, information about the Hitachi program products will not be reported.

When this check box is selected, information about Hitachi program products that have been registered in **Add/Remove Programs** on the **Control Panel** is reported as installed packages in **Add/Remove Programs**. As a result, software information including Hitachi program products that have been registered in **Add/Remove Programs** can be acquired in the batch mode. The default is that this check box is not selected.

If you select this check box, you should not execute the operations listed below. If they are executed, information about Hitachi program products will also be reported as **Hitachi program products**, resulting in a duplication of software information that is managed in the higher system.

- Acquiring software information with **Search all software** specified from the managing server
- Choosing **Collect Software Information and Update** from Package Setup Manager's **Execute** menu at the client

If JP1/Asset Information Manager is linked, and installed package information is duplicated, information may no longer be managed correctly by JP1/Asset Information Manager.

(7) Do not repeat package IDs when collecting software information

Package IDs may be repeated for the following software information, preventing accurate collection of information.

- Software listed under **Add or Remove Programs** or **Add/Remove Programs** in the Windows **Control Panel**.
- Patches applied to the computer
- Patches not applied to the computer

The programs for which software information cannot be accurately collected are generally updates after Microsoft Office 2007.

When this check box is selected, software information can be collected accurately for these programs.

When clients for which the **Do not repeat package IDs when collecting software information** check box is selected are mixed with clients for which it is not selected, note the following:

When clients on which the check box is selected are mixed with clients on which it is not selected

- Different package IDs may be set for the same software. For that reason, software cannot always be reliably identified by the package ID.

Also, when the **Do not repeat package IDs when collecting software information** check box is selected and Asset Information Manager Subset or JP1/Asset Information Manager is set in **Server Setup** to acquire package IDs, note the following:

Sharing between Asset Information Manager Subset and JP1/Asset Information Manager

- When a package ID is updated, first the software information for the previous package ID is deleted, then the software information for the updated package ID is added. Therefore, it may take some time to collect software information.
- In the update history for installed software, this appears as deleting the software information for the previous package ID and adding the software information of the updated package ID.
- Note that you can delete update histories of this type.

  For information about deleting update histories with Asset Information Manager Subset, see *10.7.3 Specifying the types of history information to be deleted and the deletion timing*. For information about deleting update histories with JP1/Asset Information Manager, see the manual *JP1/Asset Information Manager Administrator's Guide*.

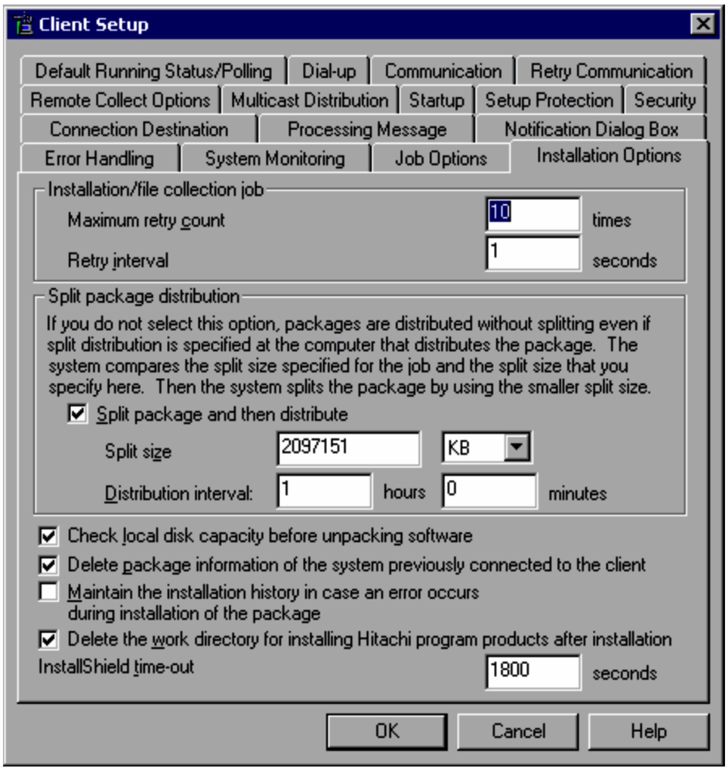
Note on JP1/Asset Information Manager

- If the installed software name is used to automatically registered software names, software names may be repeated. If this happens, unify the software names. For details, see the manual *JP1/Asset Information Manager Administrator's Guide*.

6.2.11 Installation Options page

Specify installation options, such as the retry count in the event of an error during remote installation and whether or not split package distribution is to be performed.

Figure 6–12: Installation Options page



Installation/file collection job

Maximum retry count: 10 times

Retry interval: 1 seconds

Split package distribution

If you do not select this option, packages are distributed without splitting even if split distribution is specified at the computer that distributes the package. The system compares the split size specified for the job and the split size that you specify here. Then the system splits the package by using the smaller split size.

☑ Split package and then distribute

Split size: 2097151 KB

Distribution interval: 1 hours 0 minutes

☑ Check local disk capacity before unpacking software

☑ Delete package information of the system previously connected to the client

□ Maintain the installation history in case an error occurs during installation of the package

☑ Delete the work directory for installing Hitachi program products after installation

InstallShield time-out: 1800 seconds

(1) Installation/file collection job

Specify a retry count and retry interval to be applied if an error occurs during remote installation or remote collection on user programs and data.

Maximum retry count

Specify the value in the range from 0 to 100. The default is 10. If `0` is specified, no retries are attempted.

Retry interval

Specify the value in the range from 0 to 3,600 seconds. The default is 1 second. If `0` is specified, retries occur immediately one after another without any interval.

(2) Split package distribution

If you select the **Split package and then distribute** check box and a distributed package is larger than the size specified here, the package is split into increments of the specified size and then distributed. During split package distribution, if the split size at the distribution source is greater than the size specified here, the package is further split into those size increments and then distributed. Specify this option if you wish to reduce the network load. The default is that this check box is selected.

When this check box is cleared, split package distribution will not take place even if split distribution has been specified for packages.

Split size

Specify the size into which packages are to be split. When split package distribution is executed, the system compares the value you specify here with the size of a package that is to be distributed and divides the package as appropriate. The permitted value range is shown below. The default is 2,097,151 KB.

- Specifying in kilobytes: 1 to 2,097,151
- Specifying in megabytes: 1 to 2,047

The split size applies to each package transferred. If multiple packages are transferred in the batch mode and the size of each package is no greater than the specified split size, split package distribution does not occur.

Distribution interval

Specify a rest time between transfers when split package distribution is executed. Specify the value in the range from 1 to 24 hours. The default is 1 hour.

The split sizes for the distribution source and the distribution destination are compared, and the distribution interval for the side at which the smaller split size is specified takes effect. If the split sizes are the same, the distribution interval for the distribution destination is used.

(3) Check local disk capacity before unpacking software

Select whether or not the client is to check the available disk space in the local system before it downloads a package during remote installation. The client reports an error to the higher system if the required disk space is not available in the local system. The default is that this check box is selected.

(4) Delete package information of the system previously connected to the client

Select this item to delete package information for the system to which the client was previously connected whenever the connection destination system is changed in the setup. The default is that this check box is selected. In systems where the user frequently changes the connection destination system, the amount of stored package information may fill up the available hard disk space. For this reason, you can set the client to delete package information for the previous connection destination system.

If the client is connected to multiple systems, package information for systems that have been specified as connection destination systems is not deleted even if this check box is selected.

Note that this item is displayed but cannot be specified during setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system).

(5) Maintain the installation history in case an error occurs during installation of the package

If an attempt to overwrite a package results in an error, this option specifies whether or not information about the installed package, which was to be overwritten, is to be stored. The default is that this check box is cleared. If you wish to set software conditions when a package is installed, select this check box.

- When the check box is cleared

  In the event of an error, information about the installed package that is to be overwritten is deleted. This is because normal operation of the installed package (software) can no longer be guaranteed if an error occurs during overwrite installation.

  If an error has occurred and the package information has been deleted, you can no longer install the package with the software conditions set. The Package Setup Manager places the package that had been installed in uninstalled status.

  If an overwrite installation attempt results in an error while this check box is cleared, you can no longer install the package with the version or generation number of the deleted package set as the software conditions. To install the package, execute the following procedure:

  1. Select the **Maintain the installation history in case an error occurs during installation of the package** check box.
  2. Restart the client.
  3. Re-install the package that had been installed (whose information was deleted) without setting the software conditions.
  4. Set the software conditions and install the package.

- When the check box is selected

  Information about the package that had been installed and that was to be overwritten remains stored even after the error. Therefore, you can still install the package with the software conditions set. In this case, the status of the installed package does not change on the Package Setup Manager.

  If the check box is selected and an overwrite installation attempt without the software conditions set results in an error then, when you re-install the package, select the **Replace existing package** check box that is on the **System Conditions** page of the Change Installation Conditions dialog box.

(6) Delete the work directory for installing Hitachi program products after installation

You can select whether or not the client is to delete the *Work directories for installing Hitachi products* (`NETMDMWK` directory) after Hitachi products have been installed. To delete the work directory, select this check box. The default is that this check box is selected.

You should note the following items:

- You cannot select this option if you are creating setup information in an installation set.
- In the case of Windows NT, you must set Read, Write, and Delete access permissions for the created drive. If these access permissions are not set, installation of Hitachi program products will fail.
- Even if you set this option, the `NETMDMWK` directory may still remain after installation. In such a case, the directory is deleted the next time the PC is restarted or at the next polling.

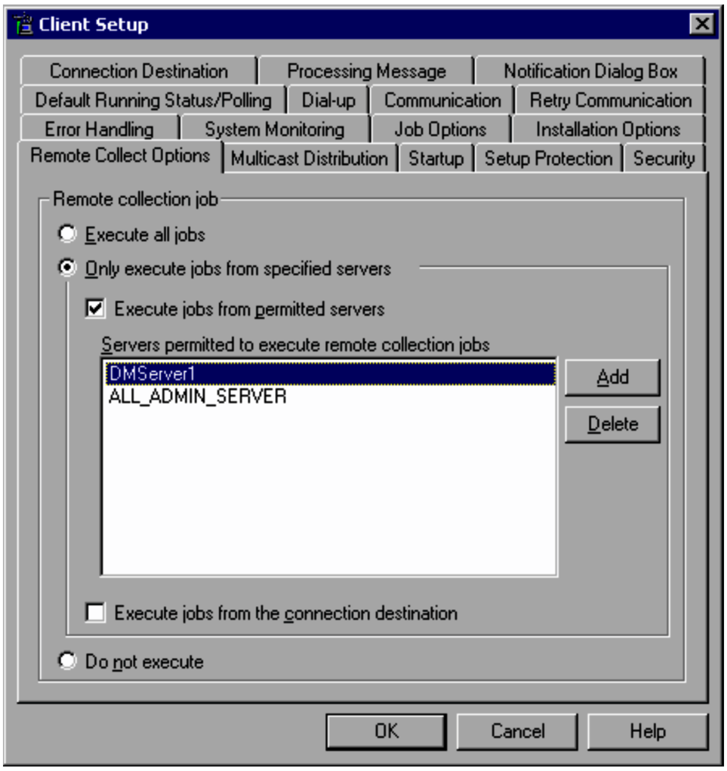
(7) InstallShield timeout

Specify the maximum wait time for a response from `InstallShield` after remote installation of Hitachi program products. If `InstallShield` does not respond before the specified amount of time elapses, the client reports an error to the higher system. Specify the value in the range from 180 to 7,200 seconds. The default is 1,800.

6.2.12 Remote Collect Options page

Specify whether or not you wish to limit the remote collection jobs that are executed at the client.

Figure 6–13: Remote Collect Options page



Remote collection job

○ Execute all jobs

● Only execute jobs from specified servers

☑ Execute jobs from permitted servers

Servers permitted to execute remote collection jobs

DMServer1
ALL_ADMIN_SERVER

□ Execute jobs from the connection destination

○ Do not execute

This limitation applies to the following remote collection jobs:

- *Collect files from client* job
- *Collect files from client to relay system* job
- *Acquire collected files from relay system* job
- *Delete collected files from relay system* job

Select **Execute all jobs**, **Only execute jobs from specified servers**, or **Do not execute**. The default is **Execute all jobs**.

Execute all jobs

Specify this option to execute all remote collection jobs from higher systems.

Only execute jobs from specified servers

Specify this option to execute only remote collection jobs from specified higher systems. You can either specify higher systems directly or only the higher connection destination.

Execute jobs from permitted servers

You can specify a maximum of eight higher systems from the **Servers permitted to execute remote collection jobs** list. Choose **Add** to display the Servers Permitted to Collect Files dialog box. Specify either the host name or IP address of a higher system, as 1-64 bytes.

To delete a higher system from the **Servers permitted to execute remote collection jobs** list, select the higher system and then choose **Delete**.

Execute jobs from the connection destination

Specify this option to execute only remote collection jobs from the higher connection destination or the higher systems specified on the **Connection Destination** page. Jobs from systems not specified on the **Connection Destination** page will not be executed.

Do not execute

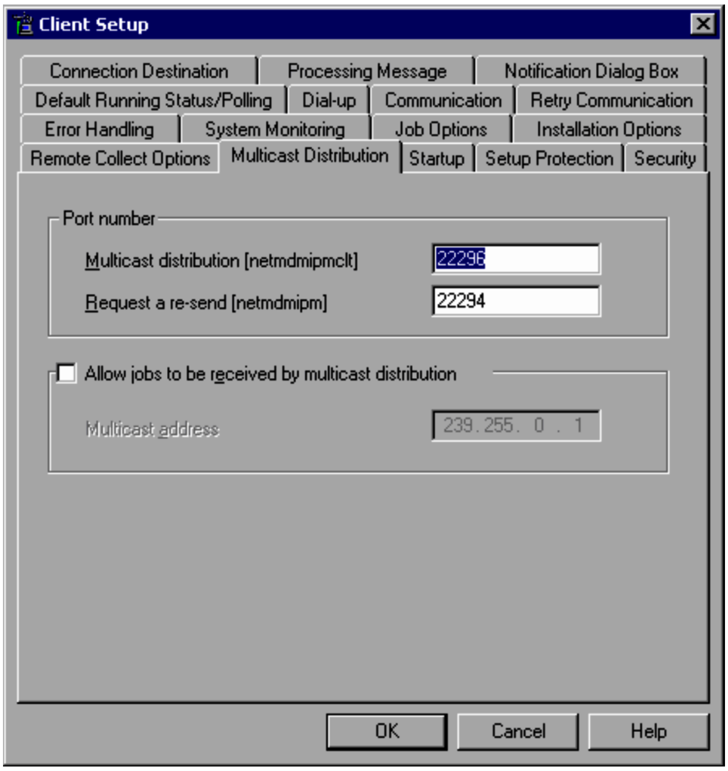
Specify this option to stop execution of all remote collection jobs from higher systems.

Note that if the connection destination is changed by the **Automatically specify the higher system that requested a job execution as the connection destination** option on the **Connection Destination** page and the new connection destination is not specified under **Higher systems** in the Specify Higher Systems dialog box, the new connection destination is not automatically added to the list.

6.2.13 Multicast Distribution page

These settings are for receiving jobs sent by multicast distribution from a higher system. The settings on this page apply to jobs for which you specify multicast distribution.

Figure 6–14: Multicast Distribution page



Port number

Multicast distribution [netmdmipmclt] 22296

Request a re-send [netmdmipm] 22294

□ Allow jobs to be received by multicast distribution

Multicast address 239 . 255 . 0 . 1

(1) Port number

Specify the following two port numbers for receiving jobs distributed by multicast distribution:

- **Multicast distribution** (default: `22296`)
- **Request a re-send** (default: `22294`)

Normally, you should use the displayed default port numbers. However, you must change a port number if some other program is using that port. It is important that you set a port number for **Request a re-send**, because multicast distribution uses the UDP protocol and packets may be resent during distribution.

If a port number is set in the `services` file of TCP/IP, the `services` file setting takes precedence.

(2) Allow jobs to be received by multicast distribution

Select the **Allow jobs to be received by multicast distribution** check box to receive jobs specified for multicast distribution from the higher system using the multicast distribution method. The default is that this check box is not selected. To receive jobs by multicast distribution, select this check box, and then specify the same multicast address specified in the connection destination higher system.

When **Allow jobs to be received by multicast distribution** check box is not selected, jobs are received by unicast distribution even if multicast distribution is specified. Conversely, even if you select this check box, jobs for which you have specified unicast distribution are received using the unicast method.

You should clear the **Allow jobs to be received by multicast distribution** check box if there is a router in the network that is not compatible with IP multicasting. If the network includes routers that are not compatible with IP multicasting, unicast distribution is used; you cannot use multicast distribution. If you do select **Allow jobs to be received by multicast distribution** check box, the system will require a long time to switch to unicast distribution in order to distribute a job.

Multicast address

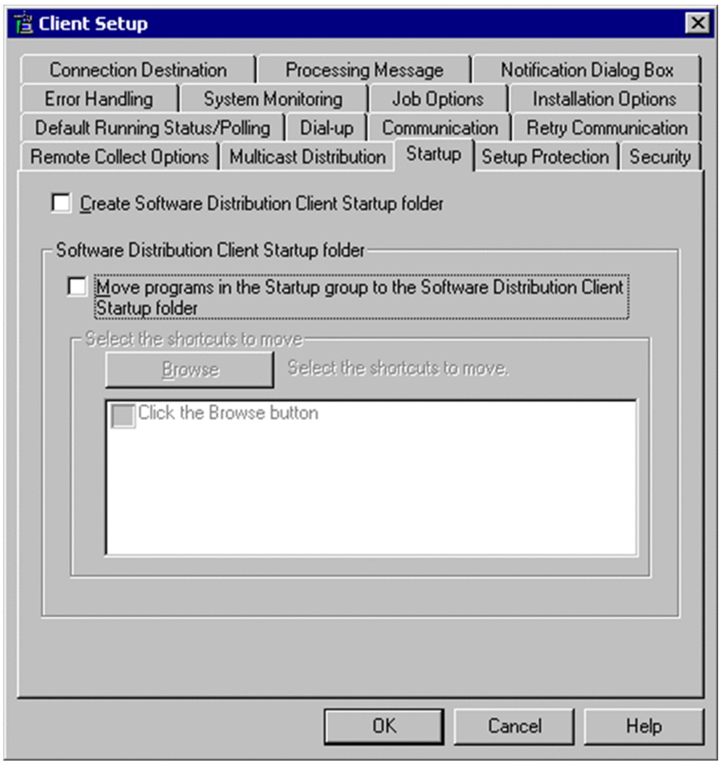
Specify the same multicast address specified in the connection destination higher system. This completes registration into a multicast group to which the higher system sends jobs. Specify a value in the range from 224.0.1.0 to 239.255.255.255. The default address is 239.255.0.1.

If the multicast address of the connection-destination higher system does not match the multicast address you specify here, the job will be distributed using unicast distribution to this client. For details about multicast groups and multicast addresses, see *6.2 Settings for multicast distribution* in the *Description and Planning Guide*.

6.2.14 Startup page

The **Startup** page provides settings required for remote installation of programs registered in the **Startup** group.

Figure 6–15: Startup page



□ Create Software Distribution Client Startup folder

Software Distribution Client Startup folder

□ Move programs in the Startup group to the Software Distribution Client Startup folder

Select the shortcuts to move

Browse   Select the shortcuts to move.

□ Click the Browse button

(1) Create Software Distribution Client Startup folder

Select whether or not you wish to create a **Software Distribution Client Startup** folder for moving programs registered in the **Startup** group. The default is that this check box is not selected.

The programs registered in the **Startup** group are started automatically when Windows starts. The timing of installation at system startup by JP1/Software Distribution is also the same as for the startup programs. If JP1/Software Distribution attempts to remote-install a program while programs are being started as startup programs, installation fails. To avoid this, create a **Software Distribution Client Startup** folder and move the startup programs into this folder. For details about moving startup programs, see *11.2.2(2) Moving startup programs* in the manual *Administrator's Guide Volume 1*.

(2) Software Distribution Client Startup folder

Move programs in the Startup group to the Software Distribution Client Startup folder

If you create a **Software Distribution Client Startup** folder for the client, you can move automatically the programs from the **Startup** group to the **Software Distribution Client Startup** folder. To do this, select the **Move programs in the Startup group to the Software Distribution Client Startup folder** check box. The default is that this check box is not selected.

Select the shortcuts to move

You can specify this item when you select **Move programs in the Startup group to the Software Distribution Client Startup folder**. To display a list of shortcuts, click the **Browse** button.

Select the check boxes of the shortcuts to be moved to the **Software Distribution Client Startup** group. The system does not move the shortcuts corresponding to the check boxes that you clear. The default is that all check boxes are selected.

If a shortcut whose check box is cleared is already registered in the **Software Distribution Client Startup** folder, the client automatically returns the shortcut from the **Software Distribution Client Startup** folder to the **Startup** group, and the client does not include it in the list of shortcuts to be moved.

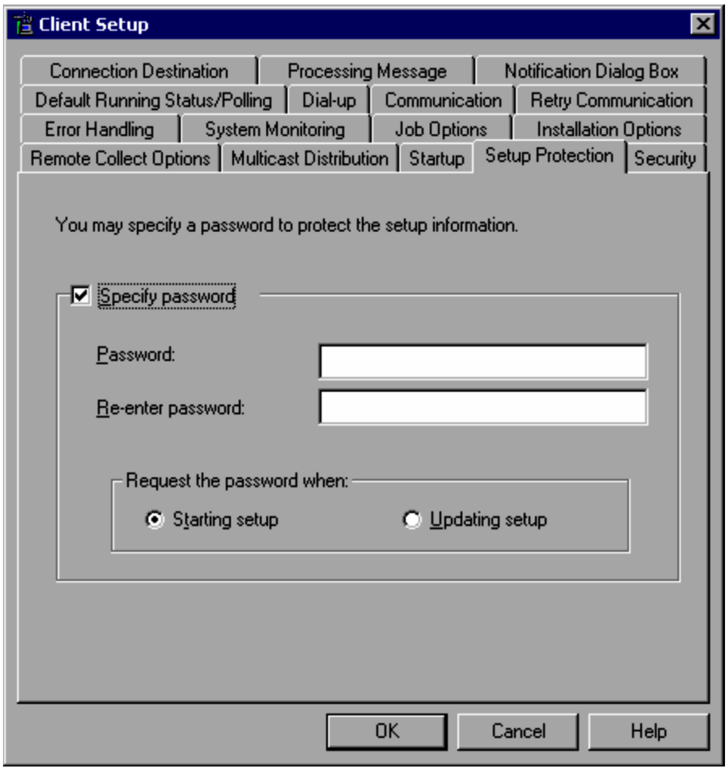
For setup information in an installation set, you cannot specify the **Select the shortcuts to move** option in advance. By selecting the **Move programs in the Startup group to the Software Distribution Client Startup folder** check box, all programs registered in the **Startup** group at the installation target of JP1/Software Distribution Client (client) are moved.

6.2.15 Setup Protection page

Specify a password for protecting the setup information.

This page is not provided during setup of client facilities for JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system).

Figure 6–16: Setup Protection page



Client Setup

You may specify a password to protect the setup information.

☑ Specify password

Password:

Re-enter password:

Request the password when:

● Starting setup ○ Updating setup

Because anyone can change information specified during client setup (setup information), operation of the program cannot be guaranteed if inappropriate changes are made. For this reason, you can protect the setup information by assigning a password. Once you have specified a password on this page, a dialog box requesting the password will be displayed each time startup of client setup is attempted and each time an attempt is made to change setup information.

Specify password

Select this check box to specify a password for the setup information. The default is that this check box is not selected.

Password

Specify a password for protecting the setup information, as 1-14 bytes of alphanumeric characters. If you select the **Specify password** check box, this item is mandatory.

Re-enter password

Re-enter the password to verify it.

Request the password when:

Select the times when the Input Password dialog box is to be displayed:

- **Starting setup**

  Password will be requested whenever client setup is started. A user who does not enter the correct password will not be able to view the setup information.

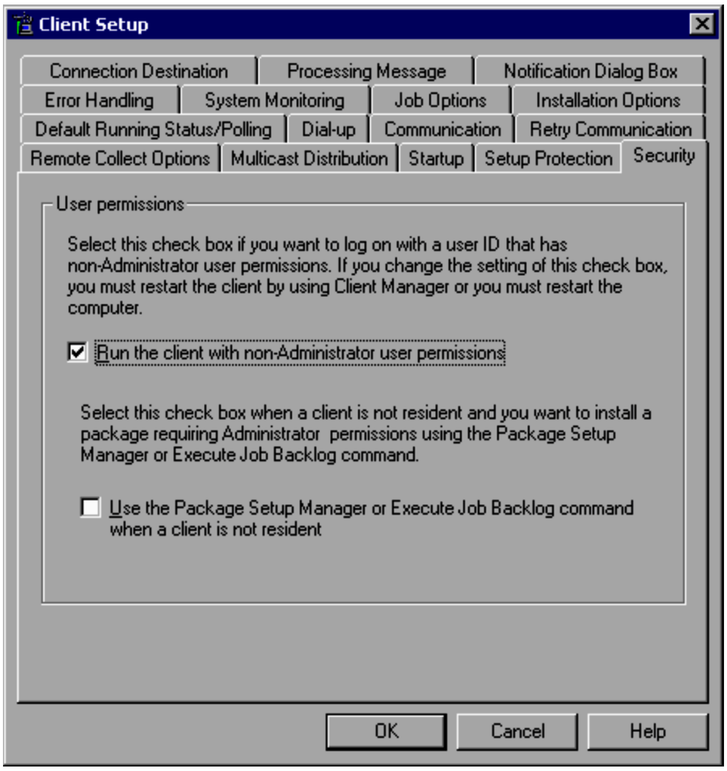
- **Updating setup**

  Password will be requested whenever an attempt is made to update the client setup. A user who does not enter the correct password will be able to view setup information but will not be able to update it.

6.2.16 Security page (for Windows NT)

Specify whether or not you wish to use the client with the non-Administrator user permissions that do not include Administrator permissions.

Figure 6–17: Security page



Select this check box if you want to log on with a user ID that has non-Administrator user permissions. If you change the setting of this check box, you must restart the client by using Client Manager or you must restart the computer.

☑ Run the client with non-Administrator user permissions

Select this check box when a client is not resident and you want to install a package requiring Administrator permissions using the Package Setup Manager or Execute Job Backlog command.

☐ Use the Package Setup Manager or Execute Job Backlog command when a client is not resident

In the case of a Windows NT client, you can set up the client so that any user can install packages, not just the user who installed the client. This page is not provided during setup of client facilities for JP1/Software Distribution Manager.

Run the client with non-Administrator user permissions

If you select this check box, a user who did not install the Client will be able to install packages in the GUI installation mode and display processing messages. This means that a user who does not have Administrator permissions (a non-Administrator user) will be able to install packages.

For JP1/Software Distribution Client (client), the default is that this check box is selected.

For JP1/Software Distribution Client (relay system), the default is that this check box is cleared.

For details about installation with non-Administrator user permissions, see *11.2.3 Installing software using non-Administrator user permissions under Windows NT* in the manual *Administrator's Guide Volume 1*.

Use the Package Setup Manager or Execute Job Backlog command when a client is not resident

This check box is not displayed during setup of client facilities for JP1/Software Distribution Client (relay system). This check box is enabled when the following settings are specified for JP1/Software Distribution Client (client):

- The **Run the client with non-Administrator user permissions** check box is selected.
- On the **Default Running Status/Polling** page, the **Client starts automatically at system boot** check box is not selected.

When you select this check box, a user logged on with a non-Administrator user permission can install the following packages using the Package Setup Manager or the **Execute Job Backlog** icon of the client even though the client is not resident:

- Packages that require registration, starting, or stopping of a service
- Packages that create new registry keys
- Packages whose installation directory and file access permissions do not include *read*, *write*, or *delete*.

Note that when you select this check box, the `dmpusers.exe` process is made resident.

6.3 Registry settings (JP1/Software Distribution Client (client))

You can set the following item, not found in the setup procedure, by editing the registry. This is described below.

Continue command processing after Windows logoff

If the PC on which JP1/Software Distribution Client (client) is installed is running any of the operating systems shown below, command processing can be made to continue even after you log off of Windows.

- Windows NT 4.0
- Windows 2000
- Windows XP
- Windows Server 2003

For the commands that can be executed, see *4.2.1 Command types* in the manual *Administrator's Guide Volume 2*.

To have command processing continue after logging off of Windows, create the registry value shown below in registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi\NETM/DM`. For 32-bit operating systems, create the registry value in registry key `HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\NETM/DM`.

Name

`CmdLogoffContinue`

Type

`REG_SZ`

Data

`YES`

If the registry key, `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi\NETM/DM` or `HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\NETM/DM` does not exist, create the registry value in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi\NETM/DM/P` or `HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\NETM/DM/P`.

Notes

- To have command processing continue after logging off of Windows, the command must be executed from the service. Processing of commands executed by any other method will not continue after logging off of Windows even if the registry is set up to do so.
- If the OS of the PC where JP1/Software Distribution Client (client) is installed is Windows Server 2012, Windows 8, Windows Vista, Windows Server 2008, or Windows 7, processing of commands executed from the service will continue after logging off of Windows regardless of the registry settings.
- To have `dcmpack.exe` (execute packaging) continue processing after logging off of Windows on a PC on which both JP1/Software Distribution Manager and JP1/Software Distribution Client (client) have been installed, set the registry for JP1/Software Distribution Manager. For more information on settings of the registry for JP1/Software Distribution Manager, see *4.6 Registry settings (JP1/Software Distribution Manager)*.
- Operation will vary depending on the combination of registry settings and whether or not the command argument `/LC`. For details, see *4.28 Command operation at logoff that depends on a registry setting and logoff option* in the manual *Administrator's Guide Volume 2*.

7 Setting Up a Relational Database

This chapter describes the system configuration for a JP1/Software Distribution System that uses a relational database and provides notes on building such a system.

7.1 Required programs and system configuration

This section describes the programs and system configuration required in order to use a relational database.

7.1.1 Required programs

If you use Embedded RDB with JP1/Software Distribution, there is no need to provide a separate relational database program.

If you use another relational database with JP1/Software Distribution, the following programs are required:

Relational database server

This is a server program for managing the database. You can use any of the following programs. Note that each of the programs requires an appropriate ODBC driver.

For Microsoft SQL Server

- Microsoft SQL Server 2012 Enterprise
- Microsoft SQL Server 2012 Business Intelligence
- Microsoft SQL Server 2012 Standard
- Microsoft SQL Server 2008 Standard#
- Microsoft SQL Server 2008 Enterprise#
- Microsoft SQL Server 2005 Standard Edition
- Microsoft SQL Server 2005 Standard x64 Edition
- Microsoft SQL Server 2005 Enterprise Edition
- Microsoft SQL Server 2005 Enterprise x64 Edition
- Microsoft SQL Server 2000 Enterprise Edition
- Microsoft SQL Server 2000 Standard Edition
- Microsoft SQL Server 7.0 Enterprise Edition
- Microsoft SQL Server 7.0

#: Corresponds to x64 and x86.

For Oracle

- Oracle9i Release 2 Enterprise Edition R 9.2.0
- Oracle9i Release 2 Standard Edition R 9.2.0
- Oracle9i Enterprise Edition R 9.0.1
- Oracle9i Standard Edition R 9.0.1
- Oracle8i Enterprise Edition R 8.1.7
- Oracle8i Workgroup Server R 8.1.7

To access the database from a computer other than the database server, you must use the client facility.

7.1.2 System configuration

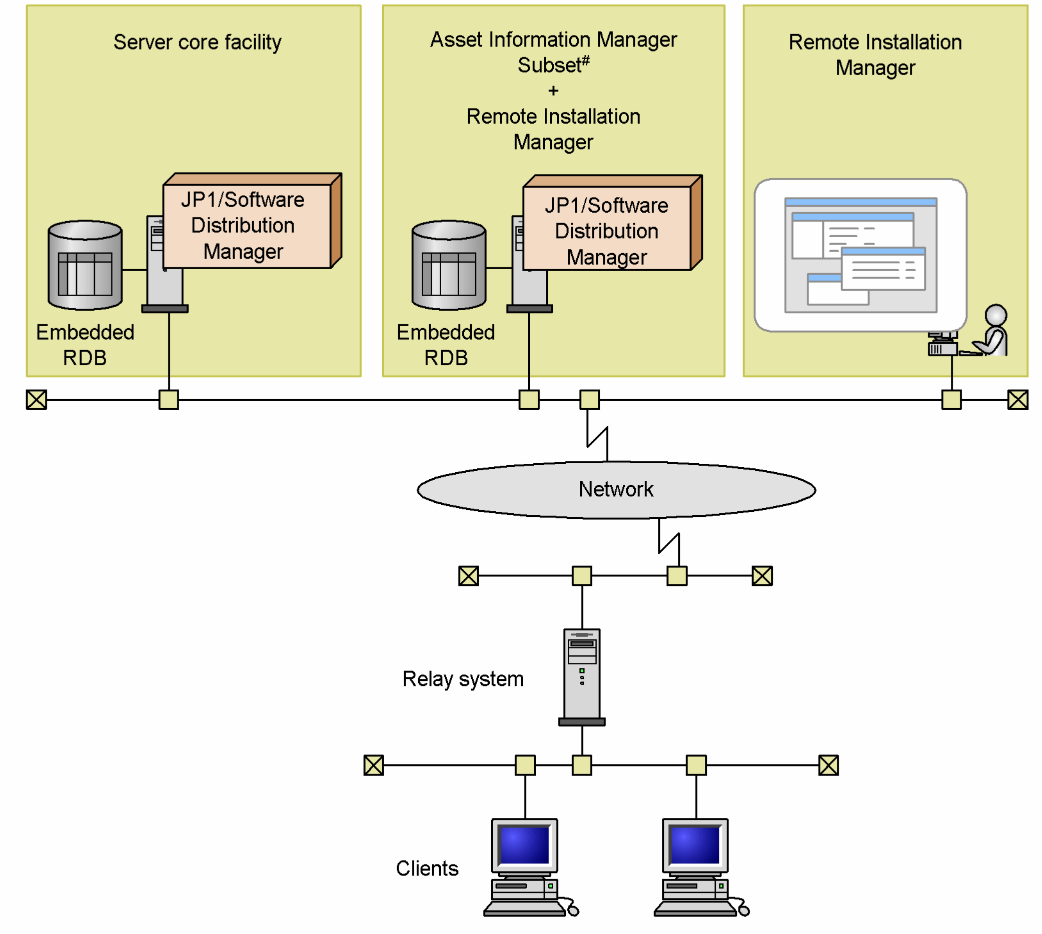
This subsection describes the system configuration required in order to use a relational database.

(1) When Embedded RDB is used

When Embedded RDB is used, the relational database server and JP1/Software Distribution Manager's Server core facility cannot be placed on separate computers. Remote Installation Manager can be placed on a separate computer.

The following figure shows an example of placing Server core facility and Remote Installation Manager on separate computers when Embedded RDB is used:

Figure 7‒1: System configuration using Embedded RDB


Server core facility
JP1/Software Distribution Manager
Embedded RDB
Asset Information Manager Subset#
+
Remote Installation Manager
JP1/Software Distribution Manager
Embedded RDB
Remote Installation Manager
Network
Relay system
Clients

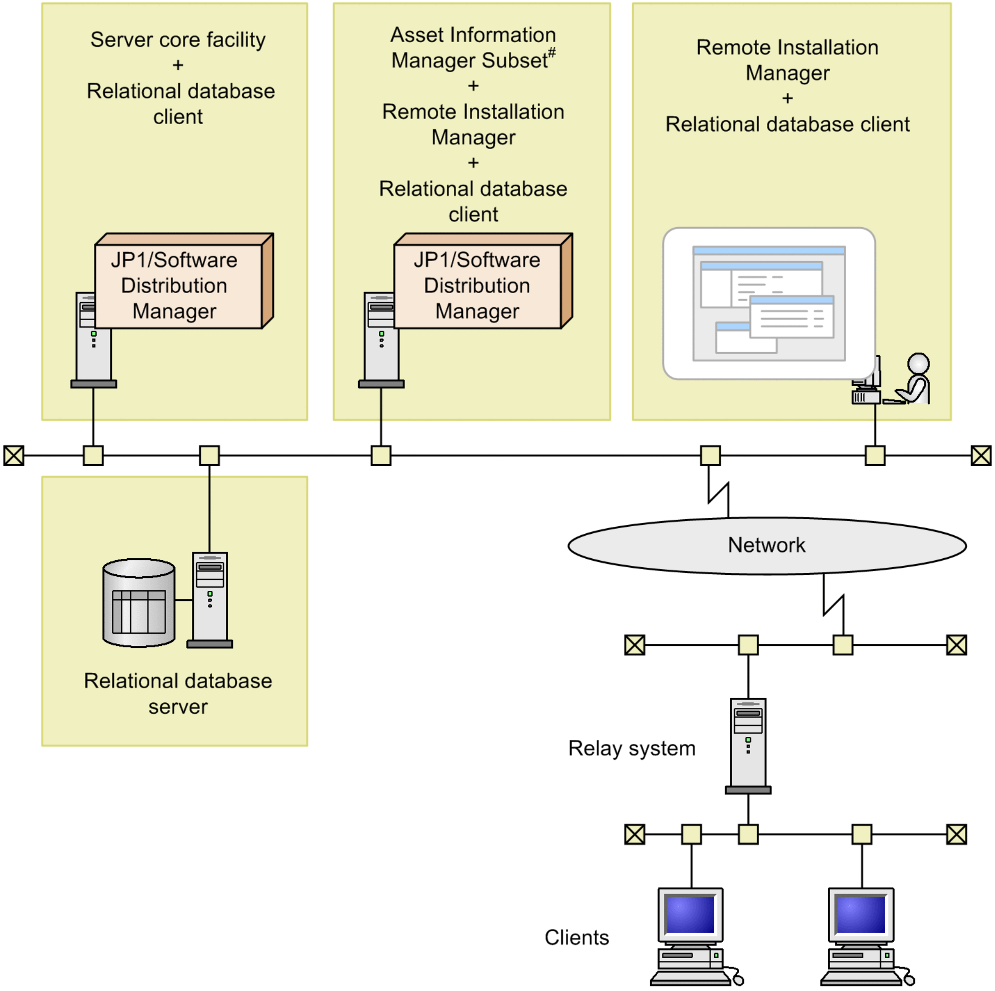
#
Asset Information Manager Subset is one of the components of JP1/Software Distribution.
You can also install it on the same machine as for the Server core facility.

A database program is not required when you use Embedded RDB.

(2) When Microsoft SQL Server or Oracle is used

When Microsoft SQL Server or Oracle is used, JP1/Software Distribution Manager and the database server can be placed on separate computers. The following figure shows an example of placing Server core facility, Remote Installation Manager, and the database server on separate computers:

Figure 7–2: System configuration using Microsoft SQL Server or Oracle


Server core facility
+
Relational database client
JP1/Software Distribution Manager
Asset Information Manager Subset#
+
Remote Installation Manager
+
Relational database client
JP1/Software Distribution Manager
Remote Installation Manager
+
Relational database client
Relational database server
Network
Relay system
Clients

#
Asset Information Manager Subset is one of the components of JP1/Software Distribution.
You can also install it on the same machine as for the Server core facility.

When you use Microsoft SQL Server or Oracle, you must install a database client on the computers on which Server core facility and Remote Installation Manager have been installed.

(a) Relational database server

You can place the Microsoft SQL Server or Oracle relational database server either on the same computer as the managing server or on a separate computer.

If you place the relational database server and the managing server on separate computers, the system will not create a database device when you create a new relational database. In such a case, you must create the database device in the relational database in advance. Alternatively, you can install Database Manager in the host in which the relational database server is running, and then create the relational database.

If your system configuration consists of multiple managing servers, you must create a relational database for each managing server. A relational database cannot be shared among multiple managing servers.

(b) Relational database client

If you install the Microsoft SQL Server or Oracle relational database server and the managing server on separate computers, you must install a relational database client on the computer where the managing server runs.

When the managing server and Remote Installation Manager are on separate hosts, you must also install a relational database client on the computer containing Remote Installation Manager.

7.2 Notes on using a relational database

You should note the following about using a relational database:

- If you are using Embedded RDB as the relational database, there are no tools that access Embedded RDB directly. Do not attempt to access Embedded RDB directly.
- If your relational database is Oracle and you change your account password, you must also change the account and password of the Remote Installer Server service.
- If you set up the server core facility on a machine that has more than one NIC while you are using Embedded RDB as the relational database, choose one of the machine's IP addresses to use for JP1 communication, and then specify that IP address as the client environment variable PDCLTRCVADDR in the files listed below. Back up the HiRDB.ini file before you edit it. Note that if you do not specify an IP address as the client environment variable PDCLTRCVADDR, an IP address on a higher-priority network adapter will be used for JP1 communication.

  JP1/Software-Distribution-installation-directory\Setup_Input\ini\HiRDB.ini

  JP1/Software-Distribution-installation-directory\Setup_Input_HA\ini\HiRDB.ini
- If you install only the remote installation manager facility on a machine with more than one NIC while you are using Embedded RDB as the relational database, choose one of the machine's IP addresses to use for JP1 communication, and then specify that IP address as the client environment variable PDCLTRCVADDR in the file below. Back up the HiRDB.ini file before you edit it. Note that if you do not specify an IP address as the client environment variable PDCLTRCVADDR, an IP address on a higher-priority network adapter will be used for JP1 communication.

  JP1/Software-Distribution-installation-directory\NETMDBCLT\HiRDB.ini
- If you use the remote installation manager facility and the server core facility on different machines, and the machine running the server core facility has more than one NIC, and you are using Embedded RDB as the relational database, then configure the IP addresses to be used for JP1 communication by following these steps:
  1. Stop Remote Installation Manager.
  2. Stop the Remote Install Server service.
  3. Open the command prompt and change the current directory to the following directory.

     JP1/Software-Distribution-installation-directory\BIN
  4. Execute netmdb_stop.bat command that is stored in the directory *JP1/Software-Distribution-installation-directory*\BIN to stop the database.
  5. Use a text editor to open the **pdsys** file that is stored in the directory shown below. Back up the **pdsys** file before you edit it.

     JP1/Software-Distribution--installation-directory\NETMDB\conf
  6. Enter an IP address to be used for the JP1 communication in the following line:

     (xxx.xxx.xxx.xxx:IP address)

     Before:

     pdstart -t SDS -s sds01 -u unt1

     After:

     pdstart -t SDS -s sds01 -u unt1 -m xxx.xxx.xxx.xxx
  7. Save the pdsys file.
  8. Execute the netmdb_start.bat command that is stored in *JP1/Software-Distribution- installation-directory*\BIN to start the database.
  9. Start the Remote Install Server service.
- If a message indicating an error communicating with RDBMS is output to the server's Windows event log (`MAIN.LOG` or `RDBSRV.LOG`), an attempt may have been made to connect to a relational database server after the server had been started but before startup had completed. If the message is output even though you waited a while before trying to connect to the relational database server, collect maintenance data and contact the system administrator. For details about collecting maintenance data, see *6.7 Collecting maintenance data* in the manual *Administrator's Guide Volume 2*.
- When a JP1/Software Distribution GUI operation or command is executed, a message or dialog box may be displayed indicating that a connection could not be made to the server or to the relational database server, or the

GUI operation may be forcibly terminated. In this case, an attempt may have been made to connect to a relational database server after the server had been started but before startup had completed. If the error recurs even though you waited a while before executing GUI operations or commands, collect maintenance data and contact the system administrator. For details about collecting maintenance data, see *6.7 Collecting maintenance data* in the manual *Administrator's Guide Volume 2*.

- Specify a directory on a local drive as the location of the database files and the backup files that are used by Asset Information Manager Subset and the managing server, and of the temporary files and result output files that are used during database maintenance.

7.3 Setting up the relational database environment

This section describes how to set up an environment for the relational database.

7.3.1 Setting up an environment for Embedded RDB

If you use Embedded RDB, you can use the procedure explained below to change the environment settings after operations have begun. It is important that you make a backup of the files used for changing the settings; if settings are wrong, database startup may fail.

(1) Renaming the host after operation has started

Before you can rename the host, you must terminate JP1/Software Distribution and Embedded RDB.

To rename the OS host after operation has started:

1. Terminate Remote Installation Manager.
2. From **Control Panel**, choose **Administrative Tools**, then **Services**, and then stop the **Remote Install Server** service.
3. Terminate the programs that are accessing the JP1/Software Distribution database.
   For example, if JP1/Asset Information Manager is being used to access the JP1/Software Distribution database, stop all JP1/Asset Information Manager services, commands, and tasks.
4. Execute the `netmdb_stop.bat` command, located in the JP1/Software Distribution Manager installation target directory `\BIN`, to stop the database.
5. Use a text editor to open the `pdsys` file that is stored in *JP1/Software-Distribution-installation-directory* `\NETMDB\conf`.
6. Change *host-name-before-change* in `pdunit -x` *host-name-before-change* `-u unt1 -d "`*JP1/Software-Distribution-installation-directory*`\NETMDB"`.[#1, #2]
7. Use a text editor to open the `pdutsys` file that is stored in *JP1/Software-Distribution-installation-directory* `\NETMDB\conf`.
8. If the setting `set pd_hostname =` *host-name-before-change* is specified, make the appropriate change to *host-name-before-change*.[#1, #3]
9. Use a text editor to open the following five files that are stored in *JP1/Software-Distribution-installation-directory* `\NETMDB\conf\emb`:
   - `HiRDB.ini` file
   - `reload.bat` file
   - `reorganization_al.bat` file
   - `reorganization_tb.bat` file
   - `unload.bat` file
10. Change *host-name-before-change* in `PDHOST=`*host-name-before-change*.[#2]
11. Rename the OS host.
12. Restart the OS.

#1

The maximum length of a single definition line is 80 characters. If a definition exceeds 80 characters, divide it into multiple lines, and specify the continuation symbol \ at the end of each line being continued.

Example:

```
pdunit -x jp1sdmanager.domain -u unt1 \
-d "C:\Program Files\Hitachi\NETMDM\NETMDB"
```

#2

To use the failover function of JP1/Software Distribution in a cluster system environment, specify the logical host name.

#3

To use the failover function of JP1/Software Distribution in a cluster system environment, specify the physical host name.

Note

The following notes apply when hosts are renamed after operations have begun:

- For details about how to specify host names, see *8.1.2 Assigning host names in a JP1/Software Distribution system*.
- If any of the following types of jobs exist, delete such jobs, make sure that the jobs have been deleted, and then rename the host:
  - Job whose execution status is anything other than normal termination or error
  - *Send package, allow client to choose* job
  - Jobs that acquire inventory information periodically

  If you rename the host without deleting such jobs, currently executing jobs may stop or deletion of lower systems' jobs may become impossible.

(2) Suppressing message output to the event log

This subsection describes how to suppress output of unneeded messages from the messages that are output to the event log by Embedded RDB. For details about the Embedded RDB messages, see the manual *HiRDB Version 8 Messages*.

Before you set suppression of message output, terminate JP1/Software Distribution and Embedded RDB.

Suppress only information messages (messages with an ID that ends with `I`). It may become difficult to resolve errors if you suppress output of warning or error messages (messages with an ID that ends with `W` or `E`).

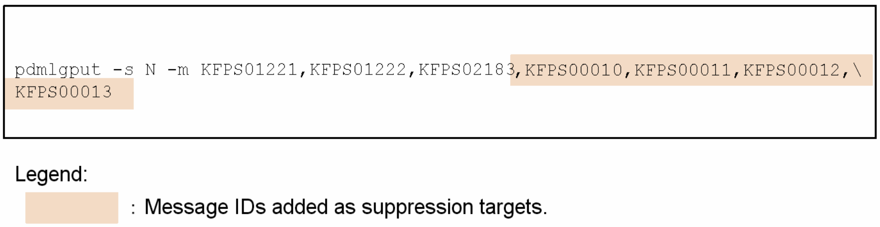
To suppress message output to the event log:

1. Terminate the Remote Installation Manager.
2. Open the **Control Panel** and choose **Administrative Tools**, then **Services** to stop the **Remote Install Server** service.
3. Terminate the product that is accessing the JP1/Software Distribution database.

   For example, if JP1/Asset Information Manager is accessing the JP1/Software Distribution database, stop all the services, commands, and tasks of JP1/Asset Information Manager.
4. Execute the `netmdb_stop.bat` command, located in the JP1/Software Distribution Manager installation target directory `\BIN`, to stop the database.
5. Use a text editor to open the `pdsys` file that is stored in *JP1/Software-Distribution-installation-directory* `\NETMDB\conf`.
6. Add to the line `pdmlgput -s N -m` *message-ID*`,`*message-ID*`,`*message-ID* the IDs of the messages whose output is to be suppressed.

   Do not include in *message-ID* the message severity code that follows the hyphen (`-`). To specify multiple message IDs, use a comma to separate the IDs. If the specification exceeds 80 columns, enter \ at the end of the line to be continued to set a linefeed.

   The following example adds message IDs to the existing settings in order to suppress output of the KFPS00010-I, KFPS00011-I, KFSP00012-I, and KFSP00013-I messages:



```
pdmlgput -s N -m KFPS01221,KFPS01222,KFPS02183,KFPS00010,KFPS00011,KFPS00012,\
KFPS00013
```

Legend:

▨ : Message IDs added as suppression targets.

7. Execute the `netmdb_start.bat` command, located in the JP1/Software Distribution Manager installation target directory `\BIN`, to start the database.
8. Open the **Control Panel** and choose **Administrative Tools**, then **Services** to start the **Remote Install Server** service.

(3) Setting an execution timeout for a command to manipulate the database

While you are executing one of the following commands to manipulate the database, if an error (such as a communication error or disk error) occurs, the command might not respond.

- Reorganizing the database (netmdb_reorganization.bat command)
- Backing up the database (netmdb_unload.bat command)
- Releasing the area for operation logs that were deleted (netmdb_reclaim.bat command)

If you cannot forcibly terminate a command that does not respond because, for example, the command was executed automatically by the Windows task feature or by JP1/AJS, perform the following steps to set an execution timeout for the command.

Terminate JP1/Software Distribution and Embedded RDB before you set the execution timeout.

1. Stop Remote Installation Manager.
2. Stop the Remote Install Server service through the **Service** of **Administrative Tools** of **Control Panel**.
3. Stop all the programs that are accessing the database of JP1/Software Distribution.

   For example, when JP1/Asset Information Manager is accessing the database of JP1/Software Distribution, stop all the commands and tasks for JP1/Asset Information Manager.
4. Execute the netmdb_stop.bat command that is stored in *JP1/Software-Distribution-Manager-installation-directory* `\BIN` to stop the database.
5. Use a text editor to open the `pdsys` file that is stored in *JP1/Software-Distribution-installation-directory* `\NETMDB\conf`.
6. Add a line for set pd_utl_exec_time = command execution timeout in the `pdsys` file. #1
7. Execute the netmdb_start.bat command that is stored in *JP1/Software-Distribution-Manager-installation-directory*`\BIN` to start the database.
8. Start the Remote Install Server service through the **Service** of **Administrative Tools** of **Control Panel**.

#1

pd_utl_exec_time = command execution timeout

Specify a command execution timeout in the range from 0 to 35791394 (minutes) for the following commands that manipulate the database. If you do not specify a value, or specify 0, the command execution timeout will not be set.

- Upgrading the database
- Reorganizing the database (netmdb_reorganization.bat command)
- Backing up the database (netmdb_unload.bat command)
- Restoring the database (netmdb_reload.bat command)
- Releasing the area for operation logs that were deleted (netmdb_reclaim.bat command)

If the command does not complete after the time specified for the execution timeout has elapsed, the command being executed will be abnormally terminated.

For this operand, specify a value that allows for some extra time compared to the actual time that the command requires for execution.

For example, if upgrading the database requires a maximum of approximately 90 minutes, and reorganizing the database requires a maximum of approximately 60 minutes, specify `pd_utl_exec_time=120` for the timeout, just in case. This is because if a process that normally finishes in 90 minutes has not responded after 120 minutes, we can assume that an error causing the command not to respond has occurred. Also, we recommend that you specify `0` for the execution timeout when you execute the following commands:

- Upgrading the database

- Restoring the database (netmdb_reload.bat command)

Sample

```
#
#-------------------------------------------------------------------
# set form
#
:

:
set pd_utl_exec_time = 120
#
#-------------------------------------------------------------------
# putenv form
#
```

7.3.2 Setting up an environment for Microsoft SQL Server

To design a Microsoft SQL Server relational database, you must configure the following settings:

- Collation settings
- Setting the network protocol
- Tuning the database environment
- Setting the memory allocation
- Tuning the environment setting options
- Setting the authentication mode
- Setting the relational database access permissions
- Setting the transaction log

You should use the data compression function of Microsoft SQL Server 2012 Enterprise or Microsoft SQL Server 2008 Enterprise in the following cases only:

- When data storage has been completed on the client or the relay manager, and data I/O operations are stable
- When `netmdm_inspackage` is used

The following describes these settings.

(1) Collation settings

When you install Microsoft SQL Server as the relational database, select **Binary** for **Sort Order** on the server. If you do not select **Binary** or **Case-sensitive** for **Sort Order**, even when you select the **Match case** check box in the Find dialog box displayed in the Destination window, the **Match case** setting is not enabled. Also, the count-clients facility of Inventory Viewer and the output range setting facility of the CSV output utility will not distinguish between uppercase letters and lowercase letters.

After you have created the database for JP1/Software Distribution, do not change the database sorting order. If you change the database sorting order and any discrepancy with the sorting order of the relational database server occurs, the system is not guaranteed to run correctly.

(2) Setting the network protocol

To use a relational database, you must set up the network protocol in both the relational database server and the clients. This subsection describes the settings for each relational database program.

- Settings in the relational database server

  Select the protocols that the relational database server can use to connect to the managing server and Remote Installation Manager. Normally, you would use **TCP/IP Sockets** or **Named Pipes**.
- Settings in the relational database client

  In the relational database client, set the same protocols you selected in the server.

For details about how to set the network protocols, see the Microsoft SQL Server documentation.

Be sure to copy down the protocol and server names that you set here, because you will need them when you create the relational database.

(3) Tuning the database environment

You do not have to set the items, because Microsoft SQL Server 2012, Microsoft SQL Server 2008, Microsoft SQL Server 2005, Microsoft SQL Server 2000, and Microsoft SQL Server 7.0 have a function that tunes the operating environment automatically. However, you can change the database server settings as necessary.

To change the setting for the number of locks, use Transact-SQL. To change the settings for the number of connected users and the maximum memory size that can be used, go to the **Connections** and **Memory** pages of the SQL Server Properties dialog box. You can also allocate a fixed memory size.

(4) Setting the memory allocation

Memory allocation for Microsoft SQL Server is important in order to use JP1/Software Distribution efficiently to perform remote installation. The following explains how to estimate the memory allocation in Microsoft SQL Server.

(a) Data cache

The data cache consists of the index page and data page of each table. The following shows the calculations for estimating the memory allocation for the index page and data page of a frequently-accessed table. It is recommended that you allocate memory for 100% of the index page and at least 20% of the data page. If there is sufficient memory, allocate memory for 100% of the data page. The number of packages includes the number of already-distributed packages and the number of packages to be distributed.

Index page

Number of managed clients **x** number of packages **x** 0.0005 (megabytes)

Data page

Number of managed clients **x** number of packages **x** 0.0045 (megabytes)

(b) Procedure cache

The procedure cache consists of Microsoft SQL Server's execution plans, etc. When you use JP1/Software Distribution, allocate about five megabytes of memory to the procedure cache.

(5) Tuning the environment setting options

Microsoft SQL Server 2012, Microsoft SQL Server 2008, Microsoft SQL Server 2005, Microsoft SQL Server 2000, and Microsoft SQL Server 7.0 adjust the memory allocations dynamically in order to optimize their performance. Normally, the system administrator does not need to set memory allocations. However, the system administrator should set maximum and minimum values, taking into account the overhead due to automatic adjustment of memory allocations.

Minimum value

At least 16 megabytes

Maximum value

Total amount of memory - (amount of memory used by the operating system + amount of memory used by JP1/Software Distribution[#] + amount of memory used by other applications + 5 megabytes)

#: See *5.3.2 Memory requirements* in the *Description and Planning Guide*.

(6) Setting the authentication mode

Select **SQL Server and Windows** as the authentication mode. You can set the authentication mode in **Security** on the **Security** page of the SQL Server Properties dialog box.

(7) Setting access permissions in the relational database

If the ID key for relational database access that you set in JP1/Software Distribution Manager is not the system administrator ID of Microsoft SQL Server, you must set access permissions for each table in the relational database. The required access permissions are `SELECT`, `INSERT`, `UPDATE`, and `DELETE`.

To set access permissions:

For Microsoft SQL Server 2012, Microsoft SQL Server 2008 and Microsoft SQL Server 2005

If you create new ID:

1. In the **Object Explorer of Microsoft SQL Server Management Studio,** select *database name***, Security,** and then **Logins.** Right-click on **Logins,** and select **New Login**.
2. In the Login - New dialog box, set a login name and authentication:

   From the **Select a page** pane of the Login - New dialog box, select the **General** page, and set a login name and authentication. If you select **SQL Server authentication,** you need to set **Password** and **Confirm password.** If you select the check box **User must change password at next login,** do the step **5.** below to change the password.
3. In the Login - New dialog box, specify the users mapped to the login and the database role membership:

   From the **Select a page** pane of the Login - New dialog box, select the **User Mapping** page.

   For **Users mapped to this login,** select the created database name. For **Database role membership for** *database name***,** select the following check boxes:
   - `db_datareader`
   - `db_datawriter`
   - `db_ddladmin`
4. Click **OK** in the Login - New dialog box.
5. Log on to the server with the created new ID. If you set **User must change password at next login** in the step **2.** , the Change Password dialog box appears. In the Change Password dialog box, change the password.

If you use the existing ID:

1. In the **Object Explorer** of **Microsoft SQL Server Management Studio,** select

   *database name***, Security**, and then **Logins**. Select ID for which you will be setting access permissions. Right-click on the selected ID and select **Properties.**
2. In the Login Properties - (selected *ID name*) dialog box, and specify

   the users mapped to the login and the database role membership. From the **Select a page** pane of the Login Properties - (selected *ID name*) dialog box, select the **User Mapping**. For **Users mapped to this login**, select the check box for the created database name. For **Database role membership for** *database name***,** select the following check boxes:

   - `db_datareader`

   - `db_datawriter`

   - `db_ddladmin`
3. Click **OK** in the Login Properties - (selected *ID name*) dialog box.

For Microsoft SQL Server 2000 and Microsoft SQL Server 7.0

If you create new ID:

1. In **SQL Server Enterprise Manager**, select *database name***, Security** and then

   Logins. Right-click on **Logins**, and select **New Login**.
2. In the SQL Server Login Properties - New Login dialog box,, set a login name and authentication:

   On the **General** page of the SQL Server Login Properties - New Login dialog box, set a login name and authentication. If you select **SQL Server authentication**, you need to set **Password**.
3. In the SQL Server Login Properties - New Login dialog box, specify database that can be accessed by the login, and the database roles:

   Select the **Database Access** page in the SQL Server Login Properties - New Login dialog box.

   For **Specify which databases can be accessed by this login**, select the check box for the created database name. For **Database roles for** *database name*, select the following check boxes:

- `db_datareader`
- `db_datawriter`
- `db_ddladmin`

4. Click **OK** in the SQL Server Login Properties - New Login dialog box. If you set **Password** in the step **2.** , the Confirm Password dialog box appears. In the dialog box, enter the password again.

If you use the existing ID:

1. In SQL Server Enterprise Manager, select *database name***, Security** and then

   Logins. Select ID for which you will be setting access permissions. Right-click on the selected ID and select **Properties**.
2. In the SQL Server Login Properties - (selected *ID name*) dialog box, specify database that can be accessed by this login and the database roles:

   Select the **Database Access** page in the SQL Server Login Properties - (selected *ID name*) dialog box.

   For **Specify which databases can be accessed by this login**, select the check box for the created database name. For **Database roles for** *database name*, select the following check boxes:

   - `db_datareader`
   - `db_datawriter`
   - `db_ddladmin`
3. Click **OK** in the SQL Server Login Properties - (selected *ID name*) dialog box.

(8) Setting the transaction log

Microsoft SQL Server collects a history of accesses for relational database updating in a *transaction log*. Although JP1/Software Distribution Manager allocates a transaction log when the relational database is created, users cannot gain access to the relational database if the transaction log becomes full. If you set the file size of the transaction log to increase automatically, the log will reach a maximum size of 2 TB, which will decrease the response speed of the disk due to decreased disk availability.

We recommend you that you set up the transaction log so that it is deleted automatically.

For Microsoft SQL Server 2012, Microsoft SQL Server 2008 and Microsoft SQL Server 2005

1. Start Management Studio.
2. Select the target database, and then open the Database Properties dialog box.
3. Choose the **Options** menu.
4. From **Recovery model** in the left-hand frame of the dialog box, select **Simple**.

For Microsoft SQL Server 2000

1. Start Enterprise Manager.
2. Select the target database and then open the Properties dialog box.
3. On the **Options** page, from **Model**, select **Simple**.

For Microsoft SQL Server 7.0

1. In the SQL Enterprise Manager window, right-click on the target database to open a pop-up menu, and then choose **Properties**.
2. In the *XXXXX* Properties dialog box (*XXXXX* is the database name), on the **Options** page, select the **Truncate log on checkpoint** check box.

If the transaction log file becomes full while the **Truncate log on checkpoint** check box is not selected, JP1/Software Distribution Manager outputs a message to `RDBSRV.LOG` that indicates no object area can be allocated in the segment. If this message is output, use the following procedure to discard the transaction log:

For Microsoft SQL Server 2012, Microsoft SQL Server 2008 and Microsoft SQL Server 2005

In Management Studio, from the menu that is displayed by right-clicking the database, choose **Tasks**, and then **Back Up** to display the Back Up Database dialog box. From the **General** tab of this dialog box, make a backup of the transaction log information. As much transaction log information as is backed up will be discarded.

For Microsoft SQL Server 2000

Use the **Backup Database** menu of Enterprise Manager to make a backup of the transaction log. The data you back up will be deleted from the log.

For Microsoft SQL Server 7.0

Use the **Truncate Log** menu of Enterprise Manager to truncate the transaction log. Alternatively, use Query Analyzer to specify a `DUMP` statement (`DUMP TRANSACTION` *database-name* `WITH NO_LOG`) and delete the transaction log.

7.3.3 Setting up an environment for Oracle

To design an Oracle relational database, you must configure the following settings:

- Creating a database instance and services
- Tuning the initialization parameter file
- Setting the relational database access permissions

If you use Asset Information Manager Subset, you must set up an environment for the Asset Information Manager Subset relational database.

The following describes these settings.

(1) Creating a database instance and services

To use a relational database, you must create a database instance at the relational database server and create services at the relational database client. For details about how to create these items, see the documentation for the Oracle database you are using.

(a) Settings in the relational database server

Create a database instance at the relational database server. To do this, use Oracle Database Configuration Assistant.

(b) Settings in the relational database client

Create services at the relational database client. To do this, use one of the following programs:

For Oracle8i

Oracle Net8 Assistant

For Oracle9i

Oracle Net Manager

Specify each service name in the following format:

`NETM_`*connection-destination-server-name*

The connection destination server means the PC where the JP1/Software Distribution Manager server is installed. Note that the connection destination server name must not include the DNS name.

Example

When the connection destination server name is `dmp380.Hitachi.co.us`, the service name is:

`NETM_dmp380`

If an IP address, not a host name, is specified as the Software Distribution server for the connection destination specified in the Software Distribution Logon dialog box of Remote Installation Manager, you must also specify the IP address in *connection-destination-server-name*. When you specify the IP address, replace dots (`.`) with underscores (_).

Example

When the connection destination server name is `172.18.22.31`, the server name becomes:

`NETM_172_18_22_31`

(2) Tuning the initialization parameter file

The following shows the parameters that require tuning and describes how to tune them.

(a) Parameters requiring tuning

`db_block_buffers`

This parameter specifies the number of database blocks. The value of this parameter controls the size of the data cache. The size of the data cache actually allocated is `db_block_size` **x** `db_block_buffers`.

`shared_pool_size`

This parameter specifies the size of the shared pool in bytes. The shared pool stores Oracle's management information (such as the library cache for SQL code analysis results and the dictionary cache).

`processes`

This parameter specifies the maximum number of users that can be connected at one time. The following shows the formula for determining the maximum number of simultaneous user connections required by JP1/Software Distribution:

Number of concurrent connections
= 25
+ number of concurrent Remote Installation Manager connections **x** 5
+ number of concurrent Packager connections **x** 2
+ number of concurrent client or relay system connections **x** 2
+ number of concurrent connections from HP NNM **x** 5

(b) Tuning method

`db_block_buffers`

This parameter indicates an estimated value for allocation. While the database is active, execute the following SQL code to acquire the hit rate of the data cache. If the hit rate is 90% or lower, increase the number of buffers.

SQL code for acquiring the hit rate of the data cache:

```
Select (a.value + b.value) "Log_Reads", c.value "Rhy_Reads",
Round(((1 - (c.value / (a.value + b.value))) * 100), 3) "Buffer Hit
Ratio"
from v$sysstat a,v$sysstat b,v$sysstat c
where a.name = 'db block gets' and b.name = 'consistent gets'
and c.name = 'physical reads';
```

`shared_pool_size`

In this parameter, specify about 32 megabytes. While the database is active, execute the following SQL code to acquire the hit rates of the library cache and dictionary cache. If the hit rates are 90% or lower, increase the allocation size.

SQL code for acquiring the hit rate of the library cache:

```
Select sum(pins) "Executions", sum(reloads) "Misses",
Round(100*(1-sum(reloads)/sum(pins)),3) "Hit Ratio" from v$librarycache;
```

SQL code for acquiring the hit rate of the dictionary cache:

```
Select sum(gets) "Gets", sum(getmisses) "Misses",
Round(100*(1-sum(getmisses)/sum(gets)),3) "Hit Ratio"
from v$rowcache where gets <> 0;
```

`processes`

In this parameter, specify the maximum number of users that can be connected at one time.

(3) Setting access permissions in the relational database

To use the relational database, you must set access permissions. This subsection describes how to set access permissions.

To create a user after creating a database:

1. Grant CONNECT, EXP_FULL_DATABASE, IMP_FULL_DATABASE, and RESOURCE as role permissions.
2. Grant all permissions to all tables of JP1/Software Distribution as object permissions.
   Example: When creating a database with the SYSTEM permission and creating NETM_USER01:
   ```
   GRANT ALL ON "SYSTEM"."NETMDM_CABINET" TO "NETM_USER01"
   ```
3. Create a synonym to allow users to view all tables of JP1/Software Distribution.
   Example: When creating a database with the SYSTEM permission and creating NETM_USER01:
   ```
   CREATE SYNONYM "NETM_USER01"."NETMDM_CABINET" FOR
   "SYSTEM"."NETMDM_CABINET"
   ```

7.4 How to use Database Manager (for Embedded RDB)

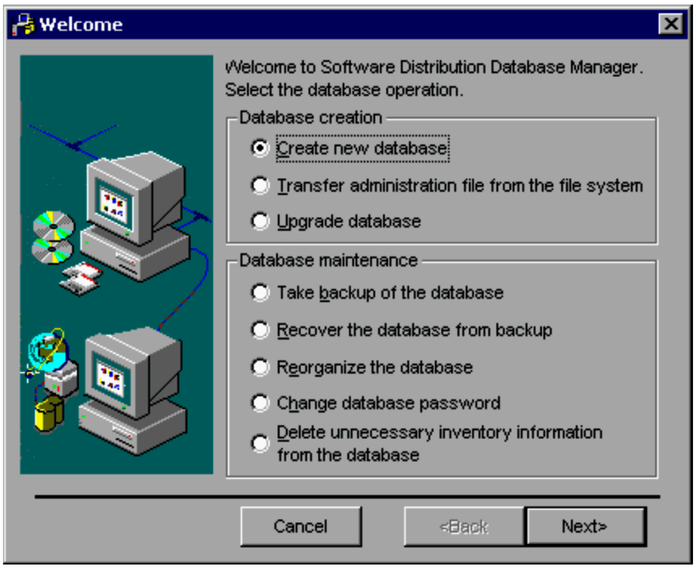
You use *Database Manager*, one of the components of JP1/Software Distribution, to create or maintain a relational database to be used by JP1/Software Distribution. To start Database Manager, from the menu, choose **Software Distribution Manager**, and then **Database Manager**.

You should note the following about using Database Manager:

- First, you must exit all applications that use JP1/Software Distribution's relational database.
- Before starting Database Manager, stop Remote Install Server by opening **Control Panel**, choosing **Administrative Tools**, and then **Services**.
- Only users who have Administrator permissions can use Database Manager.

When Database Manager starts, the Welcome dialog box is displayed, enabling you to select a Database Manager operation.

Figure 7–3: Welcome dialog box



Welcome

Welcome to Software Distribution Database Manager.
Select the database operation.

Database creation

● Create new database

○ Transfer administration file from the file system

○ Upgrade database

Database maintenance

○ Take backup of the database

○ Recover the database from backup

○ Reorganize the database

○ Change database password

○ Delete unnecessary inventory information from the database

If you are using Microsoft SQL Server or Oracle, different items are displayed in the Welcome dialog box. For details about how to use Database Manager when Microsoft SQL Server or Oracle is used, see *7.5 How to use Database Manager (for Microsoft SQL Server or Oracle)*.

Select the operation you want to perform with Database Manager.

Create new database

Creates a new relational database. After installing JP1/Software Distribution Manager, you must select this item to create a new database.

Transfer administration file from the file system

Migrates the basic database of JP1/Software Distribution JP1 Version 7i or earlier to a relational database (Embedded RDB). To select this option, a relational database must have been created previously.

Upgrade database

Upgrades the relational database. Select this option if you have upgraded your JP1/Software Distribution or migrated JP1/Software Distribution Manager Embedded RDB Edition JP1 Version 7i to JP1/Software Distribution Manager JP1 Version 8.

Select this option also when you wish to change the size of an existing database area.

Take backup of the database

Backs up a database. Select this item when you perform periodic database backup.

Recover the database from backup

Restores a database from its backup file. Select this item to restore the backup that is obtained using the **Take backup of the database** menu.

Reorganize the database

When a database's usage factor exceeds 80%, you should reorganize the database. You can determine whether or not the database usage factor has exceeded 80% by checking the messages in the event log. For details about the messages that are displayed, see *7.4.6 Reorganizing the database*.

Change database password

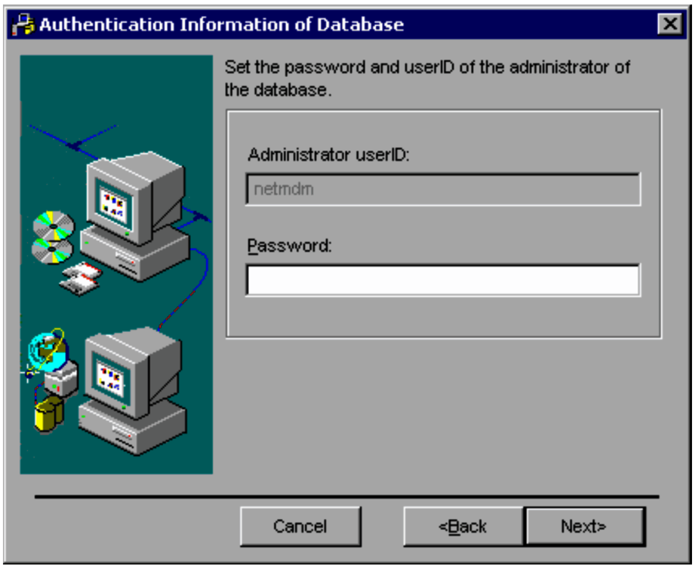
Changes the password needed in order to log on to the database.

Delete unnecessary inventory information from the database

Deletes unneeded inventory information from the database in order to increase available database space.

Selecting a desired operation and then clicking the **Next** button displays the Authentication Information of Database dialog box.

Figure 7–4: Authentication Information of Database dialog box



Authentication Information of Database

Set the password and userID of the administrator of the database.

Administrator userID: netmdm

Password:

Enter the password for logging into the database. User authentication is required in order to manipulate a database from Database Manager.

The following subsections describe each operation after user authentication.

7.4.1 Creating a new database

After installing new JP1/Software Distribution Manager, you must create a database.

This subsection describes how to create a new database and provides guidelines for the number of data items that can be expected based on the scale of your operations.

(1) How to create a database

This subsection describes how to create a new Embedded RDB database.

You must specify for the path to the database area a directory that actually exists. You can use alphanumeric characters, the space, and the following symbols:

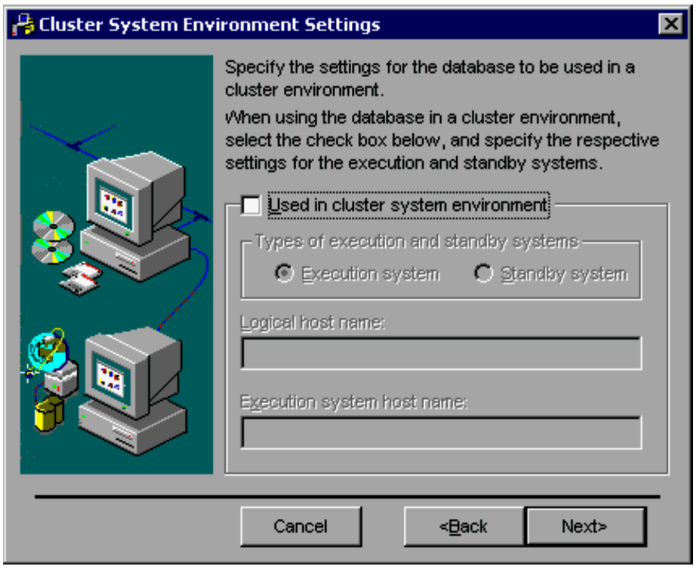
`: . \ # @ ( )`

1. In the Welcome dialog box, select **Create new database**, and then click the **Next** button.
   The Authentication Information of Database dialog box appears.

2. In the Authentication Information of Database dialog box, specify the password and then click the **Next** button.

   The Cluster System Environment Settings dialog box appears.

   Figure 7–5: Cluster System Environment Settings dialog box

   Cluster System Environment Settings

   Specify the settings for the database to be used in a cluster environment.

   When using the database in a cluster environment, select the check box below, and specify the respective settings for the execution and standby systems.

   □ Used in cluster system environment

   Types of execution and standby systems

   ● Execution system ○ Standby system

   Logical host name:

   Execution system host name:

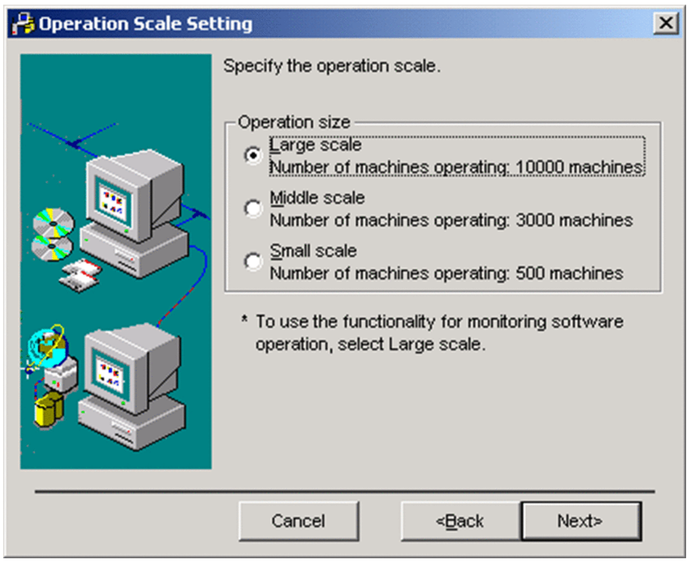
   If you are using JP1/Software Distribution Manager in a cluster system environment, select the **Used in cluster system environment** check box. For details about the settings for using JP1/Software Distribution Manager in a cluster environment, see *11.1 Constructing a JP1/Software Distribution Cluster System*.

   This section describes the procedure for creating a database that is to be used by JP1/Software Distribution Manager in a normal network environment.

3. Click the **Next** button.

   The Operation Scale Setting dialog box appears.

   Figure 7–6: Operation Scale Setting dialog box

   Operation Scale Setting

   Specify the operation scale.

   Operation size

   ● Large scale
   Number of machines operating: 10000 machines

   ○ Middle scale
   Number of machines operating: 3000 machines

   ○ Small scale
   Number of machines operating: 500 machines

   * To use the functionality for monitoring software operation, select Large scale.

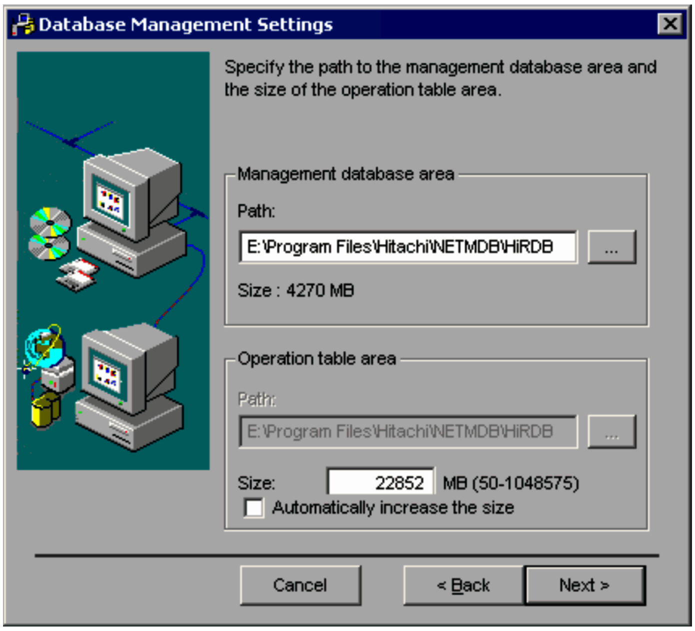
   Select a scale of operations appropriate to the environment in which JP1/Software Distribution Manager is used. The default settings for database area sizes are set in accordance with the selected scale of operations. Note that the sizes of database areas can be changed in the dialog box that follows.

   It is recommended that you select **Large scale** unless otherwise necessary. If you monitor the operation status of clients, it is important that you select **Large scale**. For guidelines for the number of data items that are expected based on the scale of operations, see *(2) Guidelines for the amount of data based on the scale of operations*.

4. Click the **Next** button.

The Database Management Settings dialog box appears.

Figure 7–7: Database Management Settings dialog box



Database Management Settings

Specify the path to the management database area and the size of the operation table area.

Management database area

Path: E:\Program Files\Hitachi\NETMDB\HiRDB

Size : 4270 MB

Operation table area

Path: E:\Program Files\Hitachi\NETMDB\HiRDB

Size: 22852 MB (50-1048575)

□ Automatically increase the size

Management database area

Specifies the directory path where the database and work table area for JP1/Software Distribution Manager are to be stored, as 1 to 46 characters.

If JP1/Software Distribution Manager is to be used in a cluster system environment, specify the path to the shared disk that stores files in the management database area other than work table area (data that needs to be inherited in the event of failover).

The size of the management database area is fixed at 4,270 megabytes. To specify a size for work table space, use the **Size** field in **Operation table area**.

Operation table area

Specifies the size of the operation table area in the range from 50 to1,048,575 megabytes.

The default size for the operation table area depends on the scale of operations selected in the Operation Scale Setting dialog box. The following table lists the default sizes:

Selected scale of operation	Default size for operation table area (megabytes)
Large scale	22,852
Middle scale	6,855
Small scale	1,142

Note that the **Path** field is enabled when the database is used in a cluster system environment. Specify the path to the local disk that stores files in the work table area (data that need not be inherited in the event of failover), as 1 to 46 characters.

Automatically increase the size

Selecting this check box specifies that when the amount of work table area needed exceeds the value entered in the **Size** field, the size of the work table area is to be increased automatically.

You should select this check box if the size of the work table area may exceed the specified value because of the type of operations to be performed. The default is that this check box is selected.

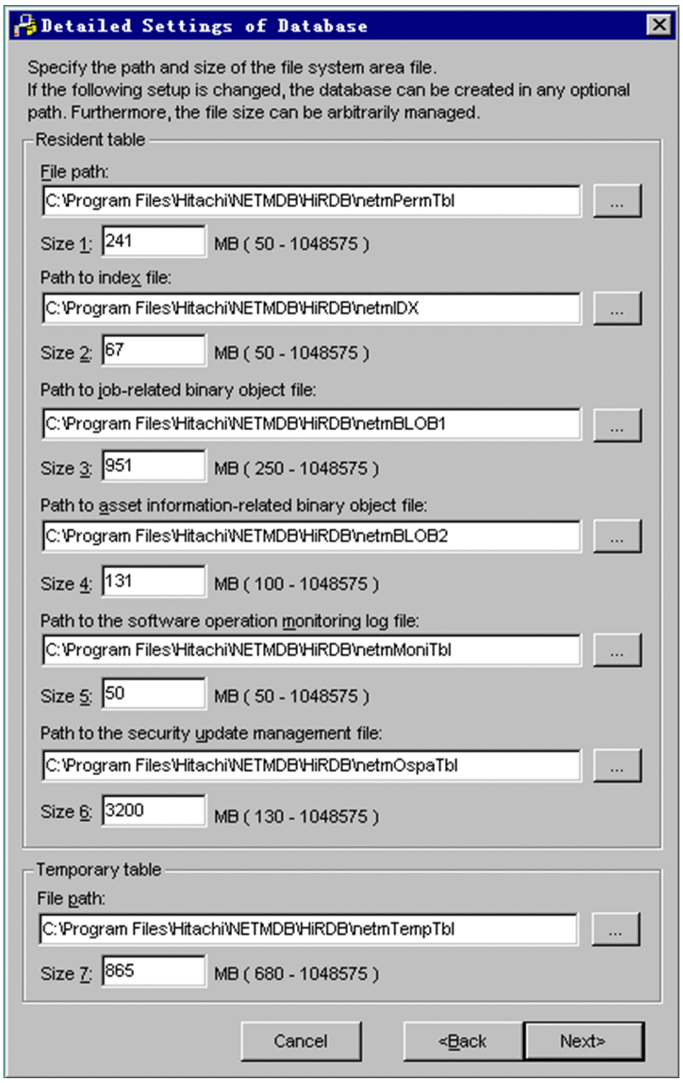
The work table area can be expanded to a maximum of 1,048,575 megabytes (assuming there is sufficient space available on the disk).

In a cluster system environment, the **Automatically increase the size** check box setting should be the same in both the executing system and the standby system.

5. Specify necessary information in the Database Management Settings dialog box and then click the **Next** button.

The Detailed Settings of Database dialog box appears.

Figure 7–8: Detailed Settings of Database dialog box



Detailed Settings of Database

Specify the path and size of the file system area file.
If the following setup is changed, the database can be created in any optional path. Furthermore, the file size can be arbitrarily managed.

Resident table

File path:
C:\Program Files\Hitachi\NETMDB\HiRDB\netmPermTbl

Size 1: 241 MB (50 - 1048575)

Path to index file:
C:\Program Files\Hitachi\NETMDB\HiRDB\netmIDX

Size 2: 67 MB (50 - 1048575)

Path to job-related binary object file:
C:\Program Files\Hitachi\NETMDB\HiRDB\netmBLOB1

Size 3: 951 MB (250 - 1048575)

Path to asset information-related binary object file:
C:\Program Files\Hitachi\NETMDB\HiRDB\netmBLOB2

Size 4: 131 MB (100 - 1048575)

Path to the software operation monitoring log file:
C:\Program Files\Hitachi\NETMDB\HiRDB\netmMoniTbl

Size 5: 50 MB (50 - 1048575)

Path to the security update management file:
C:\Program Files\Hitachi\NETMDB\HiRDB\netmOspaTbl

Size 6: 3200 MB (130 - 1048575)

Temporary table

File path:
C:\Program Files\Hitachi\NETMDB\HiRDB\netmTempTbl

Size 7: 865 MB (680 - 1048575)

In this dialog box, you can specify the paths and sizes of the database area files.

Specify the path to a database area file as 1 to 104 characters. Note that if the OS being used is a 64-bit version of Windows Server 2012, Windows Server 2008 or Windows Server 2003 (x64), a path under the `%Systemroot%\system32` directory can be specified.

The default database area file sizes depend on the scale of operations selected in the Operation Scale Setting dialog box. The following table lists the default, minimum, and maximum sizes depending on the selected scale of operations.

Table 7–1: Default, minimum, and maximum database area file sizes depending on the scale of operations

Database area file	Default size (megabytes)			Minimum size (megabytes)	Maximum size (megabytes)
	Large	Medium	Small		
Resident table file	5,060	1,455	241	50	1,048,575
Index file	22,870	404	67	50	1,048,575
Job-related binary object file	13,420	4,232	951	250	1,048,575
Asset information-related binary object file	131	131	131	100	1,048,575
Software operation monitoring log file	43,454	50	50	50	1,048,575

Database area file	Default size (megabytes)			Minimum size (megabytes)	Maximum size (megabytes)
	Large	Medium	Small		
Security update management file	3,200	3,200	3,200	130	1,048,575
Temporary table file	17,438	1,795	865	680	1,048,575

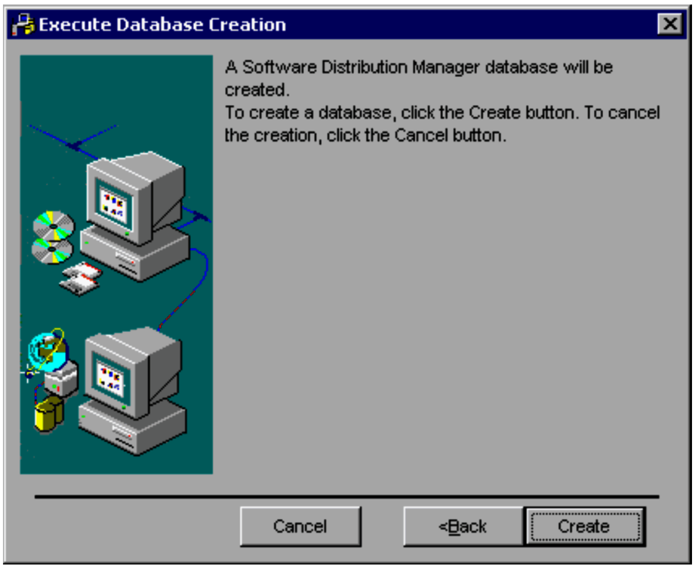
For details about how to determine the size of each database area file, see *5.4 Estimating disk space requirements for the database* in the *Description and Planning Guide*.

If the Operation Log List window is not used with the software operation monitoring facility, it is advisable to specify a small size because the software operation monitoring log file is not used. For example, specify a value of 50 megabytes (minimum value).

6. Specify necessary information in the Detailed Settings of Database dialog box and then click the **Next** button.

   The Execute Database Creation dialog box appears.

   Figure 7–9: Execute Database Creation dialog box



A Software Distribution Manager database will be created.
To create a database, click the Create button. To cancel the creation, click the Cancel button.

7. Click the **Create** button.

   The database is created.

(2) Guidelines for the amount of data based on the scale of operations

The following table provides guidelines for the number of data items that can be expected for each scale of operations, as selected in the Operation Scale Setting dialog box. The default values for the database area files that are set in the database manager are determined from the number of data items shown below.

Table 7–2: Number of data items expected for each scale of operations (database area)

No.	Item	Expected number of data items		
		Large	Medium	Small
1	Number of cabinets	5	5	5
2	Number of remote collection-related jobs	2	2	2
3	Average number of clients per job	10,000	3,000	500
4	Number of remote installation-related jobs	20	20	20
5	Average number of packages per job	1	1	1
6	Number of jobs that are not related to remote installation	8	8	8

No.	Item	Expected number of data items		
		Large	Medium	Small
7	Number of remote installation-related ID group jobs that are managed by relay managing the ID	20	20	20
8	Average number of clients per ID group	5,000	1,500	250
9	Number of ID group jobs that are not related to remote installation	8	8	8
10	Number of ID groups	10	10	10
11	Average number of managing relays per ID group	10	3	0
12	Average number of clients registered per ID group	5,000	1,500	250
13	Number of clients	10,000	3,000	500
14	Average number of files that are acquired by software inventory search	100	100	100
15	Average number of system information items that are acquired	100	100	100
16	Number of job definitions	55	55	55
17	Number of folders	5	5	5
18	Number of remote collection-related job definitions	3	3	3
19	Number of remote installation-related job definitions	20	20	20
20	Number of *Get software information from client* jobs defined	4	4	4
21	Number of *Transfer user inventory schema to client* jobs defined	1	1	1
22	Number of jobs	55	55	55
23	Number of ID group jobs managed by relay managing the ID	250	75	0
24	Total number of ID groups specified by ID group jobs	25	25	25
25	Number of items in software search list	200	200	200
26	Number of hosts in the system configuration when OpenView Linkage is used	0	0	0
27	Number of host groups	100	30	5
28	Number of packages	40	40	40
29	Number of jobs executed by scheduling	5	5	5
30	Number of jobs that are not related to remote installation	8	8	8
31	Number of user inventory items	20	20	20
32	Average number of software information items that are to be acquired	200	200	200
33	Number of all-lower-clients jobs	1	1	1
34	Total number of relay managers specified in all-lower-clients jobs	3	0	0
35	Number of hosts subject to acquisition of registry information	10,000	3,000	500
36	Number of registry items to be acquired	10	10	10
37	Number of created registry collection items	10	10	10
38	Number of hosts in the system configuration	10,000	3,000	500
39	Number of files to be managed in the software inventory dictionary	100	100	100
40	Number of files subject to license management	10	10	10

No.	Item	Expected number of data items		
		Large	Medium	Small
41	Number of files whose deletion is to be managed in the software inventory dictionary	10	10	10
42	Number of clients that are to acquire Microsoft Office products	10,000	3,000	500
43	Number of Microsoft Office products to be managed	5	5	5
44	Number of clients that are to acquire anti-virus products	10,000	3,000	500
45	Number of anti-virus products to be managed	5	5	5
46	Number of destination automatic maintenance policies	2	2	2
47	Number of ID group automatic maintenance policies	2	2	2
48	Number of system configuration information deletion logs	100	30	5
49	Number of non-Software Distribution hosts	100	30	5
50	Number of host search conditions that are set	5	5	5
51	Number of communities specified in the host search settings	5	5	5
52	Number of hosts found by host search	10,000	3,000	500
53	Number of *Report message* jobs defined	10	10	10
54	Number of software operation monitoring policies	1	0	0
55	Number of programs to be monitored	10	0	0
56	Number of programs whose operation time is to be acquired	10	0	0
57	Number of permission information items for software operation monitoring	10	0	0
58	Number of startup suppression information items in the software operation monitoring result	10	0	0
59	Number of *Set the software monitoring policy* jobs	2	0	0
60	Number of filtering conditions set by operation monitoring policy	10	0	0
61	Number of clients subject to software operation monitoring	10,000	0	0
62	Amount of operation information that is to be acquired per day per client	1,500	0	0
63	Number of days operation information is to be retained	5	0	0
64	Number of patch information items	789	789	789
65	Number of patches that have been downloaded	100	100	100
66	Number of installation scripts	10	10	10
67	Number of clients belonging to host groups	10,000	3,000	500
68	Number of clients belonging to ID groups	10,000	3,000	500
69	Number of clients with startup suppress history	10,000	3,000	500
70	Maximum number of operating information items (suppress and operation histories) per client	500,000	0	0

7.4.2 Transferring data to a relational database

To transfer data from a JP1/Software Distribution basic database JP1 Version 7i or earlier to a relational database (Embedded RDB), first create the new relational database, then transfer the contents of the basic database to the new relational database.

(1) Configuration limits when transferring data to a relational database

Relational databases have certain limits, such as the number of group levels that can be created in the database. If the configuration of the JP1/Software Distribution basic database exceeds these limits, the information in the supernumerary sections is not transferred when you transfer the data to a relational database.

Number of levels in the System Configuration window

In the System Configuration window, you can create up to seven hierarchical levels, including the end hosts. The series of host names from the top level can consist of a maximum of 255 bytes including the separators between host names.

Number of levels in the Destination window

In the Destination window, you can create up to seven hierarchical levels including the trailing host name. A series of the destination group names and the trailing host name can consist of a maximum of 255 bytes including the separators at the beginning of each host group name and the separator before the trailing host name.

Number of folder levels in the Job Definition and Job Status windows

You can create up to four levels of folders in the Job Definition and Job Status windows.

(2) Transferring data to a relational database

Note

- If you changed the package storage directory when you transferred data from a basic database to the relational database, move files from the previous package storage directory to the new package storage directory, and then follow the procedure below.
- If you are using Asset Information Manager Subset, stop the Asset Information Manager Subset services in the following order.

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before transferring to the relational database.

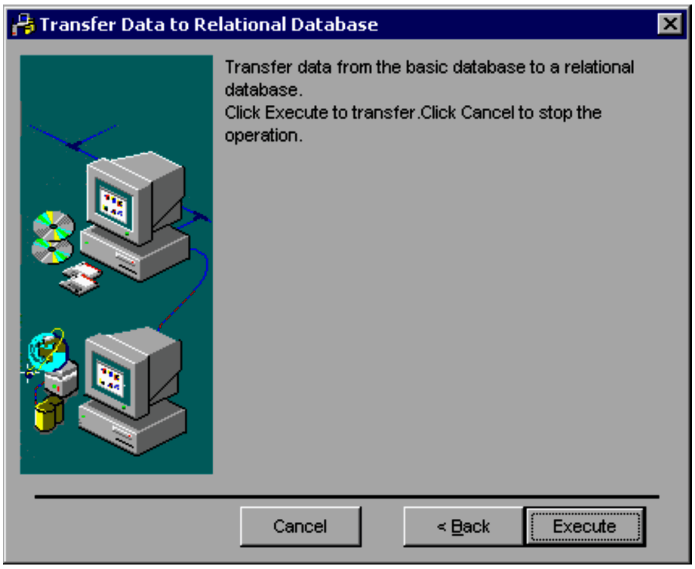
To transfer data from a JP1/Software Distribution Manager basic database JP1 Version 7i or earlier to the relational database:

1. In the Welcome dialog box, select **Transfer administration file from the file system**, and then click the **Next** button.

   The Authentication Information of Database dialog box appears.
2. In the Authentication Information of Database dialog box, specify the password, and then click the **Next** button.

   The Transfer Data to Relational Database dialog box appears.

Figure 7–10: Transfer Data to Relational Database dialog box



Transfer data from the basic database to a relational database.
Click Execute to transfer.Click Cancel to stop the operation.

3. Click the **Execute** button.

   Data is transferred from the basic database to Embedded RDB.

7.4.3 Upgrading the database

If you upgrade a JP1/Software Distribution Manager that uses Embedded RDB, you must also upgrade Embedded RDB. You also use this option to upgrade your database when you migrate from JP1/Software Distribution Manager Embedded RDB Edition JP1 Version 7i to JP1/Software Distribution Manager JP1 Version 8 that uses Embedded RDB.

(1) Notes on upgrading from version 08-00 and earlier to version 08-10 and later

When upgrading from version 08-00 or earlier to 08-10 or later, the required database capacity is different between these versions because the database structure has been changed. This may result in a space shortage error during upgrading. If this is the case, re-estimate the required database capacity and then upgrade the database. You can change the database capacity during upgrading. For details about estimating capacity during upgrading from version 08-00 or earlier to 08-10 or later, see *5.4.1(9) Notes on differences between sizes for version 08-00 and earlier and version 08-10 and later* in the *Description and Planning Guide*.

The backup files acquired prior to database upgrading cannot be restored because the database structure is different. After upgrading the database, acquire a backup again.

(2) Upgrading the database (for Embedded RDB)

Notes

- Before you upgrade the database, stop Remote Install Server service by opening **Control Panel**, and then choosing **Administrative Tools**, and **Services**.
- If you are using Asset Information Manager Subset, stop the Asset Information Manager Subset services in the following order.

1. World Wide Web Publishing Service or World Wide Web Publishing
2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

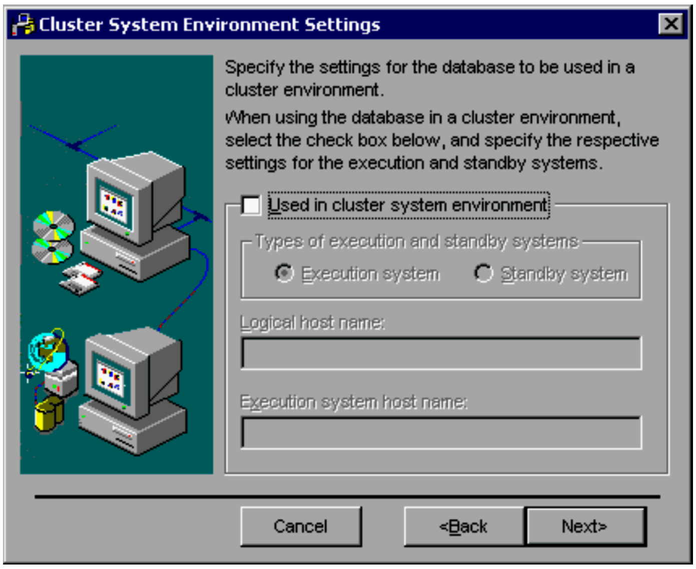
To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.

- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before upgrading the database.

To upgrade the database:

1. In the Welcome dialog box, select **Upgrade database**, and then click the **Next** button.
   The Authentication Information of Database dialog box appears.
2. In the Authentication Information of Database dialog box, specify the password, and then click the **Next** button.
   The Cluster System Environment Settings dialog box appears.

   Figure 7–11: Cluster System Environment Settings dialog box

   Cluster System Environment Settings

   Specify the settings for the database to be used in a cluster environment.

   When using the database in a cluster environment, select the check box below, and specify the respective settings for the execution and standby systems.

   □ Used in cluster system environment

   Types of execution and standby systems

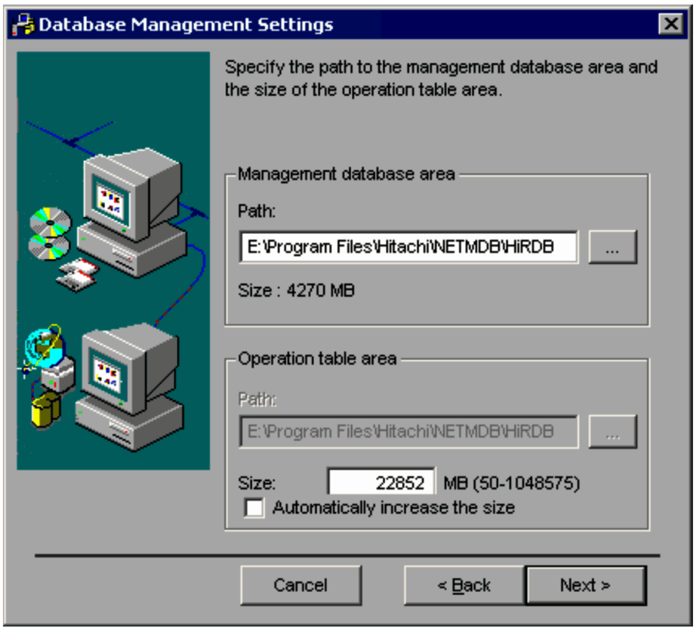
   ● Execution system ○ Standby system

   Logical host name:

   Execution system host name:

   If the database to be upgraded is used in a cluster environment, specify the same settings as when the existing database was created.
3. In the Cluster System Environment Settings dialog box, specify the settings and then click the **Next** button.
   The Database Management Settings dialog box appears.

   Figure 7–12: Database Management Settings dialog box

   Database Management Settings

   Specify the path to the management database area and the size of the operation table area.

   Management database area

   Path: E:\Program Files\Hitachi\NETMDB\HiRDB

   Size : 4270 MB

   Operation table area

   Path: E:\Program Files\Hitachi\NETMDB\HiRDB

   Size: 22852 MB (50-1048575)

   □ Automatically increase the size

You can change the size of the work table space. The default is that the value set during the creation process is displayed. However, if an automatic size increase is specified, the current size is displayed.

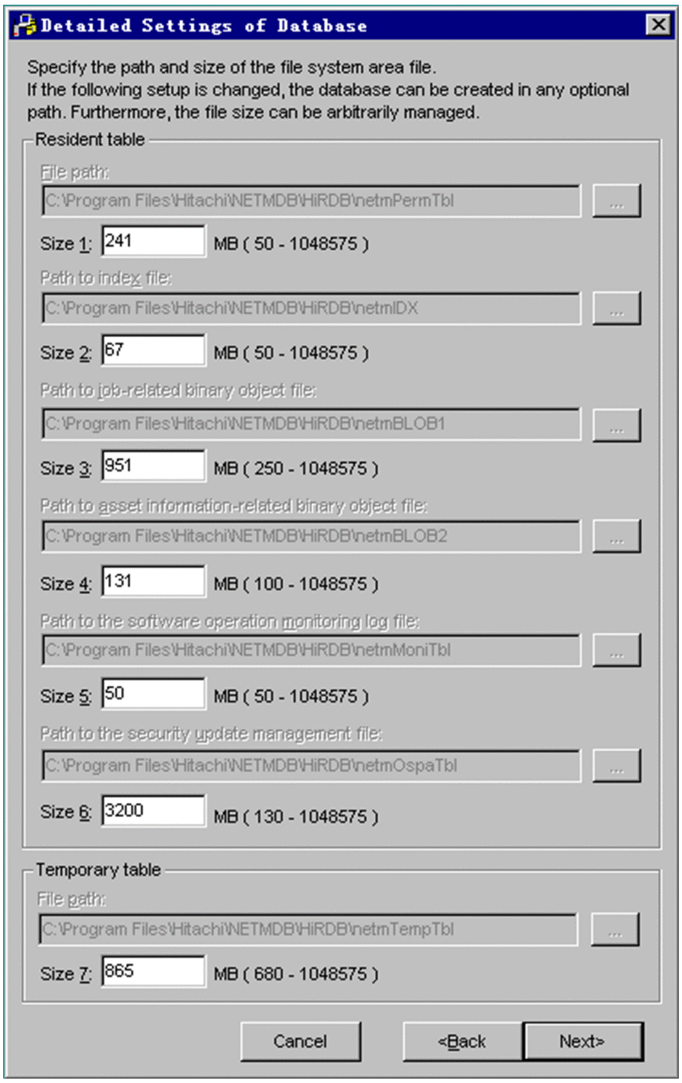
If the size of the work table space that is currently allocated is the same as the estimated size, use the automatic size increase setting.

In a cluster system environment, the **Automatically increase the size** check box setting should be the same in both the executing system and the standby system.

4. Specify the settings in the Database Management Settings dialog box, and then click the **Next** button.

   The Detailed Settings of Database dialog box appears.

   Figure 7–13: Detailed Settings of Database dialog box



Detailed Settings of Database

Specify the path and size of the file system area file.
If the following setup is changed, the database can be created in any optional path. Furthermore, the file size can be arbitrarily managed.

Resident table

File path: C:\Program Files\Hitachi\NETMDB\HiRDB\netmPermTbl

Size 1: 241 MB (50 - 1048575)

Path to index file: C:\Program Files\Hitachi\NETMDB\HiRDB\netmIDX

Size 2: 67 MB (50 - 1048575)

Path to job-related binary object file: C:\Program Files\Hitachi\NETMDB\HiRDB\netmBLOB1

Size 3: 951 MB (250 - 1048575)

Path to asset information-related binary object file: C:\Program Files\Hitachi\NETMDB\HiRDB\netmBLOB2

Size 4: 131 MB (100 - 1048575)

Path to the software operation monitoring log file: C:\Program Files\Hitachi\NETMDB\HiRDB\netmMoniTbl

Size 5: 50 MB (50 - 1048575)

Path to the security update management file: C:\Program Files\Hitachi\NETMDB\HiRDB\netmOspaTbl

Size 6: 3200 MB (130 - 1048575)

Temporary table

File path: C:\Program Files\Hitachi\NETMDB\HiRDB\netmTempTbl

Size 7: 865 MB (680 - 1048575)

You can change the sizes of database area files. The defaults are the values set when the database area files were created.

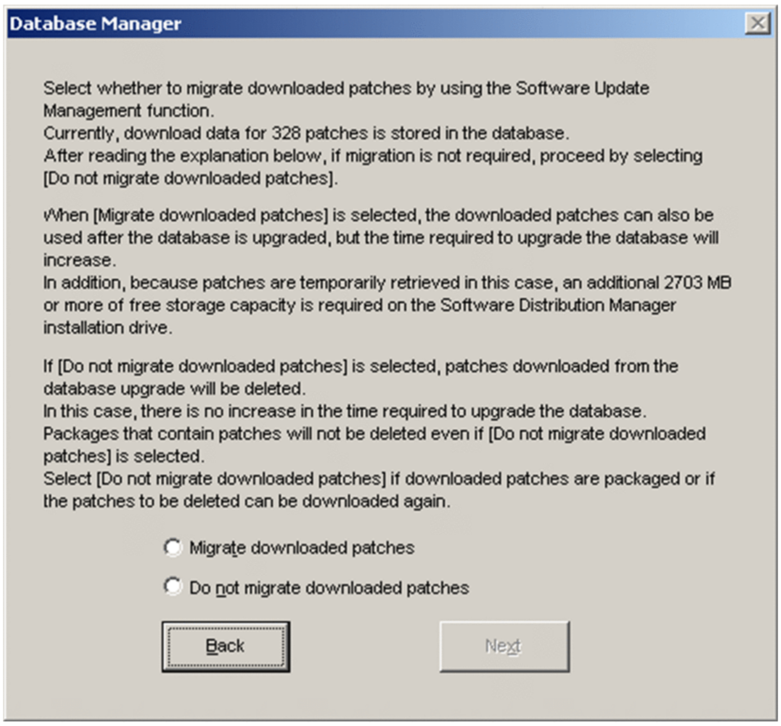
This dialog box is not displayed if you selected **Standby system** in the Cluster System Environment Settings dialog box.

5. Specify the settings in the Detailed Settings of Database dialog box, and then click the **Next** button.

   This displays a dialog box for selecting whether to migrate patches acquired by the security update management facility. The dialog box is not displayed in the following cases:

   - When upgrading from a database earlier than version 08-10
   - When the database version is 08-10, and no table was created for security update management

Figure 7–14: Dialog box for selecting whether to migrate patches acquired by the security update management facility



Database Manager

Select whether to migrate downloaded patches by using the Software Update Management function.
Currently, download data for 328 patches is stored in the database.
After reading the explanation below, if migration is not required, proceed by selecting [Do not migrate downloaded patches].

When [Migrate downloaded patches] is selected, the downloaded patches can also be used after the database is upgraded, but the time required to upgrade the database will increase.
In addition, because patches are temporarily retrieved in this case, an additional 2703 MB or more of free storage capacity is required on the Software Distribution Manager installation drive.

If [Do not migrate downloaded patches] is selected, patches downloaded from the database upgrade will be deleted.
In this case, there is no increase in the time required to upgrade the database.
Packages that contain patches will not be deleted even if [Do not migrate downloaded patches] is selected.
Select [Do not migrate downloaded patches] if downloaded patches are packaged or if the patches to be deleted can be downloaded again.

○ Migrate downloaded patches

○ Do not migrate downloaded patches

Migrate downloaded patches

During database upgrades, select this option to migrate any patches acquired by the security update management facility.

If you select this item, the patches are temporarily saved, so database upgrades will require more time. When you select this item and click the **Next** button, a dialog box will be displayed that provides a rough estimate of the increased time for the upgrade.

Also, since the patches are saved temporarily, you will need sufficient space in the JP1/Software Distribution Manager installation target directory. The required space is displayed in the dialog box for selecting whether to migrate patches acquired by the security update management facility.

Do not migrate downloaded patches

During database upgrades, select this option to not migrate patches acquired by the security update management facility.

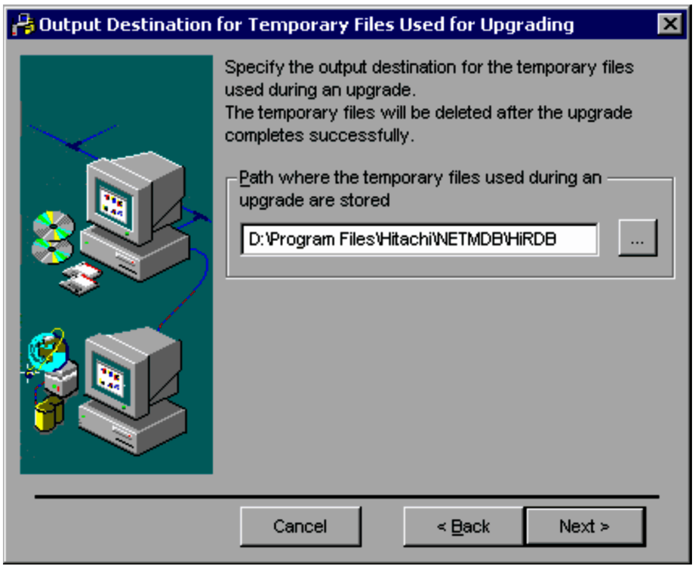
The package in which the patch is stored is not deleted when this item is selected. We recommend selecting this item when a patch is packaged or when a patch can be re-acquired.

When you select this item and click the **Next** button, a dialog box will be displayed to confirm that it is OK to delete the patch.

6. Specify a setting in the dialog box for selecting whether to migrate patches acquired by the security update management facility, and then click the **Next** button.

The Output Destination for Temporary Files Used for Upgrading dialog box appears.

Figure 7–15: Output Destination for Temporary Files Used for Upgrading dialog box



Output Destination for Temporary Files Used for Upgrading

Specify the output destination for the temporary files used during an upgrade.
The temporary files will be deleted after the upgrade completes successfully.

Path where the temporary files used during an upgrade are stored

D:\Program Files\Hitachi\NETMDB\HiRDB

Specify the output destination of the temporary files that are output during database upgrading.

This dialog box is not displayed if you selected **Standby system** in the Cluster System Environment Settings dialog box.

Path where the temporary files used during an upgrade are stored

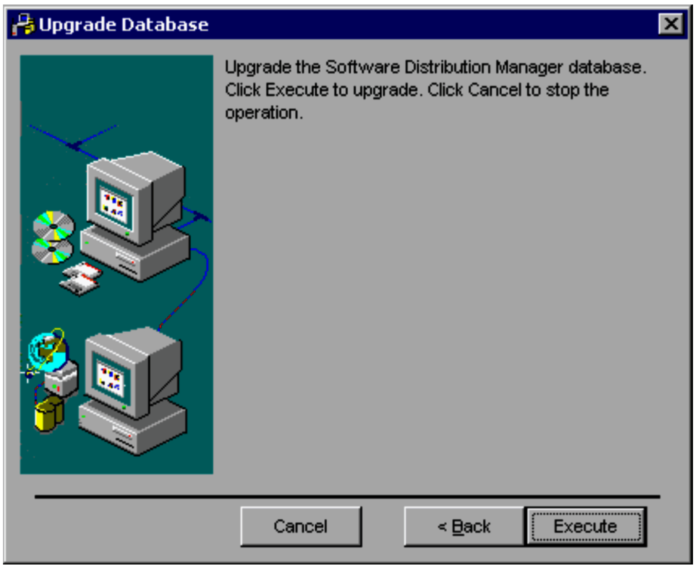
Specify the folder to which the temporary files used for upgrading are to be output. The files listed below are output to the specified folder:

- `netmUpgTemp`
- `netmdm_cabinet`
- `netmdm_collect`
- `netmdm_inspackage`
- `netmdm_jobgen_collect`
- `netmdm_jobgen_pack`
- `netmdm_package_inf`
- `UPGTemp.log`

7. Specify the settings in the Output Destination for Temporary Files Used for Upgrading dialog box, and then click the **Next** button.

   The Upgrade Database dialog box appears.

Figure 7–16: Upgrade Database dialog box



Upgrade the Software Distribution Manager database. Click Execute to upgrade. Click Cancel to stop the operation.

8. Click the **Execute** button.

   The database is upgraded.

   When upgrading is completed, the temporary files used during upgrading are automatically deleted.

   If a message indicating that migration of a patch to the database during upgrading has failed, the patch can be stored in the database by executing the `DPTInpt.exe` command. The upgrade will terminate normally when this happens. For details about the `DPTInpt` command, see *(3) DPTInpt.exe (store patch in database)*.

   If an error message indicating that there is not enough space in the database area file is displayed during upgrading, re-estimate the required database capacity, and specify a sufficient size during upgrading.

   Even when the message `The database has been upgraded successfully. Back up the database again because you cannot use a backup that was made before the upgrade` is displayed, the events listed in the following table may be output to the application log. In such a case, no action is necessary because the upgrade processing has been completed successfully.

No.	Source	Type	Event ID	Message ID
1	`HiRDBEmbeddedEdition_JN1`	Warning	`30001`	`KFPH22004-W`
2	`HiRDBEmbeddedEdition_JN1`	Warning	`30001`	`KFPH22012-W`
3	`HiRDBEmbeddedEdition_JN1`	Warning	`30001`	`KFPS04604-W`
4	`HiRDBEmbeddedEdition_JN1`	Warning	`30001`	`KFPX24231-W`
5	`HiRDBEmbeddedEdition_JN1`	Error	`30001`	`KFPH00142-E`
6	`HiRDBEmbeddedEdition_JN1`	Error	`30001`	`KFPH00306-E`
7	`HiRDBEmbeddedEdition_JN1`	Error	`30001`	`KFPH22003-E`
8	`HiRDBEmbeddedEdition_JN1`	Error	`30001`	`KFPS00349-E`
9	`HiRDBEmbeddedEdition_JN1`	Error	`30001`	`KFPX14236-E`

When you upgrade the database, suppression history and operation history for software operation monitoring are not migrated. If you use the Operation Log List window to manage operation information, use the `dcmmonrst` command to migrate the operation information. For details about the `dcmmonrst` command, see *4.13 dcmmonrst.exe (storing operating information in a database)* in the manual *Administrator's Guide Volume 2*.

(3) DPTInpt.exe (store patch in database)

This subsection describes the `DPTInpt` command, which migrates patches to the database when using Embedded RDB as the relational database. This command can only be executed on the PC on which the server core facility of JP1/Software Distribution Manager is installed. Embedded RDB must be running to execute this command.

Function

Stores patches in database. Execute this command when migrating a patch during an upgrade of Embedded RDB version 08-10 or later if the patch migration fails.

Format

```
DPTInpt.exe /U user-name/P password
```

Arguments

- `/U`

  Specifies the login ID for accessing Embedded RDB. This ID must be expressed as 1 to 8 alphanumeric characters beginning with an alphabetic character.

- `/P`

  Specifies the password for accessing Embedded RDB. Express the password as 1 to 30 alphanumeric characters beginning with an alphabetic character. Spaces cannot be used.

Return codes

The following table shows the codes returned when `DPTInpt` is executed.

Code	Description	Action
0	Terminated normally.	None.
1	Invalid value specified as argument.	Check the values of the command arguments.
2	An internal error occurred.	Check whether Embedded RDB is running.

Notes

- Do not execute more than one instance of the `DPTInpt` command.
- Do not start the security update management facility while the `DPTInpt` command is executing. Note that the security update management facility can be started using the task scheduler. Therefore, if you are using the task scheduler, be careful not to start the security update management facility while a `DPTInpt` command is executing.
- In the following cases, do not execute the `DPTInpt` command:
  - When Database Manager is running
  - When the security update management facility is running

Execution example

To execute the `DPTInpt` command with a login ID of `netmdm` and password of `abcde12345`, specify the command as follows.

```
DPTInpt.exe /U netmdm /P abcde12345
```

7.4.4 Backing up the database

Back up the database that is used by JP1/Software Distribution Manager. The two ways to back up the database are by using Database Manager and by using `netmdb_backup.bat` command.

The `netmdb_unload.bat` command is used to back up a database when the database is migrated to a different environment, such as when the PC is replaced. For details about the `netmdb_unload.bat` command, see *5.3.9(2) netmdb_unload.bat command* in the manual *Administrator's Guide Volume 2*.

If you use the Operation Log List window, it may take time to back up the database depending on the size of the managed operation log information.

To restore from a backup created by Database Manager or by the `netmdb_backup.bat` command, use Database Manager's **Recover the database from backup** option.

The following describes how to back up the database.

(1) Backing up the database using Database Manager

Notes

- Before you back up the database, stop Remote Install Server service by opening **Control Panel**, and then choosing **Administrative Tools**, and **Services**.
- If you are using Asset Information Manager Subset, stop the Asset Information Manager Subset services in the following order.

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

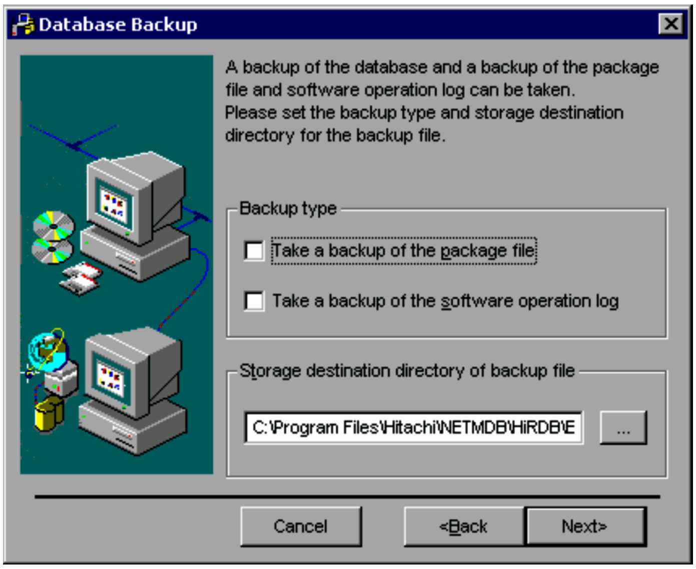
  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before backing up the database.

This subsection describes how to use Database Manager to back up a database.

To back up a database:

1. In the Welcome dialog box, select **Take backup of the database** and then click the **Next** button.
   The Authentication Information of Database dialog box appears.
2. In the Authentication Information of Database dialog box, specify the password and then click the **Next** button.
   The Database Backup dialog box appears.

   Figure 7–17: Database Backup dialog box

   A backup of the database and a backup of the package file and software operation log can be taken.
   Please set the backup type and storage destination directory for the backup file.

   Backup type
   ☐ Take a backup of the package file
   ☐ Take a backup of the software operation log

   Storage destination directory of backup file
   C:\Program Files\Hitachi\NETMDB\HiRDB\E

   Take a backup of package file
   Specifies whether or not the package files are also to be backed up when the database is backed up. The default is that this check box is not selected.

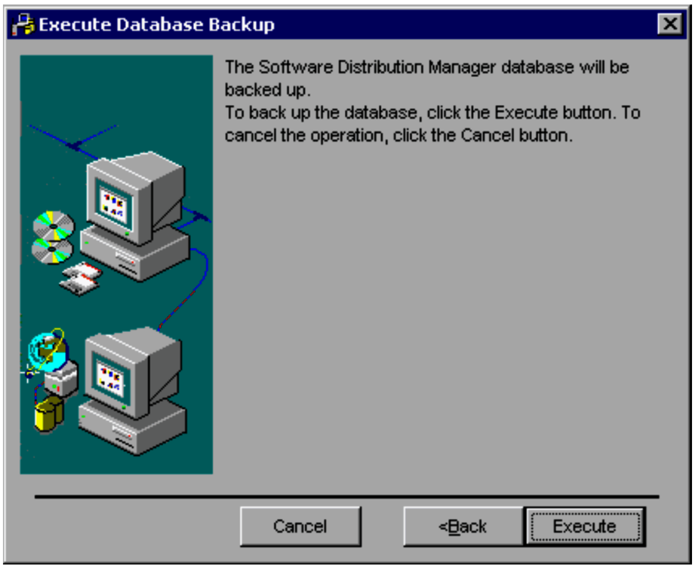
   Take a backup of software operation log
   Specifies whether or not the operation history storage directory is also to be backed up during the database backup. The default is that this check box is not selected.

   Storage destination directory of backup file
   Specifies the directory for storing the backup files that are created when the database is backed up.

3. Specify necessary information in the Database Backup dialog box and then click the **Next** button.

   The Execute Database Backup dialog box appears.

   Figure 7–18: Execute Database Backup dialog box

   Execute Database Backup

   The Software Distribution Manager database will be backed up.
   To back up the database, click the Execute button. To cancel the operation, click the Cancel button.

4. Click the **Execute** button.

   Database backup processing is executed and the backup file is created.

   The backup file is created under the name `netmdbbackup` in the backup file storage target directory. You can change the name of the backup file.

   Any backup file named `netmdbbackup` that already exists in the backup storage target directory at the time that backup processing is performed will be overwritten.

   When backing up package files

   The `RESOURCE` folder is created under the backup file storage target directory to store the package files.

   Any folder named `RESOURCE` that already exists in the backup storage target directory at the time that backup processing is performed will be overwritten.

   When backing up software operation history

   The `MONITORING` folder is created under the backup file storage target directory to store software operation history.

   Any folder named `MONITORING` that already exists in the backup storage target directory at the time that backup processing is performed will be overwritten.

(2) Database backup using a command

This subsection describes the `netmdb_backup.bat` command that can be used to back up a database. This command is stored in the JP1/Software Distribution Manager installation directory `\bin`.

Before you back up the database, stop Remote Install Server service by opening **Control Panel**, and then choosing **Administrative Tools**, and **Services**.

Also, if you are using Asset Information Manager Subset, stop the Asset Information Manager Subset services in the following order.

1. World Wide Web Publishing Service or World Wide Web Publishing
2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.

Note that if a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before backing up the database.

Function

This command backs up a database. It can also back up package files and software operation history.

Format

```
netmdb_backup.bat [/P]
                  [/h]
                   /i JP1/Software-Distribution-Manager-installation-
directory
                   /b backup-file-storage-target-directory
                   /o execution-result-output-file-name
```

Options

- /P

  Specifies that package files are to be backed up.

- /h

  Specifies that software operation history is to be backed up.

- /i

  Specifies the full path of the JP1/Software Distribution Manager installation directory.

- /b

  Specifies the full path of the backup file storage target directory. We recommend that you specify the directory name as a string of no more than 150 bytes. If the specified path is too long, directory creation may fail. For the storage directory, specify the local drive. Specify the storage directory name as a string of alphanumeric characters, the space, and the following symbols:

  `: . \ # @ ( )`

- /o

  Specifies the full path of the file to which the execution result is to be output.

Return code

The following table shows the return codes for the `netmdb_backup.bat` command:

Return code	Description
0	Normal termination
-1	Abnormal termination

Notes

- Do not change the contents of the BAT file for the `netmdb_backup.bat` command. If the contents are changed, the database can no longer be backed up.
- To use the `netmdb_backup.bat` command to back up a database, the user who executes the command must have Administrator permissions.
- When database backup is executed, the following file and folders are created in the storage directory:
  - `netmdbbackup` file
  - `RESOURCE` folder
  - `MONITORING` folder

  If any of these items already exist on the specified storage directory path at the time backup processing is performed, the existing file or folders will be overwritten.
- You must specify the `netmdb_backup.bat` command's options in the order shown above in *Format*.
- Do not execute multiple `netmdb_backup.bat` commands concurrently.

Example

This example backs up package files and software operation history when the database is backed up.

This example specifies each directory as follows:

- JP1/Software Distribution Manager installation directory

```
C:\Program Files\Hitachi\NETMDM
```

- Backup storage directory
  `C:\NETMDB`
- Execution result output file name
  `C:\NETMDB\backup.txt`

Before executing the command, you must create the backup file storage directory and the directory for storing the execution result output file.

The following shows an example of command execution:

```
netmdb_backup.bat /P /h /i "C:\Program Files\Hitachi\NETMDM" /b C:
\NETMDB /o C:\NETMDB\backup.txt
```

7.4.5 Recovering the database from a backup

Notes

- The database into which the data is to be restored must be in the same environment as the database from which the backup was made.
- The backup files acquired prior to database upgrading cannot be restored because the database structure is different. After upgrading the database, acquire a backup again.
- If you use the Operation Log List window, it may take time to restore the database depending on the size of the managed operation log information.
- Before you restore the database, stop Remote Install Server by opening **Control Panel**, and then choosing **Administrative Tools**, and **Services**.
- If you are using Asset Information Manager Subset, stop the Asset Information Manager Subset services in the following order.

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

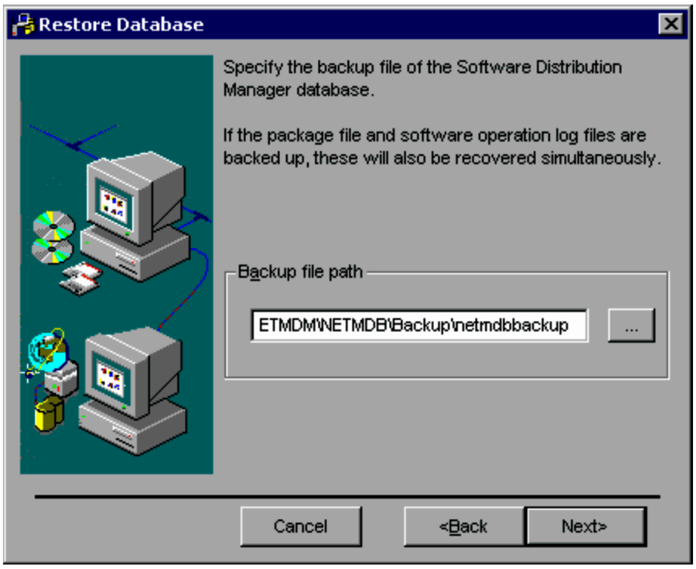
  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before restoring the database from the backup.

The procedure for restoring data from a backup file, created by Database Manager or by a `netmdb_backup.bat` command, to the Embedded RDB used by JP1/Software Distribution is outlined below.

To recover the database from a backup:

1. In the Welcome dialog box, select **Recover the database from backup**, and then click the **Next** button.
   The Authentication Information of Database dialog box appears.
2. In the Authentication Information of Database dialog box, specify the password and then click the **Next** button.
   The Restore Database dialog box appears.

Figure 7–19: Restore Database dialog box



Restore Database

Specify the backup file of the Software Distribution Manager database.

If the package file and software operation log files are backed up, these will also be recovered simultaneously.

Backup file path

ETMDM\NETMDB\Backup\netmdbbackup

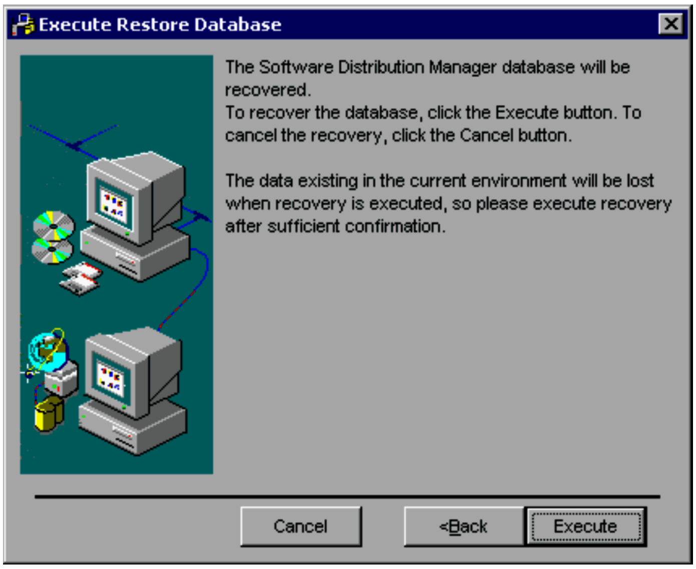
Backup file path

Specifies the backup file to be used to restore the database. Note that if the OS being used is a 64-bit version of Windows Server 2012, Windows Server 2008 or Windows Server 2003 (x64), a backup file under the `%Systemroot%\system32` directory cannot be specified.

3. In the Restore Database dialog box, specify the backup file and then click the **Next** button.

   The Execute Restore Database dialog box appears.

Figure 7–20: Execute Restore Database dialog box



Execute Restore Database

The Software Distribution Manager database will be recovered.
To recover the database, click the Execute button. To cancel the recovery, click the Cancel button.

The data existing in the current environment will be lost when recovery is executed, so please execute recovery after sufficient confirmation.

4. Click the **Execute** button.

   The database is restored.

7.4.6 Reorganizing the database

Reorganizing the database is a maintenance task performed as part of regular operations. For more information about when to reorganize the database, see *5.2.1(2) Reorganizing the database* in the manual *Administrator's Guide Volume 2*.

The two ways to reorganize Embedded RDB are by using Database Manager and by using a command. The following describes each method.

(1) Database reorganization using Database Manager

Notes

- Before you reorganize the database, stop Remote Install Server service by opening **Control Panel**, and then choosing **Administrative Tools**, and **Services**.
- If you are using Asset Information Manager Subset, stop the Asset Information Manager Subset services in the following order.

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

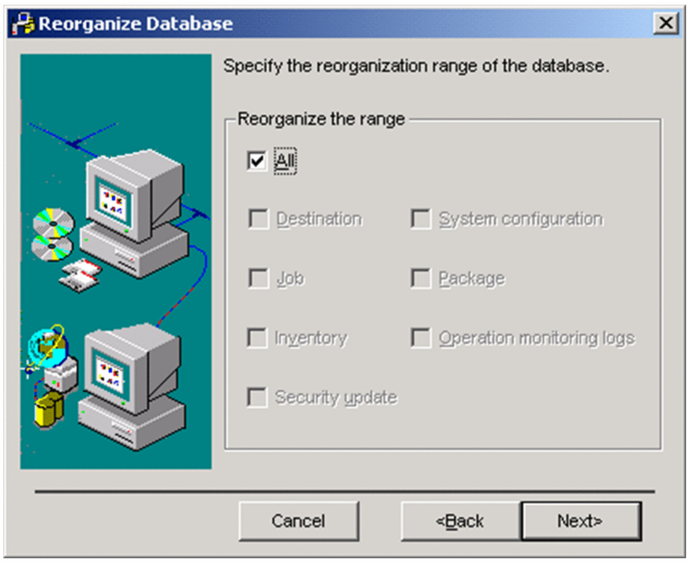
  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from which that listed above.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before reorganizing the database.

This subsection describes how to use Database Manager to reorganize a database.

To reorganize a database:

1. In the Welcome dialog box, select **Reorganize the database** and then click the **Next** button.
   The Authentication Information of Database dialog box appears.
2. In the Authentication Information of Database dialog box, specify the password and then click the **Next** button.
   The Reorganize Database dialog box appears.

   Figure 7–21: Reorganize Database dialog box



Reorganize Database

Specify the reorganization range of the database.

Reorganize the range

☑ All

□ Destination □ System configuration

□ Job □ Package

□ Inventory □ Operation monitoring logs

□ Security update

Reorganize the range

You can select the portion (range) of the database to be reorganized.

When you select the **All** check box, all the other check boxes are disabled. When you clear the **All** check box, all check boxes are enabled.

If you select any check box other than **All**, the **All** check box is disabled. The default is that the **All** check box is selected.

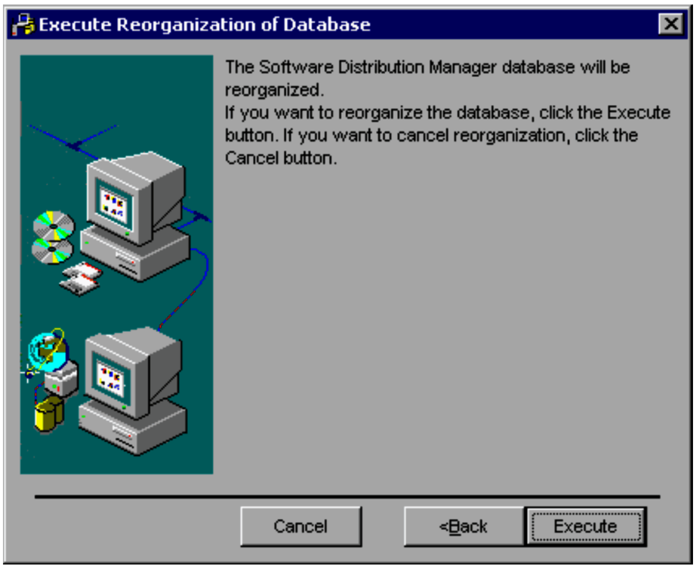
The following table lists the tables that correspond to each reorganization range.

Table 7–3: List of tables corresponding to each reorganization range

Reorganize the range		Tables
All	**System configuration**	`netmdm_nnm_management`, `netmdm_system`, `netmdm_lastupdate`, `netmdm_host_withoutdm`, `netmdm_system_delete`, `netmdm_systeminf`, `netmdm_suspend`
	Package	`netmdm_cabinet`, `netmdm_package`, `netmdm_package_inf`
	Destination	`netmdm_id`, `netmdm_id_policy`, `netmdm_identry`, `netmdm_node`, `netmdm_node_policy` `netmdm_node_policy_detail`
	Job	`netmdm_collect`, `netmdm_execution`, `netmdm_execution_site`, `netmdm_execution_summary`, `netmdm_jobgen`, `netmdm_jobgen_collect`, `netmdm_jobgen_id`, `netmdm_jobgen_node`, `netmdm_jobgen_pack`, `netmdm_jobgen_soft`, `netmdm_jobgen_system`, `netmdm_jobgen_userinv`, `netmdm_jobsch`, `netmdm_jobsch_site`, `netmdm_jobscript`, `netmdm_schedule`, `netmdm_stscnt`, `netmdm_jobgen_msg`, `netmdm_jobgen_monitoring`, `netmdm_stscnt_site`, `netmdm_stscnt_summary`, `netmdm_systemjob`
	Inventory	`netmdm_clientlist`, `netmdm_inspackage`, `netmdm_inventry`, `netmdm_mnglist`, `netmdm_registry`, `netmdm_reglist`, `netmdm_softwaredic`, `netmdm_softwaredel`, `netmdm_softwarelicence`, `netmdm_userinventry`, `netmdm_userinvlist`, `netmdm_oidlist`, `netmdm_discovery_setup`, `netmdm_discovery_community`, `netmdm_discovery_info`, `netmdm_discovery_options`, `netmdm_monitoring_filter`, `netmdm_monitoring_policy`, `netmdm_monitoring_program`, `netmdm_monitoring_permission`, `netmdm_monitoring_result`, `netmdm_monitoring_work`, `netmdm_vidlist`, `netmdm_activedirectory`, `netmdm_adproperty`, `netmdm_addictionary`, `netmdm_adupdate`, `netmdm_monitoring_webfilter`, `netmdm_adgroup`
	Operation monitoring logs	`netmdm_monitoring_security`, `netmdm_monitoring_workresult`
	Security update	`netmdm_ospatch_patchinf`, `netmdm_ospatch_productref`, `netmdm_ospatch_classref`, `netmdm_ospatch_xmlinf`, `netmdm_ospatch_script`

3. In the Reorganize Database dialog box, specify the desired reorganization range and then click the **Next** button.
   The Execute Reorganization of Database dialog box appears.

Figure 7–22: Execute Reorganization of Database dialog box



The Software Distribution Manager database will be reorganized.
If you want to reorganize the database, click the Execute button. If you want to cancel reorganization, click the Cancel button.

4. Click the **Execute** button.
   Database reorganization is executed.

(2) Database reorganization using a command

This subsection describes the `netmdb_reorganization.bat` command that can be used to reorganize a database. This command is stored in the JP1/Software Distribution Manager Embedded RDB Edition installation directory `\bin`.

Before you reorganize the database, stop Remote Install Server service by opening **Control Panel**, and then choosing **Administrative Tools**, and **Services**.

Also, if you are using Asset Information Manager Subset, stop the Asset Information Manager Subset services in the following order.

1. World Wide Web Publishing Service or World Wide Web Publishing
2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.

Note that if a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before reorganizing the database.

Function

This command reorganizes a database. It assumes **All** as the reorganization range.

Format

```
netmdb_reorganization.bat port-number
                          administrator-ID
                          password
                          /i JP1/Software-Distribution-Manager-installation-
directory
                          /o execution-result-output-file-name
```

Options

- *port-number*
  Specifies the port number used to connect the database.
- *administrator-ID*
  Specifies the administrator ID used to log in to the database.
- *password*
  Specifies the password used to log in to the database.
- `/i`
  Specifies the full path of the JP1/Software Distribution Manager installation directory.
- `/o`
  Specifies that a file containing the results of database reorganization is to be output. Specify the full path of the file to which the execution result is to be output.

Return code

The following table shows the return codes for the `netmdb_reorganization.bat` command:

Return code	Description
`0`	Normal termination
`-1`	Abnormal termination

Notes

- Do not change the contents of the BAT file for the `netmdb_reorganization.bat` command. If the contents are changed, the database can no longer be reorganized.

- To use the `netmdb_reorganization.bat` command to reorganize a database, the user who executes the command must have Administrator permissions.
- You must specify the `netmdb_reorganization.bat` command's options in the order shown above in *Format*.

Example

This example uses the `netmdb_reorganization.bat` command to reorganize the database.

This example specifies each directory as follows:

- JP1/Software Distribution Manager installation directory
  `C:\Program Files\Hitachi\NETMDM`
- Execution result output file name
  `C:\NETMDB\reorg.txt`

Before executing the command, you must create the directory for storing the execution result output file.

The following shows an example of command execution:

```
netmdb_reorganization.bat port-number user-ID-of-administrator password /i
"C:\Program Files\Hitachi\NETMDM" /o C:\NETMDB\reorg.txt
```

(3) Error handling

(a) RD area of the database is shut down

If the following message is output, indicating that an error occurred while reorganizing the database, the RD area is shut down.

`KFPH00306-E RDAREA "`*`RD area name`*`" held due to `*`error`*

For details on how to open the shut-down RD area, see *6.3.2 (8) Error in the embedded RDB environment in the manual Administrator's Guide Volume 2*.

(b) Insufficient work area that is required for exclusive use by the database

If the following message is output, indicating that an error occurs while reorganizing the database, there was insufficient work area for exclusive use by the database.

```
KFPS00443-I Insufficient memory in lock table. server=sds01, code=10, using=number,
total=number, PROGRAM=pdrorg
KFPS00447-I Insufficient exclusive control table information output to datetime.mem file
KFPA11912-E Insufficient memory for DB exclusive control
KFPL15226-E Delete request failed, table=NETMDM."NETMDM_MONITORING_SECURITY", server=sds01
KFPH00306-E RDAREA "NETMDM_NETM_MONITORING" held due to error occurred in log less utility
KFPH00306-E RDAREA "NETMDM_NETM_INDEXES" held due to error occurred in log less utility
KFPL15225-E Rollback called
KFPL00719-I Pdrorg terminated, return code=8
```

This means that the database's exclusive control work area is insufficient in RD areas **`NETMDM_NETM_MONITORING`** and **`NETMDM_NETM_INDEXES`**.

To adjust the database's exclusive control work area: (The user who executes the command below must have Administrator permissions.)

1. Start the command prompt.
2. Execute the `pdntcmd.bat` command located in JP1/Software Distribution Manager installation target directory `\NETMDB\BIN`.
3. At the command prompt, execute `pddbls -r` *RDarea-name* `-a`.

   The following are command execution examples:

   ```
   pddbls -r NETMDM_NETM_MONITORING -a
   pddbls -r NETMDM_NETM_INDEXES -a
   ```

   The RD area's unused segment and total segment counts are displayed. A display example is shown below.

```
 SEGMENT unused-segment-count / total-segment-count
```

4. Calculate the number of RD area segments in use from the information displayed.
   segments-in-use = *total-segment-count* - *unused-segment-count*
   Find the total value by calculating the number of segments in use in each RD area for all RD areas in which there was insufficient exclusive control work areas.
5. From the total number of segments in use, calculate the required number of exclusive control work area needed by the database.
   value-of-work-area-required-for-exclusive-control# = (*total-number-of-segments-in-use*) ÷ 6
   #: If necessary, round up to the next whole number.
6. Using a text editor, open the `sds01` file located in JP1/Software Distribution Manager installation target directory `\NETMDB\CONF`.
   Notes
   If the `sds01` file settings are incorrect, the database may not start. Back up the file before editing it.
7. Change the value in the `sds01` file for the exclusive control work area.
   Change *number* in the `sds01` file as shown below to the value of the exclusive control work area calculated in step 5.

```
set pd_lck_pool_size = number
```

8. At the command prompt, execute `pdconfchk`.
   Check that command execution has resulted in a message of `KFPS05007-I` (`return code = 0`).
9. Execute the `netmdb_stop.bat` command located in JP1/Software Distribution Manager installation target directory `\BIN` to stop the database.
10. Execute the `netmdb_start.bat` command located in JP1/Software Distribution Manager installation target directory `\BIN` to start the database.

7.4.7 Changing the database password

Changing the database password is a maintenance task performed as part of regular operations. Change the password periodically using Database Manager.

Notes

- Before you change the database password, stop Remote Install Server service by opening **Control Panel**, and then choosing **Administrative Tools**, and **Services**.
- If you are using Asset Information Manager Subset, stop the Asset Information Manager Subset services in the following order.

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

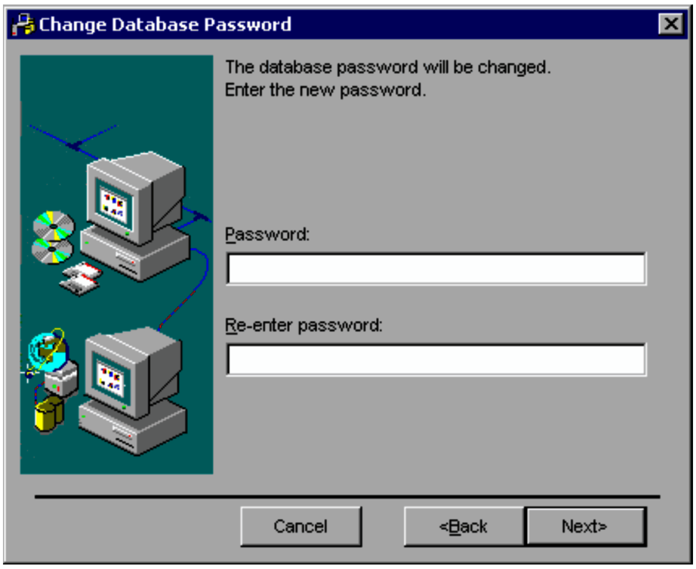
  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that shown above.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before changing the password.

This subsection describes the procedure for changing the password that is used to log on to a database.

To change a database password:

1. In the Welcome dialog box, select **Change database password** and then click the **Next** button.
   The Authentication Information of Database dialog box appears.
2. In the Authentication Information of Database dialog box, specify the password and then click the **Next** button.
   The Change Database Password dialog box appears.

Figure 7–23: Change Database Password dialog box



Change Database Password

The database password will be changed.
Enter the new password.

Password:

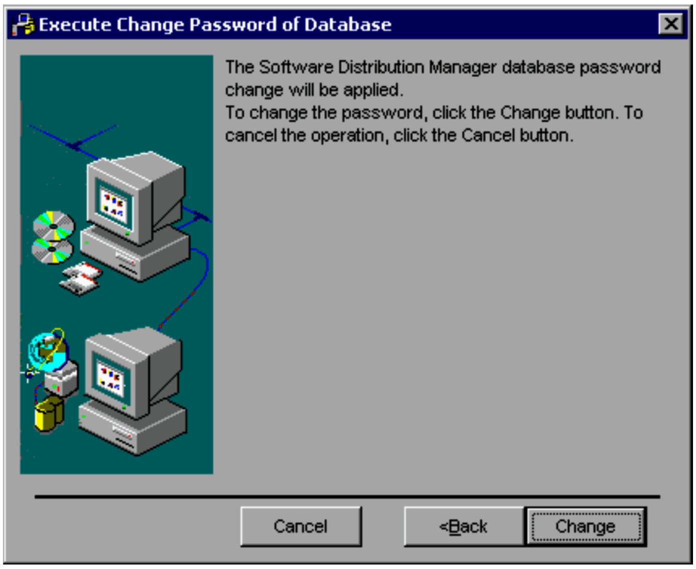
Re-enter password:

Enter a new password. Express the password as 1 to 30 alphanumeric characters beginning with an alphabetic character.

3. In the Change Database Password dialog box, specify a new password and then click the **Next** button.

   The Execute Change Password of Database dialog box appears.

   Figure 7–24: Execute Change Password of Database dialog box



Execute Change Password of Database

The Software Distribution Manager database password change will be applied.
To change the password, click the Change button. To cancel the operation, click the Cancel button.

4. Click the **Change** button.

   The database password is changed. The next time you attempt to log on to the database, you must use the new password set here.

7.4.8 Deleting unneeded inventory information from the database

Deleting unneeded inventory information from the database is a maintenance task performed as part of regular operations. For more information about deleting unneeded inventory information, see *5.2.1(4) Deleting unneeded inventory information* in the manual *Administrator's Guide Volume 2*.

Notes

- Before you delete unneeded inventory information, stop Remote Install Server service by opening **Control Panel**, and then choosing **Administrative Tools**, and **Services**.
- If you are using Asset Information Manager Subset, stop the Asset Information Manager Subset services in the following order.

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before deleting unneeded inventory information.

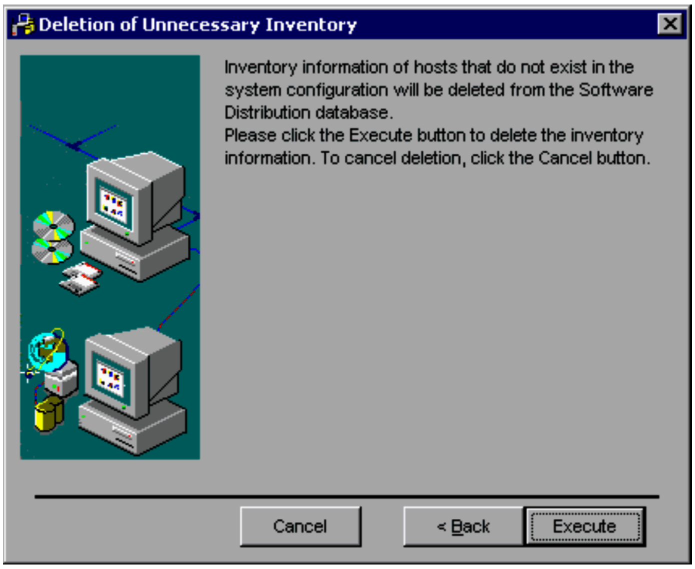
To delete unneeded inventory information:

1. In the Welcome dialog box, select **Delete unnecessary inventory information from the database**, and then click the **Next** button.

   The Authentication Information of Database dialog box appears.
2. In the Authentication Information of Database dialog box, specify the password, and then click the **Next** button.

   The Deletion of Unnecessary Inventory dialog appears.

   Figure 7–25: Deletion of Unnecessary Inventory dialog box

   Deletion of Unnecessary Inventory

   Inventory information of hosts that do not exist in the system configuration will be deleted from the Software Distribution database.
   Please click the Execute button to delete the inventory information. To cancel deletion, click the Cancel button.

3. Click the **Execute** button.

   Unneeded inventory information is deleted from Embedded RDB. After information has been deleted, the database is automatically reorganized to create free space.

7.5 How to use Database Manager (for Microsoft SQL Server or Oracle)

To create or maintain a relational database to be used by Microsoft SQL Server or Oracle, use *Database Manager*, one of the components of JP1/Software Distribution. To start Database Manager, from the menu, choose **Software Distribution Manager**, and then **Database Manager**.

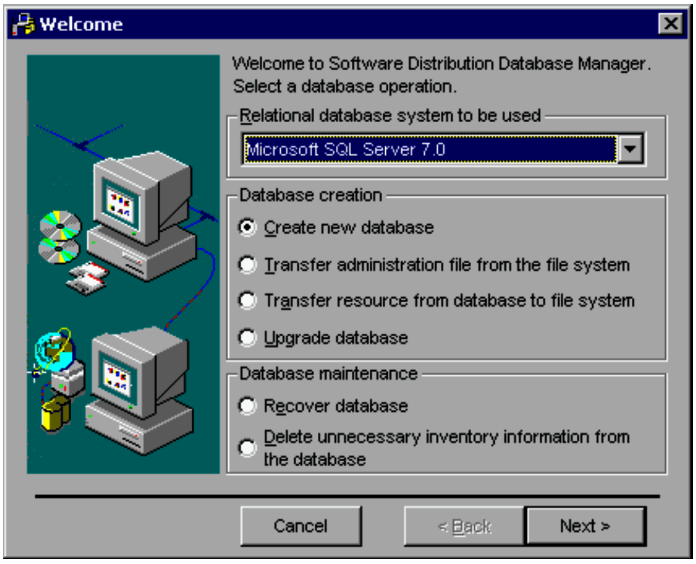
You should note the following items about using Database Manager:

- Exit all applications that use JP1/Software Distribution's relational database.
- Before starting Database Manager, stop Remote Install Server by opening **Control Panel** and then choosing **Administrative Tools**, and then **Services.**
- Only users who have Administrator permissions can use Database Manager.

The Welcome dialog box appears.

When Database Manager starts, the Welcome dialog box is displayed, enabling you to select a Database Manager operation.

Figure 7–26: Welcome dialog box



Welcome

Welcome to Software Distribution Database Manager.
Select a database operation.

Relational database system to be used: Microsoft SQL Server 7.0

Database creation
- ● Create new database
- ○ Transfer administration file from the file system
- ○ Transfer resource from database to file system
- ○ Upgrade database

Database maintenance
- ○ Recover database
- ○ Delete unnecessary inventory information from the database

If you are using Embedded RDB, different items are displayed in the Welcome dialog box. For details about how to use Database Manager when Embedded RDB is used, see *7.4 How to use Database Manager (for Embedded RDB)*.

Select the operation you want to perform with Database Manager.

Create new database

Creates a new database. After installing JP1/Software Distribution Manager, you must select this item to create a new database.

Transfer administration file from the file system

Migrates the basic database of JP1/Software Distribution JP1 Version 7i or earlier to a relational database. To select this option, a relational database must have been created previously.

Transfer resource from database to file system

Transfers the package data storage destination from the relational database to the file system. This option is disabled if Oracle was selected during server installation.

Upgrade database

Upgrades the database.

Recover database

Recovers a relational database from error. Note that this item is disabled if you select Oracle during server installation.

Delete unnecessary inventory information from the database

Deletes unneeded inventory from the database in order to increase available database space.

The following subsections describe each operation.

7.5.1 Creating a new database

This operation creates a new database for JP1/Software Distribution.

For the path to the database area, you must specify a directory that actually exists. You can use alphanumeric characters, the space, and the following symbols:

`: . \ # @ ( )`

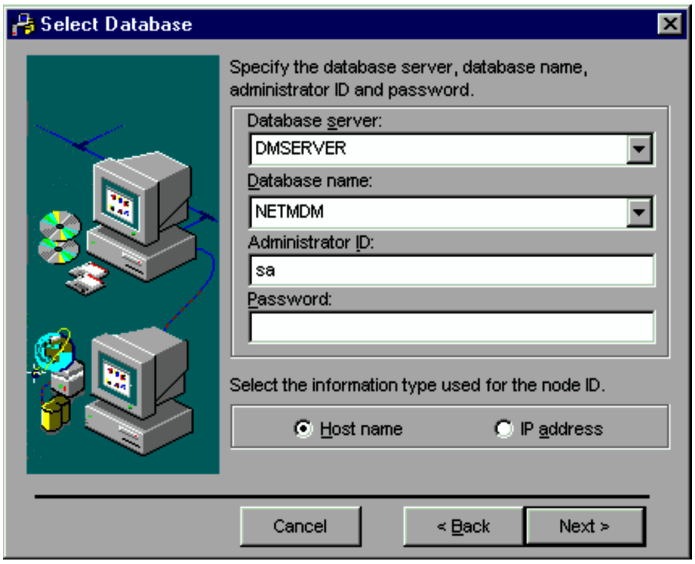
The procedure for creating a database depends on whether the database to be used is Microsoft SQL Server or Oracle. The procedure for each is described below.

(1) Creating a new relational database (Microsoft SQL Server)

To create a new relational database using Microsoft SQL Database:

1. In the Welcome dialog box, choose **Relational database system to be used**, **Create new database**, and then click the **Next** button.
   The Select Database dialog box appears.

Figure 7–27: Select Database dialog box



Select Database

Specify the database server, database name, administrator ID and password.

Database server: DMSERVER

Database name: NETMDM

Administrator ID: sa

Password:

Select the information type used for the node ID.

● Host name ○ IP address

Database server

Specify the name of the relational database server.

If you are using TCP/IP sockets as the network protocol, specify the server name. If you are using Named pipes, specify the computer name.

If you use named instances, specify the host name in the following format:

database-server-host-name\instance-name

Database name

Specify the database name that was specified at the JP1/Software Distribution Manager setup.

Administrator ID

Specify the ID of the system administrator (`SA`) of the relational database. By setting the administrator ID and password, you can prevent access to the relational database by unauthorized users.

Password

Specify the password for the administrator ID. For security purposes, the password is displayed as a series of asterisks (`*`).

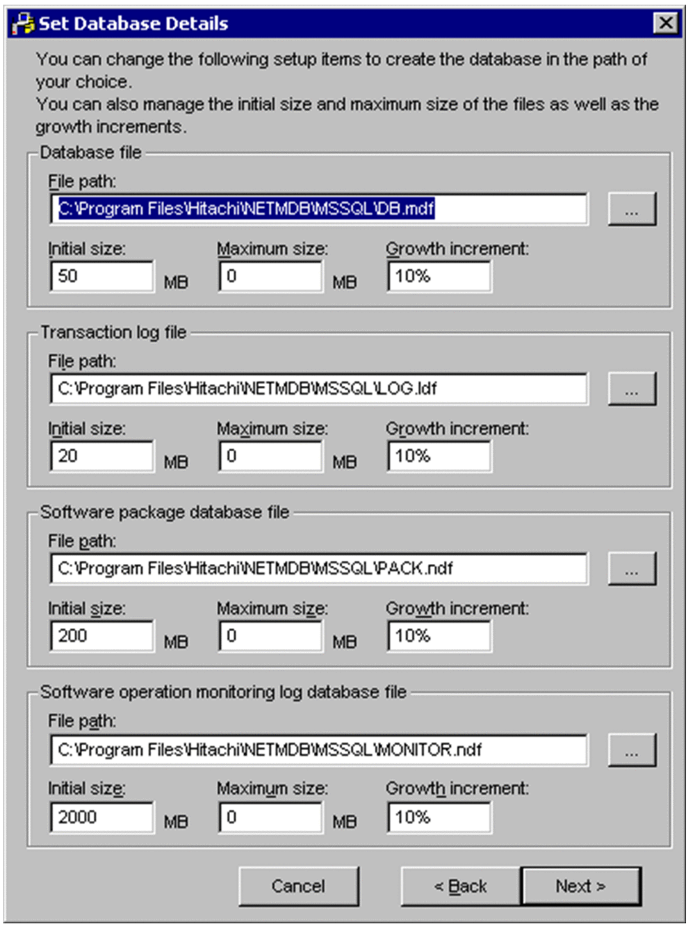
Host name or **IP address**

Select **Host name** or **IP address** for the type of information to be used for node identification.

2. Specify the items and then click the **Next** button.

The Set Database Details dialog box appears.

Figure 7–28: Set Database Details dialog box



Set Database Details

You can change the following setup items to create the database in the path of your choice.
You can also manage the initial size and maximum size of the files as well as the growth increments.

Database file
File path: C:\Program Files\Hitachi\NETMDB\MSSQL\DB.mdf
Initial size: 50 MB Maximum size: 0 MB Growth increment: 10%

Transaction log file
File path: C:\Program Files\Hitachi\NETMDB\MSSQL\LOG.ldf
Initial size: 20 MB Maximum size: 0 MB Growth increment: 10%

Software package database file
File path: C:\Program Files\Hitachi\NETMDB\MSSQL\PACK.ndf
Initial size: 200 MB Maximum size: 0 MB Growth increment: 10%

Software operation monitoring log database file
File path: C:\Program Files\Hitachi\NETMDB\MSSQL\MONITOR.ndf
Initial size: 2000 MB Maximum size: 0 MB Growth increment: 10%

In this dialog box, you can specify for each file the path to the database file, initial size, and maximum size.

To browse files to specify a file path, click the adjacent [**...**] button.

Note that if the OS being used is a 64-bit version of Windows Server 2012, Windows Server 2008 (x64) or Windows Server 2003 (x64), a path under the `%Systemroot%\system32` directory cannot be set. If you are creating a database on a different machine from the one on which the database manager has been installed, make sure that the specified database file path actually exists. If a nonexistent path is specified, database creation will fail.

For details about how to determine each size, see *5.4 Estimating disk space requirements for the database* in the *Description and Planning Guide*. The following table shows the default values.

Table 7–4: Default values for the detailed database settings (for Microsoft SQL Server)

Type of file	Path	Initial size (MB)	Maximum size (MB)#1	Growth increment#2
Database file	`C:\Program Files\Hitachi\NETMDB\MSSQL\DB.mdf`	3,250	0	10%
Transaction log file	`C:\Program Files\Hitachi\NETMDB\MSSQL\LOG.ldf`	20	0	10%
Software package database file	`C:\Program Files\Hitachi\NETMDB\MSSQL\PACK.ndf`	200	0	10%
Software operation monitoring log database file#3	`C:\Program Files\Hitachi\NETMDB\MSSQL\MONITOR.ndf`	2,000	0	10%

#1

If you specify `0`, the system may expand the file until the disk becomes full.

#2

Specify the size increase for one increment in either MB units or as a percentage (%). If you specify only a number, MB units is assumed. If you add `%` after a number, percentage is assumed.

#3

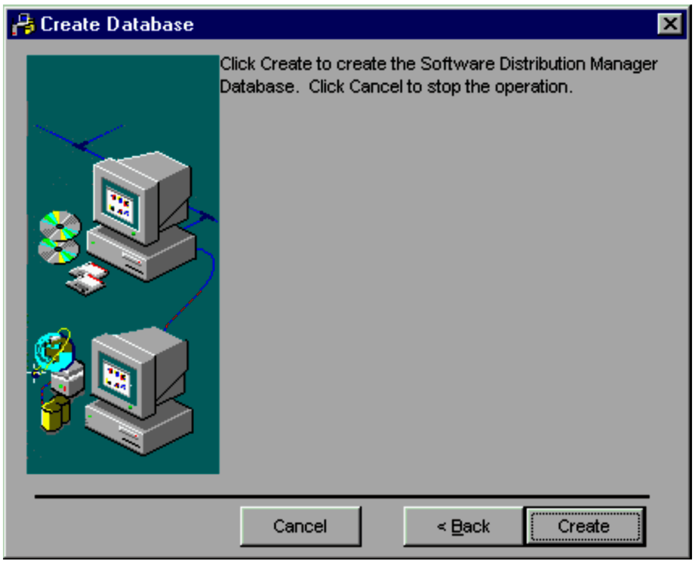
If the Operation Log List window is not used with the software operation monitoring facility, it is advisable to specify a small size because the software operation monitoring log file is not used.

In Microsoft SQL Server, the area for managing security updates is included in **Database file**.

3. Click the **Next** button.

The Create Database dialog box appears.

Figure 7–29: Create Database dialog box



Create Database

Click Create to create the Software Distribution Manager Database. Click Cancel to stop the operation.

4. Click the **Create** button.

The system creates the relational database. If files to be used by the relational database already contain data, a message is displayed asking you to confirm whether the data is to be initialized.

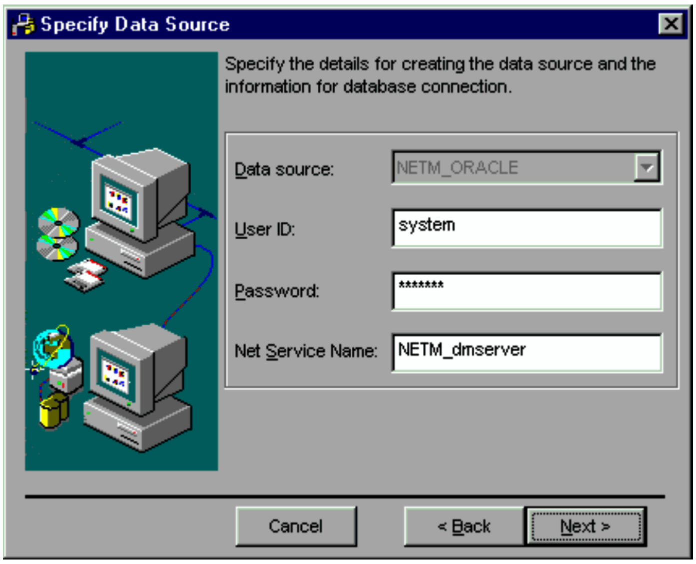
(2) Creating a new relational database (Oracle)

To create a new relational database using Oracle:

1. In the Welcome dialog box, choose **Relational database system to be used**, **Create new database**, and then click the **Next** button.

   The Specify Data Source dialog box appears.

   Figure 7–30: Specify Data Source dialog box

   Specify the details for creating the data source and the information for database connection.

   Data source: NETM_ORACLE

   User ID: system

   Password: *******

   Net Service Name: NETM_dmserver

   Data source

   The data source name is predetermined; you cannot specify this item.

   User ID

   If you have created a user, specify the user name. Before specifying the user name, check that the DBA Role permission has been granted to the user you created. If you did not create a user, specify `system`.

   Password

   If you have created a user, specify the password for the user. Otherwise, specify the password for the `system` user.

   Net Service Name

   Specify the net service name in the following format: `NETM_`*name-of-connection-destination-server*

   Do not include the DNS name in the connection destination server name.

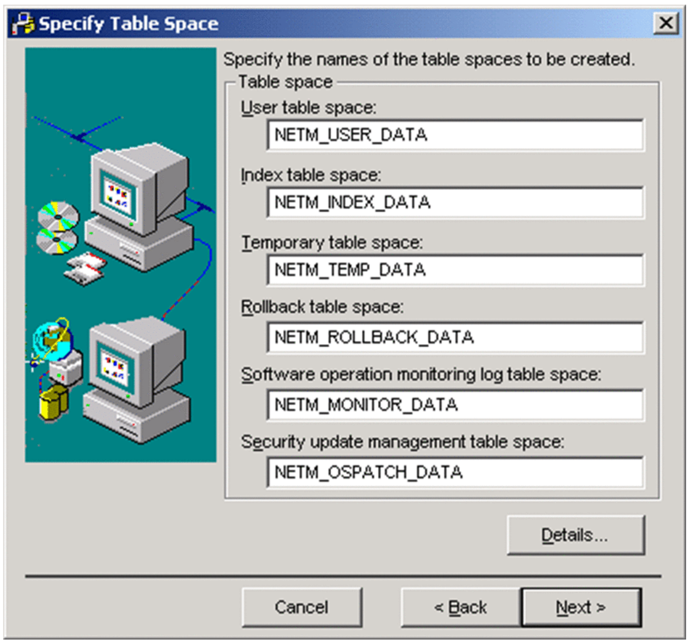
   The following example is for the connection destination server name `dmp380.Hitachi.co.us`:

   `NETM_dmp380`

2. Specify the item, and then click the **Next** button.

   The Specify Table Space dialog box appears.

Figure 7–31: Specify Table Space dialog box



In the Specify Table Space dialog box, specify the name of the table space to be created.

User table space

Specify the name of the user table space. The default is NETM_USER_DATA.

Index table space

Specify the name of the index table space. The default is NETM_INDEX_DATA.

Temporary table space

Specify the name of the temporary table space. The default is NETM_TEMP_DATA.

Rollback table space

Specify the name of the rollback table space. The default is NETM_ROLLBACK_DATA.

Software operation monitoring log table space

Specify the name of the software operation monitoring log table space. The default is NETM_MONITOR_DATA.

Security update management table space

Specify the name of the security update management table space. The default is NETM_OSPATCH_DATA.

Details button

Displays the Table Space Details dialog box that enables you to set the path of the database file as well as the initial and maximum sizes.

Figure 7–32: Table Space Details dialog box

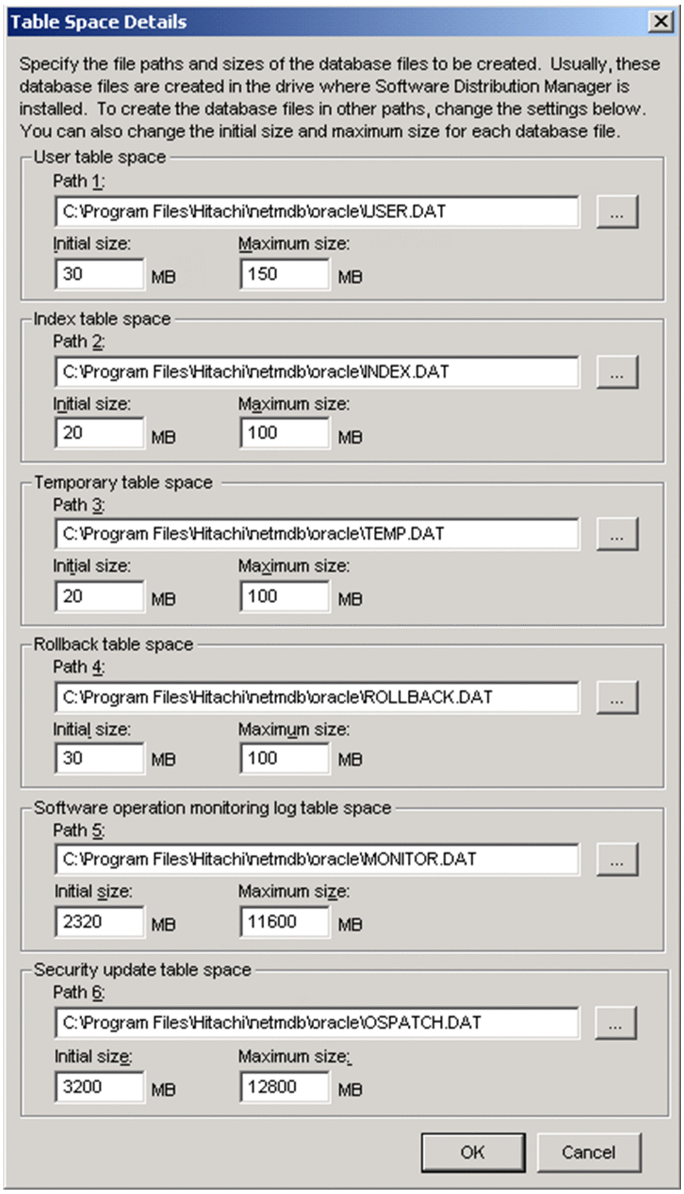


Table Space Details

Specify the file paths and sizes of the database files to be created. Usually, these database files are created in the drive where Software Distribution Manager is installed. To create the database files in other paths, change the settings below. You can also change the initial size and maximum size for each database file.

User table space

Path 1: C:\Program Files\Hitachi\netmdb\oracle\USER.DAT

Initial size: 30 MB Maximum size: 150 MB

Index table space

Path 2: C:\Program Files\Hitachi\netmdb\oracle\INDEX.DAT

Initial size: 20 MB Maximum size: 100 MB

Temporary table space

Path 3: C:\Program Files\Hitachi\netmdb\oracle\TEMP.DAT

Initial size: 20 MB Maximum size: 100 MB

Rollback table space

Path 4: C:\Program Files\Hitachi\netmdb\oracle\ROLLBACK.DAT

Initial size: 30 MB Maximum size: 100 MB

Software operation monitoring log table space

Path 5: C:\Program Files\Hitachi\netmdb\oracle\MONITOR.DAT

Initial size: 2320 MB Maximum size: 11600 MB

Security update table space

Path 6: C:\Program Files\Hitachi\netmdb\oracle\OSPATCH.DAT

Initial size: 3200 MB Maximum size: 12800 MB

To browse files to specify a file path, click the adjacent [**...**] button.

Note that if the OS being used is Windows Server 2003 (x64), a path under the `%Systemroot%\system32` directory cannot be specified. If you are creating a database on a different machine from the one on which the database manager has been installed, make sure that the specified database file path actually exists. If a nonexistent path is specified, database creation will fail.

For details about how to determine each size, see *5.4 Estimating disk space requirements for the database* in the *Description and Planning Guide*. The following table shows the default values.

Table 7–5: Default values for the detailed table space settings (Oracle)

Type of table space	Path	Initial size (MB)	Maximum size (MB)
User table space	`C:\Program Files\Hitachi\NETMDB\oracle \USER.DAT`	30	150
Index table space	`C:\Program Files\Hitachi\NETMDB\oracle \INDEX.DAT`	20	100

Type of table space	Path	Initial size (MB)	Maximum size (MB)
Temporary table space	`C:\Program Files\Hitachi\NETMDB\oracle \TEMP.DAT`	20	100[#1]
Rollback table space	`C:\Program Files\Hitachi\NETMDB\oracle \ROLLBACK.DAT`	30	100[#2]
Software operation monitoring log table space[#3]	`C:\Program Files\Hitachi\NETMDB\oracle \MONITOR.DAT`	2,320	11,600
Security update table space	`C:\Program Files\Hitachi\NETMDB\oracle \OSPATCH.DAT`	3,200	12,800

#1

Normally specify 60% of the user table space.

#2

Normally specify 10% of the user table space.

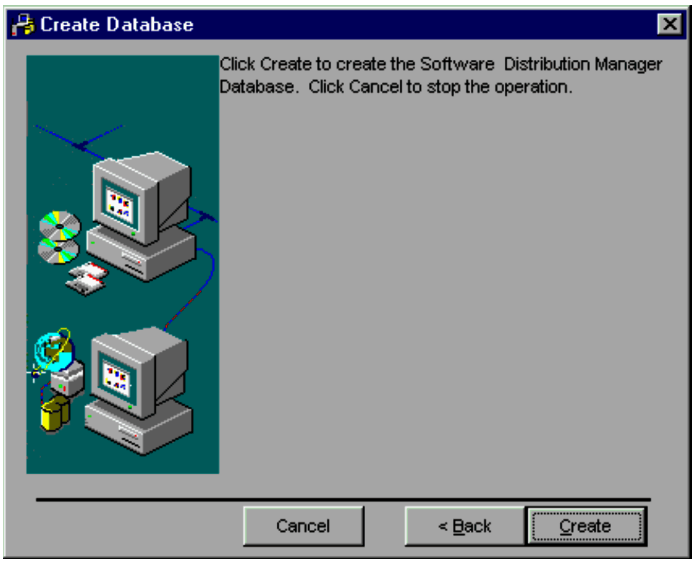
#3

If the Operation Log List window is not used with the software operation monitoring facility, it is advisable to specify a small size because the software operation monitoring log file is not used.

3. Click the **Next** button.

   The Create Database dialog box appears.

Figure 7–33: Create Database dialog box



Create Database

Click Create to create the Software Distribution Manager Database. Click Cancel to stop the operation.

4. Click the **Create** button.

   The system creates the relational database. If files to be used by the relational database already contain data, a message is displayed asking you to confirm whether the data is to be initialized.

7.5.2 Transferring administration file from the file system

To transfer data from a JP1/Software Distribution Manager basic database JP1 Version 7i or earlier to a relational database, first create a new relational database, and then transfer the contents of the basic database to the new relational database.

For the limitations on migrating the basic database to a relational database, see *7.4.2(1) Configuration limits when transferring data to a relational database*.

Note

- If you are using Asset Information Manager Subset, stop the Asset Information Manager Subset services in the following order.

    1. World Wide Web Publishing Service or World Wide Web Publishing
    2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
    3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

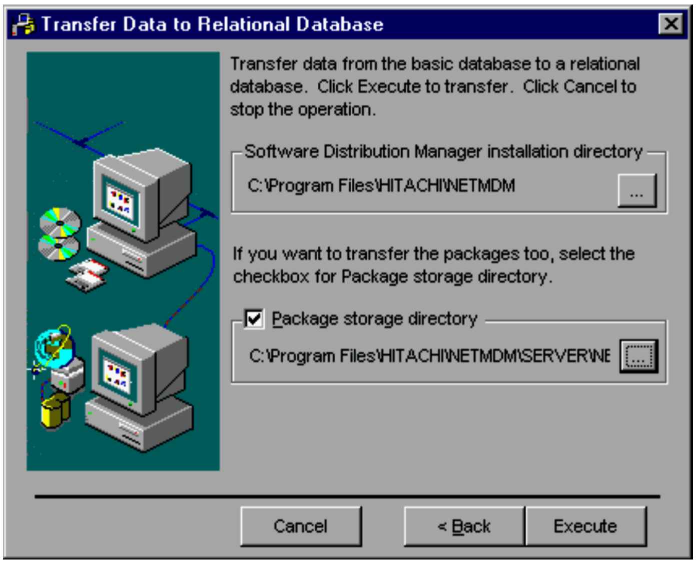
    To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before transferring administration files from the file system.
- If you changed the package storage directory when you transferred data from a basic database to the relational database, move files from the previous package storage directory to the new package storage directory, and then follow the procedure below.

To transfer data from a JP1/Software Distribution Manager basic database JP1 Version 7i or earlier to the relational database:

1. In the Welcome dialog box, choose **Relational database system to be used**, **Transfer administration file from the file system**, and then click the **Next** button.

   The Transfer Data to Relational Database dialog box appears.

   Figure 7–34: Transfer Data to Relational Database dialog box

   Transfer Data to Relational Database

   Transfer data from the basic database to a relational database. Click Execute to transfer. Click Cancel to stop the operation.

   Software Distribution Manager installation directory: C:\Program Files\HITACHI\NETMDM

   If you want to transfer the packages too, select the checkbox for Package storage directory.

   ☑ Package storage directory: C:\Program Files\HITACHI\NETMDM\SERVER\NE

   To change the JP1/Software Distribution installation directory or the package storage directory, click the **...** button next to that item. To transfer packages, select the **Package storage directory** check box.
2. Click the **Execute** button.

   The system transfers the data from the JP1/Software Distribution Manager basic database to the relational database.

7.5.3 Transferring resources from the database to the file system (Microsoft SQL Server)

This option is disabled if Oracle was selected during server installation.

Note

- When you transfer the package data storage destination to the file system, you must first use the maintenance wizard to change the package data storage destination from the relational database to the file system.
- If you are using Asset Information Manager Subset, stop the Asset Information Manager Subset services in the following order.

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

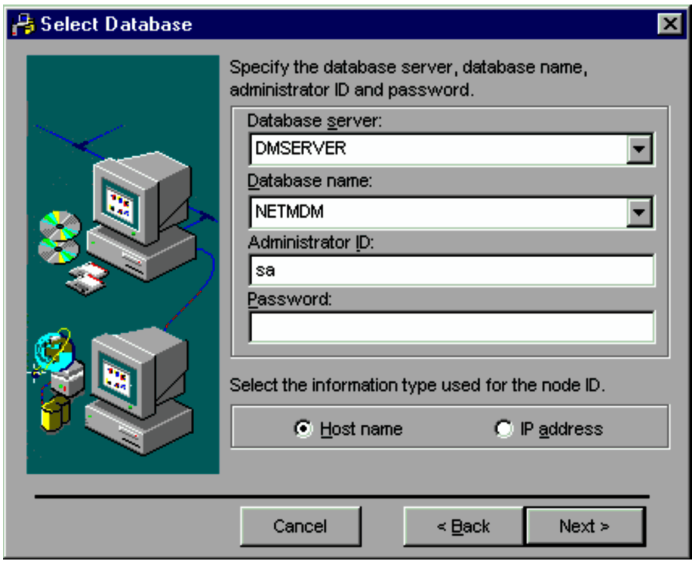
  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before transferring resources from the database to the file system.

To transfer resources from the database to the file system:

1. In the Welcome dialog box, choose **Relational database system to be used**, **Transfer resource from database to file system**, and then click the **Next** button.

   The Select Database dialog box appears.

   Figure 7–35: Select Database dialog box



Select Database

Specify the database server, database name, administrator ID and password.

Database server: DMSERVER

Database name: NETMDM

Administrator ID: sa

Password:

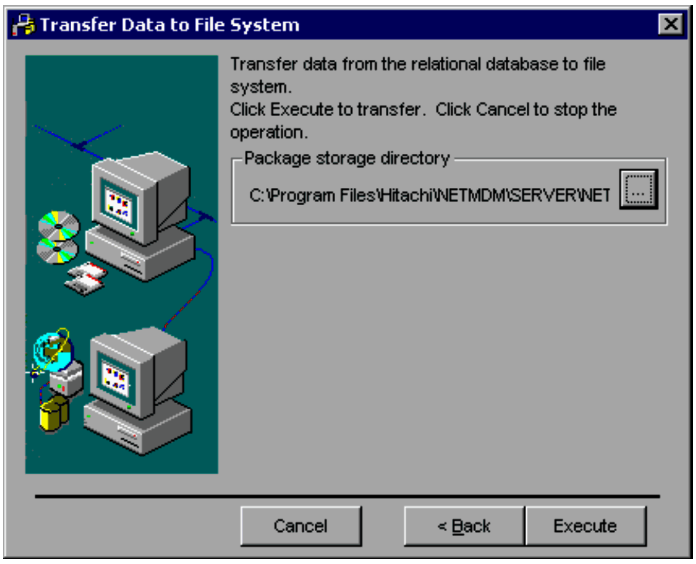
Select the information type used for the node ID.

● Host name ○ IP address

2. Specify information about the relational database from which data is to be transferred, and click the **Next** button.

   The Transfer Data to File System dialog box appears.

Figure 7–36: Transfer Data to File System dialog box



Transfer data from the relational database to file system.
Click Execute to transfer. Click Cancel to stop the operation.

Package storage directory: C:\Program Files\Hitachi\NETMDM\SERVER\NET

To change the package storage directory, click the **...** button for the item.

3. Click the **Execute** button.
   The package storage directory is transferred from the relational database to the file system.

7.5.4 Upgrading the database

This operation upgrades the relational database.

The procedure for upgrading a database depends on whether the database being used is Microsoft SQL Server or Oracle. The procedure for each is described below.

(1) Notes on using a JP1 version earlier than 7i

If you are using any of the following relational databases with a JP1 version earlier than 7i, you must upgrade your relational database when you upgrade JP1/Software Distribution to Version 7i:

- Oracle8i R8.1.5 or R8.1.6
- Oracle8
- Microsoft SQL Server 6.5

If you upgrade the relational database when you upgrade JP1/Software Distribution Manager, first upgrade the relational database and then use Database Manager to upgrade the JP1/Software Distribution database.

(2) Notes on upgrading from Microsoft SQL Server version 7.0 or earlier to Microsoft SQL Server 2008

Upgrading from Microsoft SQL Server version 7.0 or earlier to Microsoft SQL Server 2008 is not supported. You must upgrade the OS and migrate the relational database. For details about migration, see *A.2 Changing the database type*.

(3) Notes on upgrading from Microsoft SQL Server 2000 or earlier to Microsoft SQL Server 2012

Upgrading from Microsoft SQL Server 2000 or earlier to Microsoft SQL Server 2012 is not supported. You must upgrade the OS and migrate the relational database. For details about migration, see *A.2 Changing the database type*.

(4) Upgrading the database (for Microsoft SQL Server)

Notes

- If you are using Asset Information Manager Subset, stop the Asset Information Manager Subset services in the following order.

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

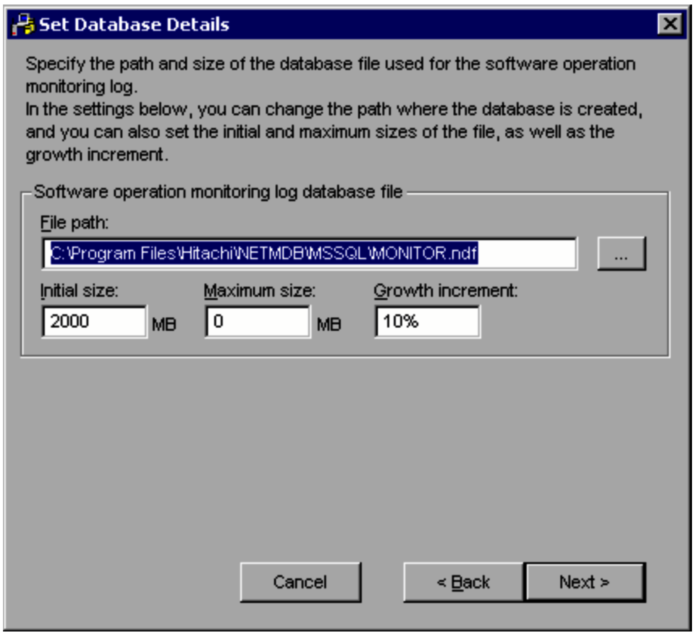
  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.

- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before upgrading the database.

To upgrade the database for Microsoft SQL Server:

1. In the Welcome dialog box, choose **Relational database system to be used**, **Upgrade database**, and then click the **Next** button.
   The Select Database dialog box appears.
2. Set information about the target relational database and then click the **Next** button.
   If there is a missing database file, the Set Database Details dialog box is displayed.

   Figure 7–37: Set Database Details dialog box

   Set Database Details

   Specify the path and size of the database file used for the software operation monitoring log.
   In the settings below, you can change the path where the database is created, and you can also set the initial and maximum sizes of the file, as well as the growth increment.

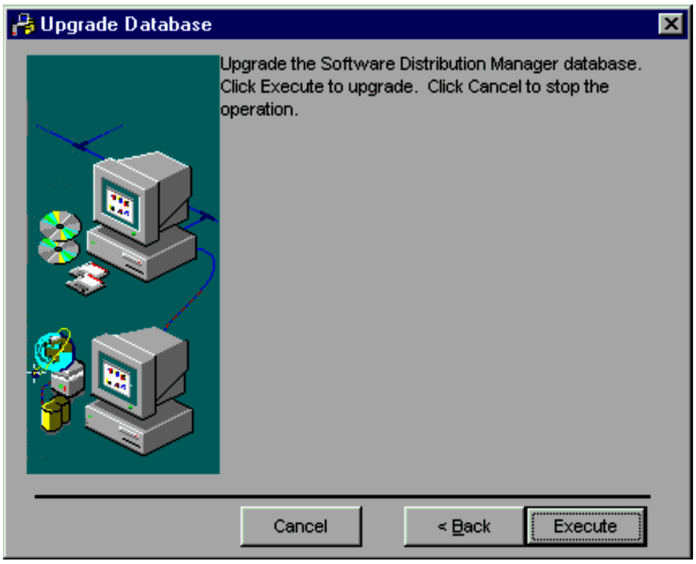
   Software operation monitoring log database file

   File path: C:\Program Files\Hitachi\NETMDB\MSSQL\MONITOR.ndf

   Initial size: 2000 MB
   Maximum size: 0 MB
   Growth increment: 10%

   You can set a software operation monitoring log database file.
3. Click the **Next** button.
   The Upgrade Database dialog box appears.

Figure 7–38: Upgrade Database dialog box



Upgrade the Software Distribution Manager database. Click Execute to upgrade. Click Cancel to stop the operation.

4. Click the **Execute** button.

   The system upgrades the relational database.

(5) Upgrading the database (for Oracle)

Notes

- If you are using Asset Information Manager Subset, stop the Asset Information Manager Subset services in the following order.

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.

- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before upgrading the database.

To upgrade the database for Oracle:

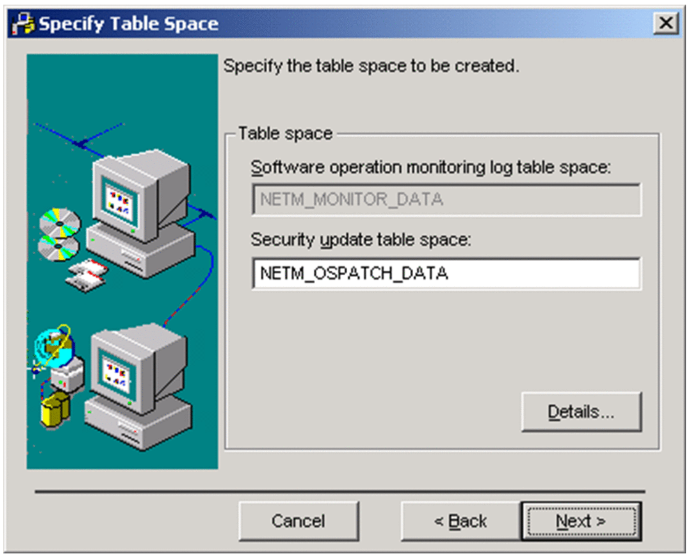
1. In the Welcome dialog box, choose **Relational database system to be used**, **Upgrade database**, and then click the **Next** button.

   The Specify Data Source dialog box appears. For details about the settings, see *7.5.1(2) Creating a new relational database (Oracle)*.

2. Click the **Next** button.

   If there is a missing database file, the Specify Table Space dialog box is displayed.

Figure 7–39: Specify Table Space dialog box



Specify Table Space

Specify the table space to be created.

Table space

Software operation monitoring log table space: NETM_MONITOR_DATA

Security update table space: NETM_OSPATCH_DATA

Clicking the **Details** button displays the Table Space Details dialog box that enables you to set the path of the database file as well as the initial and maximum sizes.

Figure 7–40: Table Space Details dialog box

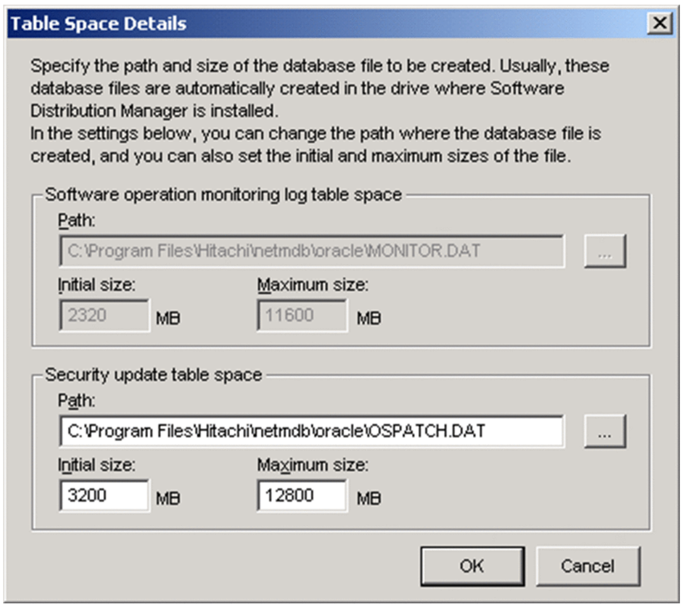


Table Space Details

Specify the path and size of the database file to be created. Usually, these database files are automatically created in the drive where Software Distribution Manager is installed.
In the settings below, you can change the path where the database file is created, and you can also set the initial and maximum sizes of the file.

Software operation monitoring log table space

Path: C:\Program Files\Hitachi\netmdb\oracle\MONITOR.DAT

Initial size: 2320 MB Maximum size: 11600 MB

Security update table space

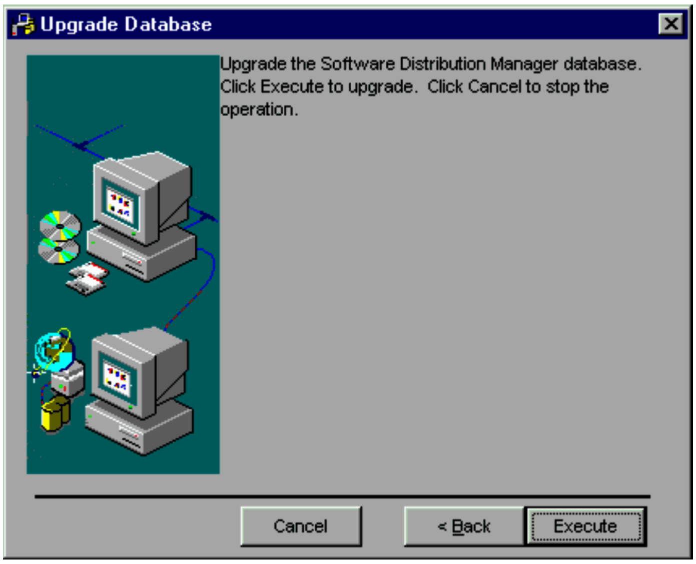
Path: C:\Program Files\Hitachi\netmdb\oracle\OSPATCH.DAT

Initial size: 3200 MB Maximum size: 12800 MB

3. Click the **Next** button.

   The Upgrade Database dialog box appears.

Figure 7–41: Upgrade Database dialog box


Upgrade Database

Upgrade the Software Distribution Manager database. Click Execute to upgrade. Click Cancel to stop the operation.

4. Click the **Execute** button.

   The system upgrades the relational database.

7.5.5 Recovering the database (Microsoft SQL Server)

Database recovery is a maintenance task performed as part of regular operations. For more information about when to recover a database, see *5.2.2(3) Recovering the database (Microsoft SQL Server)* in the manual *Administrator's Guide Volume 2*.

This option is disabled if Oracle was selected during server installation.

Notes

- If you are using Asset Information Manager Subset, stop the Asset Information Manager Subset services in the following order.

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.

- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before recovering the database.

To recover a relational database:

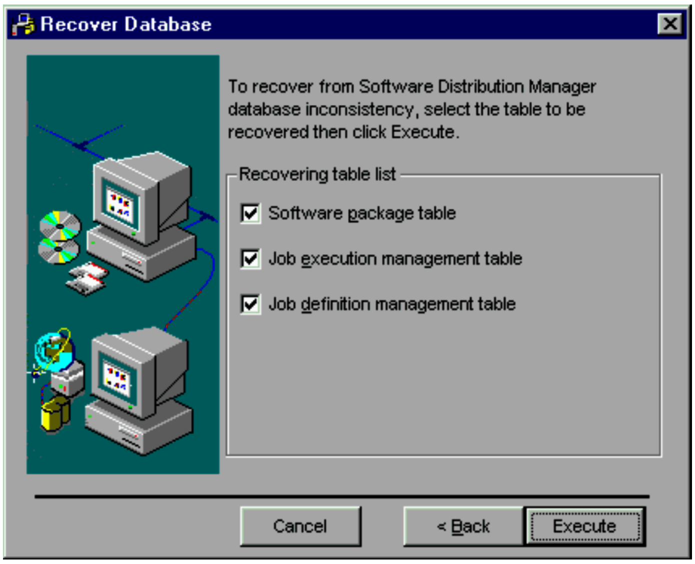
1. In the Welcome dialog box, choose **Relational database system to be used**, **Recover database**, and then click the **Next** button.

   The Select Database dialog box appears.

2. Specify the server, database name, administrator ID, and password for the database to be recovered, and click the **Next** button.

   The Recover Database dialog box appears.

Figure 7–42: Recover Database dialog box



To recover from Software Distribution Manager database inconsistency, select the table to be recovered then click Execute.

Recovering table list

☑ Software package table

☑ Job execution management table

☑ Job definition management table

The dialog box displays a list of tables to be repaired. Select the check boxes of the tables to be repaired. If you select all tables, the system searches the entire relational database and repairs all table inconsistencies.

- **Software package table**
  This option recovers the table related to packages.
- **Job execution management table**
  This option recovers the table related to job execution.
- **Job definition management table**
  This option recovers the table related to job definitions.

3. Click the **Execute** button.
   The system repairs the selected tables and recovers the relational database.

7.5.6 Deleting unneeded inventory information from the database

Deleting unneeded inventory information from the database is a maintenance task performed as part of regular operations. For more information about unneeded inventory information, see *5.2.2(4) Deleting unneeded inventory information* in the manual *Administrator's Guide Volume 2*.

Notes

- If you are using Asset Information Manager Subset, stop the Asset Information Manager Subset services in the following order.

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before deleting unneeded inventory information from the database.

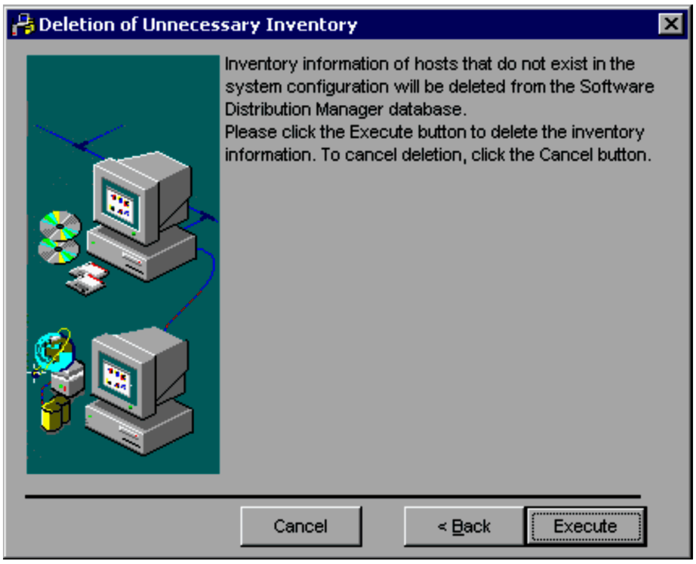
To delete unneeded inventory:

1. In the Welcome dialog box, choose **Relational database system to be used**, **Delete unnecessary inventory information from the database**, and then click the **Next** button.

The Specify Data Source dialog box (Oracle) or Select Database dialog box (Microsoft SQL Server) appears.

2. Enter the unneeded information and then click the **Next** button.
   The Deletion of Unnecessary Inventory dialog box appears.

   Figure 7–43: Deletion of Unnecessary Inventory dialog box



Inventory information of hosts that do not exist in the system configuration will be deleted from the Software Distribution Manager database.
Please click the Execute button to delete the inventory information. To cancel deletion, click the Cancel button.

3. Click the **Execute** button.
   Deletion of unneeded inventory begins. During the deletion processing, a dialog box showing the processing status is displayed.

7.6 Using data partitions to store operation monitoring history

If you are manually storing operation information, you can use data partitions to store the operation monitoring history.

This section describes storing the operation monitoring history using data partitions. This is a Microsoft SQL Server 2012, Microsoft SQL Server 2008 or Microsoft SQL Server 2005 facility.

Large users

If the number of operation information items that occur in a day exceeds 10 million, we recommend creating and storing data partitions in daily units.

Medium-sized users

If the number of operation information items that occur in a month exceeds 10 million, we recommend creating and storing data partitions in monthly units.

Small users

In the following cases data partitions are not necessary:

- User for whom only a few types of operating logs are kept, and only a few million administered operating log items are acquired per month
- User for whom the number of administered users is low, and only a few million administered operating log items are acquired per month
- Users who do not administer an operating log

Data partitions must be created separately using SQL Server Management Studio. They can only be created after a new relational database is created with Database Manager, or after an upgrade. The following subsections describe how to create and utilize data partitions.

7.6.1 Procedure for creating data partitions

The partition size for this example assumes 1,000 clients are being administered, each client collects 2,000 operation monitoring history items per day, and the database is storing eight months of data. In this case, 2 million operating information items are created daily and 40 million items are created monthly (assuming 20 days). Since this means a medium-sized user, we recommend that you create database partitions that can store a month's worth of data.

(1) Estimating the space required for the database

When creating a new JP1/Software Distribution database, you also need to include in the estimate the space required for devices other than software operation monitoring history database devices. For details, see *5.4.2 Estimating disk space required for Microsoft SQL Server* in the manual *Description and Planning Guide*. Estimate the space required monthly for the software operation monitoring history database devices and for the software operation monitoring history data partitions that hold one month of data. Here, we use 10 for the number of programs for which operating time is acquired.

To change existing JP1/Software Distribution databases to data partitions, also estimate the size of the monthly software operation monitoring history data partition.

Space required for software operation monitoring history database devices

software-operation-monitoring-history-database-device-space-required (bytes)

= (1,861[#1] **x** *number-of-software-operation-monitoring-history-information-items*)[#2]

+ (80 **x** *number-of-acquired-operating-time-information-items*)[#3]

Software operation monitoring history data partition space required for one month

software-operation-monitoring-history-data-partition-space-required-for-one-month (bytes)

= (1,861 **x** *number-of-software-operation-monitoring-history-information-items*)[#2]

= 1,861 **x** 1,000 **x** 2,000 **x** 20

= approximately 80 GB

#1

To set the maximum value for operation history information size, specify 1,861 (bytes). To specify a more average software operation monitoring history size, specify 543 (bytes).

#2

number-of-software-operation-monitoring-history-information-items

= *number-of-client-machines-subject-to-software-operation-monitoring* (1,000)

x *number-of-operation-monitoring-history-items-acquired-per-client-daily* (2,000)

x *days-to-retain-operating-information* (as secondary area, 10 days)

#3

number-of-acquired-operating-time-information-items

= 220 **x** *number-of-clients* **x** *number-of-programs-subject-to-operating-time-acquisition* (10)

= 1,861 **x** 1,000 **x** 2,000 **x** 10 + 80 **x** 220 **x** 1,000 **x** 10

= approximately 40 GB

Therefore, when creating a new JP1/Software Distribution database, create a 40-GB software operation monitoring history database device as a secondary area with Database Manager and create eight 80-GB software operation monitoring history data partitions for eight months of data using SQL Server Management Studio.

To change a JP1/Software Distribution database to a data partition, use the existing software operation monitoring history database device as a secondary area and create eight 80-GB software operation monitoring history data partitions for eight months of data using SQL Server Management Studio.

Here, we assume the following three disks are available for creating the secondary area.

- Disk 1

  500 GB, `D:` drive, specified as a secondary area, created by Database Manager#

- Disk 2

  500 GB, `E:` drive, specified as the area for creating data partitions for four months of data

- Disk 3

  500 GB, `F:` drive, specified as the area for creating data partitions for four months of data

#

Used when creating a new database.

(2) Coding query scripts for creating data partitions

In this subsection, we prepare code query scripts for creating the data partitions.

Table 7–6: Query scripts (when creating data partitions)

No.	Query script name	Description	Sample
1	`DropTable.sql`	Deletes the existing `netmdm_monitoring_security` table created by Database Manager. To create your own query script based on this sample, change the following item: • Database name in `USE` statement	*F.1*
2	`AddFilegroup.sql`	Adds a filegroup to be assigned a data partition. To create your own query script based on this sample, change the following items: • Database name in `USE` statement • Database name in `ALTER DATABASE` statement	*F.2*
3	`AddFiletoEdrive.sql`	Adds an actual file to the `E` drive and assigns it to a filegroup. To create your own query script based on this sample, change the following items:	*F.3*

No.	Query script name	Description	Sample
3	`AddFiletoEdrive.sql`	• Database name in `USE` statement • Database name in `ALTER DATABASE` statement • `FILENAME` specification path in `ALTER DATABASE` statement • `SIZE` specification size in `ALTER DATABASE` statement	*F.3*
4	`AddFiletoFdrive.sql`	Adds an actual file to the `F` drive and assigns it to a filegroup. To create your own query script based on this sample, change the following items: • Database name in `USE` statement • Database name in `ALTER DATABASE` statement • `FILENAME` specification path in `ALTER DATABASE` statement • `SIZE` specification size in `ALTER DATABASE` statement	*F.4*
5	`CreatePartition.sql`	Creates a partition function (`PARTITION FUNCTION`) and partition scheme (`PARTITION SCHEME`). To create your own query script based on this sample, change the following items: • Database name in `USE` statement • *yyyymmdd* format value of `CREATE PARTITION FUNCTION`	*F.5*
6	`CreateTable.sql`	Creates a `netmdm_monitoring_security` table in the partition scheme. To create your own query script based on this sample, change the following item: • Database name in `USE` statement	*F.6*

The data partitions shown in *Tables 7-7* and *7-8* will be created when you execute the query scripts listed in *Table 7-6*.

Table 7–7: Files and filegroups (when creating data partitions)

No.	Logical name	File name	Initial size	Upper limit	Increase amount	Filegroup name
1[#]	`NETMDM_MONI_DEVICE`	`D:\Program Files\Hitachi\NETMDB\MSSQL\MONITOR.sdf`	40,000 MB	`UNLIMITED`	10%	`netmdm_moni_seg`
2	`NETMDM_DP_0001`	`E:\NETMDP\MONITOR_DP_0001.ndf`	80 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0001`
3	`NETMDM_DP_0002`	`E:\NETMDP\MONITOR_DP_0002.ndf`	80 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0002`
4	`NETMDM_DP_0003`	`E:\NETMDP\MONITOR_DP_0003.ndf`	80 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0003`
5	`NETMDM_DP_0004`	`E:\NETMDP\MONITOR_DP_0004.ndf`	80 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0004`
6	`NETMDM_DP_0005`	`F:\NETMDP\MONITOR_DP_0005.ndf`	80 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0005`
7	`NETMDM_DP_0006`	`F:\NETMDP\MONITOR_DP_0006.ndf`	80 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0006`
8	`NETMDM_DP_0007`	`F:\NETMDP\MONITOR_DP_0007.ndf`	80 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0007`
9	`NETMDM_DP_0008`	`F:\NETMDP\MONITOR_DP_0008.ndf`	80 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0008`

#

These are the initial size, upper limit and increase amount to be specified when creating a new database.

Table 7–8: Partition function name and partition scheme name (when creating data partitions)

Partition function name	Partition scheme name
`netmdm_monitoring_security_pf`	`netmdm_monitoring_security_ps`

Operation monitoring histories are stored by this partition function and partition scheme for each month for event start times as indicated in the following table.

Table 7–9: Operation monitoring history that is stored (when creating data partitions)

No.	Filegroup name	Partition number	Operation monitoring history that is stored
1	`netmdm_moni_seg`	1	*event-start-time* < 01/01/2011
2	`netmdm_moni_dp_0001`	2	01/01/2011 ≤ *event-start-time* < 02/01/2011
3	`netmdm_moni_dp_0002`	3	02/01/2011 ≤ *event-start-time* < 03/01/2011
4	`netmdm_moni_dp_0003`	4	03/01/2011 ≤ *event-start-time* < 04/01/2011
5	`netmdm_moni_dp_0004`	5	04/01/2011 ≤ *event-start-time* < 05/01/2011
6	`netmdm_moni_dp_0005`	6	05/01/2011 ≤ *event-start-time* < 06/01/2011
7	`netmdm_moni_dp_0006`	7	06/01/2011 ≤ *event-start-time* < 07/01/2011
8	`netmdm_moni_dp_0007`	8	07/01/2011 ≤ *event-start-time* < 08/01/2011
9	`netmdm_moni_dp_0008`	9	08/01/2011 ≤ *event-start-time*

(3) Creating or upgrading a JP1/Software Distribution database

For more information about how to create a new JP1/Software Distribution database, see *7.5.1 Creating a new database*. When you create a new database, specify the initial size, upper limit, and increase amount from entry No. 1 in *Table 7-7* in the software operation monitoring history database file.

For information about changing an existing JP1/Software Distribution database to a data partition, see *7.5.4 Upgrading the database*.

(4) Creating data partitions

Create data partitions by running the query scripts from *Table 7-6* using SQL Server Management Studio.

To create a new JP1/Software Distribution database:

1. Execute `DropTable.sql` and delete the existing `netmdm_monitoring_security` table created by Database Manager.
2. Execute `AddFilegroup.sql` to add the filegroup to which the data partition will be assigned.
3. Create the folder `E:\NETMDP`.
4. Execute `AddFiletoEdrive.sql`, add an actual file to the `E` drive, and assign it to the filegroup.
5. Create the folder `F:\NETMDP`.
6. Execute `AddFiletoFdrive.sql`, add an actual file to the `F` drive, and assign it to the filegroup.
7. Execute `CreatePartition.sql` to create the partition function and partition scheme.
8. Execute `CreateTable.sql` to create the `netmdm_monitoring_security` table in the partition scheme.
9. Using SQL Server Management Studio, right-click the target database name `NETMDM_SAMPLE` to display the menu, choose **Properties**, and confirm that **File** and **Filegroup** are configured as specified. Also, right-click `NETMDM_SAMPLE` to display the menu, choose **Storage**, and confirm that

netmdm_monitoring_security_ps (under **Partition scheme**) and netmdm_monitoring_security_pf (under **Partition function**) have been created.

To change an existing JP1/Software Distribution database into a data partition:

1. Stop Remote Install Server service.
2. Using the bcp utility, batch export the existing data in the netmdm_monitoring_security table.
3. Execute DropTable.sql to delete the netmdm_monitoring_security table.
4. Execute AddFilegroup.sql to add the filegroup to which the data partition will be assigned.
5. Create the folder E:\NETMDP.
6. Execute AddFiletoEdrive.sql, add an actual file to the E drive, and assign it to the filegroup.
7. Create the folder F:\NETMDP.
8. Execute AddFiletoFdrive.sql, add an actual file to the F drive, and assign it to the filegroup.
9. Execute CreatePartition.sql to create the partition function and partition scheme.
10. Execute CreateTable.sql to create the netmdm_monitoring_security table in the partition scheme.
11. Using SQL Server Management Studio, right-click the target database name NETMDM_SAMPLE to display the menu, choose **Properties**, and confirm that **File** and **Filegroup** are configured as specified. Also right-click NETMDM_SAMPLE to display the menu, choose **Storage**, and confirm that netmdm_monitoring_security_ps (under **Partition scheme**) and netmdm_monitoring_security_pf (under **Partition function**) have been created.
12. Using the bcp utility, batch import the previous security table data.

7.6.2 Procedure for adding data partitions

In the data partition created in *7.6.1 Procedure for creating data partitions*, history starting on September 1, 2011 would also be stored in the last partition created for storing eight months of history (partition 9 in *Table 7-9*). To avoid this, you must add one or more data partitions before storing of history starting on September 1, 2011 begins. This subsection describes the procedure for added new data partitions for storing an additional four months of data.

(1) Estimating the space required for the database

Here we assume the following disk is available for the new data partitions.

- Disk 4
  500 GB, G: drive, specified as the area for creating a data partition for four months of data

(2) Creating query scripts for adding data partitions

In this subsection, we prepare query scripts for adding data partitions.

Table 7–10: Query scripts (for adding data partitions)

No.	Query script name	Description	Sample
1	AddFilegroup2nd.sql	Adds a filegroup to be assigned a data partition. To create your own query script based on this sample, change the following items: • Database name in USE statement • Database name in ALTER DATABASE statement	*F.7*
2	AddFiletoGdrive.sql	Adds an actual file to the G drive and assigns it to a filegroup. To create your own query script based on this sample, change the following items: • Database name in USE statement	*F.8*

No.	Query script name	Description	Sample
2	`AddFiletoGdrive.sql`	• Database name in `ALTER DATABASE` statement • `FILENAME` specification path in `ALTER DATABASE` statement • `SIZE` specification size in `ALTER DATABASE` statement	*F.8*
3	`AlterPartition.sql`	Changes the function and partition scheme so that history starting on Sep 2011 is stored in the added filegroup. To create your own query script based on this sample, change the following items: • Database name in `USE` statement • *yyyymmdd* format value of `ALTER PARTITION FUNCTION`	*F.9*

The data partitions listed in *Table 7-11* will be created when you execute the query scripts shown in *Table 7-10*.

Table 7–11: File and filegroups (for adding data partitions)

No.	Logical name	File name	Initial size	Upper limit	Increase amount	Filegroup name
1	`NETMDM_DP_0009`	`G:\NETMDP \MONITOR_DP_0009.ndf`	80 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0009`
2	`NETMDM_DP_0010`	`G:\NETMDP \MONITOR_DP_0010.ndf`	80 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0010`
3	`NETMDM_DP_0011`	`G:\NETMDP \MONITOR_DP_0011.ndf`	80 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0011`
4	`NETMDM_DP_0012`	`G:\NETMDP \MONITOR_DP_0012.ndf`	80 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0012`

Operation monitoring histories are stored by changing the partition function and partition scheme each month for event start times as shown in the following table.

Table 7–12: Operation monitoring history that is stored (for adding data partitions)

No.	Filegroup name	Partition number	Operation monitoring history that is stored
1	`netmdm_moni_seg`	1	*event-start-time* < 01/01/2011
2	`netmdm_moni_dp_0001`	2	01/01/2011 ≤ *event-start-time* < 02/01/2011
3	`netmdm_moni_dp_0002`	3	02/01/2011 ≤ *event-start-time* < 03/01/2011
4	`netmdm_moni_dp_0003`	4	03/01/2011 ≤ *event-start-time* < 04/01/2011
5	`netmdm_moni_dp_0004`	5	04/01/2011 ≤ *event-start-time* < 05/01/2011
6	`netmdm_moni_dp_0005`	6	05/01/2011 ≤ *event-start-time* < 06/01/2011
7	`netmdm_moni_dp_0006`	7	06/01/2011 ≤ *event-start-time* < 07/01/2011
8	`netmdm_moni_dp_0007`	8	07/01/2011 ≤ *event-start-time* < 08/01/2011
9	`netmdm_moni_dp_0008`	9	08/01/2011 ≤ *event-start-time* < 09/01/2011
10	`netmdm_moni_dp_0009`	10	09/01/2011 ≤ *event-start-time* < 10/01/2011
11	`netmdm_moni_dp_0010`	11	10/01/2011 ≤ *event-start-time* < 11/01/2011
12	`netmdm_moni_dp_0011`	12	11/01/2011 ≤ *event-start-time* < 12/01/2011
13	`netmdm_moni_dp_0012`	13	12/01/2011 ≤ *event-start-time*

(3) Adding data partitions

Add data partitions by running the query scripts from *Table 7-10* using SQL Server Management Studio.

To add a data partition:

1. Stop the Remote Install Server service.
2. Execute `AddFilegroup2nd.sql` to add the filegroup to which the data partition will be assigned.
3. Create the folder `G:\NETMDP`.
4. Execute `AddFiletoGdrive.sql`, add an actual file to the `G` drive, and assign it to the filegroup.
5. Execute `AlterPartition.sql` to alter the partition function and partition scheme.#
6. Using SQL Server Management Studio, right-click on the target database name `NETMDM_SAMPLE` to display the menu, choose **Properties**, and confirm that **File** and **Filegroup** have been added as specified.

#

If history starting September 1, 2011 has already been stored, it may take some time to execute `AlterPartition.sql`.

7.6.3 Procedure for reassigning data partitions

If there is no disk available for a new partition, unneeded history must be deleted and an existing data partition must be reassigned. This subsection describes how to delete history up to March 2011 and reassign the data partitions to store history from January through March 2012.

(1) Creating query scripts for reassigning data partitions

In this subsection, we prepare query scripts for reassigning data partitions.

Table 7–13: Query scripts (for reassigning data partitions)

No.	Query script name	Description	Sample
1	`CreateArchTable.sql`	Creates a `netmdm_monitoring_security_arch` table for transferring deleted data. To create your own query script based on this sample, change the following item: • Database name in `USE` statement	*F.10*
2	`SwitchPartition.sql`	Switches history up to March 2011 from the `netmdm_monitoring_security` table to the `netmdm_monitoring_security_arch` table. To create your own query script based on this sample, change the following item: • Database name in `USE` statement	*F.11*
3	`DropArchTable.sql`	Deletes the `netmdm_monitoring_security_arch` table. To create your own query script based on this sample, change the following item: • Database name in `USE` statement	*F.12*
4	`MergeRange.sql`	Alters the partition function so that history up to March 2011 will be stored in `netmdm_moni_seg`. To create your own query script based on this sample, change the following items: • Database name in `USE` statement • *yyyymmdd* format value of `ALTER PARTITION FUNCTION`	*F.13*

No.	Query script name	Description	Sample
5	`AlterPartition2nd.sql`	Alters the partition function and partition scheme so that history from January through March 2012 will be stored in the existing filegroup from which history was just deleted. To create your own query script based on this sample, change the following items: • Database name in `USE` statement • *yyyymmdd* format value of `ALTER PARTITION FUNCTION`	*F.14*

Operation monitoring history can be stored as shown in the following table by executing the query scripts of *Table 7-13*, deleting old history, and altering the partition scheme and partition function.

Table 7–14: Operation monitoring history that is stored (for reassigning data partitions)

No.	Filegroup name	Partition number	Operation monitoring history that is stored
1	`netmdm_moni_seg`	1	*event-start-time* < 04/01/2011
2	`netmdm_moni_dp_0004`	2	04/01/2011 ≤ *event-start-time* < 05/01/2011
3	`netmdm_moni_dp_0005`	3	05/01/2011 ≤ *event-start-time* < 06/01/2011
4	`netmdm_moni_dp_0006`	4	06/01/2011 ≤ *event-start-time* < 07/01/2011
5	`netmdm_moni_dp_0007`	5	07/01/2011 ≤ *event-start-time* < 08/01/2011
6	`netmdm_moni_dp_0008`	6	08/01/2011 ≤ *event-start-time* < 09/01/2011
7	`netmdm_moni_dp_0009`	7	09/01/2011 ≤ *event-start-time* < 10/01/2011
8	`netmdm_moni_dp_0010`	8	10/01/2011 ≤ *event-start-time* < 11/01/2011
9	`netmdm_moni_dp_0011`	9	11/01/2011 ≤ *event-start-time* < 12/01/2011
10	`netmdm_moni_dp_0012`	10	12/01/2011 ≤ *event-start-time* < 01/01/2012
11	`netmdm_moni_dp_0001`	11	01/01/2012 ≤ *event-start-time* < 02/01/2012
12	`netmdm_moni_dp_0002`	12	02/01/2012 ≤ *event-start-time* < 03/01/2012
13	`netmdm_moni_dp_0003`	13	03/01/2012 ≤ *event-start-time*

(2) Reassigning data partitions

You can add data partitions by executing the query scripts from *Table 7-13* using SQL Server Management Studio.

To re-assign a data partition:

1. Stop the Remote Install Server service.
2. Execute `CreateArchTable.sql` to create the `netmdm_monitoring_security_arch` table for transferring deleted data.#
3. Execute `SwitchPartition.sql` to transfer history up to March 2011 from the `netmdm_monitoring_security` table to the `netmdm_monitoring_security_arch` table.#
4. Execute `DropArchTable.sql` to delete the `netmdm_monitoring_security_arch` table.#
5. Execute `MergeRange.sql` to alter the partition function so that history up to March 2011 is stored in `netmdm_moni_seg`.
6. Execute `AlterPartition2nd.sql` to alter the partition function and partition scheme so that history from January through March 2012 will be stored in the existing filegroup from which history was just deleted.

#

History can also be deleted using the `dcmmonrst` command, but deletion takes less time if it is transferred to the `netmdm_monitoring_security_arch` table and then deleted in table units.

7.6.4 For large users

This subsection describes storing information in a six-month database, assuming the following conditions:

- The number of client machines administered is 10,000.
- The number of operation monitoring history items acquired per client per day is 2,000.

In this case, the number of operating information items generated daily is 20 million. Since this represents a large user, we recommend that you create data partitions that can store a day's worth of information.

(1) Estimating the space required for the database

When creating a new JP1/Software Distribution database, you also need to include in the estimate the space required for devices other than software operation monitoring history database devices. For details, see *5.4.2 Estimating disk space required for Microsoft SQL Server* in the manual *Description and Planning Guide*. Estimate as indicated below the space required monthly for the software operation monitoring history database devices and for the software operation monitoring history data partitions that hold one month of data. Here we use 10 for the number of programs for which operating time is acquired.

To change existing JP1/Software Distribution databases to data partitions, also estimate the size of the monthly software operation monitoring history data partition.

Space required for software operation monitoring history database devices

software-operation-monitoring-history-database-device-space-required (bytes)

= (1,861#1 **x** *number-of-software-operation-monitoring-history-information-items*)#2

+ (80 **x** *number-of-acquired-operating-time-information-items*)#3

Software operation monitoring history data partition space required for one month

software-operation-monitoring-history-data-partition-space-required-for-one-month (bytes)

= (1,861 **x** *number-of-software-operation-monitoring-history-information-items*)#2

= 1,861 **x** 10,000 **x** 2,000 **x** 20

= approximately 800 GB

#1

To set the maximum value for operation history information size, specify 1,861 (bytes). To specify a more average software operation monitoring history size, specify 543 (bytes).

#2

number-of-software-operation-monitoring-history-information-items

= *number-of-client-machines-subject-to-software-operation-monitoring* (10,000)

x *number-of-operation-monitoring-history-items-acquired-per-client-daily* (2,000)

x *days-to-retain-operating-information* (as secondary area, 10 days)

#3

number-of-acquired-operating-time-information-items

= 220 **x** *number-of-clients* **x** *number-of-programs-subject-to-operating-time-acquisition* (10)

= 1,861 **x** 10,000 **x** 2,000 **x** 10 + 80 **x** 220 **x** 1,000 **x** 10

= approximately 400 GB

Therefore, when creating a new JP1/Software Distribution database, create a 400-GB software operation monitoring history database device as a secondary area with Database Manager and create six 800-GB software operation monitoring history data partitions for six months of data using SQL Server Management Studio.

To change a JP1/Software Distribution database to a data partition, use the existing software operation monitoring history database device as a secondary area and create six 800-GB software operation monitoring history data partition for six months of data using SQL Server Management Studio.

Here, we assume the following disks are available for creating the secondary area.

- Disk 1
  1,000 GB, `D:` drive, specified as a secondary area, created by Database Manager#
- Disk 2
  1,000 GB, `E:` drive, specified as an area for creating data partition for one month of data
- Disk 3
  1,000 GB, `F:` drive, specified as an area for creating data partition for one month of data
- Disk 4
  1,000 GB, `G:` drive, specified as an area for creating data partition for one month of data
- Disk 5
  1,000 GB, `H:` drive, specified as an area for creating data partition for one month of data
- Disk 6
  1,000 GB, `I:` drive, specified as an area for creating data partition for one month of data
- Disk 7
  1,000 GB, `J:` drive, specified as an area for creating data partition for one month of data

#

Used when creating a new database.

(2) Coding query scripts for creating data partitions

In this subsection, we prepare query scripts for creating the data partitions.

Table 7–15: Query scripts (for large user creating data partitions)

No.	Query script name	Description	Sample
1	`DropTable.sql`	Deletes an existing `netmdm_monitoring_security` table created by Database Manager. To create your own query script based on this sample, change the following item. • Database name in `USE` statement	*F.1*
2	`LargeAddFilegroup.sql`	Adds a filegroup to be assigned a data partition. To create your own query script based on this sample, change the following items. • Database name in `USE` statement • Database name in `ALTER DATABASE` statement	*F.15*
3	`LargeAddFile.sql`	Adds an actual file to each drive and assigns it to a filegroup. To create your own query script based on this sample, change the following items. • Database name in `USE` statement • Database name in `ALTER DATABASE` statement • `FILENAME` specification path in `ALTER DATABASE` statement • `SIZE` specification size in `ALTER DATABASE` statement	*F.16*
4	`LargeCreatePartition.sql`	Creates a partition function and partition scheme. To create your own query script based on this sample, change the following items. • Database name in `USE` statement • *yyyymmdd* format value of `CREATE PARTITION FUNCTION`	*F.17*

No.	Query script name	Description	Sample
5	`CreateTable.sql`	Creates a `netmdm_monitoring_security` table in the partition scheme. To create your own query script based on this sample, change the following item. • Database name in `USE` statement	*F.6*

The data partitions shown in *Tables 7-16* and *7-17* will be created when you execute the query scripts listed in *Table 7-15*.

Table 7–16: File and filegroups (for a large user creating data partitions)

No.	Logical name	File name	Initial size	Upper limit	Increase amount	Filegroup name
1	`NETMDM_MONI_DEVICE`	`D:\Program Files\Hitachi\NETMDB\MSSQL\MONITOR.sdf`	400,000 MB	`UNLIMITED`	10%	`netmdm_moni_seg`
2	`NETMDM_DP_0001`	`E:\NETMDP\MONITOR_DP_0001.ndf`	800 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0001`
3	`NETMDM_DP_0002`	`F:\NETMDP\MONITOR_DP_0002.ndf`	800 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0002`
4	`NETMDM_DP_0003`	`G:\NETMDP\MONITOR_DP_0003.ndf`	800 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0003`
5	`NETMDM_DP_0004`	`H:\NETMDP\MONITOR_DP_0004.ndf`	800 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0004`
6	`NETMDM_DP_0005`	`I:\NETMDP\MONITOR_DP_0005.ndf`	800 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0005`
7	`NETMDM_DP_0006`	`J:\NETMDP\MONITOR_DP_0006.ndf`	800 GB	`UNLIMITED`	10%	`netmdm_moni_dp_0006`

Table 7–17: Partition function and partition scheme (for a large user creating data partitions)

Partition function name	Partition scheme name
`netmdm_monitoring_security_pf`	`netmdm_monitoring_security_ps`

Operation monitoring histories are stored by this partition function and partition scheme for each day for the event start times as indicated in the following table.

Table 7–18: Operation monitoring history that is stored (for large user creating data partitions)

No.	Filegroup name	Partition number	Operation monitoring history that is stored
1	`netmdm_moni_seg`	1	*event-start-time* < 01/01/2011
2	`netmdm_moni_dp_0001`	2	01/01/2011 ≤ *event-start-time* < 01/02/2011
3		3	01/02/2011 ≤ *event-start-time* < 01/03/2011
4		4	01/03/2011 ≤ *event-start-time* < 01/04/2011
5		5 to 29	One day stored in each respective partition number
6		30	01/29/2011 ≤ *event-start-time* < 01/30/2011
7		31	01/30/2011 ≤ *event-start-time* < 01/31/2011
8		32	01/31/2011 ≤ *event-start-time* < 02/01/2011

No.	Filegroup name	Partition number	Operation monitoring history that is stored
9	`netmdm_moni_dp_0002`	33	02/01/2011 ≤ *event-start-time* < 02/02/2011
10		34 to 59	One day stored in each respective partition number
11		60	02/28/2011 ≤ *event-start-time* < 03/01/2011
12	`netmdm_moni_dp_0003`	61	03/01/2011 ≤ *event-start-time* < 03/02/2011
13		62 to 90	One day stored in each respective partition number
14		91	03/31/2011 ≤ *event-start-time* < 04/01/2011
15	`netmdm_moni_dp_0004`	92	04/01/2011 ≤ *event-start-time* < 04/02/2011
16		93 to 120	One day stored in each respective partition number
17		121	04/30/2011 ≤ *event-start-time* < 05/01/2011
18	`netmdm_moni_dp_0005`	122	05/01/2011 ≤ *event-start-time* < 05/02/2011
19		123 to 151	One day stored in each respective partition number
20		152	05/31/2011 ≤ *event-start-time* < 06/01/2011
21	`netmdm_moni_dp_0006`	153	06/01/2011 ≤ *event-start-time* < 06/02/2011
22		154 to 181	One day stored in each respective partition number
23		182	06/30/2011 ≤ *event-start-time*

(3) Creating or upgrading a JP1/Software Distribution database

For information about how to create a new JP1/Software Distribution database, see *7.5.1 Creating a new database*. When you create a new database, specify the initial size, upper limit, and increase amount from entry No. 1 of *Table 7-16* in the software operation monitoring history database file.

For information about changing an existing JP1/Software Distribution database to a data partition, see *7.5.4 Upgrading the database*.

(4) Creating data partitions

Create data partitions by running the query scripts from *Table 7-15* using SQL Server Management Studio.

To create a new JP1/Software Distribution data partition:

1. Execute `DropTable.sql` and delete the existing `netmdm_monitoring_security` table created by Database Manager.
2. Execute `LargeAddFilegroup.sql` to add the filegroup to which the data partition will be assigned.
3. Create a `NETMDP` folder on each drive.
4. Execute `LargeAddFile.sql` to add actual files on each drive and assign them to the filegroup.
5. Execute `LargeCreatePartition.sql` to create the partition function and partition scheme.
6. Execute `CreateTable.sql` to create the `netmdm_monitoring_security` table in the partition scheme.
7. Using SQL Server Management Studio, right-click the target database name `NETMDM_SAMPLE` to display the menu, choose **Properties**, and confirm that **File** and **Filegroup** are configured as specified. Also, right-click `NETMDM_SAMPLE` to open the menu, choose **Storage**, and confirm that `netmdm_monitoring_security_ps` (under **Partition scheme**) and `netmdm_monitoring_security_pf` (under **Partition function**) have been created.

To change an existing JP1/Software Distribution database into a data partition:

1. Stop Remote Install Server service.

2. Using the `bcp` utility, batch export the existing data from the `netmdm_monitoring_security` table.
3. Execute `DropTable.sql` and delete the `netmdm_monitoring_security` table.
4. Execute `LargeAddFilegroup.sql` to add the filegroup to which the data partition will be assigned.
5. Create a `NETMDP` folder on each drive.
6. Execute `LargeAddFile.sql`, add an actual file to the `E` drive, and assign it to the filegroup.
7. Execute `LargeCreatePartition.sql` to create the partition function and partition scheme.
8. Execute `CreateTable.sql` to create the `netmdm_monitoring_security` table in the partition scheme.
9. Using SQL Server Management Studio, right-click the target database name `NETMDM_SAMPLE` to display the menu, choose **Properties**, and confirm that **File** and **Filegroup** are configured as specified. Also right-click `NETMDM_SAMPLE` to open the menu, choose **Storage**, and confirm that `netmdm_monitoring_security_ps` (under **Partition scheme**) and `netmdm_monitoring_security_pf` (under **Partition function**) have been created.
10. Using the `bcp` utility, batch import the previously exported security data.

(5) Estimating the space required for the additional data partitions

History starting on July 1, 2011 would also be stored in the partition created for storing history for June 30, 2011 (partition No. 182). To avoid this, you must add one or more data partitions before storing of history starting on July 1, 2011 begins. This example shows how to add new data partitions for storing an additional month of data.

Here, we assume the following disk is available for the new data partitions.

- Disk 8
  1,000 GB, `K:` drive, specified as the area for creating data partition for one month of data

(6) Creating query scripts for adding data partitions

In this subsection, query scripts for adding data partitions are provided.

Table 7–19: Query scripts (for a large user adding data partitions)

No.	Query script name	Description	Sample
1	`LargeAddFilegroup2nd.sql`	Adds a filegroup to be assigned a data partition. To create your own query script based on this sample, change the following items: • Database name in `USE` statement • Database name in `ALTER DATABASE` statement	*F.18*
2	`LargeAddFiletoKdrive.sql`	Adds an actual file to the `K` drive and assigns it to a filegroup. To create your own query script based on this sample, change the following items: • Database name in `USE` statement • Database name in `ALTER DATABASE` statement • `FILENAME` specification path in `ALTER DATABASE` statement • `SIZE` specification size in `ALTER DATABASE` statement	*F.19*
3	`LargeAlterPartition.sql`	Alters the function and partition scheme so that history from July 2011 will be stored daily in the added filegroup. To create your own query script based on this sample, change the following items: • Database name in `USE` statement • *yyyymmdd* format value of `ALTER PARTITION FUNCTION`	*F.20*

The data partitions shown in *Table 7-20* will be added when you execute the query scripts shown above.

Table 7–20: File and filegroups (for a large user creating data partitions)

No.	Logical name	File name	Initial size	Upper limit	Increase amount	Filegroup name
1	NETMDM_DP_0007	K:\NETMDP \MONITOR_DP_0007.ndf	800 GB	UNLIMITED	10%	netmdm_moni_ dp_0007

Operation monitoring histories are stored by changing this partition function and partition scheme each month for event start times as shown in the following table.

Table 7–21: Operation monitoring history that is stored (for large user creating data partitions)

No.	Filegroup name	Partition number	Operation monitoring history that is stored
1	netmdm_moni_dp_0006	153	06/01/2011 ≤ *event-start-time* < 06/02/2011
2		182	06/30/2011 ≤ *event-start-time* < 07/01/2011
3	netmdm_moni_dp_0007	183	07/01/2011 ≤ *event-start-time* < 07/02/2011
4		213	07/31/2011 ≤ *event-start-time*

(7) Adding data partitions

Add data partitions by running the query scripts from *Table 7-19* using SQL Server Management Studio.

To add a data partition:

1. Stop the Remote Install Server service.
2. Execute `LargeAddFilegroup2nd.sql` to add the filegroup to which the data partition will be assigned.
3. Create the folder `K:\NETMDP`.
4. Execute `LargeAddFiletoKdrive.sql`, add an actual file to the `K` drive, and assign it to the filegroup.
5. Execute `LargeAlterPartition.sql` to alter the partition function and partition scheme.#
6. Using SQL Server Management Studio, right-click the target database name `NETMDM_SAMPLE` to display the menu, choose **Properties**, and confirm that **File** and **Filegroup** are configured as specified.

#

If history starting July 1, 2011 has already been stored, it may take some time to execute `LargeAlterPartition.sql`.

(8) Reassigning data partitions

Here, since we do not have enough disk space for a new partition, we need to delete history up to January 2011 and reassign the partitions to store history for August 2011.

(9) Creating query scripts for reassigning data partitions

In this subsection, we prepare query scripts for reassigning data partitions.

Table 7–22: Query scripts (for a large user reassigning data partitions)

No.	Query script name	Description	Sample
1	CreateArchTable.sql	Creates a `netmdm_monitoring_security_arch` table for transferring deleted data. To create your own query script based on this sample, change the following item: • Database name in `USE` statement	*F.10*

No.	Query script name	Description	Sample
2	`LargeSwitchPartition.sql`	Switches history up to January 2011 from the `netmdm_monitoring_security` table to the `netmdm_monitoring_security_arch` table. To create your own query script based on this sample, change the following item: • Database name in `USE` statement	*F.21*
3	`DropArchTable.sql`	Deletes the `netmdm_monitoring_security_arch` table. To create your own query script based on this sample, change the following item: • Database name in `USE` statement	*F.12*
4	`LargeMergeRange.sql`	Alters the partition function so that history up to January 2011 will be stored in `netmdm_moni_seg`. To create your own query script based on this sample, change the following items: • Database name in `USE` statement • *yyyymmdd* format value of `ALTER PARTITION FUNCTION`	*F.22*
5	`LargeAlterPartition2nd.sql`	Alters the partition function and partition scheme so that August 2011 history will be stored in the existing filegroup from which history was deleted. To create your own query script based on this sample, change the following items: • Database name in `USE` statement • *yyyymmdd* format value of `ALTER PARTITION FUNCTION`	*F.23*

Operation monitoring history will be stored as shown in the following table when you execute the query scripts in *Table 7-22*, deleting old history, and altering the partition scheme and partition function.

Table 7–23: Operation monitoring history that is stored (for a large user reassigning data partitions)

No.	Filegroup name	Partition number	Operation monitoring history that is stored
1	`netmdm_moni_seg`	1	*event-start-time* < 01/01/2011
2	`netmdm_moni_dp_0002`	2	02/01/2011 ≤ *event-start-time* < 02/02/2011
3		3 to 28	One day stored in each respective partition number
4		29	02/28/2011 ≤ *event-start-time* < 03/01/2011
5	`netmdm_moni_dp_0003`	30	03/01/2011 ≤ *event-start-time* < 03/02/2011
6		31 to 59	One day stored in each respective partition number
7		60	03/31/2011 ≤ *event-start-time* < 04/01/2011
8	`netmdm_moni_dp_0004`	61	04/01/2011 ≤ *event-start-time* < 04/02/2011
9		62 to 89	One day stored in each respective partition number
10		90	04/30/2011 ≤ *event-start-time* < 05/01/2011
11	`netmdm_moni_dp_0005`	91	05/01/2011 ≤ *event-start-time* < 05/02/2011
12		92 to 120	One day stored in each respective partition number
13		121	05/31/2011 ≤ *event-start-time* < 06/01/2011
14	`netmdm_moni_dp_0006`	122	06/01/2011 ≤ *event-start-time* < 06/02/2011

No.	Filegroup name	Partition number	Operation monitoring history that is stored
15	netmdm_moni_dp_0006	123 to 150	One day stored in each respective partition number
16		151	06/30/2011 ≤ *event-start-time* < 07/01/2011
17	netmdm_moni_dp_0007	152	07/01/2011 ≤ *event-start-time* < 07/02/2011
18		153 to 181	One day stored in each respective partition number
19		182	07/31/2011 ≤ *event-start-time* < 08/01/2011
20	netmdm_moni_dp_0001	183	08/01/2011 ≤ *event-start-time* < 08/02/2011
21		184 to 212	One day stored in each respective partition number
22		213	08/31/2011 ≤ *event-start-time*

(10) Reassigning data partitions

You can add data partitions by executing the query scripts shown in *Table 7-22* using SQL Server Management Studio.

To re-assign a data partition:

1. Stop the Remote Install Server service.
2. Execute `CreateArchTable.sql` to create the `netmdm_monitoring_security_arch` table for transferring deleted data.#
3. Execute `LargeSwitchPartition.sql` to transfer history up to January 2011 from the `netmdm_monitoring_security` table to the `netmdm_monitoring_security_arch` table.#
4. Execute `DropArchTable.sql` to delete the `netmdm_monitoring_security_arch` table.#
5. Execute `LargeMergeRange.sql` to alter the partition function so that history up to January 2011 is stored in `netmdm_moni_seg`.
6. Execute `LargeAlterPartition2nd.sql` to alter the partition function and partition scheme so that history for August 2011 will be stored in the existing filegroup from which history was deleted.

#

History can also be deleted using the `dcmmonrst` command, but deletion takes less time if it is transferred to the `netmdm_monitoring_security_arch` table and then deleted in table units.

8 Creating System Configuration Information and Destination Groups

This chapter explains how to create system configuration information, and how to create and manage destination groups.

8.1 Creating system configuration information

Before you can start using JP1/Software Distribution, you must create *system configuration information*, which is the information needed in order to manage the configuration of the relay managers/systems and clients. System configuration information defines the system configuration and the addresses of the hosts. You set the address of each host on the basis of the address selected using the node identification key (host name or IP address).

This section describes the procedures for creating system configuration information and how to assign host names, as well as how to create and change system configuration information.

8.1.1 Different methods for creating system configuration information

This subsection describes the different methods for creating system configuration information and provides guidelines for selecting the appropriate method.

(1) Creation methods

Four methods are available for creating the system configuration:

Creating system configuration information automatically

If you set up each of the managing server, relay systems, and clients to automatically apply the system configuration, the system configuration information is created automatically on the basis of the physical network configuration and is applied to the System Configuration window. When a client or relay system is added or removed or a host name or IP address is changed, this information is reported automatically to the managing server. Therefore, no actions are required at the managing server to maintain the system configuration information.

In addition, the facility for registering the system configuration automatically can be used to change ID groups as the system configuration changes. For details about the connections between the system configuration and ID groups, see *8.4 Linking system configuration information and ID group information*.

Use of the facility for registering the system configuration automatically is not recommended if there are firewalls in your network. If you upgrade an existing JP1/Software Distribution, the facility for registering the system configuration automatically changes the system configuration that was created under the previous version.

Creating system configuration information from a file

This method creates the system configuration information in a text file and enters it into the manager for remote installation. If you use the data in the `hosts` file, you can create the system configuration information file comparatively easily.

Once there are no more changes to be made to the system configuration, you should save the system configuration information file. In the event of a system error, you can use it to restore the system configuration information.

Creating system configuration information in the System Configuration window

With this method, you use a GUI screen of the Remote Installation Manager to define the host names or IP addresses of the individual clients and relay systems.

Acquiring system configuration information about the hosts under each relay manager

In a system with a hierarchy of managing servers, in order to manage the system configuration information for the entire system from the central manager, you must use the following procedure to acquire system configuration information about the hosts under the relay managers:

1. Create system configuration information for each relay manager.
2. Execute from the central manager a *Get system configuration information* job with each relay manager specified as a destination.

   The system configuration information about the entire system is acquired at the central manager.

Once you have collected the system configuration information for the entire system, you can use the facility for registering the system configuration automatically to maintain it. When the system configuration is changed under a relay manager, the change details are sent automatically from the relay manager to the central manager.

If you use one of the following methods to change the system configuration on the relay manager, the change details are not sent automatically from the relay manager to the central manager. In this case, execute a *Get system configuration information* job for the relay manager.

- Create the system configuration from a file
- Create the system configuration from the System Configuration window
- Manually maintain the system configuation
- Automatically maintain the system configuration

In a large-scale system that has three or more hierarchical levels, if you change a connection-target relay manager or relay system, the information on the hierarchical node tree below the relay manager or relay system you moved may not be applied to the new managing server. If the information is not applied, you must execute the *Get system configuration information* job for the relay manager or relay system at the new managing server.

(2) Guidelines for selecting the creation method

You should use the System Configuration window to create the system configuration for a small-scale system or to make minor changes to an existing system configuration.

The method that automatically creates the system configuration information simplifies maintenance of the system configuration information, because it automatically sends any update information to the managing server whenever a host is added or removed, or a host name or IP address is changed. However, in the following cases, it is better to create the system configuration information from a file, rather than using the facility for registering the system configuration automatically:

- The effective duration of IP addresses is short, and DHCP and WINS are used.
- The communication volume of the system configuration information will overload the network.
  Sending system configuration information to the managing server requires the following communication volume:
  Single communication volume (in bytes) for each distribution-destination system
  = (300 + (a - 1) **x** 50) **x** (a - 1)
  a: Number of relay systems through which a job passes before reaching the distribution-destination system + 2

You specify use of the facility for registering the system configuration automatically during setup. When a new Software Distribution is installed or an existing system is migrated from Software Distribution Version 3.0, the default setting specifies that the facility for registering the system configuration automatically is to be used.

8.1.2 Assigning host names in a JP1/Software Distribution system

This subsection describes how to assign host names.

(1) Assigning host names

A host name can consist of up to 64 bytes. However, if Embedded RDB is used in the JP1/Software Distribution Manager (central manager and relay manager), a host name can consist of a maximum of 32 bytes.

A specified host name must satisfy the following conditions:

- Only alphabetic characters (A-Z, a-z), numeric digits (0-9), the minus sign (-), and the period (.) may be used.
- The period (.) may be used only as a domain name delimiter.
- If DNS is used, a host name must be in the format *host-name*`.`*domain-name*, and the length including the domain name length cannot exceed 64 bytes.
- The first character of a host name must be an alphabetic character.
- Spaces cannot be used.
- Because host names are not case-sensitive, a name that duplicates another name when uppercase letters are changed to lowercase (or vice versa) cannot be used.
- A host name cannot end with a minus sign (-) or a period (.).
- Aliases that are defined in a `hosts` file cannot be used as host names.
- In a system that uses host names as the node identification key, all hosts that use JP1/Software Distribution must be assigned unique host names.
- `localhost` cannot be used as a host name.

- For Windows 95 clients, the underscore (_) cannot be used as part of a host name.

The combined total length of all the host names in the system, from highest to lowest (including delimiters between host names), cannot exceed 255 characters. Because some systems, such as UNIX systems, require case-sensitivity, you should use only uppercase or only lowercase letters for host names in a network that uses JP1/Software Distribution.

(2) Software Distribution systems that do not allow 64 bytes for a host name

The following Software Distribution systems do not allow 64 bytes for a host name:

Managing servers

- Software Distribution Manager 03-20 and earlier
- Software Distribution 01-00

Relay systems

- Software Distribution SubManager 03-20 and earlier
- Software Distribution/W-AF 01-08 and earlier
- Software Distribution/W 01-13 and earlier
- Software Distribution/W Version 3.0 03-00

Clients

- Software Distribution Client 03-20 and earlier
- Software Distribution/W 01-13 and earlier
- Software Distribution/W Version 3.0 03-00

(3) Coexisting with systems that do not allow 64 bytes for a host name

If your configuration includes a system that does not allow 64 bytes for the host name, you must observe the following conditions in specifying host names:

- No host name may exceed 32 bytes in length.
- The combined total length of all host names in the system, from highest (managing server) to lowest, must not exceed 64 bytes.

If any lower relay system contains a Software Distribution system that does not allow a 64-byte host name, you must specify the host name of its higher relay system or managing server with no more than 32 bytes.

8.1.3 Creating the system configuration information automatically

This subsection explains how to use the *facility for automatically registering the system configuration* in order to create the system configuration information automatically. When a relay system or client is set up, this facility automatically reports and registers the system configuration information to the higher system.

(1) TCP/IP environment settings for registering system configuration information automatically

To set a managing server for specification of host names, you must first define the managing server in the TCP/IP definition database. A relay system must have definitions of the lower hosts in the TCP/IP definition database.

(2) Registering the system configuration information automatically

You specify the settings explained below during setup. When you complete the setup, the system configuration information for relay systems and clients is reported automatically to the higher system.

Managing server

On the **System Configuration** page, select the **Apply the system configuration information automatically** check box.

Relay system

On the **System Configuration** page, select **Apply the system configuration information automatically**. To change ID group information on the basis of changes in the system configuration, select the **Link with system configuration modifications** check box under **Linkage when system configuration is changed**.

Client

On the **Connection Destination** page, select the **Automatically register this computer in the system configuration** check box.

The facility for automatic registration of the system configuration enables you to change clients' connection destination from the managing server and apply the change to the system configuration information automatically.

To do this:

1. Specify the following settings during setup:

   Managing server

   On the **System Configuration** page, select the following check boxes:

   - **Apply the system configuration information automatically**

   - **Link with system configuration modifications**

   Relay system

   On the **System Configuration** page, select the following check boxes:

   - **Apply the system configuration information automatically**

   - **Link with system configuration modifications**

   Client

   On the **Connection Destination** page, select the following check boxes:

   - **Automatically specify the higher system that requested a job execution as the connection destination**

   - **Automatically register this computer in the system configuration**

2. Change the connection destination of the desired client to the new relay system, and then execute the job.

   Do not move the client in the System Configuration window prior to job execution. The client's connection destination is changed when the job executes; however, information about this client remains in the relay system that had been set before the change as the connection destination.

(3) Notes on registering system configuration information automatically

You should note the following points abut registering the system configuration information automatically.

(a) If host IDs are used

If you are newly using host IDs as the ID key for operations, you must execute system version upgrades from the higher system.

If you mistakenly delete system configuration information on the higher system, or if the database is damaged, recover the information from a backup or have the lower systems report their system configuration information files again.

(b) Handling host ID management file errors

If an error occurs in the host ID management file of a client, recover the file by executing the following procedure from the higher system:

1. In the System Configuration or Destination window of the Remote Installation Manager, choose **File** and then **Save to File** to output the system configuration information file.

2. Using the host name or IP address of the client in which the error occurred as a key, search the host group file and identify the client in which the error occurred.

   If you use host names as the node identification key, use a host name as the key for searching; if you use IP addresses as the node identification key, use an IP address as the key for searching.

3. Save the information about the client in which the error occurred as a host ID management file.

   Set the file name of the host ID management file in `netmdmp.hid`. The file format of the host ID management file is the same as the file format when you create the system configuration information from a file or create a host group from a file. For details about the file format of the system configuration information file, see *8.1.4 Creating the system configuration information from a file*. For details about the file format of the host group file, see *8.2.3 Creating a host group from a file*.
4. Transfer the created host ID management file to the client in which the error occurred, and restore the file.

   Create the host ID management file in the operating system installation directory.
5. Restart the client.

When you create the host ID management file from the host group file, do not mistakenly create the destination of another client as the host ID management file, or change the destination information that was copied from the host group file using a cut-and-paste operation. If you do, the consistency of the host IDs in the system will be lost, and system operation cannot be guaranteed.

(c) If a host name is duplicated when host IDs are not used

If you use host names instead of host IDs as the node identification key, you must assign unique host names to the hosts that use JP1/Software Distribution. If the system configuration information is reported automatically and a host name is duplicated, the system displays log information. Check the log information, and set up the TCP/IP environment again in the client that has the duplicate host name.

- Log information storage location

  The log information is stored in the following directories:

  For a managing server

  installation-directory-of-JP1/Software-Distribution-Manager`\LOG\NODE.LOG`

  For a relay system

  JP1/Software-Distribution-Client-(relay-system)-installation-directory`\LOG\NODE.LOG`
- Log information contents

  `WARNING: The host name (`*host-name*`) already exists. Processing will continue.`

  This message indicates that the client reported information about a host that has the same host name and IP address as another node that is registered in the system configuration information of the managing server (or relay system).

  `WARNING: A host with the host name (`*host-name*`) already exists, but the existing host has a different IP Address. Processing will continue.`

  This message indicates that the client reported information about a host that has the same host name but a different IP address as another node that is registered in the system configuration information of the managing server (or relay system).
- Corrective action

  Check the TCP/IP environment settings of the host that was reported in the log information. If the host name is duplicated, change the host name. After changing the host name, execute client setup again.

(d) Notes on building the system

- If the system configuration information of a relay system has not been registered, the configuration information of a lower system may be deleted when the lower system reports system configuration information. Therefore, when upgrading to a higher version of JP1/Software Distribution, upgrade the system components in the following sequence: managing servers, relay systems, and then clients.
- When the facility for automatically registering the system configuration is used, do not modify the system configuration information at the managing server. If the system configuration information has been created by using automatic registration of the system configuration, terminate the setup of JP1/Software Distribution Manager (relay manager) and JP1/Software Distribution Client (relay system) and then apply their system configuration information to the system configuration information of JP1/Software Distribution Manager.

  You must set up JP1/Software Distribution Client (client) when the system configuration information of JP1/Software Distribution Manager (relay manager) and JP1/Software Distribution Client (relay system) has already been applied to JP1/Software Distribution Manager. If the system configuration information has not been applied correctly, use JP1/Software Distribution Manager (central manager) to execute a *Get system configuration information* job.

(e) Notes on editing system configuration information

When system configuration information is registered automatically, do not edit it in the managing server. If editing is necessary, at the Remote Installation Manager, save the system configuration information to a file, back up the file, and then edit the information.

In particular, if you delete a relay system in the system configuration information, the information for the clients that are connected to that relay system will also be deleted. Even if a client whose system configuration information was deleted reports the information again, it will not be recorded in the managing server.

For details about how to output system configuration information to a file and how to create it from a file, see *8.1.4 Creating the system configuration information from a file*.

(f) Deleting a destination that was added incorrectly in a relay system

In an environment where the system configuration information is registered automatically, if you add a destination at a relay system by mistake, use the following procedure to delete the destination.

To delete a destination:

1. Choose **Start**, and then **Client Manager**. In the displayed Software Distribution - Client Manager dialog box, click the **Stop** button.
2. At relay system setup, on the **System Configuration** page, clear the **Apply the system configuration information automatically** check box.
3. Exit relay system setup.
4. In the Software Distribution - Client Manager dialog box, click the **Start** button.
5. Start the Remote Installation Manager, and delete the destination that you added incorrectly.
6. Stop the Remote Installation Manager, and in the Software Distribution - Client Manager dialog box, click the **Stop** button.
7. At relay system setup, on the **System Configuration** page, select the **Apply the system configuration information automatically** check box.
8. Exit relay system setup.
9. In the Software Distribution - Client Manager dialog box, click the **Start** button.

8.1.4 Creating the system configuration information from a file

You can create system configuration information from a file in which system configuration information has been set. You can also output system configuration information to a file.

To obtain a backup of the system configuration information, output the system configuration information to a file. To restore the system configuration information, create the system configuration information from the output file.

This subsection describes how to create a system configuration information file, how to create the system configuration information from a file, and how to output the system configuration information to a file.

(1) Creating the system configuration information file

The system configuration information file specifies the IP address, host name, host type, creation date/time, comment, and path for each host. Note that the creation date/time can be set only for JP1/Software Distribution Manager.

This is a text file, in which a line whose first column is a single quotation mark (`'`) or a pound sign (`#`) is assumed to be a comment line.

Format

```
IP-address host-name HID=host-ID,TYPE=host-type,MAC=MAC-
address,COMMENT=comment, ROOT=path,DATE=creation-date-and-time
```

Description

You can specify the operands after *IP-address* in any order.

IP-address (required)

Specify the IP address of the host.

Although JP1/Software Distribution Manager does not manage the specified IP address, you must specify this operand so that the file format matches the format of the `hosts` file of TCP/IP.

You can also directly enter the `hosts` file of TCP/IP as the system configuration information file. In such a case, the system sets all hosts as clients.

You can create a simpler system configuration information file by adding a host type (`TYPE`), a comment (`COMMENT`), and a path (`ROOT`), based on the `hosts` file of TCP/IP.

host-name (required)

For details about how to specify the host name, see *8.1.2 Assigning host names in a JP1/Software Distribution system*.

`HID=`*host-ID*

Specify a host ID that uniquely identifies the host. If you chose **File** and then **Save to File** in the System Configuration window to save the system configuration information to a file and a host ID was set, be sure to specify that host ID. If a host ID was not set in the system configuration information file that you produced using **Save to File**, or if you are adding a new host, do not specify this operand.

`TYPE=`*host-type*

Specify `MASTER` (relay system or offline folder) or `CLIENT` (client or offline machine) as the host type. If you omit this operand, the system sets `CLIENT` as the default.

If you are using both the `hosts` file of TCP/IP and a system configuration information file, specify `#` and a space before `TYPE`. In the `hosts` file of TCP/IP, the text after `#` is treated as a comment.

`MAC=`*MAC-address*

Specify the MAC address of the host. Basically, do not change this operand because MAC addresses are related to facilities such as Wake on LAN. If you change the operand, the related facilities may not function.

`COMMENT=`*comment*

Specify a comment. You cannot use commas in the comment. The comment text string can have up to 64 bytes.

`ROOT=`*path*

If the host is connected through multiple relay systems, specify the full path from the highest relay system to the lowest relay system, expressed as host names, IP addresses, or host IDs. If the host is connected through two or more relay systems, separate the relay systems with `\` or `!`. If the host is connected directly to JP1/Software Distribution Manager, you can omit this operand.

`DATE=`*creation-date-and-time*

Specify the date and time when you register (or registered) the host with the central manager or relay manager for the first time. Specify the date and time in *MM*`/`*DD*`/`*YYYY*`/`*hh*`/`*mm*`/`*ss* format (where *MM* is the month, *DD* is the day, *YYYY* is the year, *hh* is the hour, *mm* is the minute, and *ss* is the second). In *YYYY*, you can specify 1971 to 2037. In *hh*, you can specify 0 to 23.

If you omit this operand, the date and time when **Create from File** was executed is set.

(2) Creating the system configuration information from a file

To create the system configuration information from a file:

1. In the System Configuration window, choose **File**, and then **Create from File**.
   The dialog box for selecting a file appears.
2. Select the system configuration information file that was created, and click the **OK** button.
   The system creates the system configuration information from the system configuration information that was set in the file.

You should note the following points when you create the system configuration information from a file:

- If the system configuration information was created previously, the contents of the System Configuration window are replaced with the contents set in the file. A host is deleted from the system configuration information if it is in the existing system configuration information, but not in the file. When a host is deleted, its inventory information remains in the database. You can use Database Manager to delete the inventory information for such deleted hosts. For details about how to delete the inventory information, see *7.5.6 Deleting unneeded inventory information from the database*.
- The existing contents of the Destination window are deleted, except the ID group information.
- If the existing contents of the System Configuration window contain a host ID specification, be sure to set that host ID.
- If you are using the host ID, an illegal root error may occur when the facility for automatically registering the system configuration starts processing during creation of the system configuration information from the file. Wait several moments and then start again.

(3) Saving the system configuration information to a file

You can save the system configuration information displayed in the System Configuration window to a file. This feature is helpful when you need to change the system configuration information, because you simply save the current system configuration information to a file and then edit that file.

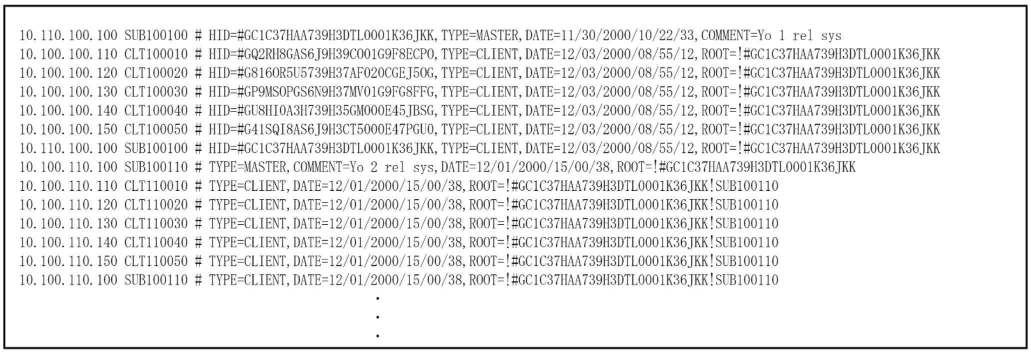
If managing servers are configured in a hierarchy, the file output at the central manager does not include system configuration information about hosts under the relay managers. To obtain system configuration information about hosts under the relay managers, you must output that system configuration information to a file at each relay manager.

To save the system configuration information to a file:

1. In the System Configuration window, choose **File**, and then **Save to File**.
   The Save System Configuration dialog box appears. Before you perform this operation, choose **Refresh** to update the system configuration information. If you do not manually update the system configuration information, the displayed information may differ from the latest internal data.
2. Specify the file name, and click the **OK** button.
   The system configuration information is saved to the file.

An output example of the system configuration information file is shown below:

Figure 8–1: Output example of the system configuration information file



```
10.110.100.100 SUB100100 # HID=#GC1C37HAA739H3DTL0001K36JKK,TYPE=MASTER,DATE=11/30/2000/10/22/33,COMMENT=Yo 1 rel sys
10.100.100.110 CLT100010 # HID=#GQ2RH8GAS6J9H39C001G9F8ECPO,TYPE=CLIENT,DATE=12/03/2000/08/55/12,ROOT=!#GC1C37HAA739H3DTL0001K36JKK
10.100.100.120 CLT100020 # HID=#G8160R5U5739H37AF020CGEJ50G,TYPE=CLIENT,DATE=12/03/2000/08/55/12,ROOT=!#GC1C37HAA739H3DTL0001K36JKK
10.100.100.130 CLT100030 # HID=#GP9MSOPGS6N9H37MV01G9FG8FFG,TYPE=CLIENT,DATE=12/03/2000/08/55/12,ROOT=!#GC1C37HAA739H3DTL0001K36JKK
10.100.100.140 CLT100040 # HID=#GU8HI0A3H739H35GM000E45JBSG,TYPE=CLIENT,DATE=12/03/2000/08/55/12,ROOT=!#GC1C37HAA739H3DTL0001K36JKK
10.100.100.150 CLT100050 # HID=#G41SQI8AS6J9H3CT5000E47PGU0,TYPE=CLIENT,DATE=12/03/2000/08/55/12,ROOT=!#GC1C37HAA739H3DTL0001K36JKK
10.110.100.100 SUB100100 # HID=#GC1C37HAA739H3DTL0001K36JKK,TYPE=CLIENT,DATE=12/03/2000/08/55/12,ROOT=!#GC1C37HAA739H3DTL0001K36JKK
10.100.110.100 SUB100110 # TYPE=MASTER,COMMENT=Yo 2 rel sys,DATE=12/01/2000/15/00/38,ROOT=!#GC1C37HAA739H3DTL0001K36JKK
10.100.110.110 CLT110010 # TYPE=CLIENT,DATE=12/01/2000/15/00/38,ROOT=!#GC1C37HAA739H3DTL0001K36JKK!SUB100110
10.100.110.120 CLT110020 # TYPE=CLIENT,DATE=12/01/2000/15/00/38,ROOT=!#GC1C37HAA739H3DTL0001K36JKK!SUB100110
10.100.110.130 CLT110030 # TYPE=CLIENT,DATE=12/01/2000/15/00/38,ROOT=!#GC1C37HAA739H3DTL0001K36JKK!SUB100110
10.100.110.140 CLT110040 # TYPE=CLIENT,DATE=12/01/2000/15/00/38,ROOT=!#GC1C37HAA739H3DTL0001K36JKK!SUB100110
10.100.110.150 CLT110050 # TYPE=CLIENT,DATE=12/01/2000/15/00/38,ROOT=!#GC1C37HAA739H3DTL0001K36JKK!SUB100110
10.100.110.100 SUB100110 # TYPE=CLIENT,DATE=12/01/2000/15/00/38,ROOT=!#GC1C37HAA739H3DTL0001K36JKK!SUB100110
                                                 .
                                                 .
                                                 .
```

Lines 1 - 7: Machines that correspond to the host ID

Lines 8 - end: Machines that do not correspond to the host ID

Note that if you save the system configuration to a file, an IP address is replaced with `xxx.xxx.xxx.xxx`. To use IP addresses to manage hosts using the created file, you must edit the IP addresses with a tool such as a text editor.

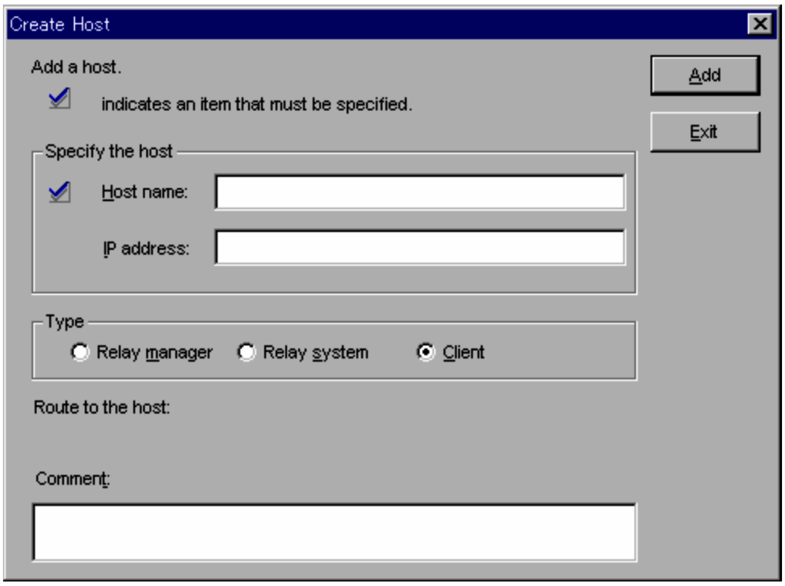
8.1.5 Creating system configuration information in the System Configuration window

This subsection describes how to define a host in the System Configuration window.

To define a host in the System Configuration window:

1. Open the System Configuration window, and select the position where the host is to be set.
   The system will set the host at the location you select.
2. Choose **File**, and then **Create Host**.
   The Create Host dialog box appears.

   Figure 8–2: Create Host dialog box



Create Host

Add a host.

✓ indicates an item that must be specified.

Type: ○ Relay manager ○ Relay system ● Client

Specify the host

Specify the host name or the IP address. If the host is a relay manager, you must specify the host name.

For details about specifying the host name, see *8.1.2 Assigning host names in a JP1/Software Distribution system*.

Type

Select **Relay manager**, **Relay system**, or **Client** as the host type. The default is **Client**.

Comment

You can specify any comment, as up to 64 bytes.

3. After specifying the items, click the **Exit** button.
   The host is defined. To add another host, click the **Add** button instead of **Exit**.

! Important note

When you manage an offline machine's inventory and operating information, an offline folder named `{OFFLINE}` is created automatically in the System Configuration window. However, do not add any hosts to the offline folder in the Create Host dialog box.

8.1.6 Getting system configuration information about hosts under relay managers

In systems with a hierarchy of managing servers, the central manager cannot create or change the system configuration information under the relay managers. You execute a *Get system configuration information* job to obtain system configuration information that the relay managers are managing, and then you can add that information to the system configuration information of the central manager. Although you can use the facility for automatically registering the system configuration, you must set up the higher systems before the lower systems to use that facility. If you are unable to follow that setup sequence (for example, when you are installing the system or making major changes to the system configuration information), you execute a *Get system configuration information* job to get the information.

Once you have obtained the system configuration information under the central manager, use the facility for automatically registering the system configuration when you need to maintain the information. If the system configuration information under a relay manager changes, that relay manager reports the changes automatically, and the information is applied to the system configuration information in the central manager.

In a large-scale system that has more than two hierarchical levels, if you move a relay manager or relay system so that is under a different higher node, it may not be possible to apply to the new managing server the information on the hierarchical node tree from the relay manager/system you moved. If the information is not applied, execute a *Get system configuration information* job on the relay manager/system at the new managing server.

(1) How to execute a Get system configuration information job

(a) Creating and executing the job

The procedure for creating a *Get system configuration information* job is described below. For details about executing the job and the job settings, see *8.2 Creating a job* in the manual *Administrator's Guide Volume 1*.

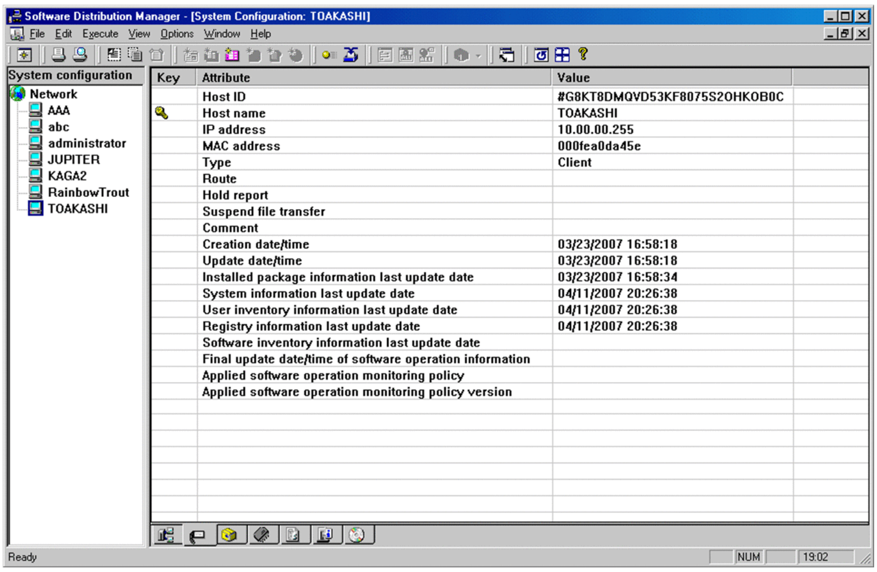
To create and execute the job:

1. In the Destination or System Configuration window, choose **Execute**, and then **Execute Job**. Alternatively, in the Job Definition window, choose **File**, and then **Create Job**.
   The Define New Job dialog box appears.
2. In the Define New Job dialog box, select the job type (**Get system configuration information**), and click the **OK** button.
   The Create Job dialog box appears.
3. Specify the items on each page.
   The pages displayed in the Create Job dialog box and their settings are described below.
   Job page
   Specify the job name.
   Destination page
   Specify the relay manager from which system configuration information is to be obtained. Specify the relay manager or the host group of the relay manager.
   Schedule page
   Specify the registration date/time, execution date/time, and execution time limit of the job.
4. Choose the **Execute**, **Save**, or **Save & Execute** button.
   The system saves and/or executes the job.

(b) Checking the execution results

When you execute the job, information on the system configurations under the relay managers is applied to the System Configuration window of the central manager.

Figure 8–3: System Configuration window



Key	Attribute	Value
	Host ID	#G8KT8DMQVD53KF8075S2OHKOB0C
🔑	Host name	TOAKASHI
	IP address	10.00.00.255
	MAC address	000fea0da45e
	Type	Client
	Route	
	Hold report	
	Suspend file transfer	
	Comment	
	Creation date/time	03/23/2007 16:58:18
	Update date/time	03/23/2007 16:58:18
	Installed package information last update date	03/23/2007 16:58:34
	System information last update date	04/11/2007 20:26:38
	User inventory information last update date	04/11/2007 20:26:38
	Registry information last update date	04/11/2007 20:26:38
	Software inventory information last update date	
	Final update date/time of software operation information	
	Applied software operation monitoring policy	
	Applied software operation monitoring policy version	

(c) Notes on job execution

When you execute a *Get system configuration information* job, in addition to the system configuration information being applied in the System Configuration window, the host group information for hosts under the relay manager is also applied in the Destination window at the central manager. The ID group information for hosts under the relay manager, however, is not applied in the Destination window at the central manager even if the system configuration information and ID group information are linked.

(2) Setting the facility for automatically registering the system configuration

If you specify the following settings in the central manager, the system configuration information managed by relay managers is reported automatically to the central manager and applied to the system configuration information in the central manager.

Settings

On the **System Configuration** page, select the **Apply the system configuration information automatically** check box. This check box is selected in the default setting, so you must first clear it and then select it after the central manager retrieves the system configuration information under the relay managers.

! Important note

If you specify use of the facility for automatically registering the system configuration, in addition to the system configuration information being applied in the System Configuration window, the host group information for hosts under the relay manager is also applied in the Destination window at the central manager. The ID group information for hosts under the relay manager, however, is not applied in the Destination window at the central manager. To apply the ID group information, you must set the linkage between the system configuration information and the ID group information. For details, see *8.4 Linking system configuration information and ID group information*.

8.1.7 Changing system configuration information

If you use the facility for automatically registering the system configuration, when you add or delete a relay system or a client, the modified information is reported automatically to the managing server. The reported information is then applied automatically to the System Configuration window. If you do not use the facility for automatically registering the system configuration, you should perform operations at the managing server to modify the system configuration information when the configuration changes. This subsection explains how to change system configuration information by performing operations from the managing server.

If you are changing the host name of the managing server or relay system (or IP address if IP addresses are used in your operation), you must either complete or delete all the jobs beforehand. Make sure that all periodic jobs have been deleted.

(1) Changing the system configuration information from a file

Save the current system configuration information to a file. Make the necessary changes, and then create the new system configuration information from the modified file.

Even when you change only part of the system configuration, make sure that you specify in the file all the hosts that are to be retained in the system configuration. Any host that is not in the file will be deleted from the system configuration.

If you are deleting a host, also be sure to delete information about that host from the file.

For details about saving the system configuration information to a file and creating the system configuration information from a file, see *8.1.4 Creating the system configuration information from a file*.

(2) Changing the system configuration information in the System Configuration window

The following explains how to change the system configuration information in the System Configuration window. For details about finding the host to be modified in or deleted from the configuration information, see *9.1.1 Finding hosts by name*.

(a) Moving a host

If you move a relay system, all the hosts subordinate to that relay system are also moved. To move more than one host at one time, on the right pane of the System Configuration window, select the hosts you want to move.

To move a host:

1. Open the System Configuration window, and select the host to be moved.
   The selected host is highlighted.
2. Choose **Edit**, and then **Cut**.
   The selected host is deleted. Once you have chosen **Cut**, do not double-click *Network* in the left-hand frame. If you double-click *Network*, **Paste** is disabled in the **Edit** menu and you will not be able to paste the host. If this has happened, choose **Cut** again.
3. Select the destination for the move operation.
   The selected location is highlighted.
4. Choose **Edit**, and then **Paste**.
   The selected host is moved to the new location.
   You can also use drag-and-drop to move a host.

(b) Deleting a host

Once you delete a host, you cannot restore it to its previous status. If you delete a relay system, the system also deletes all lower relay systems and clients. To delete multiple hosts at the same time, select the hosts in the right pane of the System Configuration window. When you delete a host in the System Configuration window, the system simultaneously deletes the host of the same name in the Destination window.

When you delete a relay system that has lower hosts, deleting inventory in the Delete Host dialog box will not delete the information for the lower hosts.

When a host is to be deleted from the System Configuration window, the Delete Host dialog box is displayed. The following describes the items displayed in the Delete Host dialog box.

The related inventory information will also be deleted check box

If this check box is selected, the system information, software information, and user inventory that are related to the host to be deleted are also deleted.

If you do not select to delete the inventory, the inventory for that host remains as is in the database, reducing the available database space by its size. We recommend that you delete all inventory related to the host being deleted, if possible.

You can use Database Manager to delete unneeded inventory information. For details about how to delete inventory information using Database Manager, see *7.5.6 Deleting unneeded inventory information from the database*.

Delete a host from the registered IDs check box

This check box is enabled when the **The related inventory information will also be deleted** check box is selected. If the **Delete a host from the registered IDs** check box is selected in such a case, the target host is also deleted from the registered ID group. Note that a relay manager/system cannot be deleted from the registered ID group.

To delete a host:

1. Open the System Configuration window, and select the host to be deleted.
   The selected host is highlighted.
2. Choose **Edit**, and then **Delete**.
   A configuration dialog box appears.
3. Click the **OK** button.
   The selected host is deleted.

After finding hosts with the Find dialog box, you can delete the hosts. For details about deleting hosts you found with the Find dialog box, see *9.1.5 Deleting a host from the system configuration information*.

(c) Changing a host name or an IP address

If you change a host name or an IP address, the modified information is reported automatically to the managing server. The reported information is then applied automatically to the System Configuration window. The procedure for changing a previously set host name or IP address from the System Configuration window is described below.

If you rename a host in the System Configuration window, the same host is also renamed in the Destination window. The host name for displaying inventory information is also changed.

To rename a host:

1. In the System Configuration window, select the host whose name is to be changed.
   The selected host is highlighted.
2. Choose **File**, and then **Rename**.
   The Rename dialog box appears.
3. Specify the new name, and then click the **OK** button.
   The system changes the host name to the name you specified.

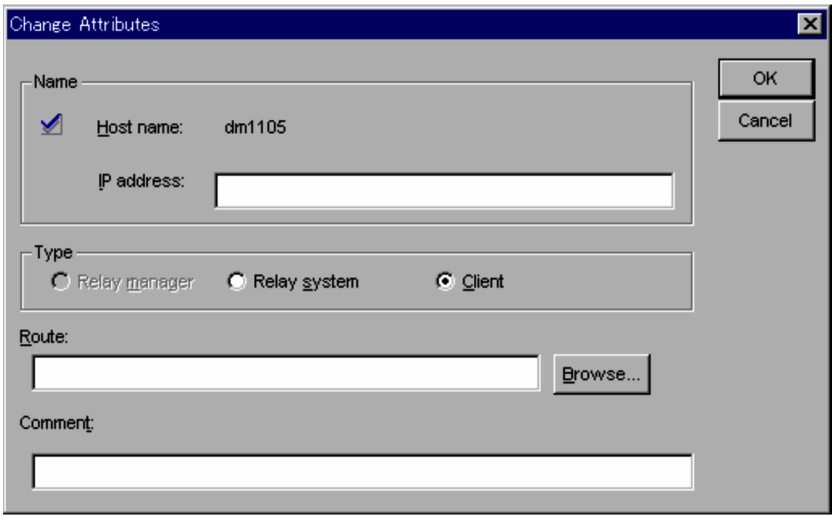
(d) Changing the attributes of a host

If you want to change a relay system to a client (or a client to a relay system) or if you want to change a path or comment, use the Change Attributes dialog box, which can be opened by choosing **File** and then **Change Attributes**.

The following notes apply to changing the host type:

- When you change the host attribute in the System Configuration window, the system also changes the attribute of the same host found in the Destination window.
- You cannot change the host type of a relay manager. For a relay manager, you can change only the IP address and the comment.

Figure 8–4: Change Attributes dialog box



Change Attributes

Name

☑ Host name: dm1105

IP address:

Type

○ Relay manager ○ Relay system ● Client

Route:

Comment:

Host name

Displays the host name.

IP address

Displays the IP address.

Type

Select either relay system or client as the type of host. If you change the host type from relay system to client, all hosts that were defined under the relay system before the change are deleted.

Route

Specify the route by separating each host name with the exclamation point (!) delimiter. If the specified route does not exist, an error results and the route is not changed.

Browse button

Displays the Set Path dialog box in which you can select a path from the system configuration.

Comment

Enter a desired comment, as 1-64 bytes.

(3) Changing the system configuration information under a relay manager

You cannot change the system configuration information under a relay manager from the central manager. If a user changes the system configuration information under a relay manager, use the facility for automatically registering the system configuration or execute a *Get system configuration information* job from the central manager to apply the modified information to the system configuration information in the central manager.

However, you can use the System Configuration window of the central manager to change the comment for a host under a relay manager.

In a large-scale system that has more that two hierarchical levels, if you move a relay manager or relay system so that it is below a different higher node, it may not be possible to apply to the new managing server the hierarchical node tree information below the relay manager/system you moved. If the information is not applied, execute a *Get system configuration information* job for the relay manager/system at the new managing server.

(4) Notes on changing the system configuration information

You should note the following points about changing system configuration information.

- If you change the node identification key

  Before changing the node identification key, delete the system configuration information from Remote Installation Manager. We recommend that you save the system configuration information to a file. Then, after you change the node identification key, you can use the file to set the system configuration information.

If you create the system configuration information manually without using a facility for registering the system configuration automatically, the obtained system configuration information file contains the address of each host specified using the current node identification key. You must therefore specify the host name or IP address of each host in the saved file. For example, if you change the node identification key from host names to IP addresses, the system configuration information file that you saved before you changed the node identification key will not contain IP addresses. Code the IP addresses in Windows Notepad or read the IP addresses from the `hosts` file, and then create the system configuration information.

- When offline machine inventory is managed
  - You cannot move, rename, or change the attributes in the offline folder.
  - If the connection destination of an offline machine has been specified in order to register it into the system configuration, the offline machine is registered in the system configuration when the connection destination receives the system configuration from the offline machine. The offline machine is handled as a client after it has been registered into the system configuration.
- When changing a host name
  - If you have changed the host name of JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system), change the host name of the connection destination at the setup of the lower systems that are connected to that host.
  - If the key item of the ID key for operations is host name, change the host name and then restart the computer.

8.1.8 Notes on creating system configuration information

The following notes apply to creation of system configuration information:

- You can create a maximum of seven hierarchical levels in the system configuration information.
- To create a relay system in the system configuration, you must create under the relay system a client with the same name as the relay system that has the address selected by the node identification key (host name or IP address). Do not move the client under the relay system that has the same name as the relay system that was created.
- If you execute remote installation or a *Get user inventory information* job on a UNIX relay system, you must define in the system configuration information a client with the same host name under the UNIX relay system, and then specify this client as the destination of the job.

8.2 Creating host groups

In the Destination window, you can divide the hosts that were set in the System Configuration window into groups and manage them in groups.

This section describes how to create host groups.

8.2.1 Methods of creating host groups

There are four ways to create host groups. Use the method that is appropriate to the characteristics of the host group.

Creating a host group from system configuration information

This method involves producing the system configuration information as a text file, creating the host group by editing this file, and then loading it into the Destination window. This method is especially convenient for creating groups according to the physical network configuration.

For details, see *8.2.3 Creating a host group from a file*.

Creating a host group in the Destination window

This is as interactive method of creating host groups directly in the Destination window. This method is convenient for creating a host group that is unrelated to the network configuration or for modifying the information about an existing host group.

For details, see *8.2.4 Creating a host group in the Destination window*.

Creating a host group automatically on the basis of conditions (policies)

This method automatically assigns a newly added host or a migrated host to a host group on the basis of predefined grouping conditions (policies). For details, see *9.3 Automatic maintenance of host groups*.

Creating a host group from count results

This method uses the count-clients facility to create a host group of hosts with an identical inventory. For example, you can create a host group consisting of Windows 2000 hosts by counting the hosts for each operating system. This method is convenient for executing specific distribution only to this host group.

For details about creating host groups from count results, see *4.2.7 Creating a host group from count results* in the manual *Administrator's Guide Volume 1*.

8.2.2 How to assign group names

You can specify up to 32 characters for a host group name or an ID group name. However, the following conditions must be satisfied:

- The following characters may not be used: `! " % ' * . / : < > ? @ / |`
- Spaces may not be used.
- Because group names are not case-sensitive, you may not use a name that duplicates another name when uppercase letters are changed to lowercase (and vice versa).

You can create a maximum of seven hierarchical levels for the host groups. The total number of characters in the host group names or host names starting from the top host group to the bottom host group (including the leading delimiter for each host group name) and to the last host name (including the leading delimiter of the host name) cannot exceed 255 bytes.

8.2.3 Creating a host group from a file

Create a file called the *host group file* that contains host group information, and then create host groups from the file.

(1) Creating a host group file

In the host group file, specify the destination name, destination type, and supervising host group for each destination. This file is a text file. In this file, a line whose first column is a single quotation mark (`'`) or a pound sign (`#`) is treated as a comment line.

A simple method for creating a host group file is to export the system configuration information to a text file, and then edit it; for an example, see *8.2.6 Example of creating host group information*.

Format

```
destination-name HID=host-ID,TYPE=destination-type,MAC=MAC-
address,ROOT=path-to-supervising-host-group,DATE=creation-date-and-time
```

Description

You can specify the operands after `TYPE=`*destination-type* in any order.

destination-name (required)

Specify the name of a host group or host.

When the destination is a host group, specify *destinationname* in the following format: `*` *hostgroupname*. Delimit the asterisk (`*`) and *hostgroupname* with a space. Specify a unique host group name. For details about assigning host group names, see *8.2.2 How to assign group names*.

When the destination is a host, the specification format depends on the node identification key.

If you are using host names as the node identification key, specify *destinationname* in the following format: `*` *host-name*. The delimiter between the asterisk (`*`) and *hostname* must be a space. You can specify a different character (other than a space) or a character string (other than spaces) for the asterisk. For example, you could specify the IP address in the `*` portion.

If you are using IP addresses as the node identification key, specify *destinationname* in the following format: *IP-address* `*`. The delimiter between the beginning *IP-address* and the asterisk (`*`) must be a space. You can specify a different character or a character string for the asterisk. For example, you could specify the host name in the `*` portion. You can also omit the asterisk.

If you create a host group file by using the manager, you can specify only the hosts that are registered in the system configuration for the destination.

`HID=`*host-ID*

Specify a host ID that uniquely identifies the host. If you chose **File** and then **Save to File** in the Destination window to save the host group information to a file and a host ID was set, be sure to specify that host ID. If a host ID was not set in the host group file that you produced with **Save to File**, or if you are adding a new host, do not specify this operand.

`TYPE=`*destination-type*

Specify one of the following host types as the type of destination (if you omit this operand, the system sets `CLIENT` as the default):

- `GROUP` (host group)
- `MANAGER` (relay manager)
- `MASTER` (relay system)
- `CLIENT` (client)

`MAC=`*MAC-address*

Specify the MAC address of the host. Basically, do not change this operand because MAC addresses are related to facilities such as Wake on LAN. If you change the operand, the related facilities may not function.

`ROOT=`*path-of-supervising-host-group*

Specify the full path of the supervising host group to which the host belongs.

If you do not set `ROOT`, the system sets the previous host group as the supervising host group and creates a destination of the type you specified in the `TYPE` operand.

`DATE=`*creation-date-and-time*

Specify the date and time when you register (or registered) the host with the central manager or relay manager for the first time. Specify the date and time in *MM*/*DD*/*YYYY*/*hh*/*mm*/*ss* format. In *YYYY*, you can specify 1971 to 2037. In *hh*, you can specify 0 to 23.

If you omit this operand, the date and time when **Create from File** was executed is set.

(2) Creating host groups from a file

When you create a host group from a host group file, the system replaces the contents of the Destination window with the information you set in the host group file. To save the host groups displayed in the existing Destination window, assign a file name and save the host group information to the file.

If the contents of the existing Destination window include a host ID, you must set the same host ID.

To create a host group from a file:

1. In the Destination window, choose **File**, and then **Create from File**.
2. Select the created host group file, and click the **OK** button.

(3) Saving the host group configuration to a file

You can save the configuration of host groups displayed in the Destination window to a file. This feature is helpful when you need to change host groups, because you simply save the current host group configuration to a file and edit that file.

To save the host group configuration to a file:

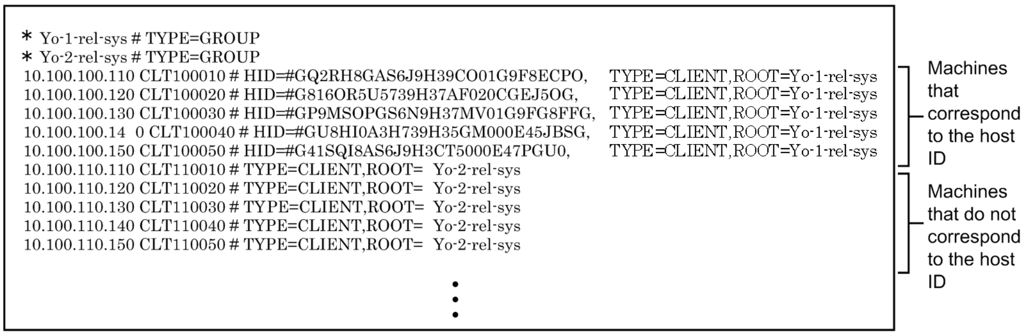
1. In the Destination window, choose **File**, and then **Save to File**.

   The Save Destination dialog box appears. Note that before you perform this operation, choose **Refresh** to update the system configuration information. If you do not manually update the system configuration information, the displayed information may differ from the latest internal data.
2. Specify a file name, and click the **OK** button.

   The system saves the host group configuration to the file.

The following shows an example of the file output of the host group configuration:

Figure 8–5: Example of the file output of the host group configuration



```
* Yo-1-rel-sys # TYPE=GROUP
* Yo-2-rel-sys # TYPE=GROUP
10.100.100.110 CLT100010 # HID=#GQ2RH8GAS6J9H39CO01G9F8ECPO,    TYPE=CLIENT,ROOT=Yo-1-rel-sys
10.100.100.120 CLT100020 # HID=#G816OR5U5739H37AF020CGEJ5OG,    TYPE=CLIENT,ROOT=Yo-1-rel-sys
10.100.100.130 CLT100030 # HID=#GP9MSOPGS6N9H37MV01G9FG8FFG,   TYPE=CLIENT,ROOT=Yo-1-rel-sys
10.100.100.14  0 CLT100040 # HID=#GU8HI0A3H739H35GM000E45JBSG,  TYPE=CLIENT,ROOT=Yo-1-rel-sys
10.100.100.150 CLT100050 # HID=#G41SQI8AS6J9H3CT5000E47PGU0,    TYPE=CLIENT,ROOT=Yo-1-rel-sys
10.100.110.110 CLT110010 # TYPE=CLIENT,ROOT=  Yo-2-rel-sys
10.100.110.120 CLT110020 # TYPE=CLIENT,ROOT=  Yo-2-rel-sys
10.100.110.130 CLT110030 # TYPE=CLIENT,ROOT=  Yo-2-rel-sys
10.100.110.140 CLT110040 # TYPE=CLIENT,ROOT=  Yo-2-rel-sys
10.100.110.150 CLT110050 # TYPE=CLIENT,ROOT=  Yo-2-rel-sys
                          •
                          •
                          •
```

Machines that correspond to the host ID

Machines that do not correspond to the host ID

8.2.4 Creating a host group in the Destination window

After you create a host group, you can register the hosts (relays systems or clients) that are to belong to that host group.

(1) Creating a host group

The procedure for creating a host group is described below. Although you can create a host group under another host group, you cannot assign the name of the higher host group to the lower host group. The maximum number of host-group levels you can create is seven.

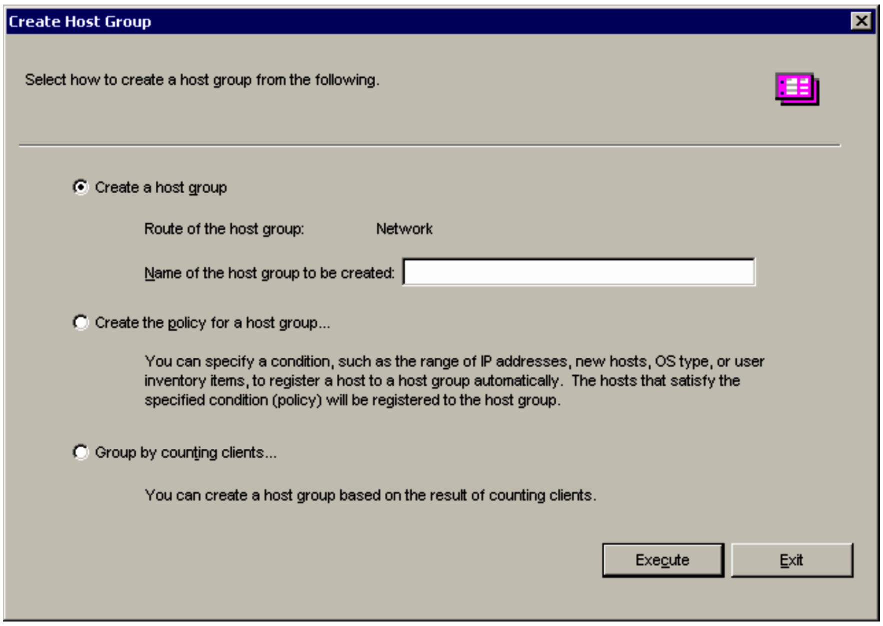
To create a host group:

1. Open the Destination window, and select the location where the host group is to be created.

   The system creates the host group at the location you select.
2. Choose **File**, and then **Create Host Group**.

The Create Host Group dialog box appears.

Figure 8–6: Create Host Group dialog box



Create Host Group

Select how to create a host group from the following.

● Create a host group

Route of the host group: Network

Name of the host group to be created:

○ Create the policy for a host group...

You can specify a condition, such as the range of IP addresses, new hosts, OS type, or user inventory items, to register a host to a host group automatically. The hosts that satisfy the specified condition (policy) will be registered to the host group.

○ Group by counting clients...

You can create a host group based on the result of counting clients.

Choose **Create a host group** and then specify a unique host group name. For details about assigning host group names, see *8.2.2 How to assign group names*.

3. After setting the items, click the **Execute** button.

   The host group is created. If you do not want to create the host group, click the **Exit** button.

(2) Registering hosts

The procedure for registering hosts into a host group you have created is described below. If a host is not displayed in the System Configuration window, you cannot set that host in the Destination window.

To register a host:

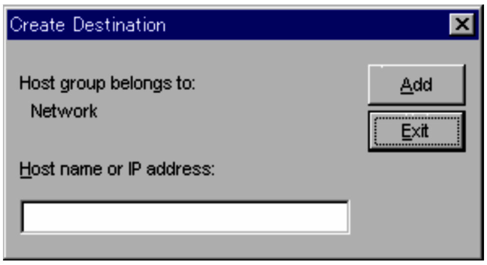
1. Open the Destination window, and select the location where the host is to be set.

   The system will set the host at the location you select.

2. Choose **File**, and then **Create Destination** (or click the **Create Host** button).

   The Create Destination dialog box appears.

   Figure 8–7: Create Destination dialog box



Create Destination

Host group belongs to:
Network

Host name or IP address:

Host group belongs to

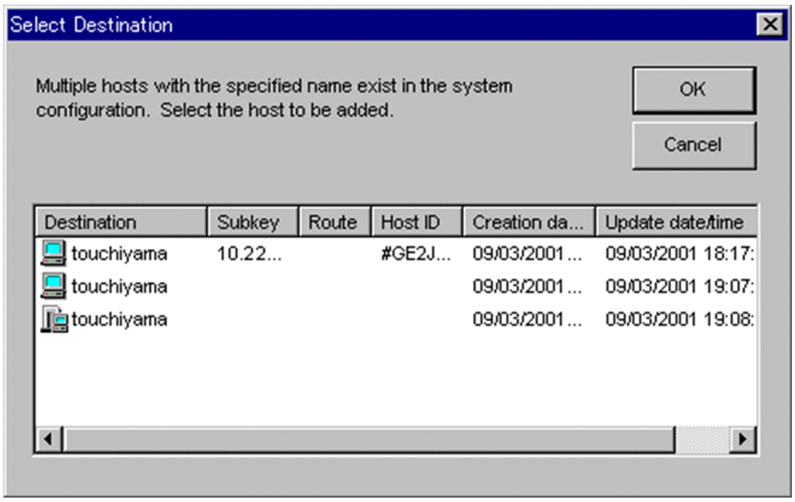
This item displays the name of the host group into which the host is to be registered.

Host name or IP address

Specify the host name or IP address of the host to be registered.

Click the **Add** button. If host IDs are being used and the system configuration contains multiple hosts with the same host name, the Select Destination dialog box appears. Specify which destination is be selected.

Figure 8–8: Select Destination dialog box



Multiple hosts with the specified name exist in the system configuration. Select the host to be added.

Destination	Subkey	Route	Host ID	Creation da...	Update date/time
touchiyama	10.22...		#GE2J...	09/03/2001 ...	09/03/2001 18:17:
touchiyama				09/03/2001 ...	09/03/2001 19:07:
touchiyama				09/03/2001 ...	09/03/2001 19:08:

3. After specifying the items, click the **Exit** button.
   The system saves the settings and closes the Create Destination dialog box.
   To add another host, click the **Add** button instead of **Exit**.

Alternatively, you can register a host by dragging it from the System Configuration window and dropping it on the host group icon.

8.2.5 Changing host groups

This subsection describes the method for changing host groups.

To register additional host groups or hosts to the existing information, see *(1) Adding host groups from a file*. To initialize the existing information and then re-register information, see *(2) Changing a host group from a file*.

(1) Adding host groups from a file

You can use JP1/Software Distribution Manager's Remote Installation Manager to add host groups or hosts from a file.

To add host groups or hosts from a file:

1. Create a host group file that contains only the host groups or hosts that are to be added.
   For details about how to create a host group file, see *8.2.3(1) Creating a host group file*.
2. In the Destination window, from the **File** menu, choose **Add from File**.
   The Add Destination dialog box appears.
3. Select the host group file created in step 1 and then click the **Open** button.
   Registration of the host groups or hosts begins.

(2) Changing a host group from a file

Before changing the host group configuration, save the current host group configuration to a file. Make the necessary changes, and then create the host groups from the modified file.

For details about the methods for saving the host group configuration to a file and creating host groups from the saved file, see *8.2.3 Creating a host group from a file*.

(3) Changing a host group in the Destination window

The procedure for changing a host group from the Destination window is described below. For details about the method for searching for the host group or host to be changed, see *9.1.1 Finding hosts by name*.

(a) Renaming a host group

The procedure for renaming a host group is described below.

Note that you cannot change the destination name of a host from the Destination window.

To rename a host group:

1. In the Destination window, select the host group to be renamed.
   The selected group is highlighted.
2. Choose **File**, and then **Rename**.
   The Rename dialog box appears.
3. Specify the new name, and then click the **OK** button.
   The group name changes to the name you specified.

(b) Editing (deleting, copying, or moving) a host group or host

To edit (delete, copy, or move) a host group or host, open the Destination window, and select the host group or host to be edited. Then, from the **Edit** menu, choose **Delete**, **Copy**, or **Cut** and **Paste**.

You can also use drag-and-drop for editing a host group or host.

Notes

- Do not double click **Network** in the left-hand frame after you have chosen **Copy** or **Cut**.
  If you do, **Paste** is disabled and you will not be able to paste the host. Should this happen, choose **Copy** or **Cut** again.
- If multiple Destination windows are open, destination groups or hosts copied in one window cannot be pasted to any other window.

(c) Notes on editing a destination

If a communication error occurs while you are editing (deleting, copying, or moving) a host group or host in the Destination window, you may not be able to restore the group or host to its previous status. Therefore, if you are editing multiple host groups or hosts, we recommend that you save the host group configuration to a file before performing the editing.

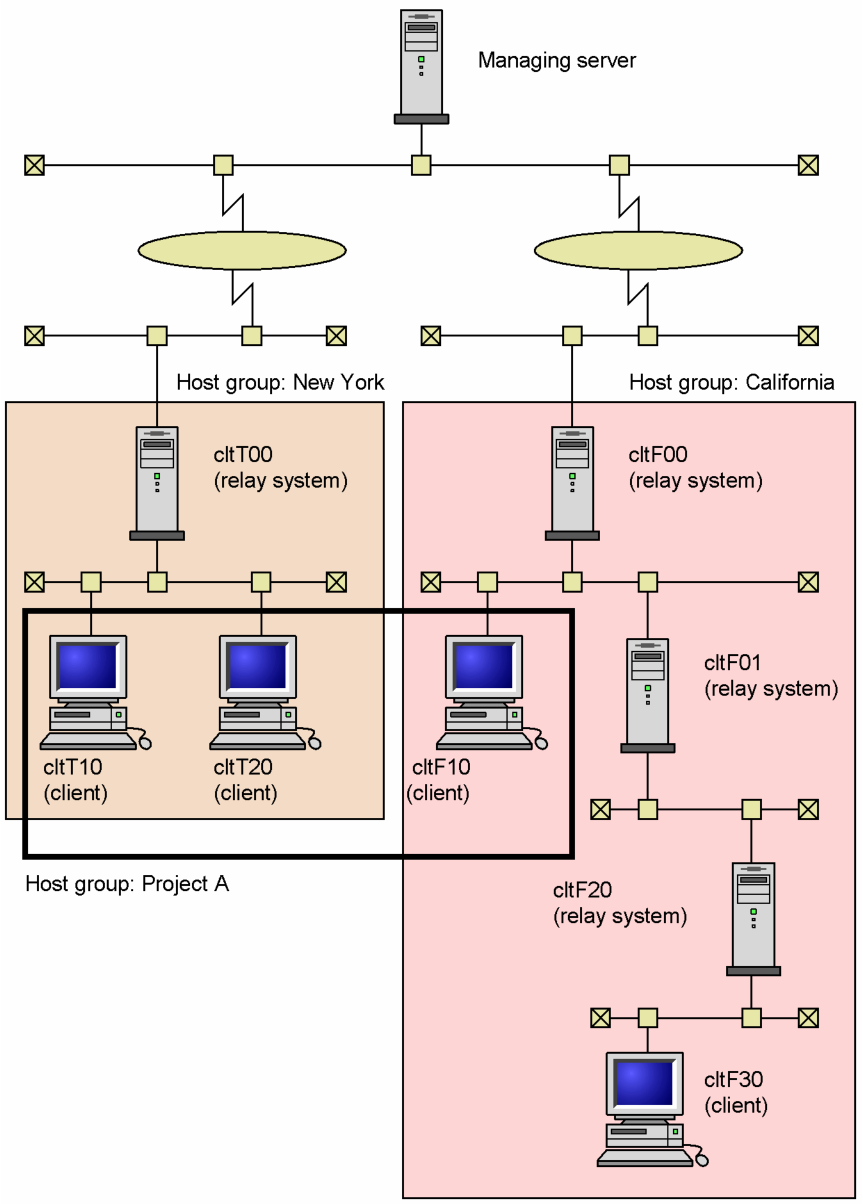
For details about the methods for saving the host group configuration to a file and creating host groups from the saved file, see *8.2.3 Creating a host group from a file*.

8.2.6 Example of creating host group information

This subsection presents an example of creating system configuration information and host group information.

- Configuration of system configuration information and host group information
  In the configuration shown in the figure below, the system creates the system configuration information automatically, and the user creates the host group information by editing the system configuration information file.

Figure 8–9: Configuration of system configuration information and host group information



- System configuration information file

  The following shows system configuration information that was created automatically and then saved to a file.

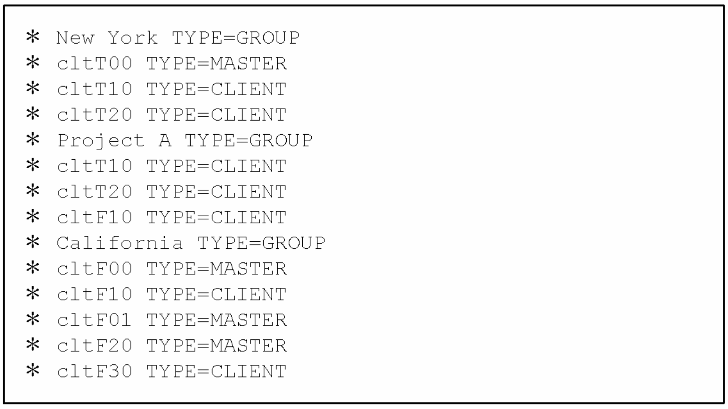
Figure 8–10: System configuration information file

```
10.100.100.100 cltT00 TYPE=MASTER
10.100.100.110 cltT10 TYPE=CLIENT
10.100.100.120 cltT20 TYPE=CLIENT
10.110.100.100 cltF00 TYPE=MASTER
10.110.100.110 cltF10 TYPE=CLIENT
10.110.100.120 cltF01 TYPE=MASTER,ROOT=cltF00
10.110.100.130 cltF20 TYPE=MASTER,ROOT=cltF00\cltF01
10.110.100.140 cltF30 TYPE=CLIENT
```

- Host group file

  The following shows a host group file that was created by editing system configuration information that was saved to a file. To save system configuration information to a file, in the System Configuration window, choose **File** and then **Save to File**.

Figure 8–11: Host group file



```
* New York TYPE=GROUP
* cltT00 TYPE=MASTER
* cltT10 TYPE=CLIENT
* cltT20 TYPE=CLIENT
* Project A TYPE=GROUP
* cltT10 TYPE=CLIENT
* cltT20 TYPE=CLIENT
* cltF10 TYPE=CLIENT
* California TYPE=GROUP
* cltF00 TYPE=MASTER
* cltF10 TYPE=CLIENT
* cltF01 TYPE=MASTER
* cltF20 TYPE=MASTER
* cltF30 TYPE=CLIENT
```

8.3 Creating ID groups

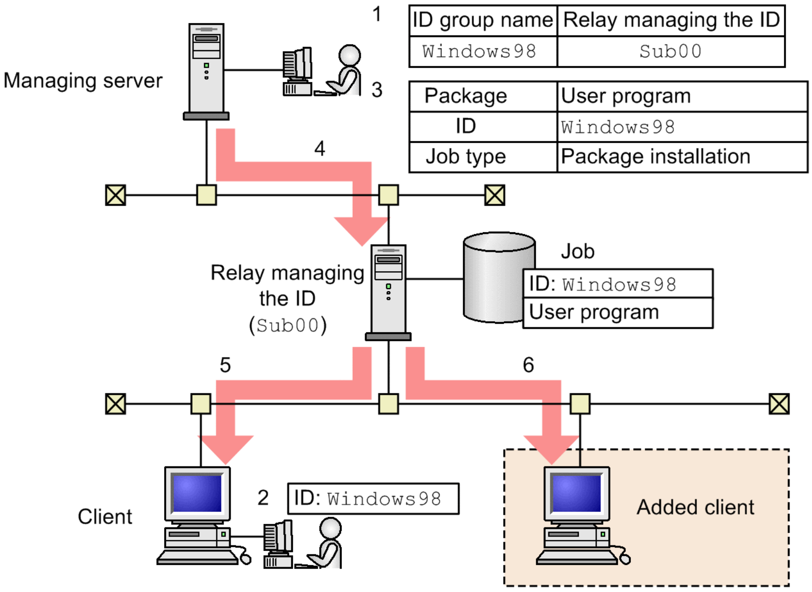
You can use the Destination window of Remote Installation Manager to create ID groups in the same manner as when you create host groups. Although it is at the managing server that an ID group is created, each ID group is relayed to and managed by the appropriate relay manager/system (*relay managing the ID*). The relay managing the ID also manages registration of clients into the ID group.

This section first provides an overview of ID group operations, and then provides details about creating ID groups and registering clients into ID groups.

8.3.1 ID group operations

The following figure shows an example of ID group operations.

Figure 8–12: Example of ID group operations



ID group name	Relay managing the ID
Windows98	Sub00

Package	User program
ID	Windows98
Job type	Package installation

1. Create an ID group.
2. Register client into ID group Windows98.
3. Create a job with Windows98 specified as the destination.
4. Execute the job.
5. The relay managing the ID distributes the package to the client.
6. When an added client registers itself into ID group Windows98, the package is distributed to it.

Next, this subsection explains procedures for ID operations, the operation method in a system with a managing server hierarchy, and the operation method when the managing server of JP1/Software Distribution Client (relay system) uses ID groups.

(1) Procedures for ID group operations

(a) Creating an ID group

To create an ID group, set the information shown below in the managing system:

- ID group name
  Specify an ID group name, which will be selected as a destination for distributing jobs.
- Password (optional)
  You can set a password to be used in order to add clients to the ID group. If you set a password here, a user must enter this password to register a client into the ID group.

- Relay managing the ID

  Specify the host (relay manager or relay system) to be used as the relay managing the ID. You cannot specify an offline machine or an offline folder. You can specify multiple relays the will manage the same ID group.

(b) Registering a client into an ID group

You register a client into an ID group at the client. Connect the client to the relay managing the ID, and then register the client into the ID group that the relay is managing. You can also perform registration into an ID group from the managing server or a relay system. Furthermore, you can automatically register into an ID group a new client that has been added to the JP1/Software Distribution system.

The *relay managing the ID* in which the client is registered into an ID group becomes the higher system specified on the **Connection Destination** page (in JP1/Software Distribution SubManager or JP1/Software Distribution Client (client)). In JP1/Software Distribution Manager, the *relay managing the ID* becomes the higher system set during setup of the relay manager. If the client operates in a multi-host environment, the relay managing the ID becomes the relay system that has the highest priority.

(c) Executing a job that specifies an ID group as the destination from the managing server

The following jobs can specify an ID group as the destination:

- *Install package* jobs
- *Send package, allow client to choose* jobs
- *Get system information from client* jobs
- *Get software information from client* jobs
- *Get user inventory information* jobs
- *Transfer registry collection definition* jobs
- *Transfer user inventory schema to client* jobs (only distribution of user inventory)
- *Report message* jobs
- *Set the software monitoring policy* jobs
- *Get software monitoring information from the client* jobs

Jobs that specify an ID group as the destination (*ID group jobs*) are transferred to the relay managing the specified ID group. The relay managing the ID saves the job and executes it to clients that are registered in the ID group. If a client is registered into an ID group after the ID group job has been executed, the saved ID group job is executed for that client when registration is completed. Therefore, when you specify an ID group in an *Install package* job or a *Send package, allow client to choose* job, you must consider the package expiration date/time at the relay system of the package being distributed. When the *expiration date* and time of a package has passed in the relay system, the package is deleted from the relay system and can no longer be distributed automatically to clients that register into the ID group.

(d) Execution results of an ID group job

If you specify an ID group as the destination in the jobs listed below, you can check the results of job execution at the clients from the managing server. For details about the method for checking the execution results of ID group jobs, see *8.4.4 Displaying the job execution status* in the manual *Administrator's Guide Volume 1*.

- *Install package* jobs
- *Send package, allow client to choose* jobs

(e) Editing an ID group

You can perform the following editing operations on an ID group from the managing server that created the ID group and the relay managing the ID.

Managing server that created the ID group

- Adding or deleting a relay managing the ID
- Changing the password.
- Deleting the ID group

- Registering a client into the ID group (from a file)
- Registering the ID group into a relay managing the ID

Relay managing the ID

- Changing the password
- Deleting the ID group
- Registering a client into the ID group (from a file)
- Registering a client into the ID group (from the Destination window)
- Deleting a registered client from the ID group

(2) ID group operations in systems with a managing server hierarchy

Described below are operations that use an ID group in a system in which multiple managing servers are configured in a hierarchy.

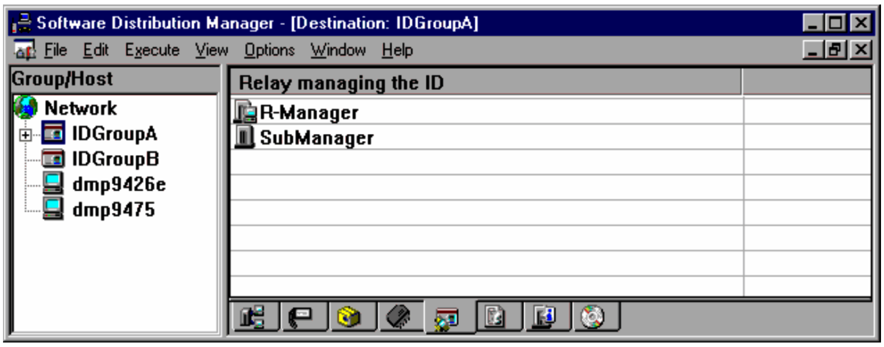
(a) Creating an ID group from the central manager

When you create an ID group from the central manager, you can set the following hosts as the relay managing the ID:

- Relay manager or relay system under the central manager
- Relay system under a relay manager

The following shows an example of an ID group created in the central manager that has a relay manager as the relay managing the ID:

Figure 8–13: ID group created from the central manager using a relay manager as the relay managing the ID


Software Distribution Manager - [Destination: IDGroupA]
File Edit Execute View Options Window Help
Group/Host
Network
IDGroupA
IDGroupB
dmp9426e
dmp9475
Relay managing the ID
R-Manager
SubManager

(b) Managing an ID group in a relay manager

In a relay manager, the Destination window displays the ID groups that the relay manager has created, as well as the ID groups for which a higher manager specified this relay manager as the relay managing the ID.

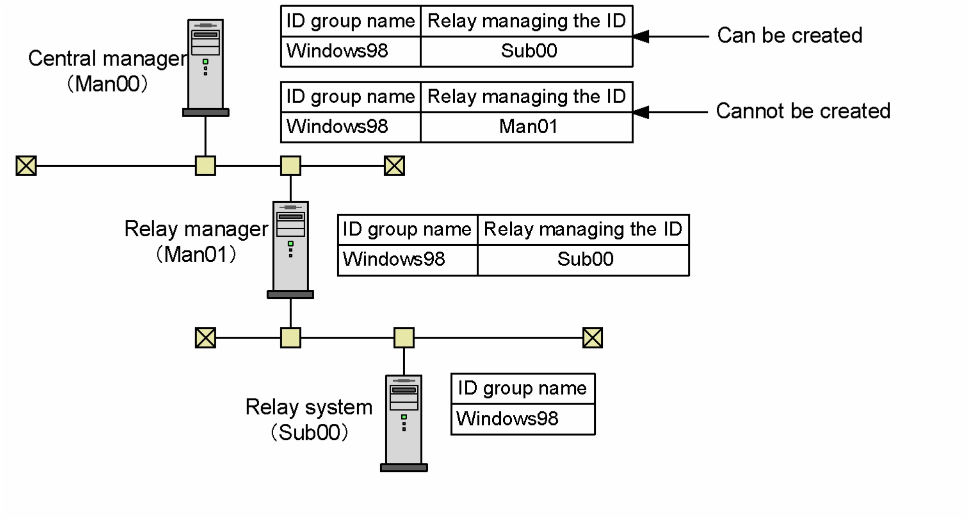
The relay manager can perform the following operations on ID groups that were created by higher managers:

- Changing the password
- Deleting the ID group
- Deleting a registered client from the ID group

(c) Managing the same ID group in multiple managing servers

As shown in the following figure, the central manager and a relay manager can create the same ID group.

Figure 8–14: Managing the same ID group in multiple managing servers



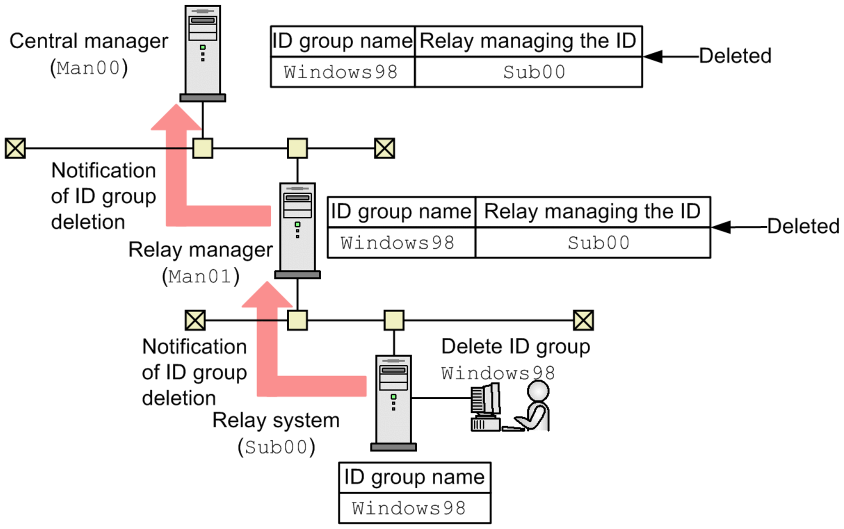
Both the central manager and the relay manager can create the ID group `Windows98` with `Sub00` as the relay managing the ID.

However, the central manager cannot create the ID group `Windows98` with `Man01` as the relay managing the ID. Because the relay manager has already created an ID group named `Windows98`, the higher manager cannot create another ID group named `Windows98` with the relay manager as the relay managing the ID.

If a system deletes an ID group or changes the relay managing the ID, the system that made the change reports the modified contents to the higher system, and the modified contents are automatically applied to the higher system.

The following figure shows an example of deleting an ID group that is managed by multiple managing servers.

Figure 8–15: Deleting an ID group managed by multiple managing servers



(3) Handling of ID groups at the relay systems

As with the managing server of JP1/Software Distribution Manager, the managing server of JP1/Software Distribution Client (relay system) can create an ID group and execute ID group jobs in subordinate clients. When the managing server of JP1/Software Distribution Client (relay system) uses an ID group, it is not necessary to set a relay managing the ID, because JP1/Software Distribution SubManager itself functions as the relay managing the ID.

Both JP1/Software Distribution Client (relay system) and the managing server of JP1/Software Distribution Manager can check the execution results of a job that specifies an ID group created by JP1/Software Distribution Client (relay system). To enable JP1/Software Distribution Manager to report the execution results of ID group jobs executed by

JP1/Software Distribution Client (relay system), you must specify the following setting in the JP1/Software Distribution Client (relay system):

- On the **Remote Installation Manager** page, select the **Report the ID group job status to the managing server** check box.

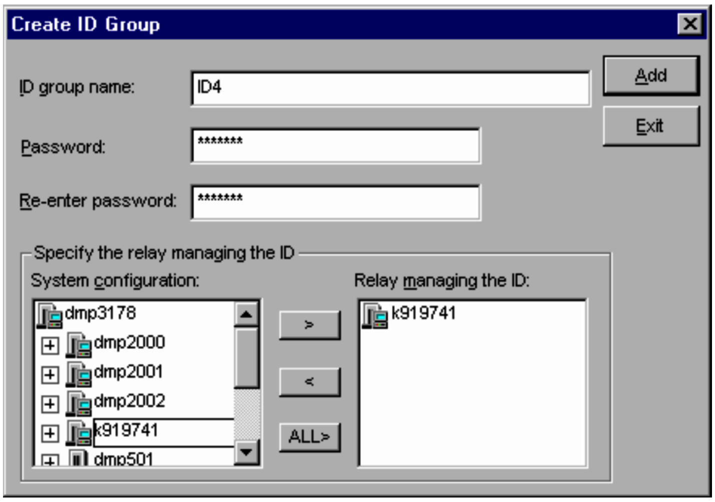
8.3.2 Creating an ID group

This subsection describes the procedure for creating an ID group.

To create an ID group:

1. In the Destination window, choose **File**, and then **Create ID Group**.
   The Create ID Group dialog box appears.

   Figure 8–16: Create ID Group dialog box

   Create ID Group

   ID group name: ID4

   Password: *******

   Re-enter password: *******

   ID group name

   Specify a name for the ID group. For details about assigning ID group names, see *8.2.2 How to assign group names*.

   Password

   Specify a password that a client user must enter in order to register a client into the ID group. The password can have up to 14 bytes. You can omit the password specification. The entered characters are displayed as asterisks (`*`) for security purposes.

   Specify the relay managing the ID

   This pane lets you specify the relay managing an ID. You can specify multiple hosts as the relay managing the ID.

   The **System configuration** list displays the relay managers and relay systems that are hosts displayed in the System Configuration window. Offline machines and offline folders are not displayed. From the **System Configuration** list, select a host you want to use as the relay managing the ID, and then click the **>** button. The selected host is set as the relay managing the ID. In the **System Configuration** list, you can select multiple hosts at one time.

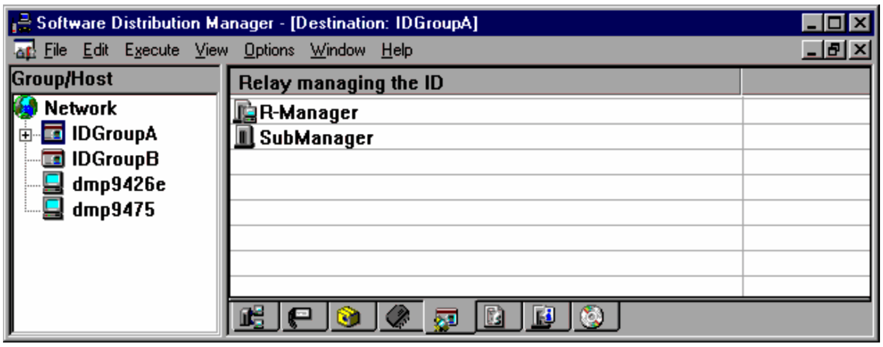
   Clicking the **All>** button sets all the relay managers and relay systems as relays managing the ID at one time.

2. After all the settings are completed, click the **Add** button.
   An ID group is created.
   If addition of a relay managing the ID fails, its status may remain as `Registering`. If this occurs, eliminate the cause of the failure and then re-execute the operation.
   You can use **Delete ID Group** to forcibly delete a relay managing the ID that is in `Registering` status.

3. Click the **Exit** button.
   The Create ID Group dialog box closes.

You can check the new ID group in the Destination window. The relay system that manages the ID group is displayed when you select the **Relays Managing ID** tab in the right pane of the Destination window.

Figure 8–17: Relay managing the ID page in the Destination window


Software Distribution Manager - [Destination: IDGroupA]
File Edit Execute View Options Window Help
Group/Host
Network
IDGroupA
IDGroupB
dmp9426e
dmp9475
Relay managing the ID
R-Manager
SubManager

8.3.3 How to register clients

There are four ways of registering a client into an ID group. Note that offline machines cannot be registered into an ID group.

- Register the client into the ID group from the client.
- Use a file to register the client into the ID group from the managing server.
- Register the client into the ID group from the relay managing the ID.
- Register the client into the ID group using automatic maintenance of ID groups.

(1) Registering the client into an ID group from the client

To register the client into the ID group, use the Register in ID Group dialog box, which is displayed by choosing the **Register in ID Group** menu item.

Registration into the ID group is processed when the client connects to the relay managing the ID. However, you can still set the wait status for registration into or deletion from the ID group even if the client is not connected to the relay managing the ID. Then, after the client connects to the relay managing the ID, the client reports the actual registration or deletion to the relay managing the ID when the user logs on or chooses the **Register in ID Group** menu item. You can thus register a client into an ID group even during the pre-installation and system construction stages. While a client is executing remote installation, it is connected to the relay managing the ID via a different facility and is regarded as not being connected from the relay managing the ID.

For details about the method for registering a client into an ID group from the client, see *11.2.1 Registering into an ID group* in the manual *Administrator's Guide Volume 1*.

(2) Using a file to register clients into an ID group from a managing server

In a system consisting of JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system) with version 05-20 or later, you can use a file to register clients into an ID group on the managing server. This method is particularly convenient when for registering a large number of clients into an ID group, such as when you first install the system. In the file, set the ID group registration information of multiple clients. This file is called the *ID group file*. The following explains how to use a file to register clients into an ID group.

(a) Creating an ID group file

In the ID group file, specify the host name, host ID, ID group name, and the name of the relay managing the ID for each host.

The is a text file. In this file, a line whose first column is a single quotation mark (`'`) or a pound sign (`#`) is treated as a comment line.

Format

```
host-name HID=host-ID,MAC=MAC-address,ID=ID-group-name, MASTER=name-of-
relay-managing-the-ID
```

Description

host-name (required)

Specify either the host name or the IP address of the client to be added to the ID group. You can specify up to 64 bytes.

`HID=`*host-ID*

Specify a host ID that uniquely identifies the host. If you chose **File** and then **Save ID Hosts to File** to save the ID group information to a file and a host ID was set for the ID group, be sure to specify the host ID even if you plan to register clients into the ID group using **Use File for ID Registration**. If no host ID was set for the ID group in the file that you produced using **Save ID Hosts to File**, or if you are adding a new host, do not specify this operand.

`MAC=`*MAC-address*

Specify the MAC address of the host. Basically, do not change this operand because MAC addresses are related to facilities such as Wake on LAN. If you change the operand, the related facilities may not function.

`ID=`*ID-group-name* (required)

Specify the name of the ID group to be added. You can specify up to 32 bytes.

`MASTER=`*name-of-relay-managing-the-ID*

Specify the name of the relay system or relay manager containing the ID group to be added. For a relay system, specify the host name, IP address, or host ID. For a relay manager, specify the host name or host ID. If you used **Save ID Hosts to File** to save the ID group to a file and a host ID was set, be sure to specify that host ID.

You can specify up to 64 bytes. If you omit this parameter in a managing server or a relay manager, clients will be registered into the ID group in the managing system. If you specify this parameter in a relay system, it is ignored; in such a case, clients are registered into the ID group in the relay system.

(b) Registering clients into an ID group from a file

To register clients into an ID group from the created ID group file, in the Destination window of the managing server, from the **File** menu, choose **Use File for ID Registration**, and then select the ID group file to be used.

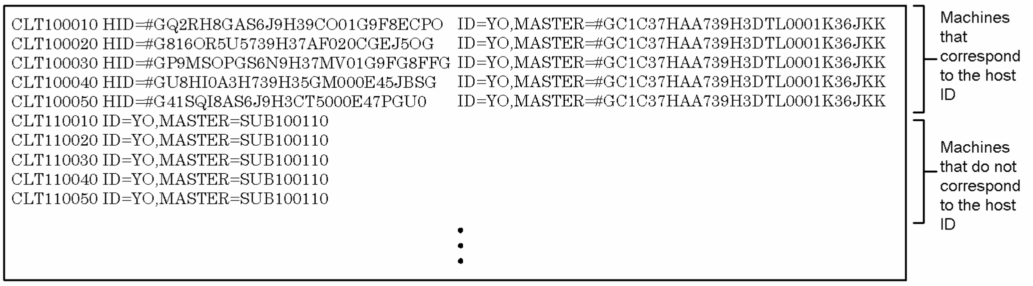
In a system consisting of JP1/Software Distribution Manager or JP1/Software Distribution SubManager with version earlier than 05-20, clients cannot be registered from a file into a selected ID group. If an attempt is made to do so, a client in the **Registering** status remains in the Destination window. Delete such a client. Additionally, in the Job Status window, an **Add entry** job remains in the folder with the ID group name under the **Edit ID Group** folder. Also delete such a job.

(c) Saving ID group information to a file

To output the information about ID groups specified by the managing server and the information about hosts registered into the ID groups, choose **File** and then **Save ID Hosts to File** in the Destination window. Note that before you perform this operation, you should choose **Refresh** to update the system configuration information. If you do not manually update the displayed system configuration information, the correct information might not be output because a mismatch occurs between the displayed information and the internal data due to automatic registration of system configuration information.

The following shows an output example of a file of ID group information.

Figure 8–18: Output example of a file of ID group information



```
CLT100010 HID=#GQ2RH8GAS6J9H39CO01G9F8ECPO  ID=YO,MASTER=#GC1C37HAA739H3DTL0001K36JKK
CLT100020 HID=#G816OR5U5739H37AF020CGEJ5OG   ID=YO,MASTER=#GC1C37HAA739H3DTL0001K36JKK
CLT100030 HID=#GP9MSOPGS6N9H37MV01G9FG8FFG ID=YO,MASTER=#GC1C37HAA739H3DTL0001K36JKK
CLT100040 HID=#GU8HI0A3H739H35GM000E45JBSG   ID=YO,MASTER=#GC1C37HAA739H3DTL0001K36JKK
CLT100050 HID=#G41SQI8AS6J9H3CT5000E47PGU0    ID=YO,MASTER=#GC1C37HAA739H3DTL0001K36JKK
CLT110010 ID=YO,MASTER=SUB100110
CLT110020 ID=YO,MASTER=SUB100110
CLT110030 ID=YO,MASTER=SUB100110
CLT110040 ID=YO,MASTER=SUB100110
CLT110050 ID=YO,MASTER=SUB100110
                                        •
                                        •
                                        •
```

Machines that correspond to the host ID
Machines that do not correspond to the host ID

(3) Registering clients into an ID group from the relay managing the ID

If you are using a PC on which JP1/Software Distribution SubManager is installed as the relay managing the ID, you can register clients that are connected to that relay (local system) into an ID group by using the Destination window. If you need to register many clients into an ID group, you can do so from the relay managing the ID in a batch operation and eliminate the effort of registering them individually.

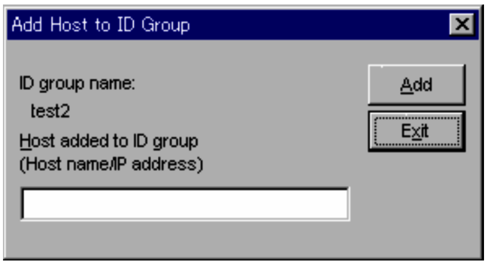
When you perform registration into an ID group from a relay managing the ID, make sure that the connection destination of the clients is the local system (the relay managing the ID).

You can register into an ID group by using a menu or by using drag-and-drop.

(a) Using a menu

To register into an ID group:

1. In the Destination window of Remote Installation Manager, select the ID group to which the client is to be added.
2. Choose **File**, and then **Add Host to ID Group**.
   The Add Host to ID Group dialog box appears.
   Figure 8–19: Add Host to ID Group dialog box



ID group name:
test2
Host added to ID group
(Host name/IP address)

ID group name

This item displays the name of the ID group that you selected in the Destination window.

Host added to ID group

Specify the host name or IP address of the client to be added to the ID group.

Note that you can add to the ID group only those clients that have set the local system as their connection destination. Make sure that the local system is the connection destination of the client.

3. Click the **Add** button.
   The system registers the client into the ID group you specified.

(b) Using drag-and-drop

1. In the Destination window of Remote Installation Manager, select the client to be registered into the ID group.
   You cannot select a host group, ID group, or host that belongs to an ID group.
2. Drag the client to the ID group in which it is to be registered and drop it.
   The system registers the client into the ID group.

(4) Registering clients into an ID group using automatic maintenance of ID groups

You can use the automatic ID group maintenance function to automatically register into an ID group the clients that satisfy specific conditions.

For details about how to register clients into an ID group using automatic maintenance of ID groups, see *9.4 Automatic maintenance of ID groups*.

8.3.4 Editing an ID group

You can perform the following editing operations on an ID group from the managing server that created the ID group or the relay managing the ID:

- Changing the relay managing the ID
- Changing the password
- Deleting the ID group
- Registering a client into the ID group
- Delete a registered client from the ID group
- Register the ID group into a relay managing the ID

(1) Changing the relay managing the ID or the password

To change the relay managing the ID or the password required for registration into the ID group:

1. In the Destination window, choose **File**, and then **Change ID Group Attribute**.
   The Change ID Group Attribute dialog box appears.
2. Specify the new relay for managing the ID group.
   Specify the new relay for managing the ID group or the new password. You can change only the password from the relay managing the ID. Note that the entered password characters are displayed as asterisks (*) for security purposes.
3. After changing the relay managing the ID, click the **OK** button.
   The system changes the relay managing the ID.
   The processing for changing the relay managing the ID may take a while. If the change information does not appear in the Destination window, wait a few moments. Then, from the menu, choose **Window**, and then **Refresh** to refresh the Destination window.

(2) Deleting an ID group

To delete an ID group:

1. In the Destination window, select the ID group to be deleted, choose **File**, and then choose **Delete ID Group**.
   A dialog box appears, requesting confirmation of the deletion.
2. Click the **OK** button.
   The system deletes the selected ID group. The Destination window displays the **Deleting** status for the deleted ID group but the ID group is not deleted from the window. After the deletion process is completed, choose **Window** and then **Update** to delete the ID group from the window.

(3) Deleting a registered client from an ID group

To delete a registered client from an ID group:

1. In the Destination window, select the client to be deleted, choose **Edit**, and then choose **Delete**.
   A dialog box appears, requesting confirmation of the deletion.
2. Click the **OK** button.
   The system deletes the client you selected. In a multi-level configuration, the deletion may take a while.

When the deletion occurs, the deleted client is displayed with the **Deleting** status in the Destination window. After the registered client is deleted from the ID group, from the menu choose **Window** and then **Refresh** to delete the client from the display.

(4) Registering an ID group into a relay managing the ID

In the managing server where an ID group was created, you can register the ID group into a relay managing the ID. Because you can register multiple ID groups into a relay managing the ID in a batch operation, this feature is convenient when a new relay managing the ID is added to the system.

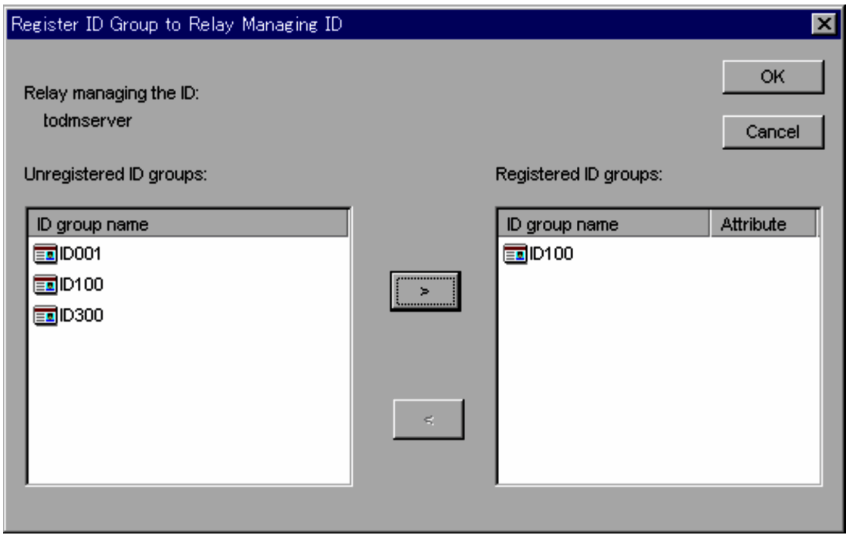
For details about the method for registering an ID group into a relay managing the ID, see *(1) Changing the relay managing the ID or the password*.

(a) Registering an ID group into a relay managing the ID

To register an ID group into a relay managing the ID:

1. In the System Configuration window, choose **File**, and then **Register ID Group**.
   The Register ID Group to Relay Managing ID dialog box appears.

Figure 8–20: Register ID Group to Relay Managing ID dialog box



Relay managing the ID:
todmserver

Unregistered ID groups:

ID group name
ID001
ID100
ID300

Registered ID groups:

ID group name	Attribute
ID100	

2. From the **Unregistered ID groups** list, select the ID group to be registered, and then click the > button.
   The ID group is added to the **Registered ID groups** list.
3. Click the **OK** button.
   The system registers the ID into the relay managing the ID.

(b) Deleting an ID group from a relay managing the ID

To delete an ID group from a relay managing the ID:

1. In the System Configuration window, choose **File**, and then **Register ID Group**.
   The Register ID Group to Relay Managing ID dialog box appears.
2. From the **Registered ID groups** list, select the ID group to be deleted, and then click the < button.
   The ID group is deleted from the **Registered ID groups** list.
3. Click the **OK** button.
   The system deletes the ID group from the relay managing the ID.

8.3.5 Notes on using ID groups

This subsection provides notes on using ID groups.

(1) Renaming a client host

In an environment that uses ID groups, the system does not automatically change ID group information. Therefore, if you want to rename the host of a client, you must first delete the client from the ID groups in which it is registered. Then, after you rename the host, register the client into the ID groups again.

(2) Deleting system configuration information in a client registered in an ID group

Even if you use the settings to delete system configuration information for a client that is registered in an ID group, the system does not automatically delete the client's ID group registration information. Therefore, before deleting the system configuration information for a client, you should delete its ID group registration.

If you have deleted a client's system configuration information without deleting its ID group registration, you can delete the ID group registration from the Remote Installation Manager. For details about the deletion method, see *8.3.4 Editing an ID group*.

You can also automatically link system configuration information and ID group information. For details, see *8.4 Linking system configuration information and ID group information*.

(3) When the Edit ID Group folder is created

If an `Edit ID Group` folder is created in the Job Status window, do not delete this folder or the jobs in the folder.

The `Edit ID Group` folder is used to store jobs for registering clients into ID groups and for adding relays managing IDs. These ID group editing jobs are created automatically and are then deleted upon normal termination.

If you have deleted the ID group editing jobs manually, ID group editing no longer takes place. In such a case, re-execute the ID group editing operation (such as registering clients into an ID group and adding relays managing IDs).

8.4 Linking system configuration information and ID group information

You can link system configuration information and ID group information so that when you change system configuration information, the system changes the related ID group information as well. Using this facility reduces the system administrator's workload associated with management of ID groups.

8.4.1 Requirements for linking system configuration information and ID group information

To link system configuration information and ID group information, you must make the following settings:

- For JP1/Software Distribution Manager
  In the JP1/Software Distribution Manager setup, on the **System Configuration** page, select the **Link with system configuration modifications** check box.
- For JP1/Software Distribution Client (relay system)
  In the JP1/Software Distribution Client (relay system) setup, on the **System Configuration** page, select the **Link with system configuration modifications** check box.

8.4.2 Examples of linkage between system configuration information and ID group information

This subsection presents examples of linkage between system configuration information and ID group information.

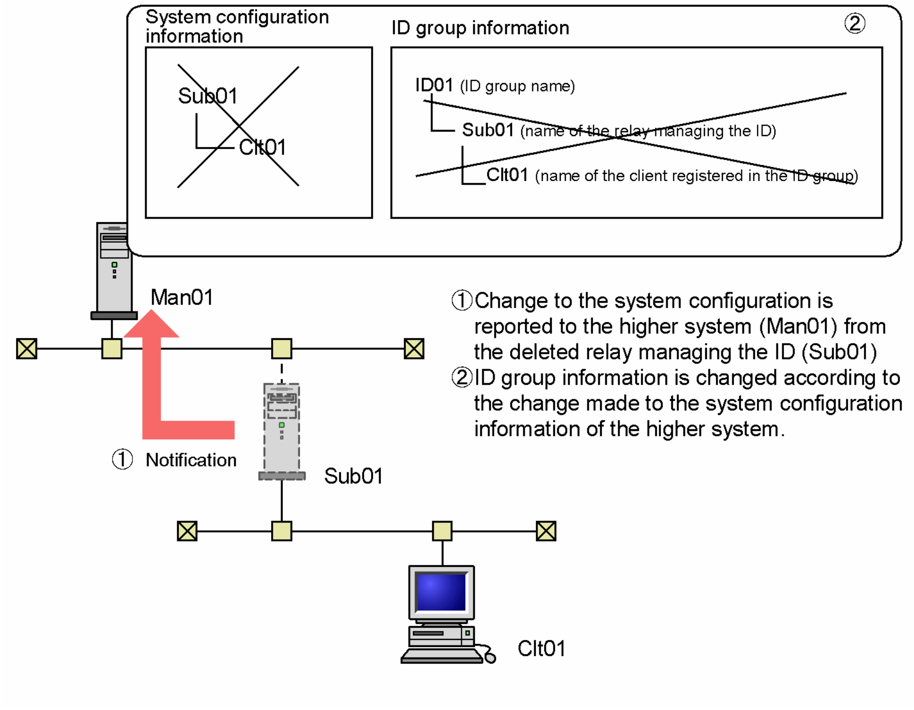
(1) Deleting from the system configuration information

This subsection explains the linkage between system configuration information and ID group information when a relay managing the ID or a client registered in an ID group is deleted from the system configuration information.

(a) When a relay managing the ID is deleted

The following figure shows an example in which a relay system that was defined as a relay managing the ID is deleted.

Figure 8–21: Example of deleting a relay system defined as a relay managing the ID


System configuration information
~~Sub01~~
~~Clt01~~
ID group information
②
~~ID01 (ID group name)~~
~~Sub01 (name of the relay managing the ID)~~
~~Clt01 (name of the client registered in the ID group)~~
Man01
① Notification
Sub01
Clt01

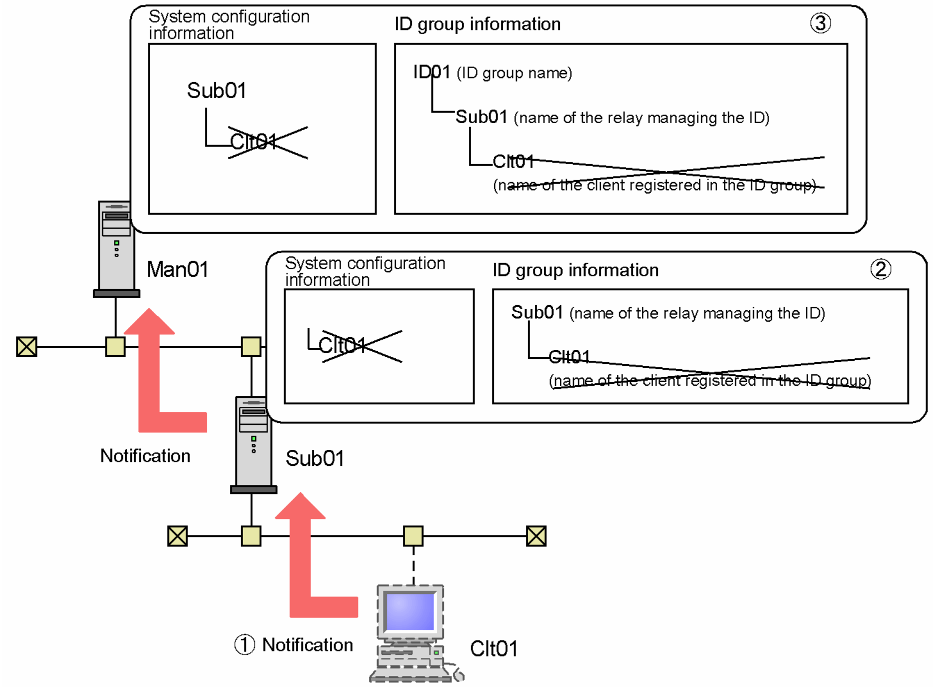
①Change to the system configuration is reported to the higher system (Man01) from the deleted relay managing the ID (Sub01)

②ID group information is changed according to the change made to the system configuration information of the higher system.

(b) When a client registered in an ID group is deleted

The following figure shows an example in which a client registered in an ID group is deleted.

Figure 8–22: Example of deleting a client registered in an ID group


System configuration information
Sub01
~~Clt01~~
ID group information
③
ID01 (ID group name)
Sub01 (name of the relay managing the ID)
~~Clt01~~
~~(name of the client registered in the ID group)~~
Man01
System configuration information
~~Clt01~~
ID group information
②
Sub01 (name of the relay managing the ID)
~~Clt01~~
~~(name of the client registered in the ID group)~~
Notification
Sub01
① Notification
Clt01

① Change to the name is reported from the client registered in the deleted ID group to the higher system.

② ID group information is changed according to the change made to the system configuration information of the relay managing the ID (Sub01).

③ ID group information is changed according to the change made to the system configuration information of the managing server (Man01).

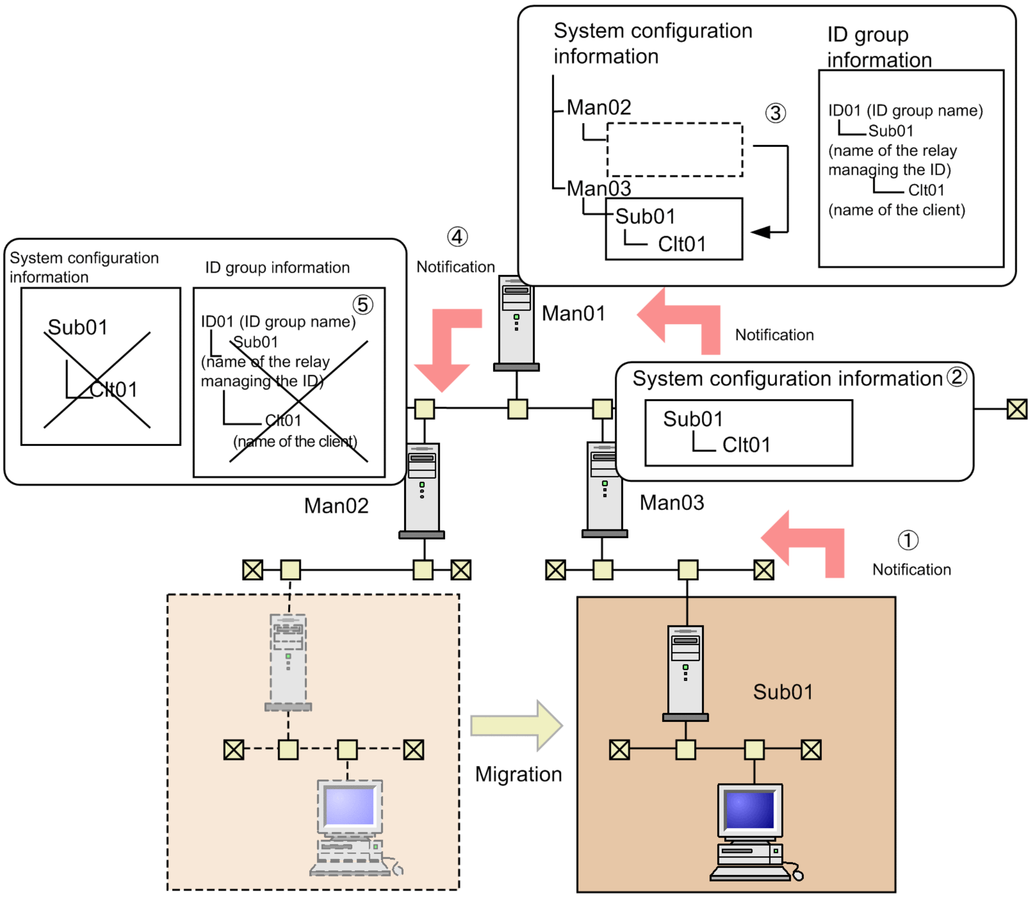
(2) Changing a path in the system configuration information

This subsection explains the linkage between system configuration information and ID group information when the path of a relay managing the ID or of a client registered in an ID group is changed in the system configuration information.

(a) When the path of a relay managing the ID is changed

The following figure shows an example in which the connection destination of a relay system defined as the relay managing the ID is changed.

Figure 8–23: Example of changing the connection destination of a relay system defined as a relay managing the ID

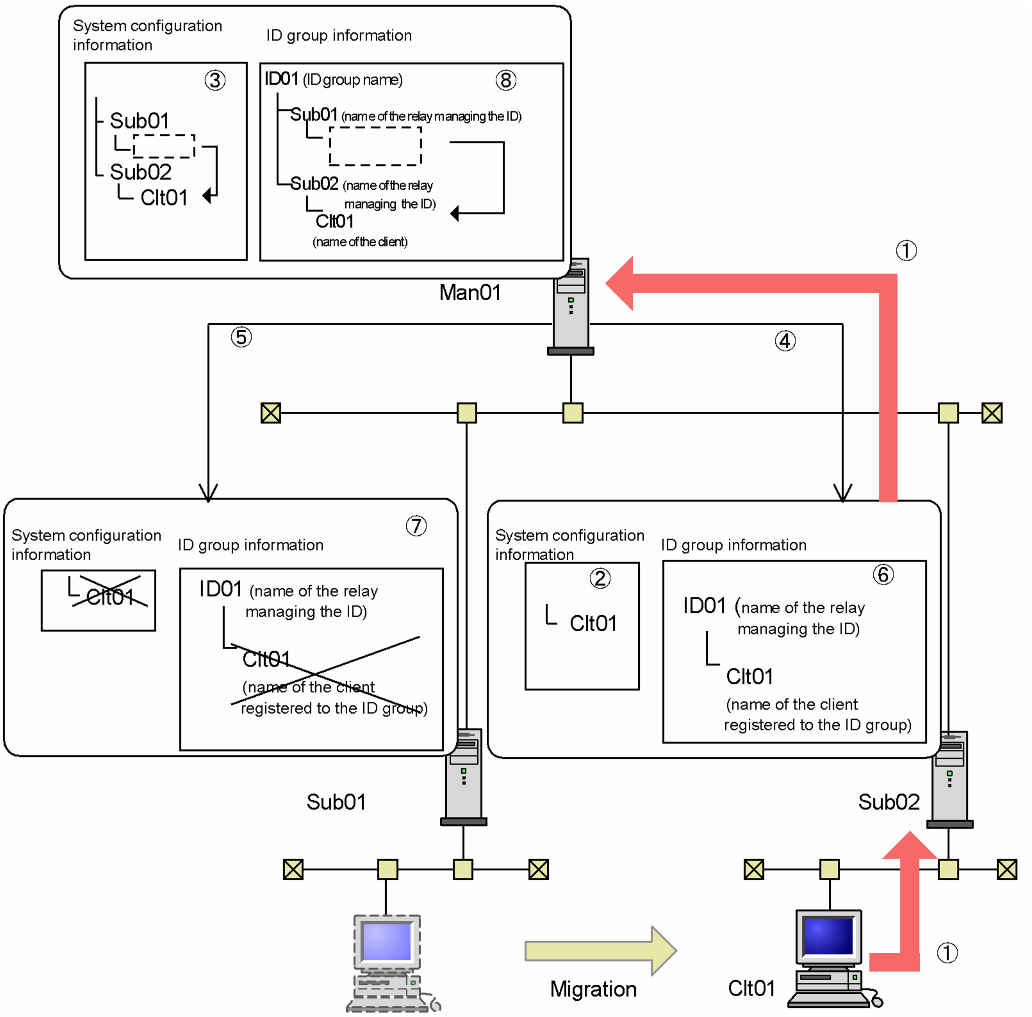


① Automatic registration of system configuration is reported from the relay system whose connection destination was changed (`Sub01`) to the new connection destination.
② The relay system is added to the system configuration information of the relay manager at the next connection destination (`Man03`).
③ Route is changed in the system configuration information of the server that uses the relay system (`Sub01`) as a relay managing the ID.
④ Job that deletes the system configuration and ID group information remaining on the old route is reported to the relay manager (`Man02`).
⑤ The system configuration and ID group information of the relay system on the old path that moved from the relay manager (`Man02`) that received the job is deleted.

(b) When the path of a client registered in an ID group is changed

The following figure shows an example in which the connection destination of a client registered in an ID group is changed.

Figure 8–24: Example of changing the connection destination of a client registered in an ID group


System configuration information
ID group information
③
Sub01
Sub02
Clt01
ID01 (ID group name)
⑧
Sub01 (name of the relay managing the ID)
Sub02 (name of the relay managing the ID)
Clt01
(name of the client)
①
Man01
⑤
④
System configuration information
ID group information
⑦
Clt01
ID01 (name of the relay managing the ID)
Clt01
(name of the client registered to the ID group)
System configuration information
ID group information
②
Clt01
⑥
ID01 (name of the relay managing the ID)
Clt01
(name of the client registered to the ID group)
Sub01
Sub02
Migration
Clt01
①

① System configuration is registered automatically to the new connection destination that was changed from `Clt01`.
② A client is added to the system configuration information at the new connection destination (`Sub02`).
③ On the Manager (`Man01`) that detected the route change, the client route is changed in the system configuration and the client (`Clt01`) is deleted from the ID group information for the old relay managing the ID (`Sub01`).
④ An instruction to add a client to the ID group with the new route is issued to the ID group to which the client used to belong.
⑤ Job that notifies deletion of the client that used to belong to the relay system (`Sub01`) of the old route is executed on that relay system.
⑥ Receiving the instruction of ④, the new relay managing the ID (`Sub02`) adds the client to its own ID group.
⑦ Receiving the instruction of ⑤, the relay system on the old route deletes the client from its system configuration information and ID group information.
⑧ A client is added under the relay managing the ID (`Sub02`) that has become the new connection destination.

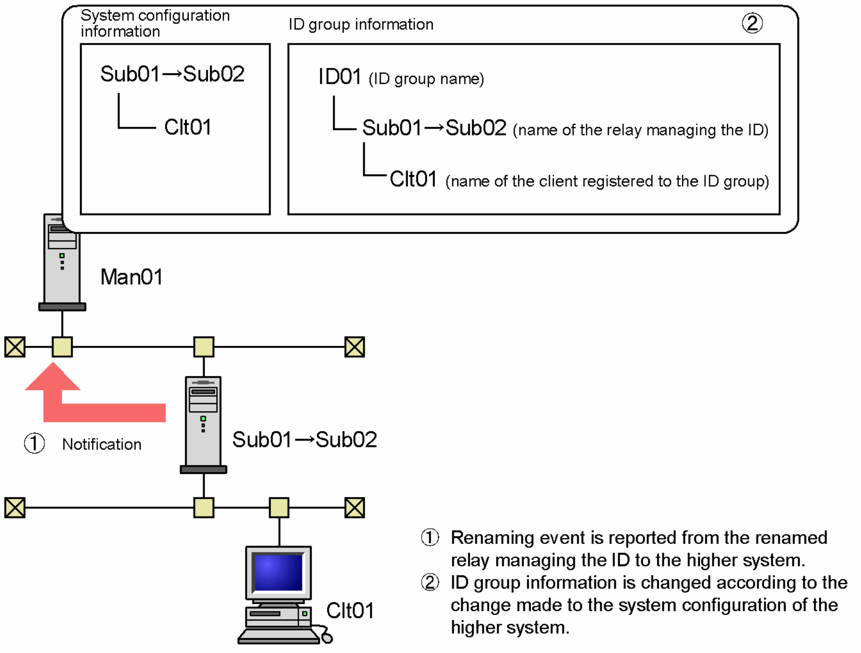
(3) Renaming from the system configuration information

This subsection explains the linkage between system configuration information and ID group information when a relay managing the ID or a client registered in an ID group is renamed in the system configuration information.

(a) When a relay managing the ID is renamed

The following figure shows an example in which a relay system defined as the relay managing the ID is renamed.

Figure 8–25: Example of renaming a relay system defined as the relay managing the ID

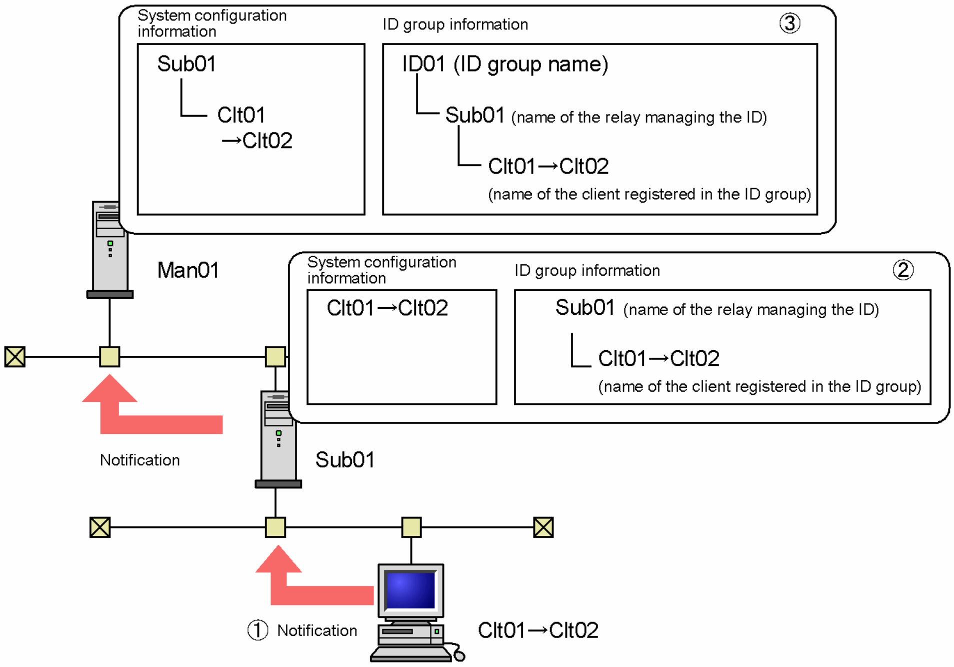

System configuration information
ID group information
②
Sub01→Sub02
Clt01
ID01 (ID group name)
Sub01→Sub02 (name of the relay managing the ID)
Clt01 (name of the client registered to the ID group)
Man01
① Notification
Sub01→Sub02
Clt01

① Renaming event is reported from the renamed relay managing the ID to the higher system.
② ID group information is changed according to the change made to the system configuration of the higher system.

(b) When a client registered in an ID group is renamed

The following figure shows an example in which a client registered in an ID group is renamed.

Figure 8–26: Example of renaming a client registered in an ID group


System configuration information
ID group information
③
Sub01
Clt01
→Clt02
ID01 (ID group name)
Sub01 (name of the relay managing the ID)
Clt01→Clt02
(name of the client registered in the ID group)
Man01
System configuration information
ID group information
②
Clt01→Clt02
Sub01 (name of the relay managing the ID)
Clt01→Clt02
(name of the client registered in the ID group)
Notification
Sub01
① Notification
Clt01→Clt02

① Renaming event is reported from the renamed client (`Clt01`) registered in the ID group to the higher system.
② ID group information is changed according to the change made to the system configuration of the higher system (`Sub01`).
③ ID group information is changed according to the change made to the system configuration of the higher system (`Man01`)

8.4.3 Notes on linking system configuration information and ID groups

This subsection provides notes on linking the system configuration information and ID group information.

(1) Handling of ID groups with passwords

If a user changes the system configuration information of a client registered in an ID group that has a password, the ID group information remains unchanged. Sometimes a password is set in the relay managing the ID rather than in the host that created the ID group. In such a case as well, the ID group information does not change when a user changes the system configuration information of a client registered in the ID group.

(2) If the connection destination is changed to one that uses a different ID key for operations

If a user changes the connection of a client registered in an ID group or a relay managing the ID from an environment that does not use host IDs to an environment that uses a different operation key, the ID group information remains unchanged because the client registered in the ID group or relay managing the ID whose connection has been changed is treated as a new addition.

(3) Linking with jobs

- If a user deletes a relay managing the ID or a client registered in an ID group from the system configuration information, the system deletes jobs addressed to and passing through the relay and jobs addressed to that client, respectively.
- Jobs are not linked when the path of a relay managing the ID or of a client registered in an ID group is changed. This means that ID group jobs found on old paths are not deleted.
- Job are not linked when a relay managing the ID or a client registered in an ID is renamed. This means that when a relay managing the ID or a client registered in an ID is renamed, jobs addressed to and passing through the relay can no longer be used.

(4) Settings at setup

- To link the system configuration information and ID groups, you must select the **Link with system configuration modifications** check box in the setup of every JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system). If the settings do not match, inconsistencies in the management information may develop between higher and lower systems.
- You cannot use this linking facility if the system contains JP1/Software Distribution Manager or JP1/Software Distribution SubManager version 05-21 or earlier. In such a case, you must clear the **Link with system configuration modifications** check box for every JP1/Software Distribution Manager and JP1/Software Distribution SubManager in the system.

(5) Removing from the network, with removal specified at a client

If you remove clients or relay systems from the network at your client, they are also removed from the ID group registered with the previous connection destination. However, the ID group linkage with the new connection destination is not performed. Because the removed clients are assumed to be new clients at the new connection destination, you must re-register them with the ID group.

(6) Relay manager/system

You can only specify the local system as the ID group registration target of a relay manager or relay system. If you specify a higher system as the ID group registration target, the system configuration information may not be correctly linked with the ID group for that system.

(7) When changing the connection destination of a client registered in an ID group

If you change the connection destination of a client registered in an ID group, the client is registered automatically into the ID group of the new connection destination. However, this automatic registration may take time. Before you execute a job with an ID group specified, make sure that the client has been registered with the new ID group. When an ID group is linked with the system configuration information, the job for adding the client to the ID group is generated automatically. You can view this job in the Job Status window of Remote Installation Manager.

(8) When the system configuration includes UNIX relay systems

In a system configuration that consists of a Windows managing server and UNIX relay systems, if the system configuration information between the UNIX relay systems and the Windows managing server and relay systems is changed, you cannot link system configuration information and ID group information.

8.4.4 Handling when automatic notification from the relay managing the ID is delayed

If a client alters a route while automatic notification from the relay managing the ID is delayed, the new route may not be updated in the route information, or registration in the ID group may be canceled. How to handle these problems is described below. In this subsection, both the managing server and the relay manager that create and manage the ID are called the *ID management manager*.

(1) Handling route changes that are not updated in the information associated with the ID

If a client changes the route in the ID management manager while the ID registration notification from the relay managing the ID is delayed, the route shown in the information associated with the ID may not be updated. Clients for which route information was not updated can be identified by comparing their ID group files to the clients' information files. This subsection describes how to identify clients whose route information was not updated, as well as the corrective action to take.

(a) Create an ID group file

You create an ID group file to determine which of the relays that are managing ID groups are also managing clients. The ID group file is output in NDI format. The following describes how to create an ID group file in CSV format to facilitate comparison.

To create an ID group file:

1. In the Destination window of the ID management manager's remote installation manager, choose **File**, and then **Save ID Hosts to File**.
   An ID group file (.NDI format) is created.
2. Open the file with a text editor and replace △`HID=`, △`MAC=`, △`ID=`, and, `MASTER=` with commas.
   Do not replace the , `MASTER=` in the ID name with a comma (△ indicates a single-byte space character).
3. Save the ID group file as a CSV file.

For details about what information is output to an ID group file, see *8.3.3(2)(a) Creating an ID group file*.

(b) Create a client information file

You output information about the clients managed by the ID management manager into a CSV file. Using the CSV output utility, choose the destination attribute template and output the following information.

- Information that allows the client to be identified, such as host name, IP address, and host ID
- Route
- Associated groups

For information on how to output client information files, see *9.1 Using the CSV output utility to output information to a file* in the manual *Administrator's Guide Volume 1*.

(c) Identify clients whose route changes have not been captured

The subsection describes how to compare an ID group file to a client information file to identify those clients whose route information is not correct.

To identify clients whose route information is not correct:

1. In the ID group file, check the host ID of the relay managing the ID group associated with the clients whose route information you are checking. This gives you the host name (or IP address) of the relay managing the ID group.
2. Use an ends-with condition to compare the host name (or IP address) of the relay managing the ID group from step 1 against the route information from the information file of the clients whose route information you want to check.

   The route information of clients that does not match the ends-with condition has not been updated.

   You do not need to check those clients whose only host ID for the relay managing the ID is a hash mark (#).

(d) Correct the route information

Correct the route information of the clients whose route information was not updated. Use either of the following methods.

To edit and re-register the ID group file:

1. In the Destination window of the ID management manager's remote installation manager, choose **File**, and then **Save ID Hosts to File**.

   This creates an ID group file.
2. Open the file with a text editor and revise the host ID of the relay managing the ID of the client whose route information was not updated.
3. In the Destination window of the ID management manager's remote installation manager, choose **File**, and then **Use File for ID Registration**.

   The client is re-registered in the ID group.

To delete information belonging to the ID group in the relay managing the ID and re-register information from the client to the ID group:

1. In the Destination window of the ID management manager's remote installation manager, choose the client to be deleted, then choose the **Edit** menu and select **Delete**.

   The selected client will be deleted from the ID group.
2. Request that the client deleted from the ID group be re-registered in the ID group.

(2) Handling when ID group registration is not canceled

ID group registration is not canceled if the client alters the route in the ID management manager while the ID group registration cancellation notification from the relay managing the ID is delayed. If this happens, use one of the following methods resolve the problem.

- Do another ID registration cancellation from the client whose ID group registration was not canceled

  For more about cancelling registrations from IDs, see *11.2.1 Registering into an ID group* in the manual *Administrator's Guide Volume 1*.
- Use the ID management manager's remote installation manager to delete the target client's ID registration information

  For more on how to delete clients registered in ID groups, see *8.3.4(3) Deleting a registered client from an ID group*.

Notes

One way to prevent this problem is to not cancel an ID group registration immediately before changing a route. After changing a route, also check whether the ID group registration was canceled by the client has been applied.

9 Maintaining System Configuration Information and Destination Groups

This chapter explains how to maintain system configuration information and destination groups after operation has started. It also describes how to detect hosts on which JP1/Software Distribution is not installed.

9.1 Maintaining the system configuration information manually

You can use JP1/Software Distribution Manager's System Configuration window or Destination window to search for newly added hosts and register them into host groups; you can also search for unneeded hosts and delete them from the system configuration information.

Three search methods are provided, as follows:

- Search using a name as the search key value (such as destination name, host group name, or ID group name)
- Search using a date as the search key value (such as host registration date or last date inventory information was updated)
- Search for hosts with the same MAC address, IP address, or host name but different host IDs (duplicate hosts)

This section describes each search method. It also describes how to copy the resulting hosts to the Destination window and how to delete them from the system configuration information.

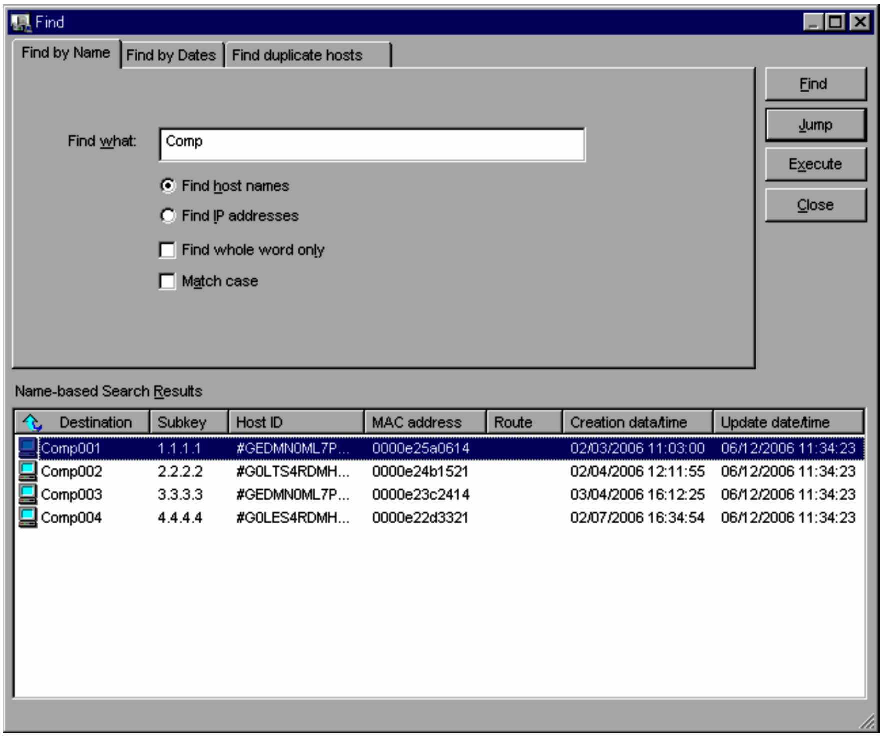
9.1.1 Finding hosts by name

This subsection describes how to find hosts using the IP address or a name, such as destination name, host group name, or ID group name as the search key value.

To search for hosts by name:

1. In the System Configuration window or Destination window, choose **Options**, and then **Find**.
   The Find dialog box appears. What is displayed in this dialog box vary depends on whether it is displayed from the System Configuration window or the Destination window.
   The following shows the Find dialog box displayed from each window.

Figure 9–1: Find dialog box displayed from the System Configuration window



Find what: Comp

● Find host names

○ Find IP addresses

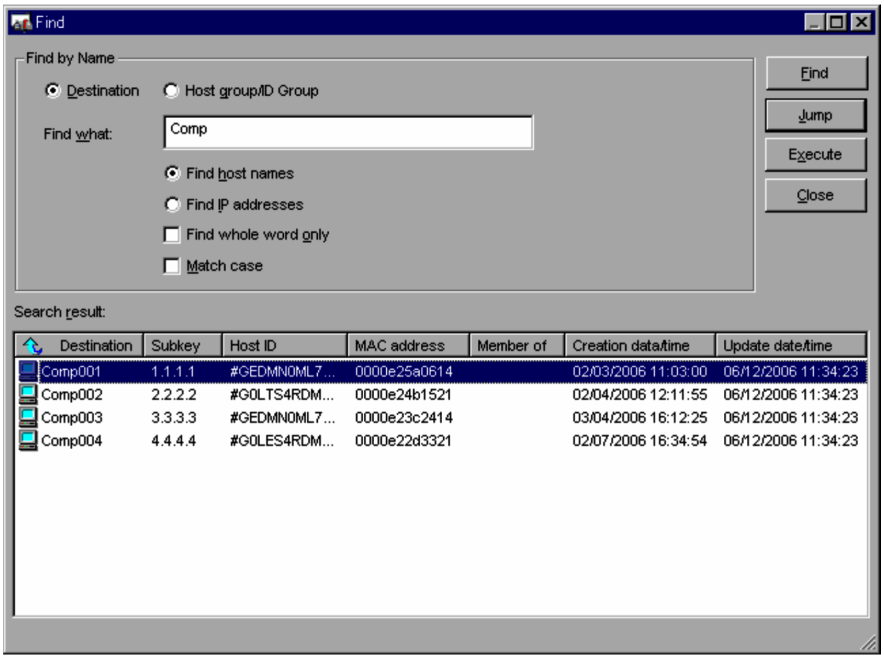
□ Find whole word only

□ Match case

Name-based Search Results

Destination	Subkey	Host ID	MAC address	Route	Creation data/time	Update date/time
Comp001	1.1.1.1	#GEDMN0ML7P...	0000e25a0614		02/03/2006 11:03:00	06/12/2006 11:34:23
Comp002	2.2.2.2	#G0LTS4RDMH...	0000e24b1521		02/04/2006 12:11:55	06/12/2006 11:34:23
Comp003	3.3.3.3	#GEDMN0ML7P...	0000e23c2414		03/04/2006 16:12:25	06/12/2006 11:34:23
Comp004	4.4.4.4	#G0LES4RDMH...	0000e22d3321		02/07/2006 16:34:54	06/12/2006 11:34:23

Figure 9–2: Find dialog box displayed from the Destination window



Find by Name

● Destination ○ Host group/ID Group

Find what: Comp

● Find host names

○ Find IP addresses

□ Find whole word only

□ Match case

Search result:

Destination	Subkey	Host ID	MAC address	Member of	Creation data/time	Update date/time
Comp001	1.1.1.1	#GEDMN0ML7...	0000e25a0614		02/03/2006 11:03:00	06/12/2006 11:34:23
Comp002	2.2.2.2	#G0LTS4RDM...	0000e24b1521		02/04/2006 12:11:55	06/12/2006 11:34:23
Comp003	3.3.3.3	#GEDMN0ML7...	0000e23c2414		03/04/2006 16:12:25	06/12/2006 11:34:23
Comp004	4.4.4.4	#G0LES4RDM...	0000e22d3321		02/07/2006 16:34:54	06/12/2006 11:34:23

Destination (when displayed from the Destination window)

Select this option to search destination names.

Host group/ID Group (when displayed from the Destination window)

Select this option to search host group names and ID group names.

Find what:

Specify a maximum of 64 bytes as the search string. This search string cannot contain spaces or any of the following symbols:

`\ / * " : ! | < > ? % @ '`

The system searches for the destinations with names containing the specified character string.

Find host names

Select this option to use the host name as the search key value.

This option is disabled when the Find dialog box is displayed from the Destination window and **Host group/ID Group** is selected as the search target.

Find IP addresses

Select this option to use the IP address as the search key value.

This option is disabled when the Find dialog box is displayed from the Destination window and **Host group/ID Group** is selected as the search target.

Find whole word only

Select this check box if you want to search for the destinations whose names completely match the specified string.

Match case

Select this check box if you want to distinguish uppercase from lowercase letters. If you use Microsoft SQL Server as a relational database and select **Case-sensitive** for the sort order for Microsoft SQL Server, the **Match Case** check box in the Find dialog box is ignored.

2. After specifying the search conditions, click the **Find** button.

   The system starts the search and displays the search results in the **Search Result** list at the bottom of the dialog box.

   You can resize the Find dialog box.

3. From the **Search Result** list, select a desired destination and click the **Jump** button or double-click on a desired destination.

The System Configuration window or Destination window becomes active and displays the information about the destination you selected.

9.1.2 Finding hosts by date

You can use any of the following dates as a search key:

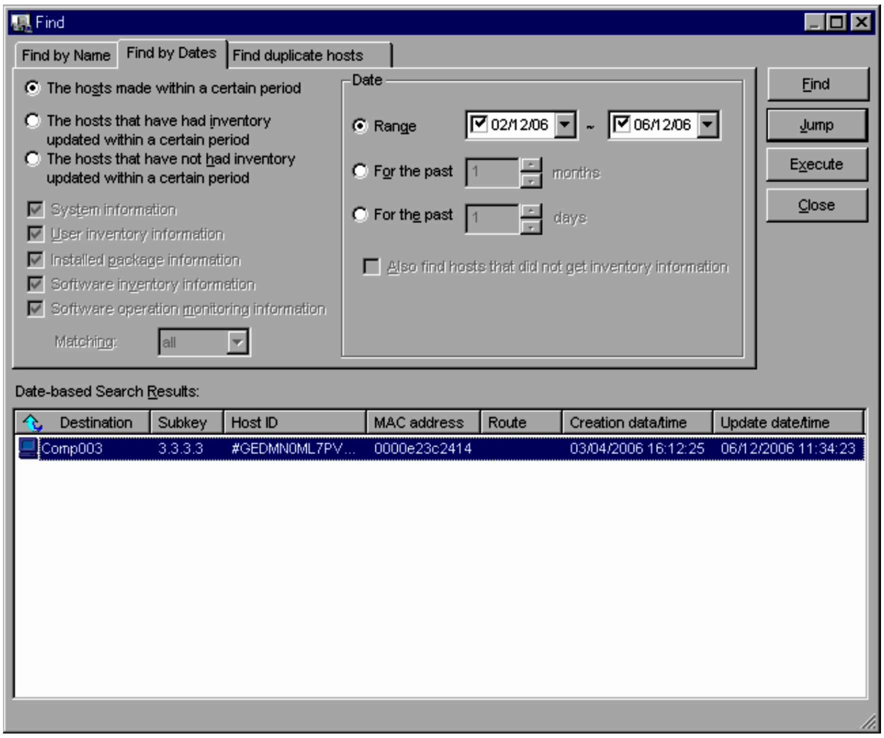
- Creation date and time
  The date and time when the host was first registered with the central manager or relay manager
- Last system information update date
  The most recent date and time a *Get system information from client* job was used to acquire information
- Last user inventory information update date
  The most recent date and time the user inventory information was updated
- Last installed package information update date
  The most recent date and time a *Get software information from client* job specifying **Search software installed by Software Distribution**, **Search all software**, or **Search software listed in Add/Remove Programs** was used to acquire software information
- Last software inventory information update date
  The most recent date and time a *Get software information from client* job specifying **Search for a file**, **Search for Microsoft Office products**, or **Search for anti-virus products** was used to acquire software information
- Last software activity monitoring information update date
  The most recent date and time the software activity status was monitored and suppression history or operation history was updated

The following describes how to find hosts using a date as the search key value.

To search for hosts by date:

1. In the System Configuration window, choose **Options**, and then **Find**.
   The Find dialog box appears.
2. Choose the **Find by Dates** tab.

Figure 9–3: Find by Dates page



● The hosts made within a certain period
○ The hosts that have had inventory updated within a certain period
○ The hosts that have not had inventory updated within a certain period

☑ System information
☑ User inventory information
☑ Installed package information
☑ Software inventory information
☑ Software operation monitoring information

Matching: all

Date

● Range ☑ 02/12/06 ~ ☑ 06/12/06
○ For the past 1 months
○ For the past 1 days
□ Also find hosts that did not get inventory information

Date-based Search Results:

Destination	Subkey	Host ID	MAC address	Route	Creation data/time	Update date/time
Comp003	3.3.3.3	#GEDMN0ML7PV...	0000e23c2414		03/04/2006 16:12:25	06/12/2006 11:34:23

3. Select the type of hosts to be searched.

The hosts made within a certain period

Select this option to search for hosts that were newly added within the period specified in **Date**.

The hosts that have had inventory updated within a certain period

Select this option to search for hosts whose inventory information or software operation information has been updated within the period specified in **Date**.

The hosts that have not had inventory updated within a certain period

Select this option to search for hosts whose inventory information or software operation information has not been updated within the period specified in **Date**.

4. If you selected **The hosts that have had inventory updated within a certain period** or **The hosts that have not had inventory updated within a certain period**, select the type of information to be searched.

System information

The program searches the most recent date and time a *Get system information from client* job acquired information.

User inventory information

The program searches the most recent date and time user inventory information was updated.

Installed package information

The program searches the most recent date and time a *Get software information from client* job acquired information with an option other than **Search for a file** specified.

Software inventory information

The program searches the most recent date and time a *Get software information from client* job acquired information with the **Search for a file** option specified.

Software operation monitoring information

The program monitors the software activity status and searches for the most recent date and time that suppression or operation history was updated.

Matching

If you select more than one type of information, select **all** to retrieve only the hosts that satisfy all the specified conditions or **any** to retrieve hosts that satisfy any of the conditions.

5. Specify the range of dates that the search is to cover.

   Range

   Specify both or either of the start date and end date to determine the range of dates. The entry format is *YY*/*MM*/*DD*, where *YY* is the last 2 digits of the year, *MM* is the month, and *DD* is the date. You can specify dates within the range from January 1, 1971 to December 31, 2037.

   If you specify only a start date or only an end date, do not select the check box for the one you do not specify.

   For the past *n* months

   Specify the number of past months from the current date as the search range. You can specify 1-999 months. However, if the specified start month is earlier than January 1, 1971, the search range is from January 1, 1971, to the current date.

   For the past *n* days

   Specify the number of past days from the current date as the search range. You can specify 1-999 days. However, if the specified start date is earlier than January 1, 1971, the search range is from January 1, 1971, to the current date.

   Also find hosts that did not get inventory information

   Select this option to also search for hosts that have never acquired inventory information or software operation information. This option is available only when **The hosts that have had inventory updated within a certain period** is selected.

6. After setting all search conditions, click the **Find** button.

   The search begins and the results are displayed in the **Date-based Search Results** list at the bottom of the dialog box.

   By dragging the corner or border of the Find dialog box, you can change its size.

7. Select a desired host from the **Date-based Search Results** list and then click the **Jump** button or double-click the host.

   The System Configuration window becomes active and displays the information about the host you selected.

9.1.3 Finding duplicate hosts

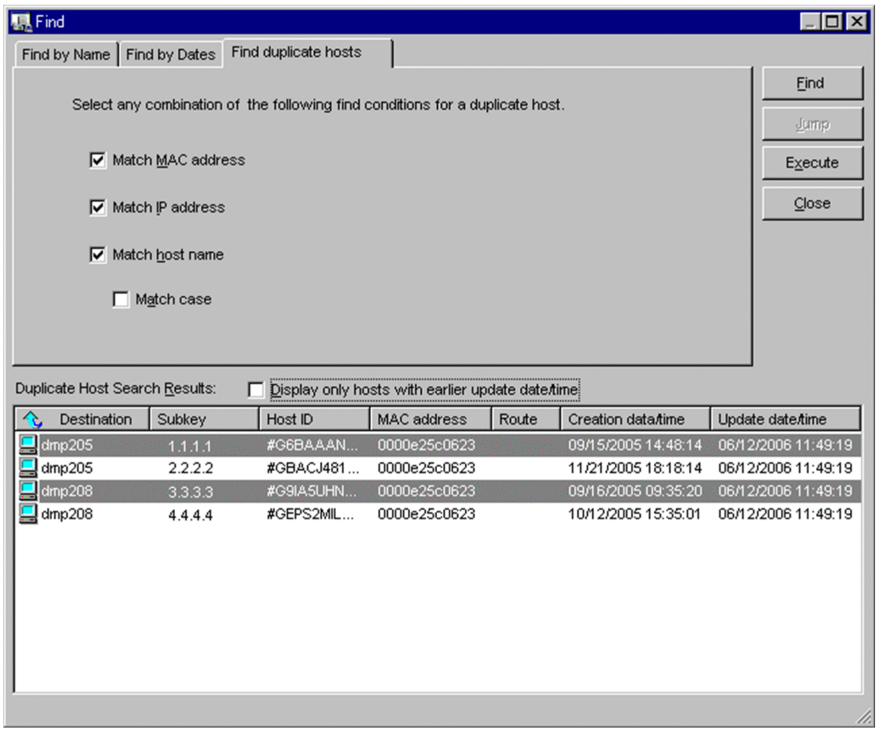
To find multiple hosts that have the same MAC address, IP address, or host name but different host IDs (duplicate hosts):

1. In the System Configuration window, choose **Options**, and then **Find**.

   The Find dialog box appears.

2. Choose the **Find duplicate hosts** tab.

Figure 9–4: Find duplicate hosts page



Select any combination of the following find conditions for a duplicate host.

☑ Match MAC address

☑ Match IP address

☑ Match host name

□ Match case

Duplicate Host Search Results: □ Display only hosts with earlier update date/time

Destination	Subkey	Host ID	MAC address	Route	Creation data/time	Update date/time
dmp205	1.1.1.1	#G6BAAAN...	0000e25c0623		09/15/2005 14:48:14	06/12/2006 11:49:19
dmp205	2.2.2.2	#GBACJ481...	0000e25c0623		11/21/2005 18:18:14	06/12/2006 11:49:19
dmp208	3.3.3.3	#G9IA5UHN...	0000e25c0623		09/16/2005 09:35:20	06/12/2006 11:49:19
dmp208	4.4.4.4	#GEPS2MIL...	0000e25c0623		10/12/2005 15:35:01	06/12/2006 11:49:19

3. Select a combination of search conditions.

   The system will search for hosts with different host IDs that satisfy the conditions you select here. When you select multiple conditions, they are treated as `AND` conditions. If you include MAC address as a condition, neither UNIX clients nor clients with PPP connection will be searched. In the case of a UNIX client with version 08-10 or later, if MAC addresses are set to be acquired in the system configuration information, duplicate hosts can be searched.

   Match MAC address

   Searches for multiple hosts that have the same MAC address in the system configuration information.

   Match IP address

   Searches for multiple hosts that have the same IP address in the system configuration information.

   Match host name

   Searches for multiple hosts that have the same host name in the system configuration information.

   Match case

   Select this check box to distinguish upper-case from lower-case letters in the host names. Note that the **Match case** check box in the Find dialog box is ignored if you use Microsoft SQL Server as the relational database and selected **Case-sensitive** for the sort order for Microsoft SQL Server.

4. After specifying the search conditions, click the **Find** button.

   The system starts the search and displays the search results in the **Duplicate Host Search Results** list at the bottom of the dialog box. Any host whose date is not up-to-date is displayed in reverse video.

   By dragging the corner or border of the Find dialog box, you can change its size.

5. From the search results list, select a desired host and click the **Jump** button or double-click the desired host.

   The System Configuration window becomes active and displays the information about the host you selected.

9.1.4 Copying a found host into the Destination window

You can copy a host found in the System Configuration window into the Destination window. This feature is useful after a search for newly added hosts in order to register the found hosts into a host group.

To copy a found host to the Destination window:

1. Display the Destination window.
2. Open the System Configuration window, choose **Options**, and then **Find**.
   The Find dialog box appears.
3. In the Find dialog box, search hosts.
4. In the search results list, right-click a desired host and then from the displayed menu, choose **Copy**.
5. In the Destination window, right-click on a host group and then choose the **Paste** menu.
   The host is copied into the specified host group.

Instead of the above procedure, you can use drag-and-drop to copy a host into the Destination window.

9.1.5 Deleting a host from the system configuration information

When a host is found in the System Configuration window, you can delete it from the system configuration information. Only hosts that are clients can be deleted. Note that you cannot delete a client from a PC in which a relay manager or relay system is installed.

When you delete a client, the client is also deleted from the system configuration information and at the same time deleted from any host group and ID group to which it belongs. All inventory information of the deleted client is also deleted.

If the version of the relay system is 05-21 or later and the system configuration information is linked to the ID group, you can delete clients in the relay manager/system relayed from the central manager. In this case, the deleted clients are also deleted from the system configuration information managed by the relay system, host group, and ID group, and then the inventory information is also deleted. For details about linkage to the ID group, see *8.4 Linking system configuration information and ID group information*.

If you have deleted a client at a relay manager, execute a *Get system configuration information* job from that relay manager's higher system to conform the system configuration information in the entire system.

- Notes on deleting many clients
  Before you delete many clients, be sure to back up the system configuration information, host groups, and ID groups to enable recovery if you delete necessary data by mistake. For details about saving such information to a file and creating such information from a file, see *8.1.4 Creating the system configuration information from a file*, *8.2.3 Creating a host group from a file*, and *8.3.3(2)(c) Saving ID group information to a file*.

(1) Deleting a client

To delete a client found by a search, from the system configuration information:

1. In the Find dialog box, specify the search conditions and search for a host.
2. In the search results list, right-click the client to be deleted and from the displayed menu, choose **Delete from System Configuration Information**.
3. When the confirmation message appears, click the **OK** button.
   The specified client is deleted from the system configuration information, host group, and ID group. Inventory information is also deleted.

(2) Referencing information about deleted clients

The information about deleted clients is output to a log file, and a maximum of nine files can be stored in `rmtins\gui` in the installation directory.

The name of the log file is `rimfind`*n*`.log`, where *n* is 1- 9. Whenever you delete a client, the number is incremented and the log file is named as `rimfind1`, `rimfind2`, `rimfind3`, ..., `rimfind9`. When log file `rimfind9` is reached, the next log file created overwrites the oldest file.

At the beginning of the log file, the search conditions are added and information about the deleted client is listed in the same format as used in the system configuration information file. Reference this information whenever necessary.

The following shows an example of the output log file:

Figure 9–5: Example of output log file

```
# Deletion time = 05/18/2001 16:48:28
# Search type = Find by Dates
# Date type = System information last update date, User inventory information last update date
# Search option = any, Also find hosts that did not get inventory information
# Start date = 11/18/2000
# End date = 02/18/2001

172.20.20.10 tcstomi # TYPE=CLIENT,ROOT=tcsikeda,DATE=01/20/2001/16/48/18
172.20.20.20 Client1 # TYPE=CLIENT,ROOT=tcsikeda,DATE=09/17/2000/11/19/40
172.20.30.25 tcsokui # HID=#G62BFI36T4VAH399V000E4AHBBK,TYPE=CLIENT,DATE=11/18/2000/11/40/30
```

9.1.6 Examples of maintaining the system configuration information manually

This subsection describes examples of manual maintenance of system configuration information, including examples of managing newly added clients and examples of deleting unneeded clients.

(1) Examples of managing newly added clients

JP1/Software Distribution can search for new clients that were added during a specific period of time on the basis of the dates when the hosts were registered for the first time with the central manager or relay manager. By periodically searching for newly added clients, you can achieve thorough management including job execution and registration into host groups.

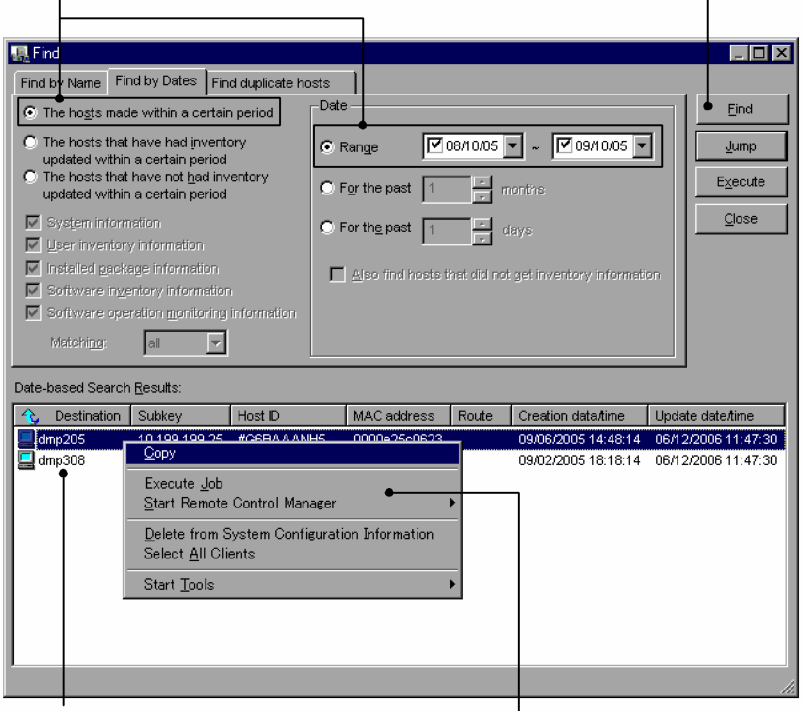
The following figure shows an example of managing the new clients added within a specified time period:

Figure 9–6: Example of managing the new clients added within a specified time period (1/2)

■ First search: September 10, 2005

1. The search targets new clients added between August 10 and September 10.

2. Starts the search.



● The hosts made within a certain period
○ The hosts that have had inventory updated within a certain period
○ The hosts that have not had inventory updated within a certain period

☑ System information
☑ User inventory information
☑ Installed package information
☑ Software inventory information
☑ Software operation monitoring information

Matching: all

Date

● Range ☑ 08/10/05 ~ ☑ 09/10/05
○ For the past 1 months
○ For the past 1 days
□ Also find hosts that did not get inventory information

Date-based Search Results:

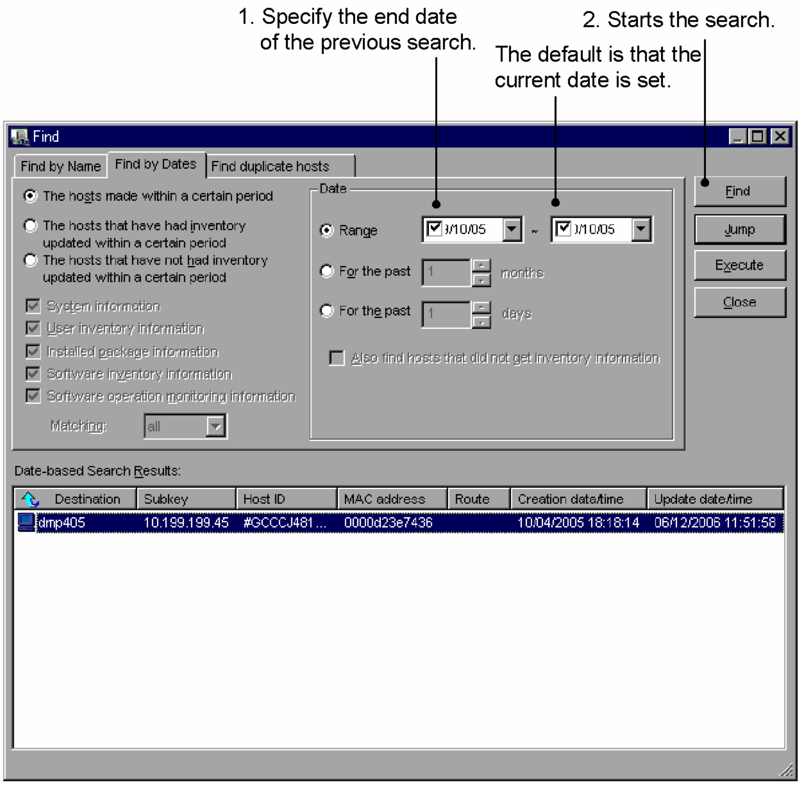
Destination	Subkey	Host ID	MAC address	Route	Creation data/time	Update date/time
dmp205	10.199.199.25	#G6BAAANH5	0000e25c0623		09/06/2005 14:48:14	06/12/2006 11:47:30
dmp308					09/02/2005 18:18:14	06/12/2006 11:47:30

3. The clients added between August 10 and September 10 are retrieved.

4. You can take actions on the clients, such as registering them into host groups, and executing jobs.

Figure 9–7: Example of managing the new clients added within a specified time period (2/2)

■ Second search: October 10, 2005



1. Specify the end date of the previous search.

2. Starts the search.

The default is that the current date is set.

● The hosts made within a certain period

○ The hosts that have had inventory updated within a certain period

○ The hosts that have not had inventory updated within a certain period

☑ System information

☑ User inventory information

☑ Installed package information

☑ Software inventory information

☑ Software operation monitoring information

Matching: all

Date

● Range ☑ /10/05 ~ ☑ /10/05

○ For the past 1 months

○ For the past 1 days

□ Also find hosts that did not get inventory information

Date-based Search Results:

Destination	Subkey	Host ID	MAC address	Route	Creation date/time	Update date/time
dmp405	10.199.199.45	#GCCCJ481 ...	0000d23e7436		10/04/2005 18:18:14	06/12/2006 11:51:58

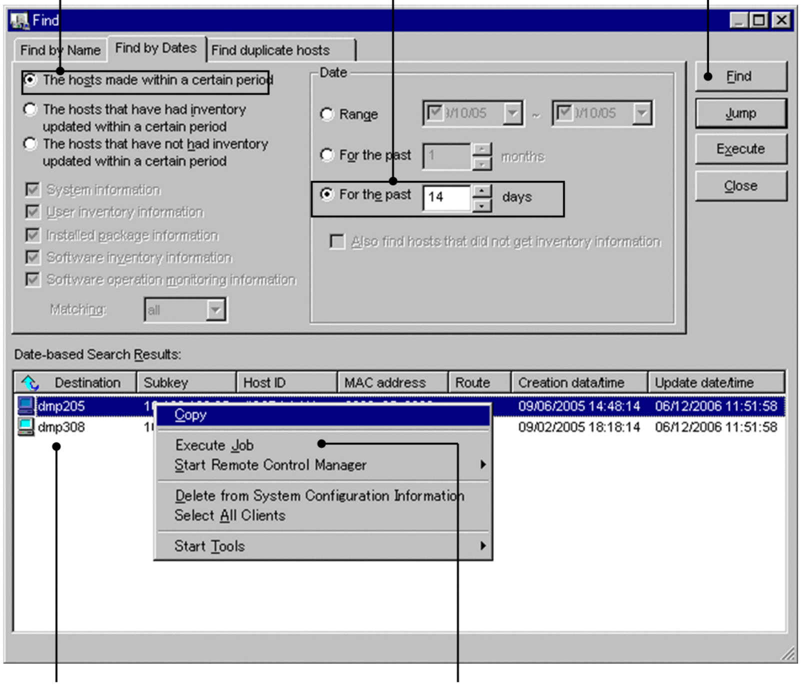
The figure below shows an example of managing newly added clients every 14 days (biweekly). To manage newly added clients at a specific interval, specify as shown in this example.

Figure 9–8: Example of managing newly added clients every 14 days (biweekly) (1/2)

- First search: September 10, 2005

1. The search targets new clients added within the 14 days ending September 10 (between August 27 and September 10).

2. Starts the search.



● The hosts made within a certain period
○ The hosts that have had inventory updated within a certain period
○ The hosts that have not had inventory updated within a certain period
☑ System information
☑ User inventory information
☑ Installed package information
☑ Software inventory information
☑ Software operation monitoring information
Matching: all

Date
○ Range ☑ 9/10/05 ~ ☑ 9/10/05
○ For the past 1 months
● For the past 14 days
□ Also find hosts that did not get inventory information

Date-based Search Results:

Destination	Subkey	Host ID	MAC address	Route	Creation data/time	Update date/time
dmp205	1[illegible]	[illegible]	[illegible]		09/06/2005 14:48:14	06/12/2006 11:51:58
dmp308	1[illegible]	[illegible]	[illegible]		09/02/2005 18:18:14	06/12/2006 11:51:58

3. The clients added between August 27 and September 10 are retrieved.

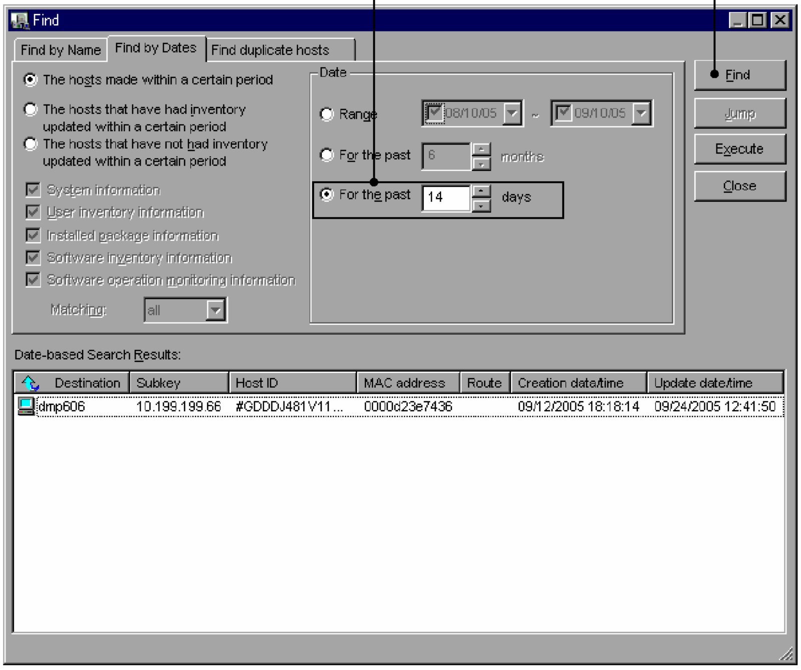
4. You can take actions on the clients, such as registering them into host groups, and executing jobs.

Figure 9–9: Example of managing newly added clients every 14 days (biweekly) (2/2)

■ Second search: September 24, 2005

The default is that the same number of days used in the previous search (14) is set.

1. Starts the search.



Find

Find by Name | Find by Dates | Find duplicate hosts

● The hosts made within a certain period

○ The hosts that have had inventory updated within a certain period

○ The hosts that have not had inventory updated within a certain period

☑ System information

☑ User inventory information

☑ Installed package information

☑ Software inventory information

☑ Software operation monitoring information

Matching: all

Date

○ Range ☑ 08/10/05 ~ ☑ 09/10/05

○ For the past 6 months

● For the past 14 days

Find | Jump | Execute | Close

Date-based Search Results:

Destination	Subkey	Host ID	MAC address	Route	Creation data/time	Update date/time
dmp606	10.199.199.66	#GDDDJ481V11...	0000d23e7436		09/12/2005 18:18:14	09/24/2005 12:41:50

(2) Example of deleting unneeded clients

When you periodically execute a job that obtains inventory information and there is a client that does not actually exist registered in the system configuration information, the date and time when the inventory of the client was last updated remain without being updated because the job has never executed.

By searching for the dates and times when the inventory information was last updated, you can identify clients whose inventory information could not be obtained over a specified period. Such clients are probably unneeded resources, so you may want to delete from the system configuration information.

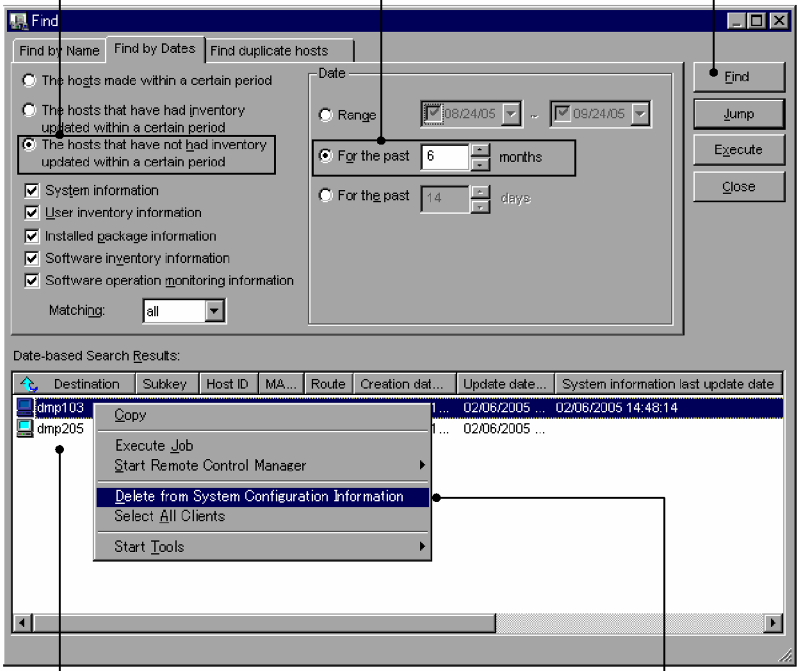
The following figure shows an example of deleting from the system configuration information clients whose inventory information has not been obtained for at least six months.

Figure 9–10: Example of deleting clients whose inventory information has not been obtained for at least six months

■ Search date: September 24, 2005

1. The search targets clients whose inventory information has not been updated for at least 6 months.

2. Starts the search.



○ The hosts made within a certain period
○ The hosts that had inventory updated within a certain period
● The hosts that have not had inventory updated within a certain period

☑ System information
☑ User inventory information
☑ Installed package information
☑ Software inventory information
☑ Software operation monitoring information

Matching: all

Date

○ Range ☑ 08/24/05 ~ ☑ 09/24/05
● For the past 6 months
○ For the past 14 days

Date-based Search Results:

Destination	Subkey	Host ID	MA...	Route	Creation dat...	Update date...	System information last update date
dmp103					1...	02/06/2005 ...	02/06/2005 14:48:14
dmp205					1...	02/06/2005 ...	

3. The clients whose inventory information was last updated before March 24, 2005 (which is 6 months ago) are found. The clients whose inventory information has never been collected are also included.

4. Deletes the retrieved clients from the system configuration information.

(3) Example of deleting duplicate clients

Operations using host IDs sometimes result in duplicate clients in the system configuration because the host IDs are regenerated in the following cases:

- JP1/Software Distribution Client (client) is re-installed on a PC whose hard disk was replaced
- JP1/Software Distribution Client (client) was uninstalled without the uninstallation being reported to the higher system, and then was re-installed
- A PC was replaced and a new JP1/Software Distribution Client (client) was installed

If duplicate clients with different host IDs are registered in the system configuration, jobs may not be executed on the correct client.

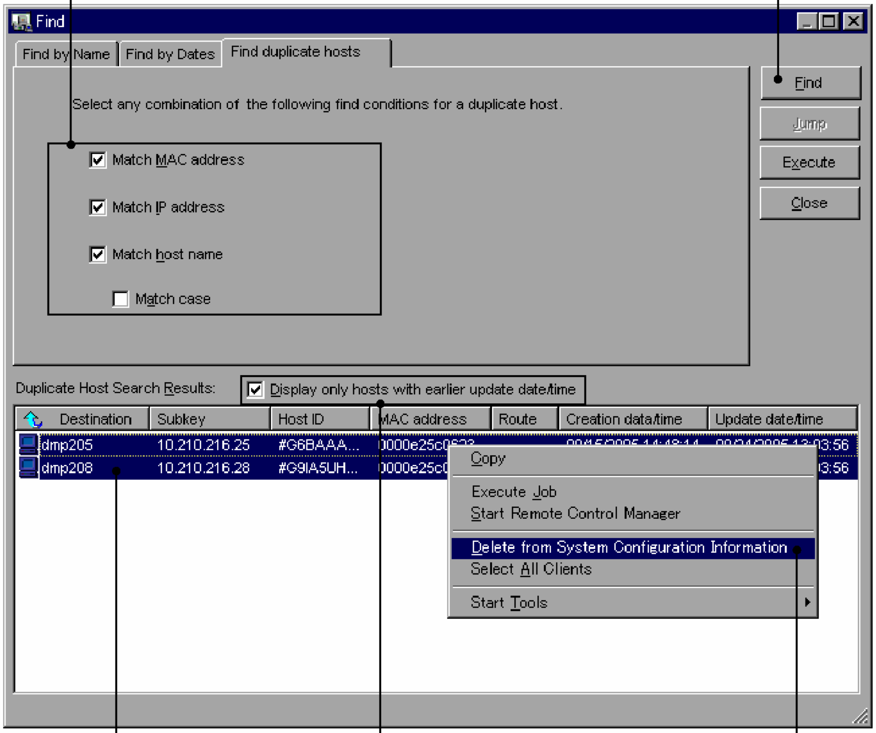
In such a case, you can delete the duplicate host from the system configuration information by searching for them and deleting the one with the older update date/time.

The example shown in the following figure searches for clients that have different host IDs but the same MAC address, IP address, or host name, and then deletes them from the system configuration information:

Figure 9–11: Example of deleting clients that have different host IDs but the same information, such as MAC address, from the system configuration information

1. Selects MAC address, IP address, and host name as conditions.

2. Starts the search.



Select any combination of the following find conditions for a duplicate host.

☑ Match MAC address

☑ Match IP address

☑ Match host name

□ Match case

Duplicate Host Search Results: ☑ Display only hosts with earlier update date/time

Destination	Subkey	Host ID	MAC address	Route	Creation data/time	Update date/time
dmp205	10.210.216.25	#G6BAAA...	0000e25c0623		09/15/2005 14:48:14	09/24/2005 13:03:56
dmp208	10.210.216.28	#G9IA5UH...	0000e25c			3:56

3. Duplicate hosts are retrieved and displayed in reverse video (unless their update date/time is up-to-date).

4. Select this check box to display only hosts whose update date/time is not up-to-date.

5. Selects the displayed hosts and deletes them from the system configuration information.

9.2 Automatic maintenance of system configuration information

You can detect unneeded hosts and automatically delete them from the system configuration information, host groups, and ID groups.

There are two ways to automatically maintain system configuration information:

- Automatically deleting unupdated clients
- Automatically deleting duplicate clients

This section describes how to automatically maintain system configuration information and output log files; it also provides notes on using automatic maintenance.

9.2.1 Automatically deleting unupdated clients

This facility uses the following inventory information updating dates/times to identify hosts as being unneeded, because their inventory information has not been updated for a specific period of time:

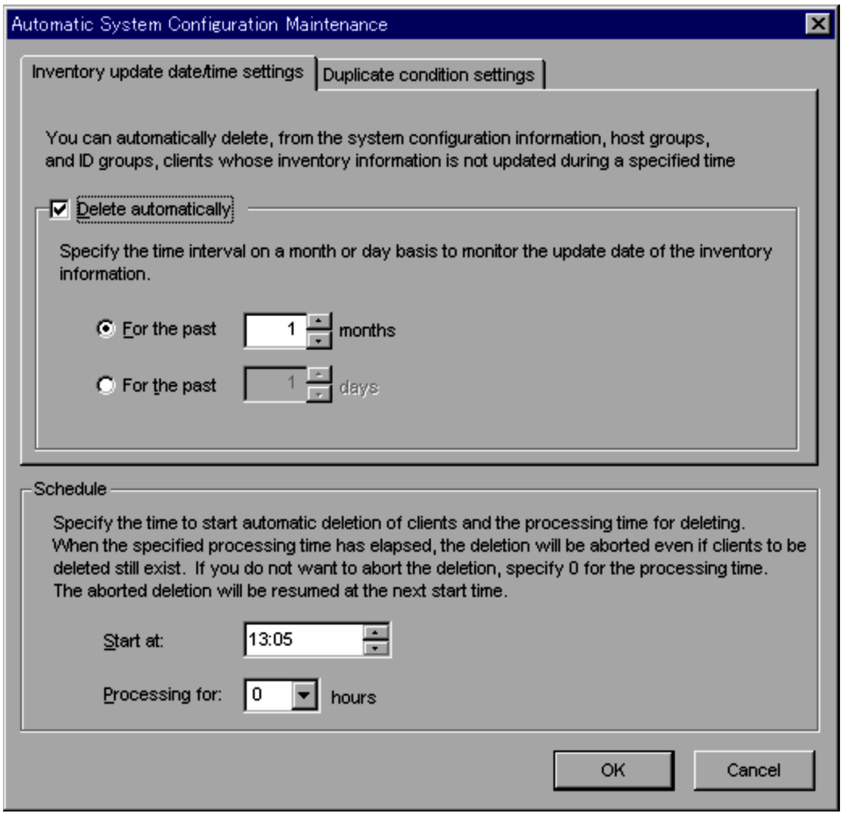
- Last time system information was updated
- Last time installed package information was updated
- Last time user inventory information was updated
- Last time registry information was updated
- Last time software inventory information was updated

This subsection describes how to set an inventory updating date/time and automatically delete unupdated clients.

To set automatic maintenance:

1. In the System Configuration window, choose **Options**, and then **Auto System Configuration Maintenance**.
   The Automatic System Configuration Maintenance dialog box appears.
2. Choose the **Inventory update date/time settings** tab.
   The **Inventory update date/time settings** page is displayed.

Figure 9–12: Inventory update date/time settings page



Automatic System Configuration Maintenance

Inventory update date/time settings | Duplicate condition settings

You can automatically delete, from the system configuration information, host groups, and ID groups, clients whose inventory information is not updated during a specified time

☑ Delete automatically

Specify the time interval on a month or day basis to monitor the update date of the inventory information.

● For the past 1 months

○ For the past 1 days

Schedule

Specify the time to start automatic deletion of clients and the processing time for deleting. When the specified processing time has elapsed, the deletion will be aborted even if clients to be deleted still exist. If you do not want to abort the deletion, specify 0 for the processing time. The aborted deletion will be resumed at the next start time.

Start at: 13:05

Processing for: 0 hours

3. Select **Delete automatically**, and specify the settings.

   For the past *n* months

   This item lets you specify a search range of months in the past from the current date to find hosts whose inventory information has not changed within the specified period. You can specify 1-999. However, the search range cannot cover the period earlier than January 1, 1971.

   For the past *n* days

   This item lets you specify a search range of days in the past from the current date to find the hosts whose inventory information has not changed within the specified period. You can specify 1-999. However, the search range cannot cover the period earlier than January 1, 1971.

   Schedule

   These items enable you to specify a time for starting automatic client deletion and a maximum processing time for automatic client deletion. When automatic client deletion starts, it will terminate when the maximum processing time elapses, even if there are still clients remaining to be deleted. If the maximum processing time is set to 0, the deletion processing will not be terminated until all clients that should be deleted have been deleted. Whenever some clients that should have been deleted remain, they are deleted the next time deletion processing is performed.

4. After specifying the settings, click the **OK** button.

   Regardless of the time on the day when you choose **OK**, automatic maintenance of the system configuration is activated for the first time the next day, even if the specified start time has not been reached on the current day.

9.2.2 Automatically deleting duplicate clients

To set conditions for finding duplicate hosts and to automatically delete those duplicate clients whose update date/time is old:

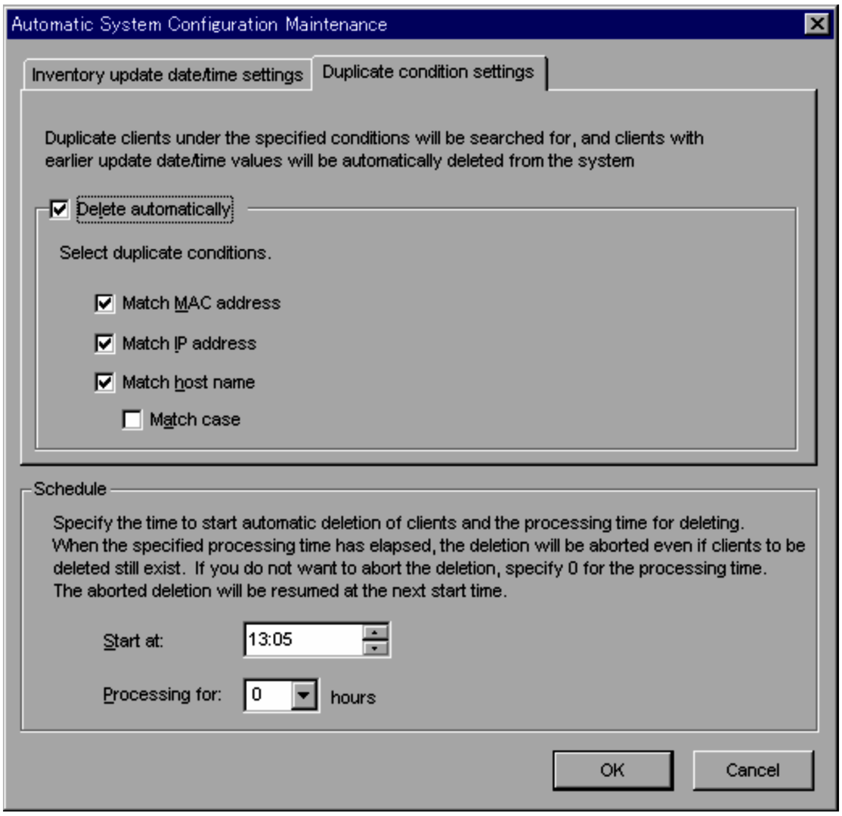
1. In the System Configuration window, choose **Options**, and then **Auto System Configuration Maintenance**.

   The Automatic System Configuration Maintenance dialog box appears.

2. Choose the **Duplicate condition settings** tab.

The **Duplicate condition settings** page is displayed.

Figure 9–13: Duplicate condition settings page



Automatic System Configuration Maintenance

Inventory update date/time settings
Duplicate condition settings

Duplicate clients under the specified conditions will be searched for, and clients with earlier update date/time values will be automatically deleted from the system

☑ Delete automatically

Select duplicate conditions.

☑ Match MAC address

☑ Match IP address

☑ Match host name

□ Match case

Schedule

Specify the time to start automatic deletion of clients and the processing time for deleting. When the specified processing time has elapsed, the deletion will be aborted even if clients to be deleted still exist. If you do not want to abort the deletion, specify 0 for the processing time. The aborted deletion will be resumed at the next start time.

Start at: 13:05

Processing for: 0 hours

3. Select the **Delete automatically** check box and set the applicable items.

   The system will search for hosts that have different host IDs but which satisfy the conditions you select here. When you select multiple conditions, they are treated as `AND` conditions. If you include MAC address as a condition, neither UNIX clients nor clients with PPP connection will be searched. In the case of a UNIX client with version 08-10 or later, if MAC addresses are set to be acquired in the system configuration information, duplicate hosts can be searched.

   Match MAC address

   Searches for multiple hosts that have the same MAC address in the system configuration information.

   Match IP address

   Searches for multiple hosts that have the same IP address in the system configuration information.

   Match host name

   Searches for multiple hosts that have the same host name in the system configuration information.

   Schedule

   Specifies a time for starting automatic client deletion and a maximum processing time for automatic client deletion. When automatic client deletion starts, it will terminate when the maximum processing time elapses, even if there are still clients remaining to be deleted. If the maximum processing time is set to 0, the deletion processing will not be terminated until all clients that should be deleted have been deleted. Whenever some clients that should have been deleted remain, they are deleted the next time deletion processing is performed.

4. After specifying the settings, click the **OK** button.

   Regardless of the time on the day when you choose **OK**, automatic maintenance of the system configuration is activated for the first time the next day, even if the specified start time has not been reached on the current day.

9.2.3 Log files for automatic maintenance of the system configuration information

Information about the deleted clients is output to log files together with the search conditions. The log files are contained in the `\log` directory in the installation directory. The `\log` directory can contain up to five log files.

Each time a deletion is performed, a new log file is created until five log files have been created. The name `CLTDEL.LOG` is assigned to the first log file, `CLTDEL.LOG1` to the second, `CLTDEL.LOG2` to the third, `CLTDEL.LOG3` to the fourth, and `CLTDEL.LOG4` to the fifth. After five log files have been created, the next log file overwrites the oldest log file with the latest information.

Reference these log files as required.

9.2.4 Notes on automatic maintenance of the system configuration information

- If a deleted host is left in a job definition as a destination, the destination is not deleted.
- In the following cases, immediately after a client is registered in the system configuration information, the last inventory update date and time is cleared. Therefore, the client is handled as a client from which inventory information was not acquired.
  - When the client version is 06-51 and the inventory information is not reported during automatic registration of the system configuration
  - When the client version is 06-01 or earlier
  - The client is manually added in the system configuration information

  Before executing automatic maintenance of the system configuration, use a function such as Manual System Configuration Maintenance to detect such clients and execute a job to acquire their inventory information. We recommend that you acquire inventory information on a periodic basis.
- If you execute automatic maintenance of system configuration information at a relay manager, you should periodically execute a *Get system configuration information* job from the relay manager's higher system to conform the system configuration information in the entire system.
- Offline machines are also subject to automatic maintenance of system configuration information. Because the inventory information in an offline machine is not updated periodically, it may be deleted from the system configuration during automatic maintenance. To prevent this, you should make a backup of the inventory information in the offline machine and store the backup medium. Alternatively, you can maintain the system configuration information manually so that it will not be deleted from the offline machine.

9.3 Automatic maintenance of host groups

JP1/Software Distribution can detect automatically newly added hosts and moved hosts and assign them to host groups on the basis of predefined grouping conditions (a *policy*). This facility is called *auto host group maintenance*.

This section describes how to set a policy for host groups and how to apply the policy to host groups in batch mode. It also describes examples of operations that involve policy setting for host groups.

9.3.1 Setting a policy for host groups

This subsection shows the method for setting a policy for host groups.

For details about specifying host group names when you set a policy, see *8.2.2 How to assign group names*.

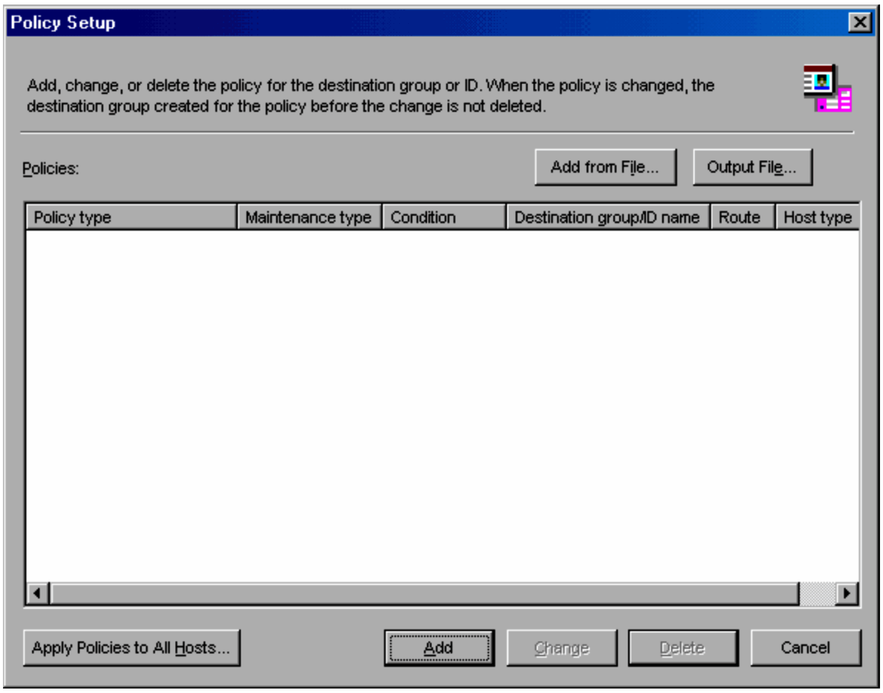
To set the policy for host groups:

1. In the Destination window, choose **Options**, and then **Auto Host Group/ID Maintenance**.

   The Policy Setup dialog box appears.

   Another way to display this dialog box is to choose **File**, and then **Create Host Group** to display the Create Host Group dialog box. Then, in this dialog box, choose **Create the policy for a host group**.

   Figure 9–14: Policy Setup dialog box



Policy Setup

Add, change, or delete the policy for the destination group or ID. When the policy is changed, the destination group created for the policy before the change is not deleted.

Policies:

Policy type	Maintenance type	Condition	Destination group/ID name	Route	Host type

   For the conditions, the Policy Setup dialog box displays a maximum of 260 characters. No subsequent characters, if any, are displayed but they are set correctly in the conditions.

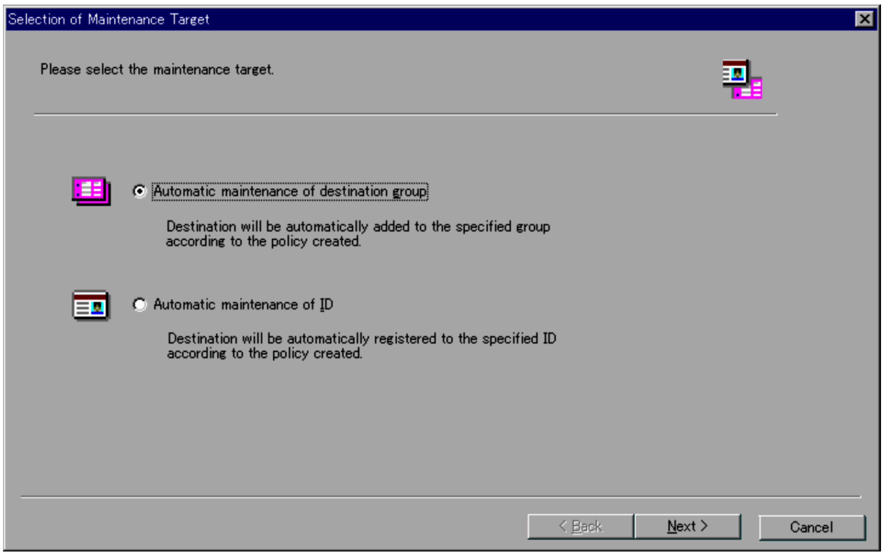
   To add a new policy, click the **Add** button. To change an existing policy, select the desired policy and then click the **Change** button. You can edit an existing policy directly by double-clicking **Host group name** and **Route** in the list.

   To delete an existing policy, select the desired policy and then click the **Delete** button. Deleting a policy does not delete the host group created by that policy. The hosts registered by the policy are not deleted from the corresponding host group.

2. Click the **Add** button.

   The Selection of Maintenance Target dialog box appears.

Figure 9–15: Selection of Maintenance Target dialog box



Selection of Maintenance Target

Please select the maintenance target.

● Automatic maintenance of destination group

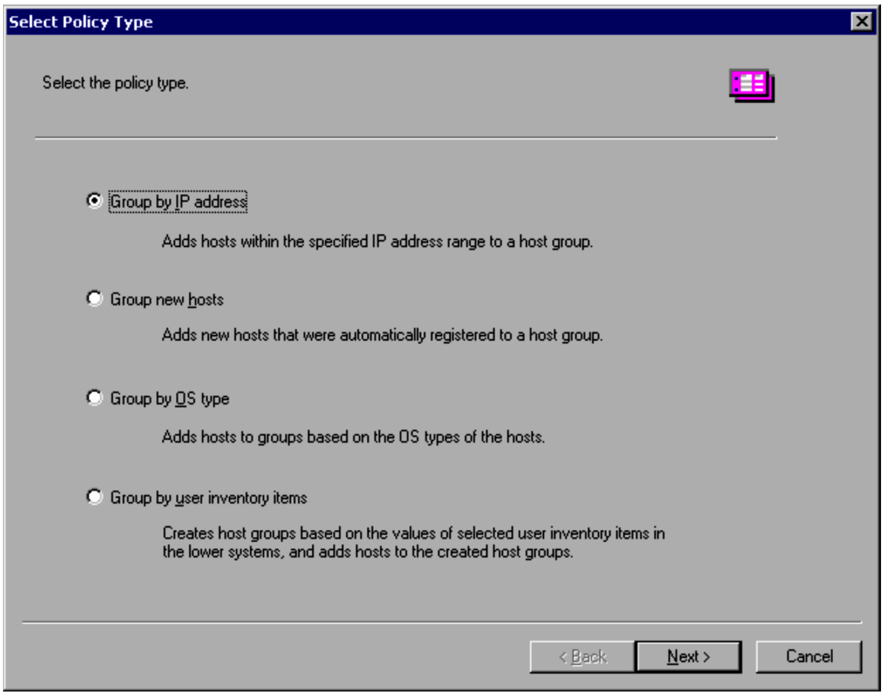
Destination will be automatically added to the specified group according to the policy created.

○ Automatic maintenance of ID

Destination will be automatically registered to the specified ID according to the policy created.

3. Choose **Automatic maintenance of destination group** and then click the **Next** button.
   The Select Policy Type dialog box appears.

Figure 9–16: Select Policy Type dialog box



Select Policy Type

Select the policy type.

● Group by IP address

Adds hosts within the specified IP address range to a host group.

○ Group new hosts

Adds new hosts that were automatically registered to a host group.

○ Group by OS type

Adds hosts to groups based on the OS types of the hosts.

○ Group by user inventory items

Creates host groups based on the values of selected user inventory items in the lower systems, and adds hosts to the created host groups.

4. Select the desired type of policy and then click the **Next** button.
5. In the displayed dialog box, set the policy.
   The dialog box that is displayed depends on the selected policy type. For details about the settings in the dialog box for each policy type, see subsections (1) through (4) below, as indicated in the following table:

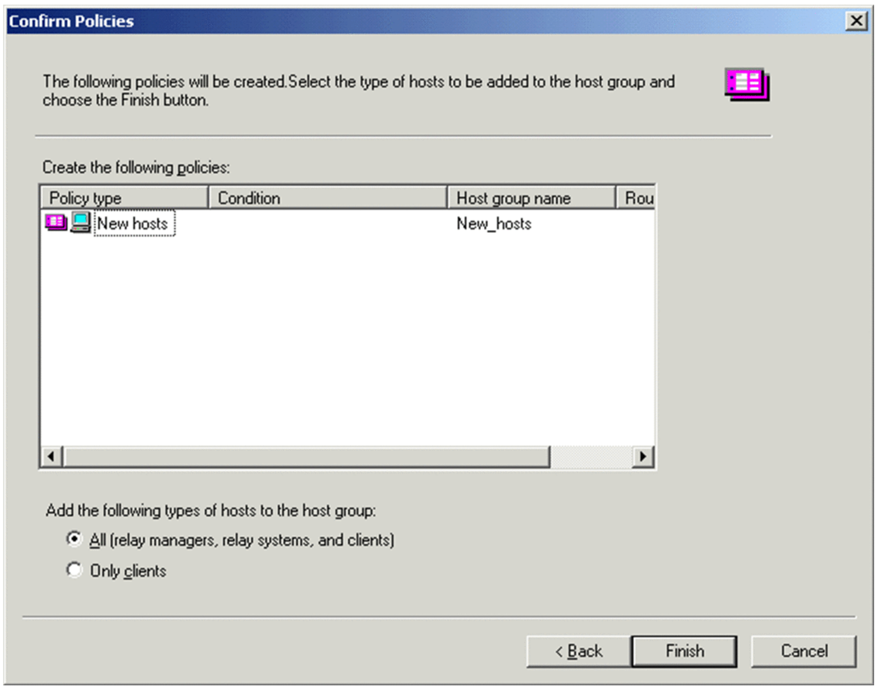
Selection item	Reference
Group by IP Address dialog box	*(1) Settings in the Group by IP Address dialog box*
Group New Hosts dialog box	*(2) Settings in the Group New Hosts dialog box*
Group by OS Type dialog box	*(3) Settings in the Group by OS Type dialog box*

Selection item	Reference
Group by User Inventory Items dialog box	*(4) Settings in the Group by User Inventory Items dialog box*

6. When you finish specifying the policy settings, click the **Next** button.

   The Confirm Policies dialog box appears.

   Figure 9–17: Confirm Policies dialog box



Confirm Policies

The following policies will be created.Select the type of hosts to be added to the host group and choose the Finish button.

Create the following policies:

Policy type	Condition	Host group name	Rou
New hosts		New_hosts	

Add the following types of hosts to the host group:

● All (relay managers, relay systems, and clients)

○ Only clients

For the conditions, the Confirm Policies dialog box displays a maximum of 260 characters. No remaining characters, if any, are displayed, but they are set correctly in the conditions.

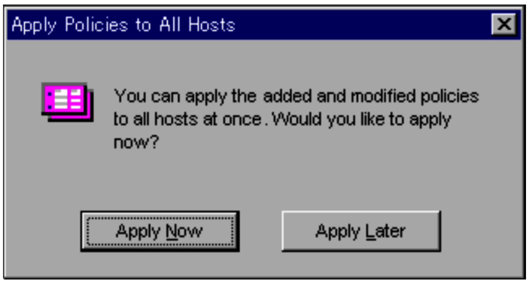
Add the following types of hosts to the host group:

This item lets you select the type(s) of hosts that are added by the policy. When you select **Only clients**, clients on the same PC as a relay manager or relay system are not added. Select this if you do not need to distribute jobs to a relay manager or relay system, or if you do not need to acquire inventory from a relay manager or relay system.

7. Click the **Finish** button.

   The policy is created and the Apply Policies to All Hosts dialog box appears. However, if you created a Policy type that is a new host, the Policy Setup dialog box reappears instead of the Apply Policies to All Hosts dialog box.

   Figure 9–18: Apply Policies to All Hosts dialog box



Apply Policies to All Hosts

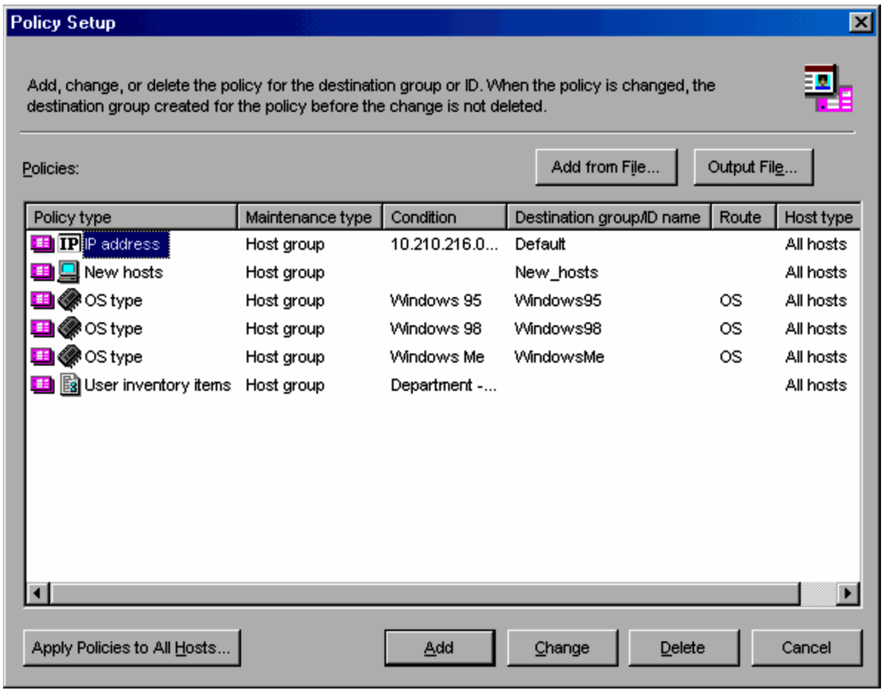
You can apply the added and modified policies to all hosts at once. Would you like to apply now?

Select in the Apply Policies to All Hosts dialog box whether or not added or modified policies are to be applied immediately in the batch mode.

Click the **Apply Now** button to immediately apply the added or modified policies to all host groups. **Click** the **Apply Later** button to return to the Policy Setup dialog box. Clicking the **Apply Later** button displays the Policy Setup dialog box again.

Note that if more than one policy adds hosts to the same host group, no error occurs.

Figure 9–19: Policy Setup dialog box



Add, change, or delete the policy for the destination group or ID. When the policy is changed, the destination group created for the policy before the change is not deleted.

Policies:

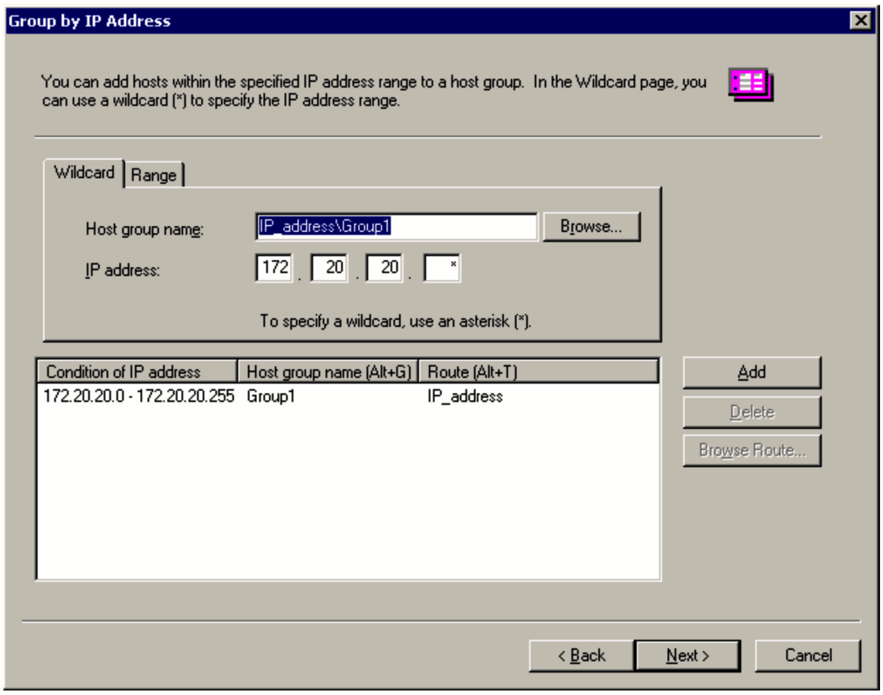
Policy type	Maintenance type	Condition	Destination group/ID name	Route	Host type
IP address	Host group	10.210.216.0...	Default		All hosts
New hosts	Host group		New_hosts		All hosts
OS type	Host group	Windows 95	Windows95	OS	All hosts
OS type	Host group	Windows 98	Windows98	OS	All hosts
OS type	Host group	Windows Me	WindowsMe	OS	All hosts
User inventory items	Host group	Department -...			All hosts

(1) Settings in the Group by IP Address dialog box

You use this dialog box to group clients by a specified range of IP addresses. You can select batch specification (**Wildcard**) or range specification (**Range**).

Wildcard page

Figure 9–20: Wildcard page



You can add hosts within the specified IP address range to a host group. In the Wildcard page, you can use a wildcard (*) to specify the IP address range.

Host group name: IP_address\Group1

IP address: 172 . 20 . 20 . *

To specify a wildcard, use an asterisk (*).

Condition of IP address	Host group name (Alt+G)	Route (Alt+T)
172.20.20.0 - 172.20.20.255	Group1	IP_address

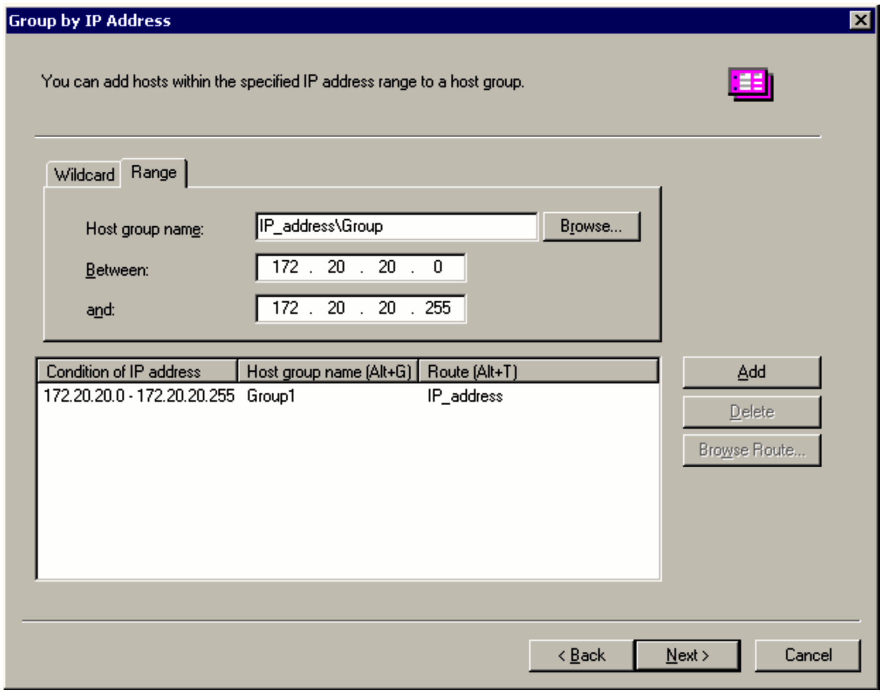
On this page, specify host group names and IP addresses. Use the asterisk (`*`) as a wildcard in the IP address you specify.

For example, you can specify `172.20.20.*` to create a group consisting of the IP addresses `172.20.20.0` through `172.20.20.255`.

When you click the **Add** button, the condition is added to the list. You can set multiple conditions in the Group by IP Address dialog box. To delete an existing condition, click the **Delete** button.

Range page

Figure 9–21: Range page



Group by IP Address

You can add hosts within the specified IP address range to a host group.

Host group name: IP_address\Group

Between: 172 . 20 . 20 . 0

and: 172 . 20 . 20 . 255

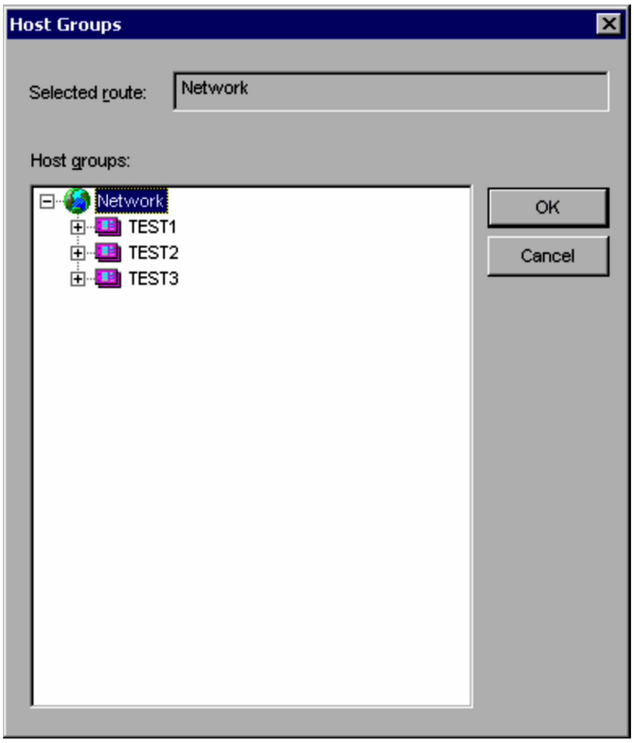
Condition of IP address	Host group name (Alt+G)	Route (Alt+T)
172.20.20.0 - 172.20.20.255	Group1	IP_address

On this tab, you can specify a range of IP addresses. When you add a policy, *IP-address*`\Default` is displayed in **Host group name** as the default path.

Browse Route button

On each tab, clicking the **Browse Route** button displays the Host Groups dialog box.

Figure 9–22: Host Groups dialog box



Selected route: Network

Host groups:

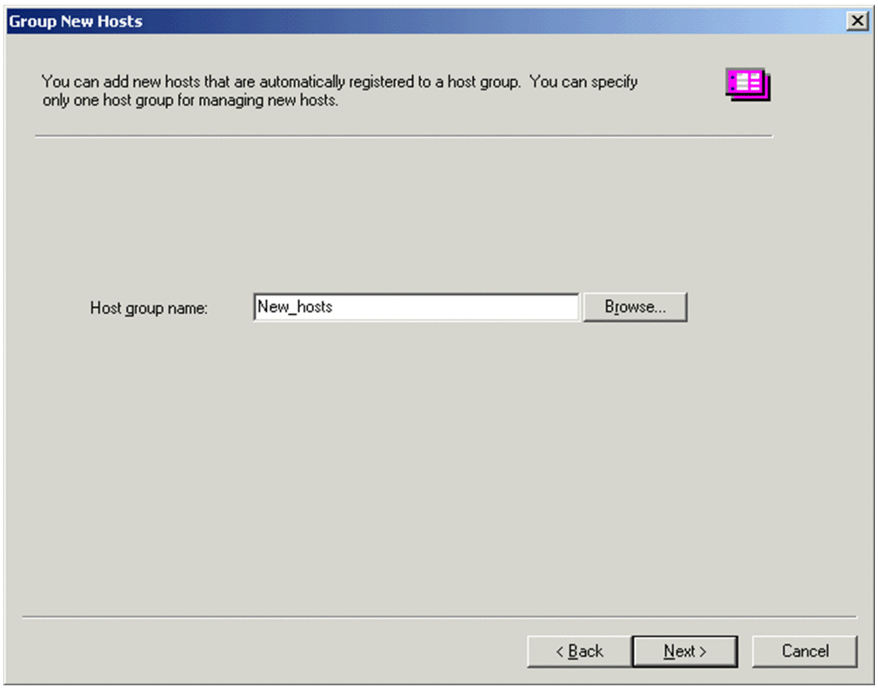
- Network
  - TEST1
  - TEST2
  - TEST3

This dialog box displays as a tree structure a listing of the current host groups. You can use this tree to set the route of a host group.

(2) Settings in the Group New Hosts dialog box

You use this dialog box to add to a group new hosts that have been registered in the system configuration information. When you use this policy, you can set only one host group.

Figure 9–23: Group New Hosts dialog box



You can add new hosts that are automatically registered to a host group. You can specify only one host group for managing new hosts.

Host group name: New_hosts

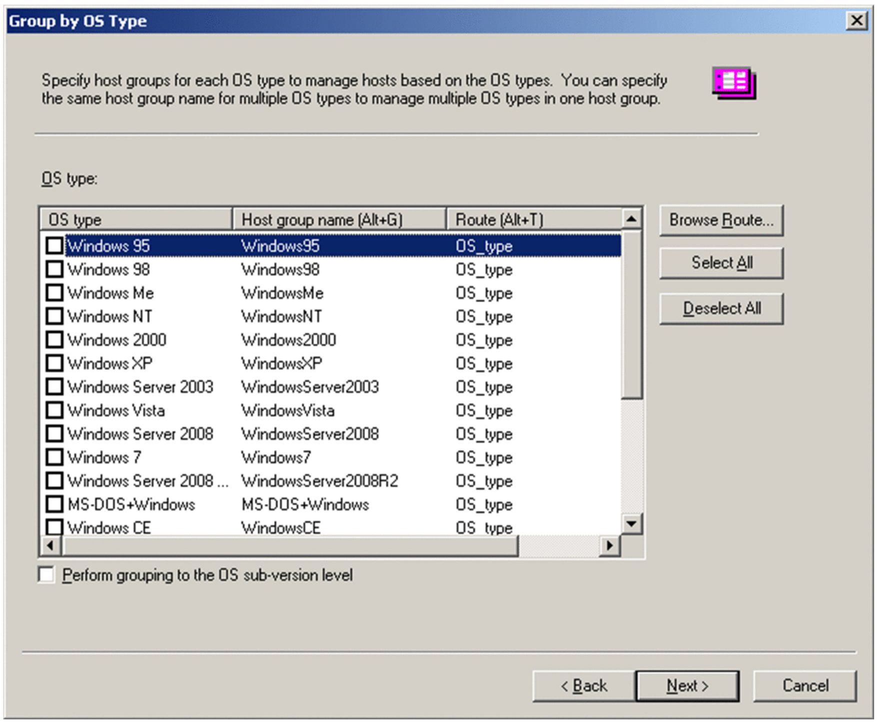
When you add this policy, **New host** is displayed by default in **Host group name**.

Clicking the **Browse Route** button displays the Host Groups dialog box described in (1), enabling you to select a route.

(3) Settings in the Group by OS Type dialog box

You use this dialog to group clients by the **OS type** system information.

Figure 9–24: Group by OS Type dialog box



Group by OS Type

Specify host groups for each OS type to manage hosts based on the OS types. You can specify the same host group name for multiple OS types to manage multiple OS types in one host group.

OS type:

OS type	Host group name (Alt+G)	Route (Alt+T)
□ Windows 95	Windows95	OS_type
□ Windows 98	Windows98	OS_type
□ Windows Me	WindowsMe	OS_type
□ Windows NT	WindowsNT	OS_type
□ Windows 2000	Windows2000	OS_type
□ Windows XP	WindowsXP	OS_type
□ Windows Server 2003	WindowsServer2003	OS_type
□ Windows Vista	WindowsVista	OS_type
□ Windows Server 2008	WindowsServer2008	OS_type
□ Windows 7	Windows7	OS_type
□ Windows Server 2008 ...	WindowsServer2008R2	OS_type
□ MS-DOS+Windows	MS-DOS+Windows	OS_type
□ Windows CE	WindowsCE	OS_type

□ Perform grouping to the OS sub-version level

Each OS type whose check box is selected is a target for grouping. You can set any desired host group name for each OS type. By setting the same host group name for more than one OS, you can use only one host group to manage the hosts with several OS types.

When you add a policy, `OS_type\` is displayed as the default path.

Clicking the **Browse Route** button displays the Host Groups dialog box described in (1), enabling you to select a route.

Clicking the **Select All** button selects the check boxes for all OS types. Clicking the **Deselect All** button clears the check boxes for all OS types.

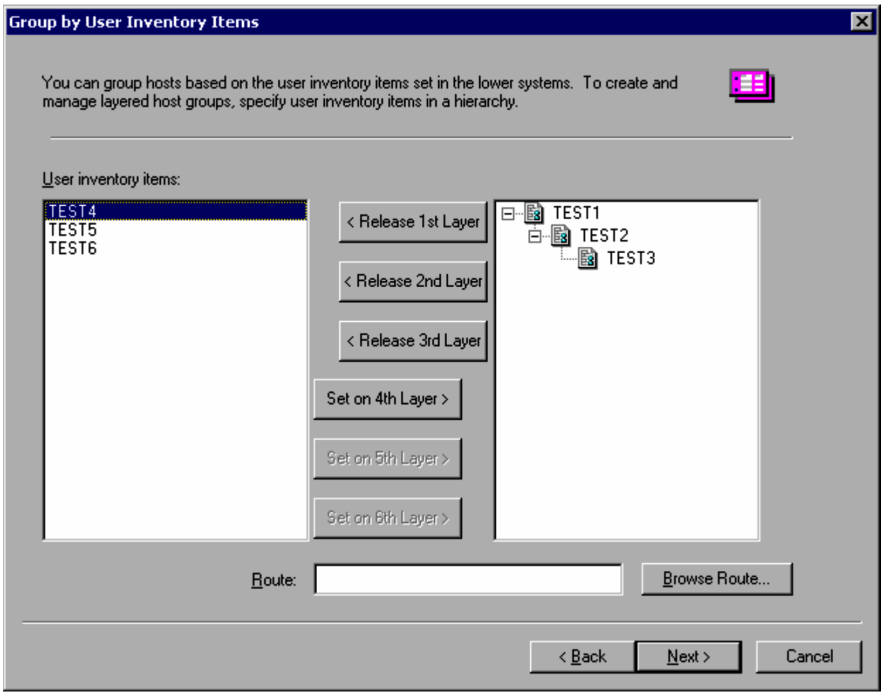
If you select the **Perform grouping to the OS sub-version level** check box, clients are grouped by OS sub-versions, such as Service Pack, under the OS-type host groups. However, if OS sub-version system information cannot be acquired, the clients are registered in host groups by OS type. If the value of OS sub-version exceeds 32 characters, the host group is treated as `unknown`.

(4) Settings in the Group by User Inventory Items dialog box

You use this dialog box to group clients by user inventory items. The user inventory information entered from clients provides the host group names for grouping of clients.

This dialog box displays only the items managed on local server, and the items managed on higher and local servers. You can create a maximum of 16 policies.

Figure 9–25: Group by User Inventory Items dialog box



Group by User Inventory Items

You can group hosts based on the user inventory items set in the lower systems. To create and manage layered host groups, specify user inventory items in a hierarchy.

User inventory items:

TEST4
TEST5
TEST6

TEST1
TEST2
TEST3

Route:

By specifying the user inventory in a hierarchical structure, you can manage the created host groups in a hierarchical structure; the hierarchy can have up to six levels.

Clicking the **Browse Route** button displays the Host Groups dialog box described in (1), enabling you to select a route.

The following restrictions apply to the user inventory information entered at a client during auto host group maintenance:

- User inventory information exceeding 32 bytes is not interpreted as a host group.
- You cannot use a tab character or the following special characters:
  `\ / * " ' : ; , & ! | . < > ? @ %`
- Trailing spaces are ignored.
- Do not use a space in the middle of data.
- Alphabetic letters are not case-sensitive for grouping hosts.
- The same user inventory information cannot be specified for multiple user inventory items that have different hierarchy levels in the policy. Because each host group name must be unique, a host group is not created if it has the same user inventory information as another host group.

  When you click the **Set on** *n* **Layer** button, the selected user inventory item is set as the host group for the *n*-th layer. After you set this, the button label changes to **Release** *n* **Layer**. Clicking the **Release** *n* **Layer** button releases the set layer. If there are sub-items, all of them are also released.

  Note that if a space is specified in the data part of user inventory information, host groups cannot be created as specified with the policy.
- On the higher system, if you delete or change a user inventory item that is managed on higher and local servers, the change or deletion of the user inventory item does not take effect on the relay manager/system even when the item is set in the policy in the relay manager/system. In such a case, an invalid user inventory item may be set in the policy in the relay manager/system, thereby preventing correct execution of automatic maintenance.

9.3.2 Applying policies to all host groups

This subsection describes how to apply an existing policy to all host groups. Note that you can only apply policies using this method to hosts that are already registered in the system configuration information. You cannot use this method for newly created hosts.

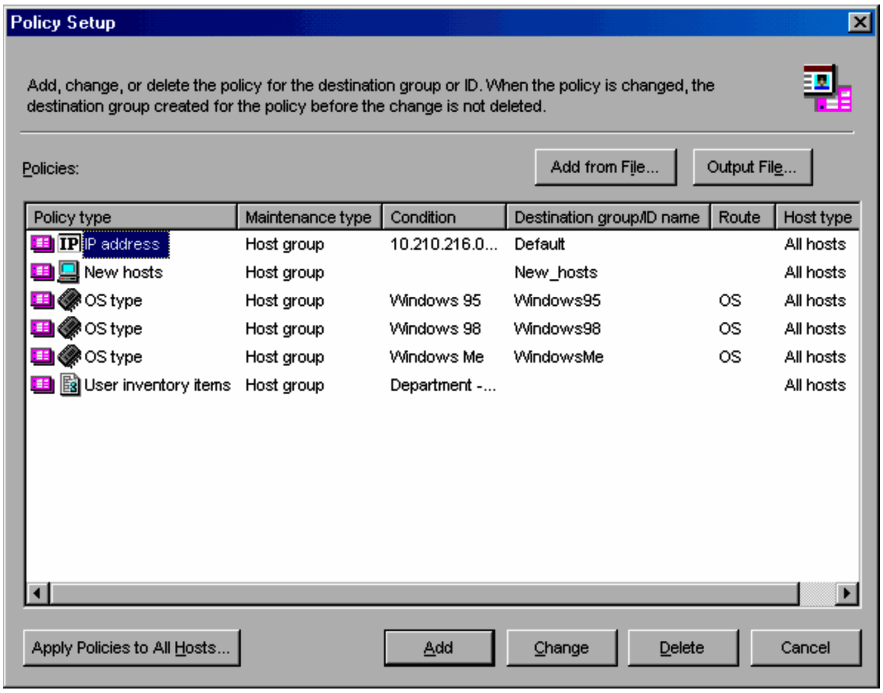
To apply policies to all host groups:

1. In the Destination window, choose **Options**, and then choose **Auto Host Group/ID Maintenance**.

   The Policy Setup dialog box appears.

   Another way to display this dialog box is to choose **File**, and then **Create Host Group** to display the Create Host Group dialog box. Then, in this dialog box, choose **Create the policy for a host group**.

   Figure 9–26: Policy Setup dialog box



Policy Setup

Add, change, or delete the policy for the destination group or ID. When the policy is changed, the destination group created for the policy before the change is not deleted.

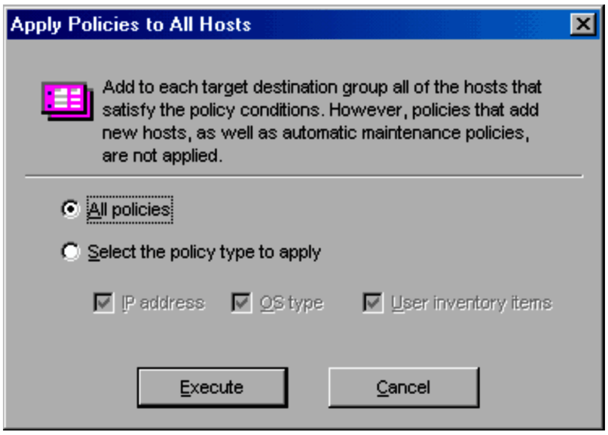
Policies:

Policy type	Maintenance type	Condition	Destination group/ID name	Route	Host type
IP address	Host group	10.210.216.0...	Default		All hosts
New hosts	Host group		New_hosts		All hosts
OS type	Host group	Windows 95	Windows95	OS	All hosts
OS type	Host group	Windows 98	Windows98	OS	All hosts
OS type	Host group	Windows Me	WindowsMe	OS	All hosts
User inventory items	Host group	Department -...			All hosts

2. Click the **Apply Policies to All Hosts** button.

   The Apply Policies to All Hosts dialog box appears.

   Figure 9–27: Apply Policies to All Hosts dialog box



Apply Policies to All Hosts

Add to each target destination group all of the hosts that satisfy the policy conditions. However, policies that add new hosts, as well as automatic maintenance policies, are not applied.

● All policies

○ Select the policy type to apply

☑ IP address ☑ OS type ☑ User inventory items

3. Select the policy type to be applied to all hosts, and then click the **Execute** button.

All policies

Choose **All policies** to add all policies displayed in the policy list of the Policy Setup dialog box to the host group. Note, however, that policies for newly created hosts are not applied.

Batch application is not applicable to a policy for ID groups regardless of the type.

Select the policy type to apply

Select the following policy types to be applied to all hosts; you can select more than one policy type:

IP address

OS type

User inventory items

Select the policy type(s) and then click the **Execute** button. Hosts registered in the system configuration information are added to host groups according to the selected policy.

(1) Immediately adding new hosts to host groups

If you want to immediately add new hosts to host groups according to the policy you set, use the following methods to update the host groups:

- **Group by IP address**
  For the relay manager and relay systems, execute a *Get system configuration information* job. For a client on the same PC as the relay manager, in the Destination window, choose **File**, and then **Create Destination** to open the Create Destination dialog box. Use this dialog box to add the hosts.
- **Group new hosts**
  In the System Configuration window, choose **Options**, and then **Find** to open the Find dialog box. Use this dialog box to find hosts by date, and then register the found hosts into the host group.
- **Group by OS type**
  Re-execute a *Get system configuration information* job.
- **Group by user inventory items**
  Re-execute a *Get user inventory information* job.

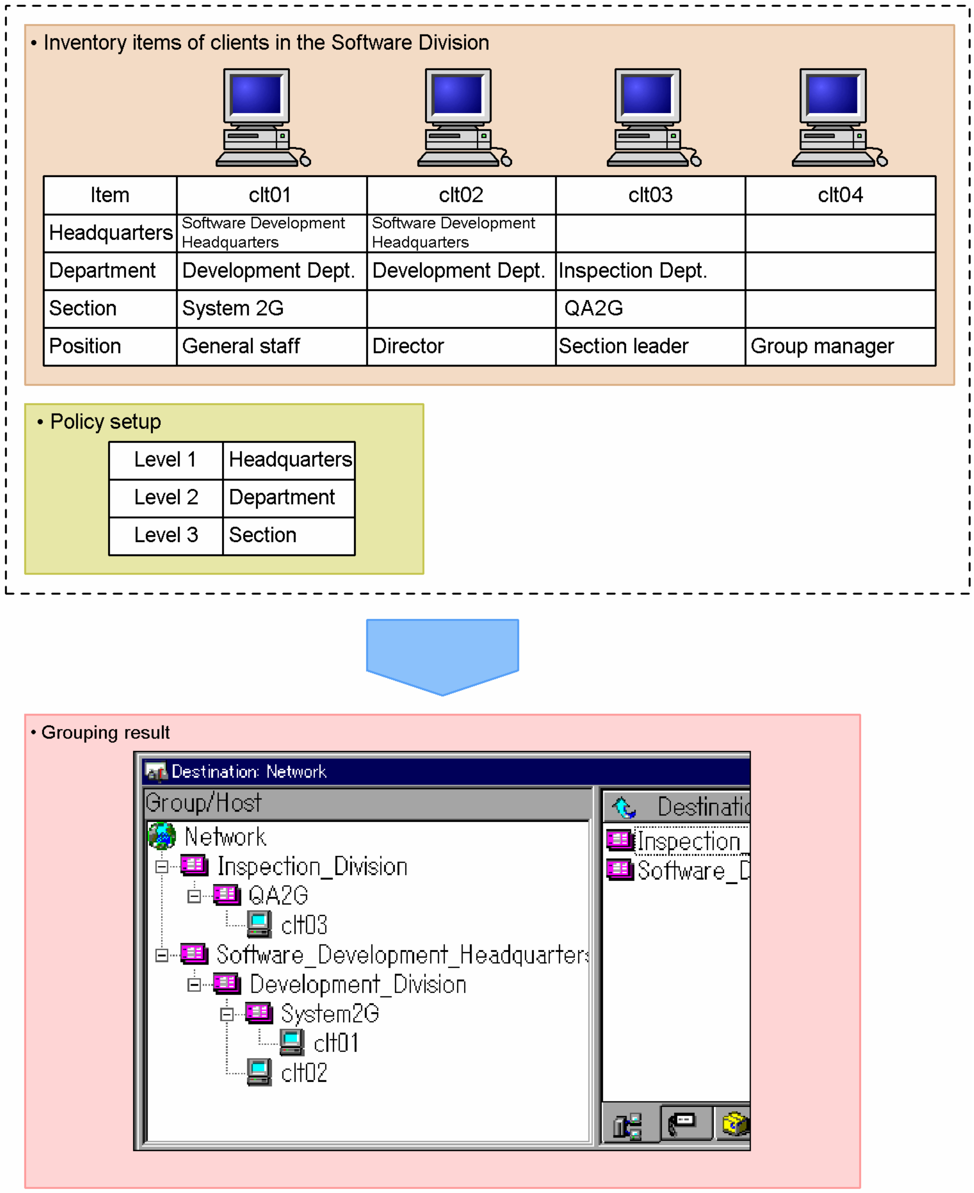
(2) Backing up a host group

To back up a host group, display the Destination window and rename the host group you want to save in a backup. When you rename a host group, the host group with the new name is excluded from auto host maintenance and can therefore be saved as a backup. If you add or change hosts after renaming the host group, the host group with the original name is re-created according to the policy setup and is subsequently updated.

9.3.3 Example of grouping using user inventory items

The figure below is an example of grouping when you set user inventory items in the policy. This example is based on clients in a Software Division.

Figure 9–28: Example of grouping by user inventory items (1)



• Inventory items of clients in the Software Division

Item	clt01	clt02	clt03	clt04
Headquarters	Software Development Headquarters	Software Development Headquarters		
Department	Development Dept.	Development Dept.	Inspection Dept.	
Section	System 2G		QA2G	
Position	General staff	Director	Section leader	Group manager

• Policy setup

Level 1	Headquarters
Level 2	Department
Level 3	Section

• Grouping result

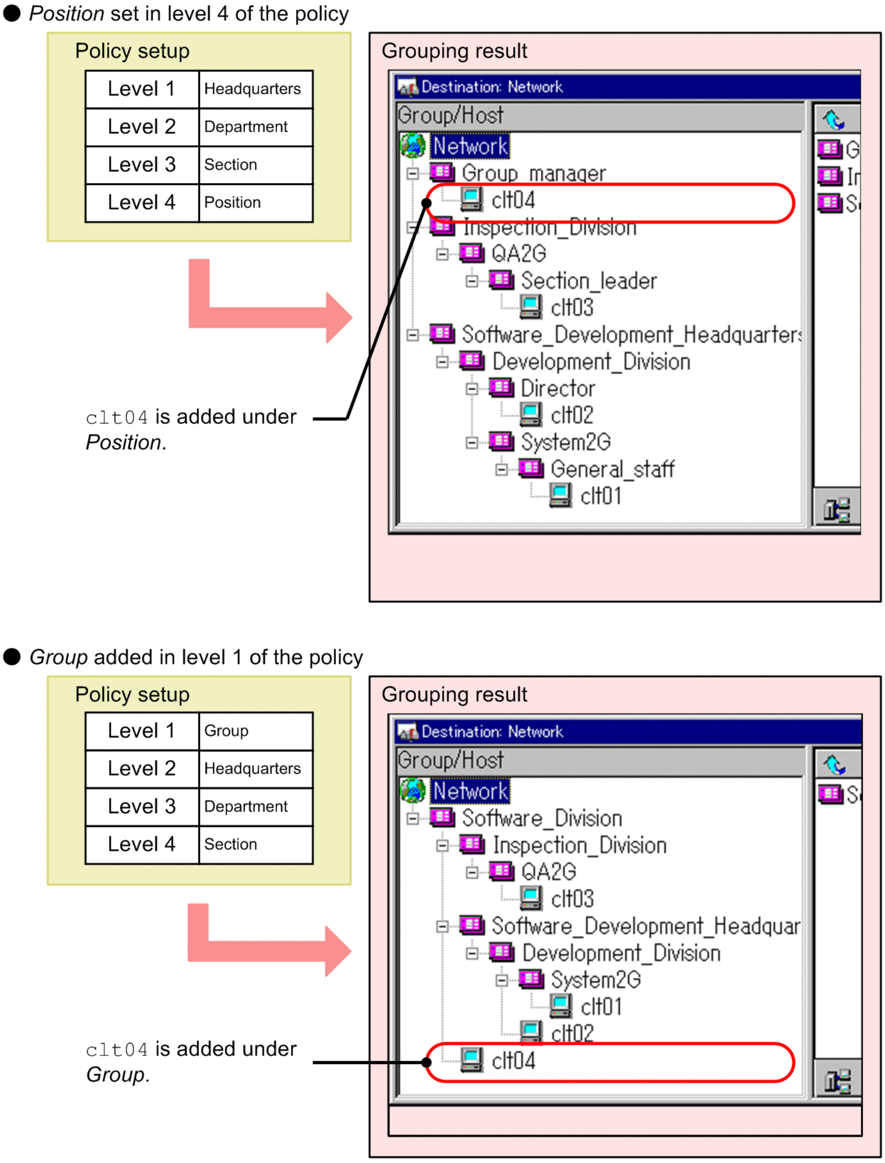
```
Network
  Inspection_Division
    QA2G
      clt03
  Software_Development_Headquarters
    Development_Division
      System2G
        clt01
      clt02
```

The following describes the result of the grouping in Figure 9-28.

- `clt01` is added under *Section* according to the policy setup.
- `clt02` does not have a *Section* because the *Position* is *Director*. In this case, the level corresponding to *Section* is moved up and `clt02` is added under *Department*.
- In `clt03`, the *Inspection* division is under the Software Division so there is no *Headquarters*. In this case, as with `clt02`, the level corresponding to *Headquarters* is moved up, *Department* is added at the top, and *Section* is added under *Department* and `clt03` is added under *Section*.
- `clt04` is not grouped by the policy setup in Figure 9-28. One way to group `clt04` would be to set the policy as follows:
    - Set *Position* in level 4 of the policy.
    - Insert *Group* in level 1 of the policy.

  The following figure shows the result of regrouping using these settings.

Figure 9–29: Example of grouping by user inventory items (2)



● *Position* set in level 4 of the policy

Policy setup

Level 1	Headquarters
Level 2	Department
Level 3	Section
Level 4	Position

Grouping result

`clt04` is added under *Position*.

● *Group* added in level 1 of the policy

Policy setup

Level 1	Group
Level 2	Headquarters
Level 3	Department
Level 4	Section

Grouping result

`clt04` is added under *Group*.

9.4 Automatic maintenance of ID groups

The operations that involve setting a policy for an ID group and then registering clients into the ID group automatically is called *automatic maintenance of ID groups*.

This section describes how to set policies for ID groups and provides notes on using automatic maintenance of ID groups.

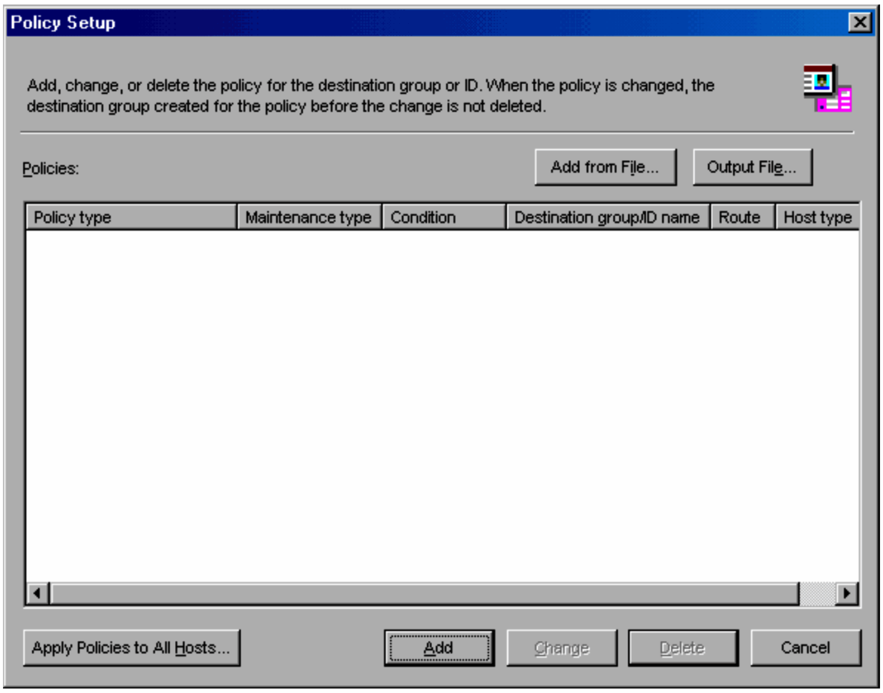
9.4.1 Setting a policy for an ID group

You can set a policy for an ID group from the central manager that manages the ID group or the relay manager specified as the relay managing the ID. This subsection describes how to set a policy for an ID group.

To set a policy for an ID group:

1. In the Destination window, choose **Options**, and then **Auto Host Group/ID Maintenance**.
   The Policy Setup dialog box appears.

   Figure 9–30: Policy Setup dialog box



Policy Setup

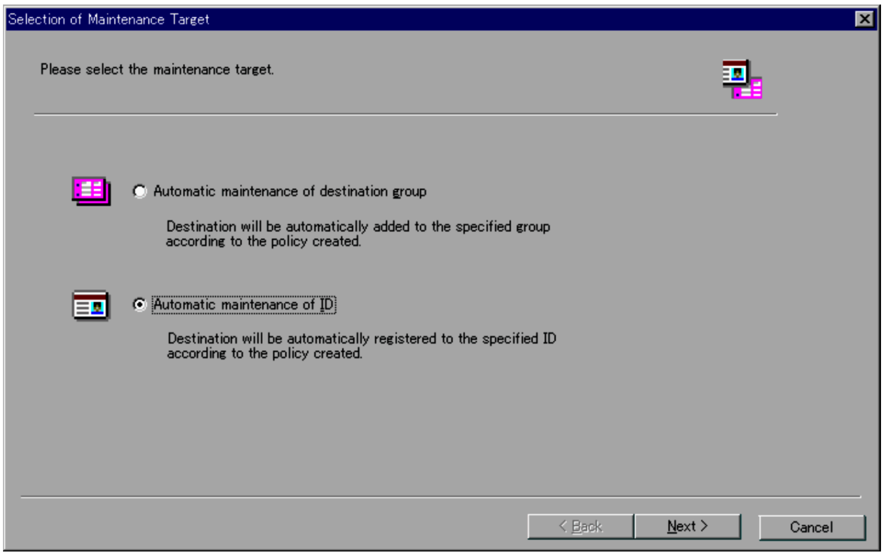
Add, change, or delete the policy for the destination group or ID. When the policy is changed, the destination group created for the policy before the change is not deleted.

Policies:

Policy type	Maintenance type	Condition	Destination group/ID name	Route	Host type

2. Click the **Add** button.
   To change an existing policy, select the applicable policy and then click the **Change** button. To delete a policy, select the applicable policy and then click the **Delete** button.
   Clicking the **Add** button displays the Selection of Maintenance Target dialog box.

Figure 9–31: Selection of Maintenance Target dialog box



Selection of Maintenance Target

Please select the maintenance target.

○ Automatic maintenance of destination group

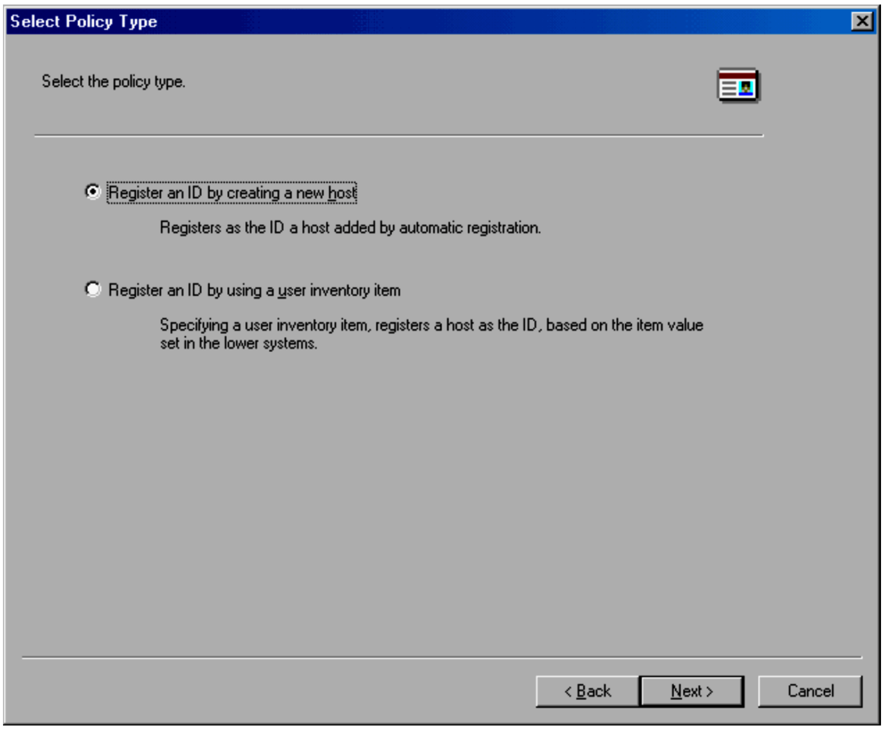
Destination will be automatically added to the specified group according to the policy created.

● Automatic maintenance of ID

Destination will be automatically registered to the specified ID according to the policy created.

Select **Automatic maintenance of ID**.

3. Click the **Next** button.
   The Select Policy Type dialog box appears.
   Figure 9–32: Select Policy Type dialog box



Select Policy Type

Select the policy type.

● Register an ID by creating a new host

Registers as the ID a host added by automatic registration.

○ Register an ID by using a user inventory item

Specifying a user inventory item, registers a host as the ID, based on the item value set in the lower systems.

4. Select a policy type that you want to set and then click the **Next** button.
5. In the displayed dialog box, set the policy.
   The dialog box to be displayed depends on the selected item. For details about the settings in each dialog box, see (1) or (2) shown in the following table:

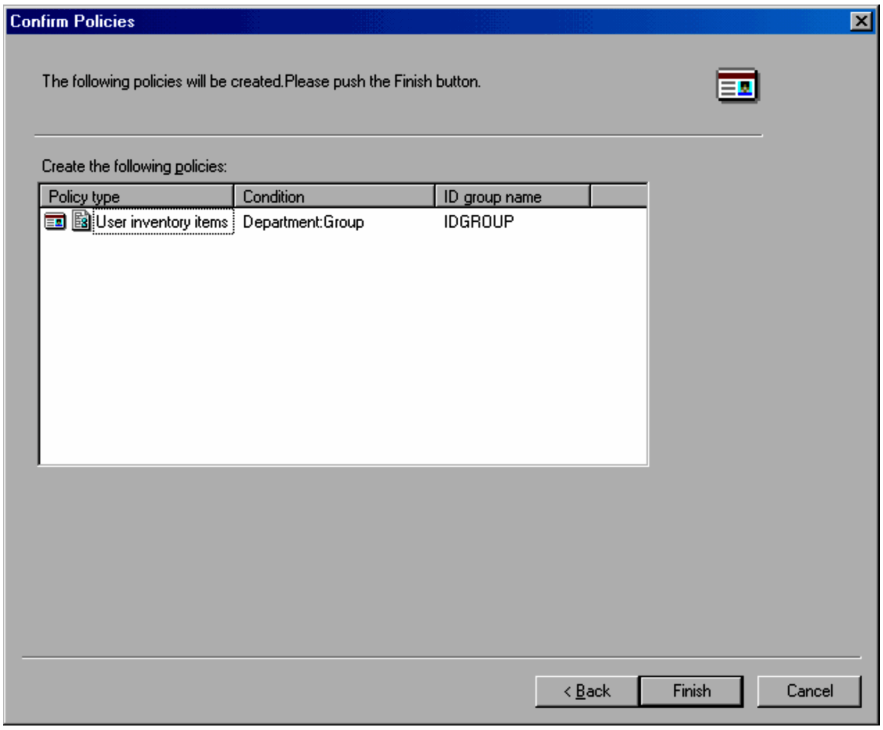
Selection item	See
Register an ID by creating a new host	*(1) Settings in the Register ID Based on New Host dialog box*

Selection item	See
Register an ID by using a user inventory item	*(2) Settings in the Register ID by Using User Inventory Item dialog box*

6. Click the **Next** button.

   The Confirm Policies dialog box appears.

   Figure 9–33: Confirm Policies dialog box



Confirm Policies

The following policies will be created.Please push the Finish button.

Create the following policies:

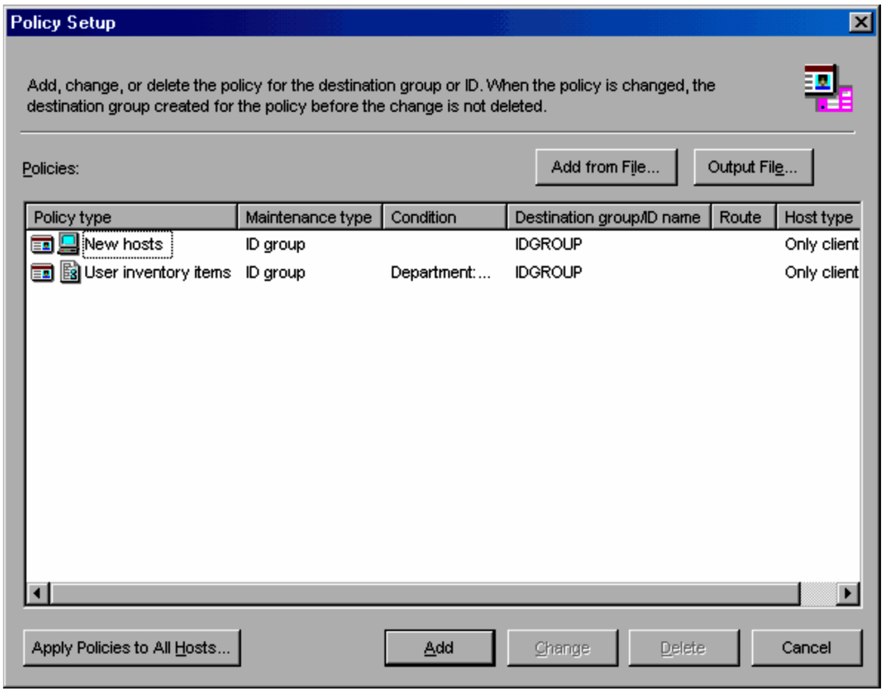
Policy type	Condition	ID group name
User inventory items	Department:Group	IDGROUP

   Confirm the ID group for which the policy is to be set. To select a different ID group, click the **Back** button to display the previous dialog box and then select the desired ID group.

7. Click the **Finish** button.

   The policy is displayed in the Policy Setup dialog box.

Figure 9–34: Policy Setup dialog box



Add, change, or delete the policy for the destination group or ID. When the policy is changed, the destination group created for the policy before the change is not deleted.

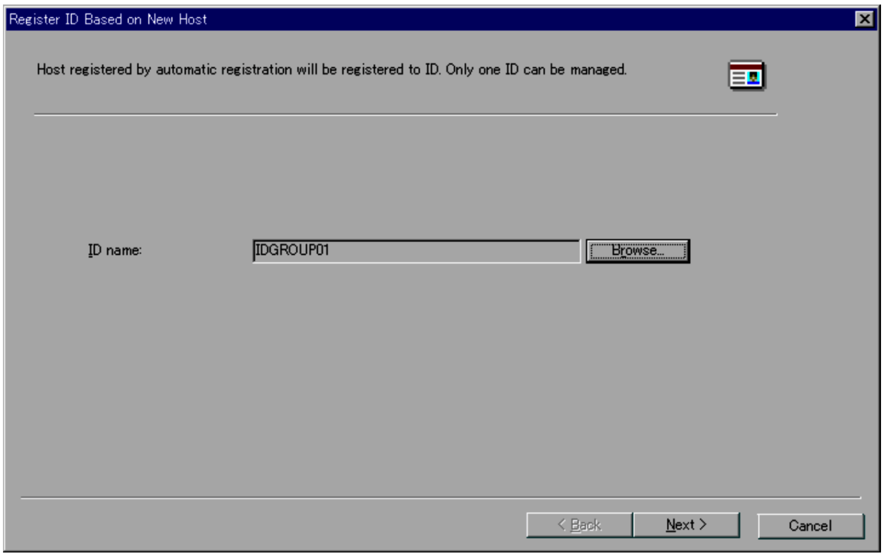
Policies:

Policy type	Maintenance type	Condition	Destination group/ID name	Route	Host type
New hosts	ID group		IDGROUP		Only client
User inventory items	ID group	Department:...	IDGROUP		Only client

(1) Settings in the Register ID Based on New Host dialog box

You can automatically register a new host that has been registered in the system configuration information to an ID group. Only one policy can be set.

Figure 9–35: Register ID Based on New Host dialog box



Host registered by automatic registration will be registered to ID. Only one ID can be managed.

ID name: IDGROUP01

Clicking the **Browse** button displays the ID List dialog box. Select the ID group for which the policy is to be set.

To create a new ID group, click the **Create ID Group** button in the ID List dialog box.

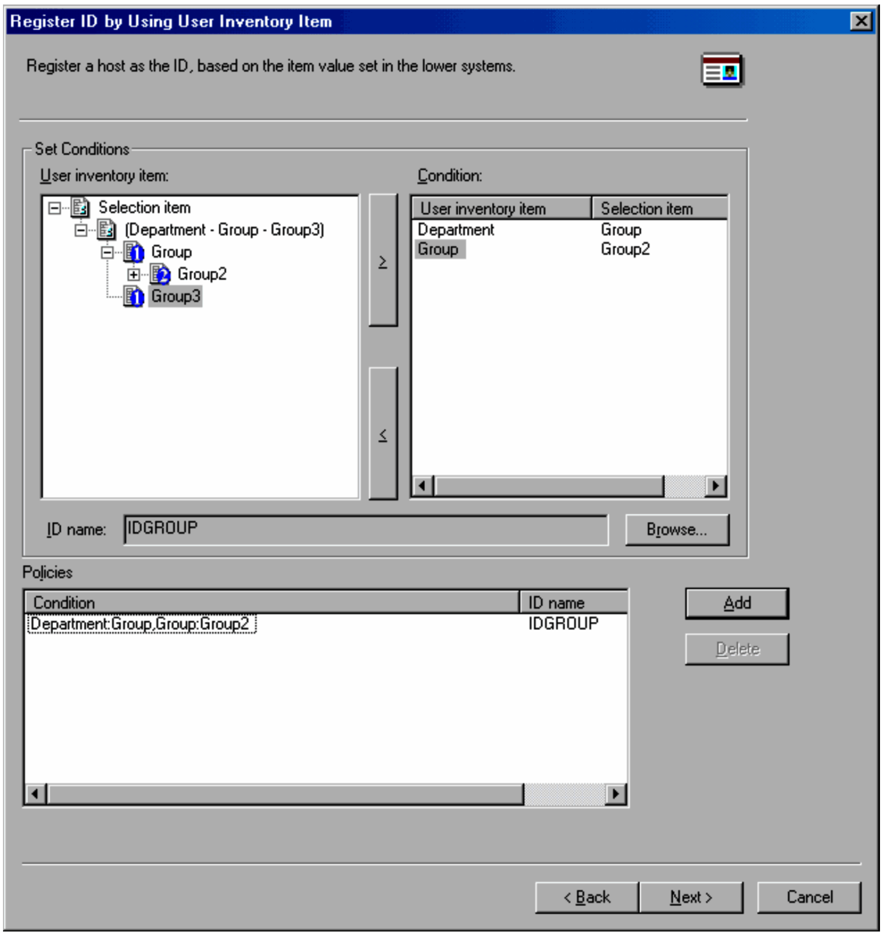
(2) Settings in the Register ID by Using User Inventory Item dialog box

You can register a client to an ID group on the basis of the user inventory information reported by the client. Only the items managed on the local server and on higher servers can be specified in policies. There is no limit to the number of policies that can be set.

The time required for executing automatic maintenance of ID groups depends on the number of policies that have been set. The following shows the formula for estimating the time required for automatic maintenance of ID groups:

(Number of ID groups registered by policies **x** 15) + (number of jobs executed by target ID groups **x** 50) + 20 (milliseconds)

Figure 9–36: Register ID by Using User Inventory Item dialog box



Register a host as the ID, based on the item value set in the lower systems.

User inventory item:

- Selection item
  - (Department - Group - Group3)
    - Group
      - Group2
    - Group3

Condition:

User inventory item	Selection item
Department	Group
Group	Group2

ID name: IDGROUP

Policies

Condition	ID name
Department:Group,Group:Group2	IDGROUP

To specify settings in the Register ID by Using User Inventory Item dialog box:

1. In the desired **User inventory item** column, select an item and then click the > button.

   The selected item is added to the **Condition** column. You can set a maximum of 10 conditions. The same user inventory item can be specified only once within a policy.

   To delete an item from the **Condition** column, select the item and then click the < button.

2. Click the **Browse** button.

   The ID List dialog box appears. Select the ID group for which the policy is to be set.

   To create a new ID group, click the **Create ID Group** button in the ID List dialog box.

3. Click the **Add** button.

   The policy specified in the **Condition** column is added to **Policies**.

   To delete a policy, select the policy and then click the **Delete** button.

9.4.2 Notes on using automatic maintenance of ID groups

You should note the following points when you use automatic maintenance of ID groups:

- The same policy can be set only once.

- Automatic maintenance of ID groups registers clients automatically, whether or not there is a password for the ID group.
- Relay managers and systems are not subject to automatic maintenance of ID groups. If necessary, they must be registered manually into an ID group.
- Once a client is registered into an ID group, the ID group job is executed at the time communication is established with the higher system. If you use automatic maintenance of ID groups after executing the ID group job, the client is registered automatically into the ID group, but the timing of execution of the ID group job depends on the client.

  To execute the ID group job when the client is registered into the ID group, perform the following operation at the client:

  1. From the **Start** menu, choose the **Register in ID Group** icon to display the Register in ID Group dialog box. In this dialog box, confirm that the client has been registered into the ID group.
  2. From the **Start** menu, choose the **Execute Job Backlog** icon to receive the ID group job.
- If an ID group is deleted, the policy specifying that ID group is also automatically deleted. If an ID group is deleted by another Remote Installation Manager while a policy is being set, the policy specifying that ID group is not automatically deleted. In such a case, you must delete the corresponding policy or change the ID group specification. Automatic maintenance no longer applies because the specified ID group does not exist.
- Deleting a policy does not release the registered clients from the ID group.
- If a user inventory item that is managed on higher and local servers is deleted or changed on the higher system and that item has been set in a policy in the relay manager/system, the change or deletion of the user inventory item is not applied to that relay manager/system. In such a case, an invalid user inventory item may be set in policies in the relay manager/system and automatic maintenance of ID groups may not be executed correctly.
- If you set an ID group and a user inventory item that is managed on higher and local servers and that has been created on the higher system in a policy on the relay manager, do not use the same conditions as for the higher system to set a different target ID group.
- To create a new ID group during policy setting and manage that ID group by the relay managing the ID, the relay manager/system must be set in the relay managing the ID before the policy setting is completed. Before completing the policy setting, make sure that the relay manager/system has been set in the relay managing the ID.

9.5 Creating a policy from a file

You can output policies for the automatic maintenance of host and ID groups to a text file. By creating multiple policies and reading the file according to purposes, you can set policies in batch mode. Additionally, you can create new policies from existing policies by editing the text file containing the policies

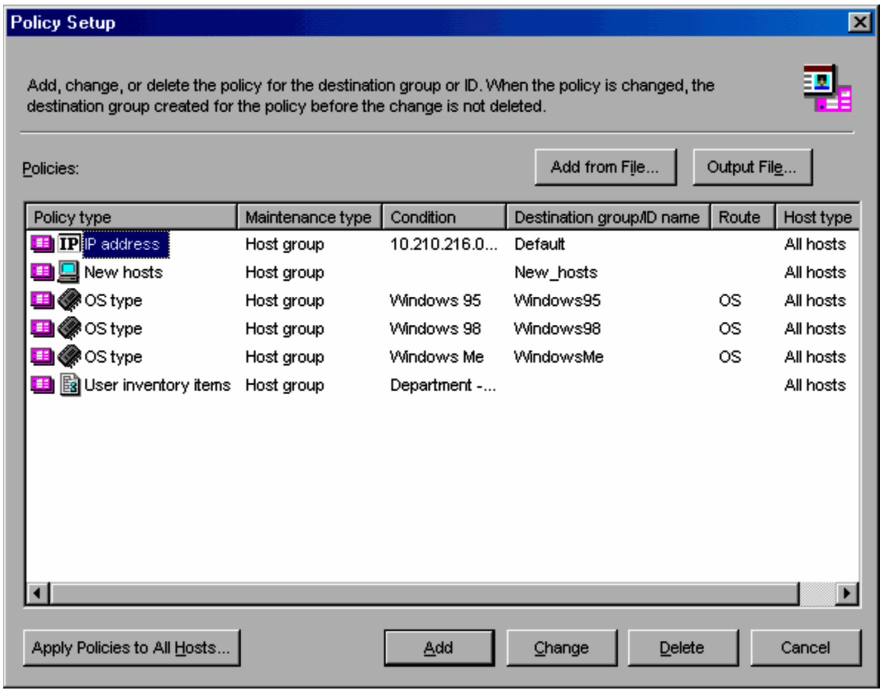
A file containing the description of set policies is called an *automatic maintenance policy file*.

This section describes how to input, output, and edit automatic maintenance policy files.

9.5.1 How to input and output an automatic maintenance policy file

To input and output an automatic maintenance policy file, use the **Add from File** and **Output File** buttons in the Policy Setup dialog box.

Figure 9–37: Policy Setup dialog box



Policy Setup

Add, change, or delete the policy for the destination group or ID. When the policy is changed, the destination group created for the policy before the change is not deleted.

Policies:

Policy type	Maintenance type	Condition	Destination group/ID name	Route	Host type
IP address	Host group	10.210.216.0...	Default		All hosts
New hosts	Host group		New_hosts		All hosts
OS type	Host group	Windows 95	Windows95	OS	All hosts
OS type	Host group	Windows 98	Windows98	OS	All hosts
OS type	Host group	Windows Me	WindowsMe	OS	All hosts
User inventory items	Host group	Department -...			All hosts

Add from File button

Clicking the **Add from File** button displays the Add Automatic Maintenance Policy dialog box. Specifying the automatic maintenance policy file to be input and then clicking the **Open** button adds the policy with the information specified in the file.

When you input an automatic maintenance policy file, note the following:

- A comment entered by the user in the automatic maintenance policy file is erased when the file is input. Therefore, no comment is included when the file is output.
- There is a limit to the number of policies that can be set depending on the policy type. If you use the **Add** button in the Policy Setup dialog box to create policies and the maximum number of policies is reached for that policy type, policy creation is automatically restricted. If the number of policies created in the automatic maintenance policy file exceeds the maximum value, an error message is displayed when the file is input, in which case policies in the automatic maintenance policy file are not applied. The following table shows the policy types and the permitted numbers of policies.

Table 9–1: Policy types and maximum numbers

Automatic maintenance type	Policy type	Maximum number
Host group	New host	1

Automatic maintenance type	Policy type	Maximum number
Host group	User inventory item	16
ID group	New host	1

Output File button

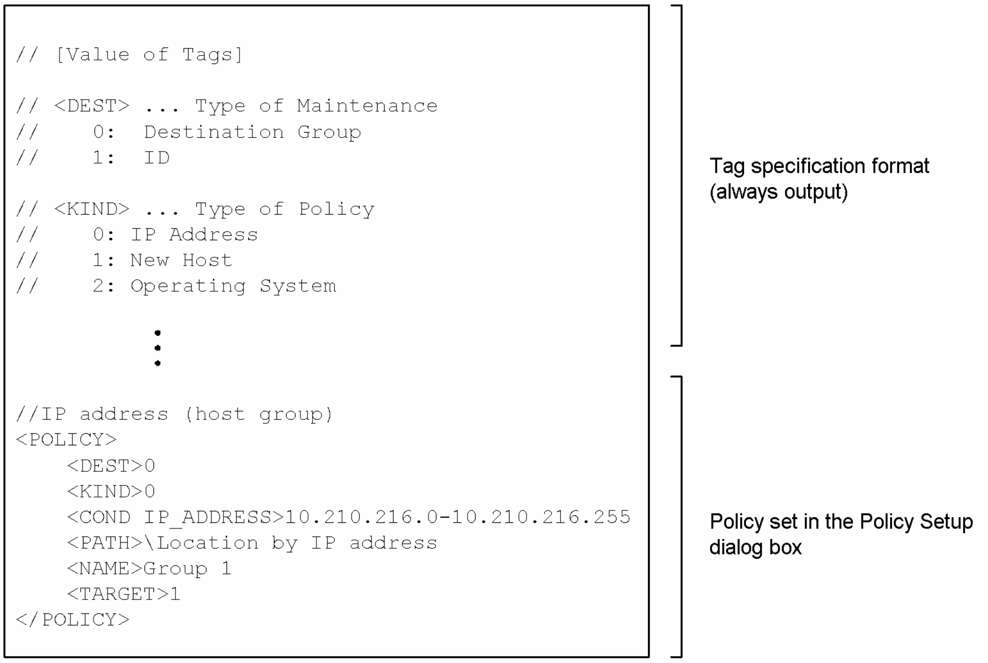
Clicking the **Output File** button displays the Output Automatic Maintenance Policy dialog box. To output a file, specify the storage directory and then click the **Save** button.

9.5.2 How to edit an automatic maintenance policy file

An automatic maintenance policy file consists of comments beginning with `//` and policies enclosed in the `<POLICY>` and `</POLICY>` tags.

The following figure shows an output example of an automatic maintenance policy file.

Figure 9–38: Output example of an automatic maintenance policy file



```
// [Value of Tags]

// <DEST> ... Type of Maintenance
//    0:  Destination Group
//    1:  ID

// <KIND> ... Type of Policy
//    0: IP Address
//    1: New Host
//    2: Operating System

           ⋮

//IP address (host group)
<POLICY>
    <DEST>0
    <KIND>0
    <COND IP_ADDRESS>10.210.216.0-10.210.216.255
    <PATH>\Location by IP address
    <NAME>Group 1
    <TARGET>1
</POLICY>
```

Tag specification format (always output)

Policy set in the Policy Setup dialog box

You can change policy settings by changing the description between the `<POLICY>` and `</POLICY>` tags.

The following table lists and describes the tags that are used in automatic maintenance policy files.

Table 9–2: Tags used in automatic maintenance policy files

Tag	Description	Required tag
`<DEST>`	Sets the type of automatic maintenance.	Y
`<KIND>`	Sets a policy type.	Y
`<COND>`	Sets a condition for the selected policy type.	N
`<PATH>`	Sets a path used to group hosts.	N
`<NAME>`	Sets a host group name or ID group name.	N
`<TARGET>`	Sets a host type.	N
`<SUBVER>`	Sets an OS sub-version.	N

Legend: Y: Yes, N: No.

The following subsections describe the rules for specifying tags between the `<POLICY>` and `</POLICY>` tags, descriptive notations, and detailed specification methods.

(1) Tag specification rules

The following describes the rules for specifying the tags:

- Express tags as upper case letters, symbols, and space.
- A tag and a value cannot consist of multiple lines.
- A tag and a comment cannot be on the same line.
- Neither comment nor tag can be on the same line as `<POLICY>` or `</POLICY>`.
- A value for a tag cannot be omitted.
- Tags between `<POLICY>` and `</POLICY>` can be specified in any order.

(2) Descriptive notations for tags

This manual uses the following format to describe each tag in the automatic maintenance policy files:

Format

Indicates the format of the tag.

Description

Describes how to specify the tag.

Note

Describes notes about specifying the tag.

Example

Presents a coding example when the value of a tag is not a number.

(3) <DEST> (sets the type of automatic maintenance)

This tag sets the type of automatic maintenance. Make sure that you always set this tag.

Format

`<DEST>`*automatic-maintenance-type*

Description

Specify `0` or `1` as the type of automatic maintenance.

Automatic maintenance type	Value
Host group	0
ID group	1

Notes

- No value other than `0` or `1` can be specified.
- Any space or tab is ignored before and after the value.

(4) <KIND> (sets a policy type)

This tag specifies the policy type. Make sure that you always set this tag.

Format

`<KIND>`*policy-type*

Description

Specify a value in the range from 0 to 3 as the policy type. The value permitted for policy type depends on the value of `<DEST>`.

Value of <DEST>	Policy type	Value
`0` (host group)	IP address	`0`
	New host	`1`
	OS type	`2`
	User inventory item	`3`
`1` (ID group)	New host	`1`
	User inventory item	`3`

Notes

- No combination other than the above is permitted.
- Any space or tab is ignored before and after the value.

(5) <COND> (sets a condition)

This tag sets the condition for the policy type specified in `<KIND>`.

The tag to be specified depends on the values of `<DEST>` and `<KIND>`.

The following table shows the tags to be specified according to the combination of `<DEST>` and `<KIND>`:

Value of <DEST>	Value of <KIND>	Tag to be specified
`0` (host group)	`0` (IP address)	`<COND IP_ADRESS>`
	`2` (OS type)	`<COND OS>`
	`3` (User inventory item)	`<COND USER>`
`1` (ID group)	`3` (User inventory item)	`<COND USER_VALUE>`

The following describes how to specify each tag.

(a) <COND IP_ADRESS> (sets an IP address)

If an IP address is set as the condition of automatic maintenance for host groups, this tag specifies the range of IP addresses that are to be the target of automatic maintenance.

Format

`<COND IP_ADRESS>`*IP-address-range*

Description

Specify a range of IP addresses using a hyphen (-).

The permitted range of IP addresses is from 0.0.0.0 to 255.255.255.254.

A single-digit or two-digit value may not require leading zeros.

Notes

- Make sure that the specified range begins with a smaller IP address, followed by a hyphen (-), then a larger IP address.
- Neither space nor tab may be placed before or after the hyphen (-).
- Any space or tab is ignored before and after the value.

Example

```
<COND IP_ADRESS>172.16.10.0-172.16.10.255
```

(b) <COND OS> (sets an OS type)

If an OS type is set as the condition of automatic maintenance for host groups, this tag specifies the OS type that is to be the target of automatic maintenance.

Format

`<COND OS>`*OS-type*

Description

Specify the OS type as a value in the range from 0 to 22. Only one value can be specified at a time.

OS type	Value
Windows 95	0
Windows 98	1
Windows Me	2
Windows NT	3
Windows 2000	4
Windows XP	5
Windows Server 2003	6
MS-DOS+Windows	7
Windows CE	8
Windows CE .NET	9
HP-UX	10
Solaris	11
AIX	12
HP Tru64 UNIX	13
HI-UX/WE2	14
Linux	15
Windows Vista	19
Windows Server 2008	20
Windows 7	21
Windows Server 2008 R2	22
Windows 8	23
Windows Server 2012	24

Notes

- To set multiple OS types in policies, create multiple different policies.
- Any space or tab is ignored before and after the value.

(c) <COND USER> (sets a user inventory item (host group))

If a user inventory item is set as the condition of automatic maintenance for host groups, this tag specifies the user inventory item that is to be the target of automatic maintenance.

Format

`<COND USER>`*user-inventory-item-(hierarchy-1)*`,...,` *user-inventory-item-(hierarchy-6)*

Description

Specify a user inventory item for each hierarchy separated by a comma (`,`). You can specify a maximum of six hierarchies of user inventory items.

Notes

- The value for a user inventory item cannot be a space or tab alone.
- There must be no comma (`,`) after the last hierarchy.
- An error results if nothing is specified between two commas.
- All trailing spaces are ignored.

Example

`<COND USER>`*headquarters-name*`,`*department-name*`,`*employee-number*

(d) <COND USER_VALUE> (sets a user inventory item (ID group))

If a user inventory item is set as the condition of automatic maintenance for host groups, this tag specifies the user inventory item to be registered to the ID group and the selection item for the user inventory item.

Format

`<COND USER_VALUE>`*user-inventory-item*`,` *selection-item-for-user-inventory-item*

Description

Specify a user inventory item and a selection item for user inventory item separated by a comma (`,`). You can set a maximum of 10 tags in a single policy.

Notes

- The value for a user inventory item cannot be a space or tab alone.
- All trailing spaces are ignored.

Example

`<COND USER_VALUE>`*headquarters*`,`*software-development-department*

`<COND USER_VALUE>`*department*`,`*public-affairs-department*

`<COND USER_VALUE>`*section*`,`*section-1*

(6) <PATH> (sets a path)

This tag sets a path where the host group is to be created.

Format

`<PATH>`*path*

Description

Specify the path where the group is to be created.

You can specify multiple paths separated by a `\`. Each path must be no longer than 32 bytes. If multiple paths are specified, the permitted maximum length is 190 bytes including the host group name and delimiters (`\`).

The path names cannot include `\`, `/`, `*`, `"`, `'`, `:`, `!`, `|`, `.`, `<`, `>`, `?`, `@`, `%`, or a space.

Notes

- If `<DEST>1` is specified, `<PATH>` is ignored, if specified.
- The same name cannot be specified for each path.
- When a new path is specified, that path is created during execution of automatic maintenance.
- Any space or tab is ignored before and after the value.

Example

```
<PATH>\group1\group2\group
```

(7) <NAME> (sets a host group name or an ID group name)

This tag specifies the host group name or ID group name that is to be the target of automatic maintenance.

Format

`<NAME>`*host-group-name-or-ID-group-name*

Description

Specify a host group name or ID group name in a maximum of 32 bytes. It cannot contain `\`, `/`, `*`, `"`, `'`, `:`, `!`, `|`, `.`, `<`, `>`, `?`, `@`, `%`, or a space.

Notes

- If you have specified the `<DEST>0` tag and `0`, `1` or `2` as the value of `<KIND>`, make sure that you specify a host group name.
- If you have specified the `<DEST>1` tag, make sure that you specify an ID group name.
- The specified name cannot be the same as the host group name that was specified in path.
- Any space or tab is ignored before and after the value.

(8) <TARGET> (sets a host type)

This tag sets the host type that is to be the target of automatic maintenance. Specification of this tag is optional.

Format

`<TARGET>`*host-type*

Description

Specify `0` or `1` as the host type.

Host type	Value
All hosts	`0`
Clients only	`1`

Notes

- If the value of `<KIND>` is `0` or `2`, make sure that the values of `<TARGET>` are the same.
- If this tag is omitted and `<DEST>0` is specified, `0` is automatically set; if `<DEST>1` is specified, `1` is automatically set.
- Any space or tab is ignored before and after the value.

(9) <SUBVER> (sets whether or not there is an OS sub-version)

If OS type is specified as the policy type, this tag sets whether or not there is an OS sub-version. Specification of this tag is optional.

`<SUBVER>` can be specified only when OS type is specified as the policy type.

Format

`<SUBVER>`*whether-or-not-there-is-an-OS-sub-version*

Description

Specify `0` or `1` to indicate whether or not there is an OS sub-version.

Whether or not there is an OS sub-version	Value
No	`0`
Yes	`1`

Notes

- If this tag is omitted, `0` is automatically specified.
- If the specified policy type is not OS type, this tag is ignored, if specified.
- Any space or tab is ignored before and after the value.

9.5.3 Example of policy creation

For automatic maintenance of host groups, this example sets a policy for registering clients whose IP address is in the range from 100.0.0.0 to 100.0.0.255 to the host group `Group 1` with the path `Development department`. The following shows the specification in the automatic maintenance policy file:

Figure 9–39: Example of creating an automatic maintenance policy file

```
//IP address (host group)
<POLICY>
    <DEST>0
    <KIND>0
    <COND IP_ADDRESS>10.0.0.0-10.0.0.255
    <PATH>\Development department
    <NAME>Group 1
</POLICY>
```

By copying this policy and then changing information, such as the range of the IP addresses and host group name, you can create a different policy that uses the IP address as a condition. Thus you can efficiently create multiple automatic maintenance policies by copying and editing existing policies.

9.6 Managing the deletion history of system configuration information

JP1/Software Distribution Manager enables you to manage deletion history in terms of when and how systems were removed from the system configuration information.

To manage the deletion history of system configuration information, you must specify the following setting in the JP1/Software Distribution Manager setup:

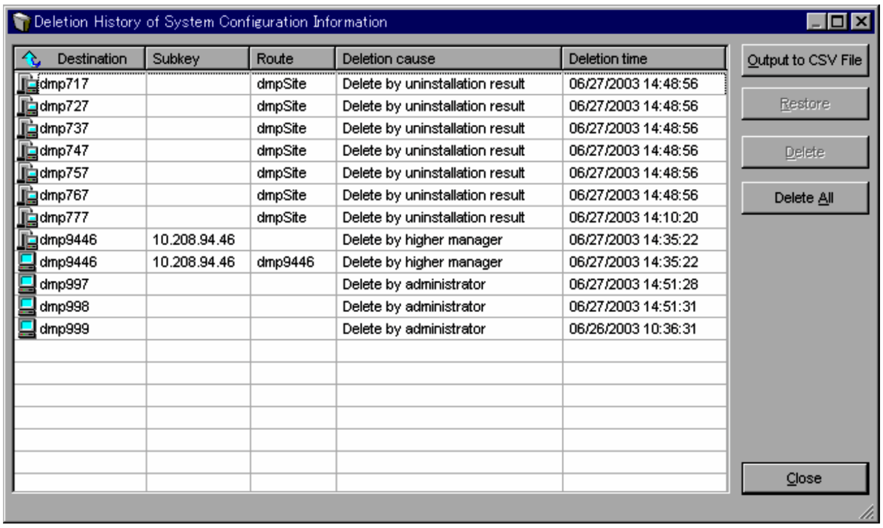
JP1/Software Distribution Manager setup

On the **System Configuration** page, select the check box for **Save deletion history**.

9.6.1 Displaying deletion history

The deletion history of system configuration information is displayed in the Deletion History of System Configuration Information dialog box. To display this dialog box, choose **File**, and then **Deletion History of System Configuration Information**. You can also display this dialog box from any of the windows of Remote Installation Manager.

Figure 9–40: Deletion History of System Configuration Information dialog box



Destination	Subkey	Route	Deletion cause	Deletion time
dmp717		dmpSite	Delete by uninstallation result	06/27/2003 14:48:56
dmp727		dmpSite	Delete by uninstallation result	06/27/2003 14:48:56
dmp737		dmpSite	Delete by uninstallation result	06/27/2003 14:48:56
dmp747		dmpSite	Delete by uninstallation result	06/27/2003 14:48:56
dmp757		dmpSite	Delete by uninstallation result	06/27/2003 14:48:56
dmp767		dmpSite	Delete by uninstallation result	06/27/2003 14:48:56
dmp777		dmpSite	Delete by uninstallation result	06/27/2003 14:10:20
dmp9446	10.208.94.46		Delete by higher manager	06/27/2003 14:35:22
dmp9446	10.208.94.46	dmp9446	Delete by higher manager	06/27/2003 14:35:22
dmp997			Delete by administrator	06/27/2003 14:51:28
dmp998			Delete by administrator	06/27/2003 14:51:31
dmp999			Delete by administrator	06/26/2003 10:36:31

The Deletion History of System Configuration Information dialog box displays **Destination**, **Subkey**, and **Route** from the system configuration information as well as the following two items for each deleted host:

Deletion cause

One of the following three items is displayed as the cause of deletion of a host from the system configuration information:

Deletion cause	Description
Deletion by uninstallation result	• Removal was reported from a client, relay system, or relay manager. • Host was deleted by a *Get system configuration information* job.
Deletion by administrator	• From the System Configuration window, a client, relay system, or relay manager was deleted manually. • A client was deleted by automatic or manual maintenance of system configuration information.
Deletion by higher manager	• When a lower system changed its connection destination, the relay manager received notification from its higher manager

Deletion cause	Description
Deletion by higher manager	indicating the removal of system configuration information of a lower system remaining in the previous route. • The relay manager received notification from the higher manager indicating the removal of system configuration information by automatic or manual maintenance.

Deletion time

This is the date and time the host was removed from the system configuration information.

In the Deletion History of System Configuration Information dialog box, you can also display the following items:

Host ID, **MAC address**, **Comment**, **Create date/time**, and **Update date/time**

To add these items, from the menu displayed by right-clicking, choose **Select Information**, and then select desired items.

By dragging the corner or border of the Deletion History of System Configuration Information dialog box, you can change its size. When you click on a column name, the sort order of the displayed data is toggled between ascending order and descending order.

9.6.2 Outputting deletion history to a CSV file

You can save the deletion history of system configuration information to a CSV file. The following information is saved for each host:

host-name, *IP-address*, *host-ID*, *MAC-address*, *type*, *route*, *comment*, *deletion-cause*, *deletion-date/time*, *creation-date/time*, and *update-date/time*

To save deletion history to a CSV file:

1. Choose **File**, and then **Deletion History of System Configuration Information**.
   The Deletion History of System Configuration Information dialog box appears.
2. Click the **Output to CSV File** button.
   The Output Deletion History to CSV File dialog box appears.
3. Specify the location and name of the file, and then click the **Save** button.
   The deletion history is saved to the specified file in CSV format.
   To cancel saving of the deletion history to the CSV file while the processing is underway, click the **Cancel** button.

9.6.3 Restoring a deleted host to the system configuration information

You can restore a deleted host to the system configuration information on the basis of the deletion history of system configuration information. However, the host group, ID group, and inventory information for a deleted host are not restored.

You cannot restore a deleted host if there is no route during host deletion but the host was registered in the system configuration information. Also, in a system where multiple managing servers are configured in a hierarchy, you cannot restore a relay system or client under a relay manager from its higher manager.

Even if you restore a deleted host to the system configuration information, the host still remains in the deletion history in the Deletion History of System Configuration Information dialog box. You can delete this deletion history as necessary.

To restore a deleted host to the system configuration information:

1. Choose **File**, and then **Deletion History of System Configuration Information**.
   The Deletion History of System Configuration Information dialog box appears.
2. Select the host you want to restored, and then click the **Restore** button.
   The host is restored to the system configuration information.
   You can also select multiple hosts and restore them in the batch mode.

9.6.4 Deleting deletion history

When you restore a deleted host to the system configuration information, the host still remains in the deletion history in the Deletion History of System Configuration Information dialog box. If there is a large volume of deletion history, a space shortage may occur in the database. For this reason, you should periodically delete unneeded deletion history information.

To delete deletion history, open the Deletion History of System Configuration Information dialog box. In this dialog box, select the hosts whose history is no longer needed, and then click the **Delete** button. If you click the **Delete All** button, all deletion history is deleted.

If you delete a host from the System Configuration window manually and have selected the setting for not deleting the inventory information, the host is deleted from the system configuration information but its inventory information remains. In such a case, deleting the deletion history will not delete the inventory information.

9.7 Detecting hosts on which JP1/Software Distribution is not installed

You can check the JP1/Software Distribution installation status by searching hosts in the network from the managing server for those hosts on which JP1/Software Distribution is not installed.

This function enables you to detect hosts in the local department network on which JP1/Software Distribution is not installed. By using the detection results to install JP1/Software Distribution on all hosts on which it is not already installed, you can place all computers in the local department network under the management of JP1/Software Distribution.

This section describes the conditions for deleting hosts on which JP1/Software Distribution is not installed, how to detect hosts on which JP1/Software Distribution is not installed, and the handling after such hosts have been deleted.

9.7.1 Conditions for detecting hosts on which JP1/Software Distribution is not installed

The system detects hosts on which JP1/Software Distribution is not installed by comparing the MAC addresses of the hosts registered in the managing server with the MAC addresses of the hosts found in the network.

This subsection describes MAC addresses and JP1/Software Distribution versions that can be detected.

Two types of MAC addresses are registered in the managing server:

- MAC addresses registered as system configuration information
- MAC addresses obtained by the *Get system information from client* job

If the MAC address of a found host does not match either of these MAC addresses, the system assumes that JP1/Software Distribution is not installed on that host and treats it as a host on which JP1/Software Distribution is not installed.

If the system cannot obtain a MAC address, it assumes that JP1/Software Distribution is not installed on that host. Therefore, to use the results of detecting hosts on which JP1/Software Distribution is not installed, your system must consist of JP1/Software Distribution versions that support MAC addresses. The following table lists the JP1/Software Distribution versions that are capable of obtaining MAC addresses.

Table 9–3: JP1/Software Distribution versions capable of obtaining MAC addresses

JP1/Software Distribution		Version
Windows version	Manager (relay manager)	05-12 or later#1
	SubManager	03-10 or later#1
	Client	03-10 or later#1
UNIX version		06-71 or later#2

#1

If inventory is not managed, MAC addresses can be obtained only from JP1/Software Distribution version 06-00 or later.

In an environment in which at least one host uses multiple network adapters, MAC addresses can be obtained only from JP1/Software Distribution version 06-01 or later.

#2

If inventory is not managed, MAC addresses can be obtained only from JP1/Software

Distribution version 08-10 or later. You must specify the settings for MAC addresses to be acquired in the system configuration information.

9.7.2 How to detect hosts on which JP1/Software Distribution is not installed

There are two ways to detect hosts on which JP1/Software Distribution is not installed:

- By executing a host search
- By reading a network configuration information file

These methods are explained below.

(1) Executing a host search to detect hosts on which JP1/Software Distribution is not installed

This method executes a host search and compares the MAC addresses of the found hosts with the MAC addresses registered in the managing server to detect hosts on which JP1/Software Distribution is not installed.

You use this method when a new JP1/Software Distribution system has been created or after hosts have been added in the network.

To execute a host search to detect hosts on which JP1/Software Distribution is not installed:

1. Display the Detection of Hosts Not Containing Software Distribution dialog box.
   For details about how to display the Detection of Hosts Not Containing Software Distribution dialog box, see *9.7.3 Manipulating the Detection of Hosts Not Containing Software Distribution dialog box*.
2. From the Detection of Hosts Not Containing Software Distribution dialog box, display the Host Search dialog box.
3. Execute the host search.
   When the host search is completed, any hosts on which JP1/Software Distribution is not installed will have been detected automatically.
4. Display the detection results in the Detection of Hosts Not Containing Software Distribution dialog box.
   Click the **Latest information** button in the Detection of Hosts Not Containing Software Distribution dialog box to display the results of detecting hosts on which JP1/Software Distribution is not installed.

For details about how to detect hosts on which JP1/Software Distribution is not installed by executing a host search, see *9.7.4 Detecting hosts on which JP1/Software Distribution is not installed*.

(2) Reading the network configuration information file to detect hosts on which JP1/Software Distribution is not installed

Instead of executing a host search, you can detect hosts on which JP1/Software Distribution is not installed by reading a network configuration information file.

You use this method to detect hosts on which JP1/Software Distribution is not installed in the case of an environment in which the host configuration in the network is fixed, or when the network workload must be minimized.

To read a network configuration information file in order to detect hosts on which JP1/Software Distribution is not installed:

1. Create a network configuration information file.
   For details about how to create a network configuration information file, see *9.7.8 Creating a network configuration information file*.
2. Display the Detection of Hosts Not Containing Software Distribution dialog box.
   For details about how to display the Detection of Hosts Not Containing Software Distribution dialog box, see *9.7.3 Manipulating the Detection of Hosts Not Containing Software Distribution dialog box*.
3. Click the **CSV input** button and read the network configuration information file.
   The hosts on which JP1/Software Distribution is not installed are detected and the detection results are displayed in the Detection of Hosts Not Containing Software Distribution dialog box.

You can also use the `dcmhstwo` command, which is provided by JP1/Software Distribution, to detect from the network configuration information file those hosts on which JP1/Software Distribution is not installed. For details about how to use the `dcmhstwo` command to detect hosts on which JP1/Software Distribution is not installed, see *4.9 dcmhstwo.exe (detecting a host on which JP1/Software Distribution is not installed)* in the manual *Administrator's Guide Volume 2*.

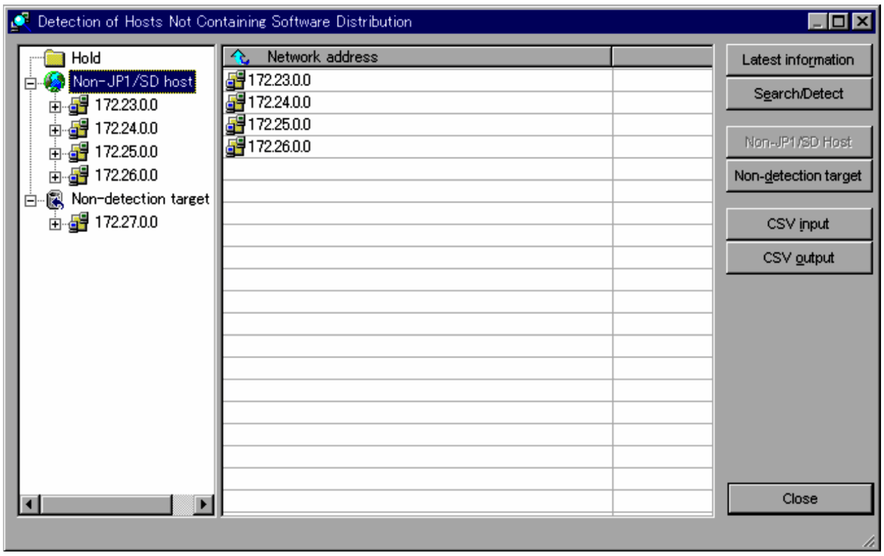
9.7.3 Manipulating the Detection of Hosts Not Containing Software Distribution dialog box

In the Detection of Hosts Not Containing Software Distribution dialog box, you can detect and manage hosts on which JP1/Software Distribution is not installed. This dialog box is also used to display the Host Search dialog box, which is used to search hosts.

To display the Detection of Hosts Not Containing Software Distribution dialog box, from Remote Installation Manager, choose **Options**, and then **Detection of hosts not containing Software Distribution**.

The following shows the Detection of Hosts Not Containing Software Distribution dialog box:

Figure 9–41: Detection of Hosts Not Containing Software Distribution dialog box



The left-hand frame of the dialog box displays in tree format the detected hosts by network address. A host with no subnet mask information is displayed as `Unknown`.

The right-hand frame displays information about the hosts included in a network address and information about a selected host for any item selected in the left-hand frame. You can use the host information to check the first date and time the host was detected (detection date and time) and the last date and time the host was detected (last update date and time). The detection date and time are set when the host is detected for the first time and is not updated during subsequent detections. The last update date and time are set whenever host information is updated, such as when the host is detected again or when it is removed as a detection target. By comparing these dates and time, you can determine the period during which JP1/Software Distribution has not been installed on the host.

The following describes the icons and buttons in the Detection of Hosts Not Containing Software Distribution dialog box:

Hold icon

If the **Hold the newly detected results** check box is selected on the **Server Customization** page during JP1/Software Distribution Manager setup, all detected hosts on which JP1/Software Distribution is not installed are displayed under the **Hold** icon.

When the **Hold** icon is used, you can manually specify any detected computer as a host on which JP1/Software Distribution is not installed or remove any detected computer as a detection target. This feature is useful in an environment in which Windows hosts and UNIX hosts coexist, because it enables you to manage only the Windows hosts as hosts on which JP1/Software Distribution is not installed.

Non-JP1/SD host icon

Displays the hosts that are being managed as hosts on which JP1/Software Distribution is not installed. The default is that all detected hosts on which JP1/Software Distribution is not installed are displayed under the **Non-JP1/SD host** icon.

Non-detection target icon

Displays the hosts that are not to be included in the detection target range for hosts on which JP1/Software Distribution is not installed. The hosts displayed here will not be detected during subsequent detections as hosts on which JP1/Software Distribution is not installed even if JP1/Software Distribution is not installed on them.

During detection, any host whose type is not **Computer** is displayed automatically under the **Non-detection target** icon.

Latest information button

Refreshes the information displayed in the Detection of Hosts Not Containing Software Distribution dialog box. This button is used for purposes such as displaying the detection result of hosts on which JP1/Software Distribution is not installed after a host search has executed.

For details about the timing of refreshing the information displayed in the Detection of Hosts Not Containing Software Distribution dialog box, see *9.7.5 Updating the detection results*.

Search/Detect button

Clicking this button displays the following menus:

Start host search screen menu

Displays the Host Search dialog box, in which you can search hosts in the network to detect hosts on which JP1/Software Distribution is not installed.

For details about how to search hosts in the network to detect hosts on which JP1/Software Distribution is not installed, see *9.7.4 Detecting hosts on which JP1/Software Distribution is not installed*.

Detect unintroduced host menu

Used to detect hosts on which JP1/Software Distribution is not installed by comparing the MAC addresses of the hosts registered in the results of a previous host search with the MAC addresses of the hosts registered in the managing server.

There is no need to execute a host search if there has been no change to the host configuration in the network since the previous host search. If this is the case, use this menu to detect hosts on which JP1/Software Distribution is not installed.

For details about the timing of using the **Detect unintroduced host** menu to detect hosts on which JP1/Software Distribution is not installed, see *9.7.5 Updating the detection results*.

Non-JP1/SD Host button

Sets a selected host as a host on which JP1/Software Distribution is not installed. This button is enabled when a host displayed under the **Hold** or **Non-detection target** icon is selected.

Non-detection target button

Specifies a selected host as a *Non-detection target* so that it will not be detected as a host on which JP1/Software Distribution is not installed when detection processing is executed subsequently. This button is enabled when a host displayed under the **Hold** or **Non-JP1/SD host** icon is selected.

For details about managing hosts as non-detection targets, see *9.7.6 Setting a host as a non-detection target*.

CSV input button

Displays a dialog box for entering a network configuration information file.

You use this button to detect hosts on which JP1/Software Distribution is not installed by reading a network configuration information file instead of by executing a host search.

CSV output button

Clicking this button displays the following menus:

Host search results menu

Exports to a CSV file the results of a host search.

Unintroduced host information menu

Exports to a CSV file the results of detection of hosts on which JP1/Software Distribution is not installed.

For details about the results of a host search, how to export the results of detection of hosts on which JP1/Software Distribution is not installed to a CSV file, and the output items, see *9.7.7 Exporting the detection results to a CSV file*.

9.7.4 Detecting hosts on which JP1/Software Distribution is not installed

This subsection describes how to execute a host search and detect hosts on which JP1/Software Distribution is not installed.

When the host search is completed, hosts on which JP1/Software Distribution is not installed will have been detected automatically. The detection results are displayed in the Detection of Hosts Not Containing Software Distribution dialog box.

(1) Detection procedure

To execute a host search and detect hosts on which JP1/Software Distribution is not installed:

1. Display the Detection of Hosts Not Containing Software Distribution dialog box.
2. From the Detection of Hosts Not Containing Software Distribution dialog box, display the Host Search dialog box.

   You can execute a host search from the Host Search dialog box. For details about how to display and manipulate the Host Search dialog box, see *(3) Manipulating the Host Search dialog box*.
3. Set details for the host search.

   Host search is executed according to *Host search settings* that specify the range of the network to be searched and the search schedule. For details about how to specify the host search settings, see *(4) Detailed host search settings*.

   You can also set a validity period for the information about found hosts. For settings for the validity period of information about found hosts, see *(5) Settings for the validity period of search results*.
4. Execute the host search.

   For details about how to execute a host search, see *(6) Executing a search*.

   When the search is completed, hosts on which JP1/Software Distribution is not installed will have been detected automatically.
5. Display the detection results.

   Click the **Latest information** button in the Detection of Hosts Not Containing Software Distribution dialog box to display the detection results of hosts on which JP1/Software Distribution is not installed.

The following notes apply to detecting hosts on which JP1/Software Distribution is not installed:

- For a UNIX JP1/Software Distribution host that uses multiple network adapters, only one MAC address is registered in the managing server. Such a host is always detected as a host on which JP1/Software Distribution is not installed due to its other MAC addresses.

  You should handle this by specifying the hosts detected by the other MAC addresses as non-detection targets.
- If you are using a relay manager to detect hosts on which JP1/Software Distribution is not installed, execute the host search within the range of the system configuration that is managed by the relay manager. All hosts outside this range that are managed by the relay manager would be detected as non-Software Distribution hosts.
- If a new host is registered in the managing server by a facility for registering the system configuration automatically or by the reporting of system information while hosts on which JP1/Software Distribution is not installed are being detected, a newly registered host may be detected as a host on which JP1/Software Distribution is not installed. In such a case, re-execute detection from the **Detect unintroduced host** menu. Information about a host registered in the managing server is deleted from the detection results of hosts on which JP1/Software Distribution is not installed. To determine whether or not such a host has been registered correctly, compare the system configuration information in the managing server with the detection results of hosts on which JP1/Software Distribution is not installed.

(2) Host search conditions

During a host search, the system uses SNMP to search for hosts whose power is on within the range of IP addresses specified in the host search settings. The system does not search any host whose power is off.

During the host search, the system also acquires information about the hosts. You can manage this information for the hosts on which JP1/Software Distribution is not installed.

The host information that can be acquired depends on whether or not the detected hosts support SNMP. The following table shows the host information that can be acquired during a host search.

Table 9–4: Host information that can be acquired during a host search

Host information	Host supporting SNMP	Host not supporting SNMP
MAC address[#1]	Yes	Yes
IP address	Yes	Yes
Host name[#2]	Yes	Yes
Subnet mask[#3]	Yes	No
Node type[#4]	Yes	No
Description[#3]	Yes	No

Legend:

Yes: Can be acquired.

No: Cannot be acquired.

#1

Information can be acquired if the router supports SNMP.

#2

Information can be acquired if the host name can be resolved from the IP address.

#3

Information can be acquired if a value is set in MIB.

#4

If the type cannot be identified or the host does not support SNMP, **Computer** is set.

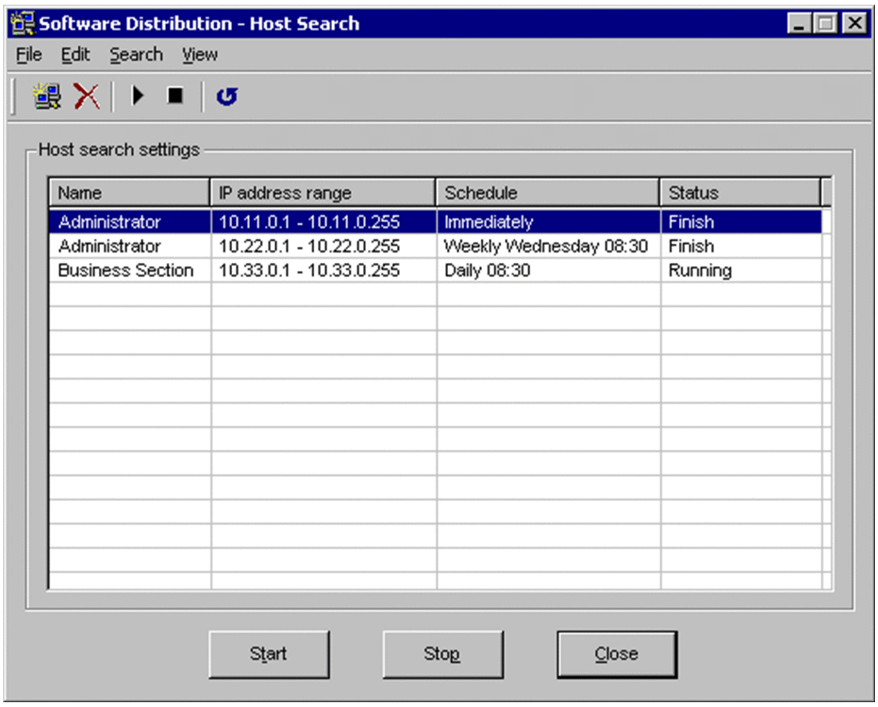
(3) Manipulating the Host Search dialog box

In the Host Search dialog box, you can execute the host search and add and change host search settings.

To display the Host Search dialog box:

1. In the Detection of Hosts Not Containing Software Distribution dialog box, click the **Search/Detect** button.
2. From the displayed menu, choose **Start host search screen**.
   The Host Search dialog box appears.

Figure 9–42: Host Search dialog box



Name	IP address range	Schedule	Status
Administrator	10.11.0.1 - 10.11.0.255	Immediately	Finish
Administrator	10.22.0.1 - 10.22.0.255	Weekly Wednesday 08:30	Finish
Business Section	10.33.0.1 - 10.33.0.255	Daily 08:30	Running

Displays the Addition of Host Search Setup dialog box that enables you to create host search settings.

✕

Deletes the settings selected on the **Host search settings** page.

▶

Starts a host search using the settings selected on the **Host search settings** page.

■

Stops the current host search that was selected on the **Host search settings** page.

↺

Refreshes screen display of the host search status (**Status**).

Host search settings

Displays information about the host search, such as the host search settings specified in the Addition of Host Search Setup dialog box and the host search status. For details about how to specify settings in the Addition of Host Search Setup dialog box, see *(4) Detailed host search settings*.

On this page, you can also change the displayed host search settings. To change host search settings for the host search currently underway, you must stop the host search.

To change host search settings, select the desired host search settings, choose **Edit**, and then **Change** to display the Change Host Search Settings dialog box. You can specify settings in this dialog box in the same manner as in the Addition of Host Search Setup dialog box. However, **Name** cannot be changed in the Change Host Search Settings dialog box.

Name

Displays the name of the host search settings that was specified in the Addition of Host Search Setup dialog box. This column is always displayed.

IP address range

Displays the range of the network subject to the host search that was specified in the Addition of Host Search Setup dialog box. This column is always displayed.

Schedule

Displays the host search schedule that was specified in the Addition of Host Search Setup dialog box. The default is that this column is displayed.

Status

Displays the host search execution status. The default is that this column is displayed.

The execution status is updated automatically. You can specify the updating interval in the Display Option dialog box.

Completion count

Displays the number of IP addresses that have been processed by this host search out of all the IP addresses included in the specified **IP address range**. The default is that this column is not displayed.

Start date/time

Displays the date and time the host search started. The default is that this column is not displayed.

End date/time

Displays the date and time the host search ended. The default is that this column is not displayed.

Start button

Starts a host search using the settings set on the **Host search settings** page.

Stop button

Stops the current host search that was set on the **Host search settings** page.

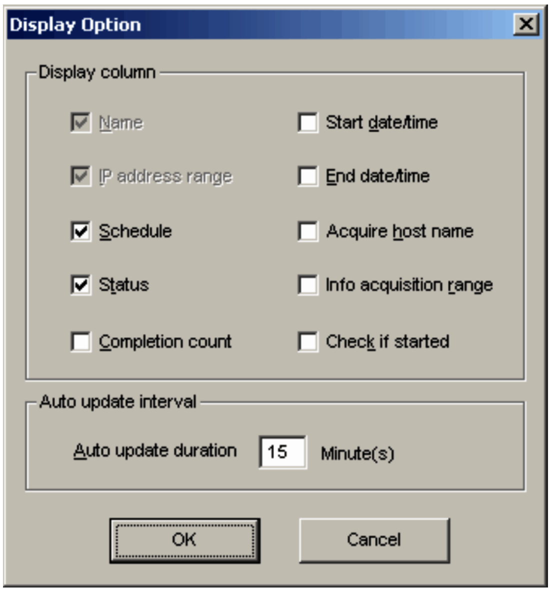
Close button

Closes the Host Search dialog box.

To change the display items in the **Host search settings** page and the updating interval for the host search status (**Status**), use the Display Option dialog box.

You can display the Display Option dialog box by choosing **View**, and then **Display Options**.

Figure 9–43: Display Option dialog box



Display Option

Display column

☑ Name
☑ IP address range
☑ Schedule
☑ Status
☐ Completion count
☐ Start date/time
☐ End date/time
☐ Acquire host name
☐ Info acquisition range
☐ Check if started

Auto update interval

Auto update duration 15 Minute(s)

Display column

Specifies the items to be displayed on the **Host search settings** page. To display an item, select its check box; to hide an item, clear its check box.

Note that **Name** and **IP address range** are always displayed.

The default is that the **Schedule** and **Status** check boxes are selected.

Auto update interval

Specifies the interval at which the host search status (**Status**) displayed on the **Host search settings** page is to be updated, in the range from 0 to 60 minutes. The default is 15 minutes. If `0` is specified, the display will not be updated.

(4) Detailed host search settings

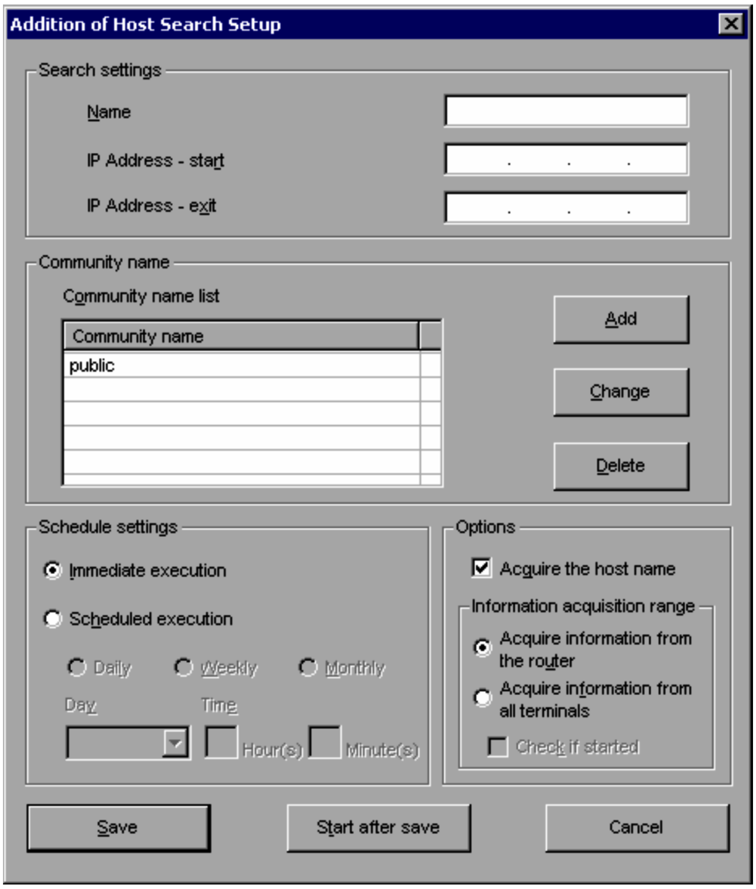
To execute a host search, you must specify host search settings, such as the IP address range in the network that is to be subject to the host search and the date and time the host search is to be executed.

You specify host search settings in the Addition of Host Search Setup dialog box. There are two ways to display the Addition of Host Search Setup dialog box:

- By clicking in the Host Search dialog box.
- By choosing **Edit** and then **Add** in the Host Search dialog box.

The following shows the Addition of Host Search Setup dialog box:

Figure 9–44: Addition of Host Search Setup dialog box



Addition of Host Search Setup

Search settings

Name:

IP Address - start: . . .

IP Address - exit: . . .

Community name

Community name list

Community name
public

Schedule settings

● Immediate execution

○ Scheduled execution

○ Daily ○ Weekly ○ Monthly

Day: Time: Hour(s) Minute(s)

Options

☑ Acquire the host name

Information acquisition range

● Acquire information from the router

○ Acquire information from all terminals

□ Check if started

Search settings

Specifies a name for the host search settings and the network search range.

Name

Specifies a name for the host search settings, as 1-64 characters. Because you can set up multiple sets of host search settings, we recommend that you use a name that is easy to manage. This item is optional.

IP Address - start (mandatory)

Specifies the start IP address of the network range that is to be subject to this host search.

IP Address - exit (mandatory)

Specifies the end IP address of the network range that is to be subject to this host search.

Community name (mandatory)

Specifies the community name of SNMP that will be used in the host search, as 1-255 characters. The default is `public`.

You can register a maximum of ten community names for each set of host search settings.

To register a community name, click the **Add** button and then specify the community name. To change or delete a community name that is displayed in the **Community name** field, select the applicable community name and click the **Change** or **Delete** button.

Schedule settings

Selects whether the host search is to be executed immediately or at a specified date and time.

Immediate execution

If you select **Immediate execution**, clicking the **Start after save** button sets the host search settings and executes the host search immediately.

Scheduled execution

Executes the host search at a scheduled date and time.

If you select **Monthly**, select the host search execution date within each month from the **Date** pull-down list. If the specified date does not exist in a particular month, such as `31` specified in **Date** and the month is April, the host search will be executed on the last day of the month.

If you select **Weekly**, select from the **Day** pull-down list the day of the week on which the host search is to be executed every week.

Specify the host search execution time in the following range:

- **Hour(s)**: 0 to 23
- **Minute(s)**: 0 to 59

Options

Selects the method for acquiring host information.

Acquire the host name

Select this checkbox to acquire the host name in a host search. The default is that this check box is selected.

If the host names are not needed as part of the information about hosts on which JP1/Software Distribution is not installed, clear this check box; in such a case, the host search time may be reduced because name resolution is not performed.

In the case of hosts that support SNMP, their host names are acquired even when this check box is cleared.

Information acquisition range

Acquires hosts by searching on the basis of a range of host information. The default is **Acquire information from the router**.

Acquire information from the router

Acquires host information using SNMP for the hosts that were found from the router. Selecting this option is recommended.

Acquire information from all terminals

Acquires host information using SNMP for all the IP addresses specified as the search range. You should select this option when the search path includes a router that does not respond to SNMP, such as a VPN environment. Also select this option when the number of hosts resulting from selection of the **Acquire information from the router** option is too small for the actual number of hosts.

A search for hosts using this option may take some time because the system attempts to acquire host information even when there is no host with a specified IP address or from target hosts that are shut down (power off).

Check if started

When this check box is selected in conjunction with selection of the **Acquire information from all terminals** radio button, the system checks whether each host is active before attempting to acquire its host information.

If more than half the IP addresses specified within the search range are for hosts that are shut down or are addresses for which there is no corresponding host, selecting this check box may reduce the host search time.

You should make sure that this check box is not selected if the network search range includes any host that cannot use the ICMP port, such as a host whose OS is Windows XP Service Pack 2 or Windows Server 2003 Service Pack 1.

Save button

Sets the host search settings. The host search settings are displayed on the **Host search settings** page of the Host Search dialog box.

Start after save button

Sets the host search settings and starts the host search. If you have selected **Immediate execution**, clicking this button sets the host search settings and executes the host search immediately. If you have selected **Scheduled execution**, the host search is executed in accordance with the specified schedule date and time.

The host search settings are displayed on the **Host search settings** page of the Host Search dialog box.

Cancel button

Closes the Addition of Host Search Setup dialog box without saving the host search settings.

(5) Settings for the validity period of search results

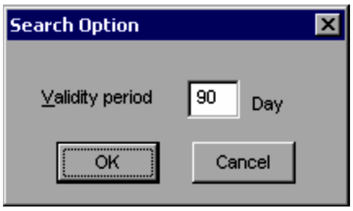
If the intended information is not obtained from a host, you can determine if it is simply because the host's power was off, or if the host has been removed from the network. You do this by setting a validity period for the search results.

If a search does not yield intended information from a host, that host is assumed at the completion of the host search to be nonexistent in the network as of the time of detection of hosts on which JP1/Software Distribution is not installed. In order to avoid this, you may set a validity period for the host information.

When a host search is executed after the specified validity period since the last host search has expired, any host that still does not yield intended information will be assumed to have been removed from the network and will no longer be detected as a host on which JP1/Software Distribution is not installed.

You set the validity period for search results in the Search Option dialog box, which is displayed by choosing **Search** and then **Search Options**.

Figure 9–45: Search Option dialog box



Validity period 90 Day

Validity period

Specifies the period for which the information about the searched hosts is to remain valid, in the range from 1 to 365 days. The default is 90 days.

(6) Executing a search

To execute a host search, select the desired host search settings in the Host Search dialog box and then click the ▶ or **Start** button.

The host search begins and **Running** is displayed in the **Status** column.

When the host search is completed, the **Status** changes to **Finish** and any hosts on which JP1/Software Distribution is not installed will have been detected automatically.

Note that these detection results are not applied to the Detection of Hosts Not Containing Software Distribution dialog box. To display the detection results, you must click the **Latest information** button in the Detection of Hosts Not Containing Software Distribution dialog box to refresh the screen display.

To stop a host search, click the ■ or **Stop** button. The **Status** changes to **Cancel** and the host search stops. When the host search is cancelled, the host information that has been obtained up to that point is registered in the managing server. However, detection of hosts on which JP1/Software Distribution is not installed is not executed.

9.7.5 Updating the detection results

By updating the detection results, you can obtain the most recent information about hosts on which JP1/Software Distribution is not installed.

In the cases described below, information about hosts on which JP1/Software Distribution is not installed has been updated or hosts on which JP1/Software Distribution is not installed have been added to the network, but these changes are not applied automatically to the detection results. You use the Detection of Hosts Not Containing Software Distribution dialog box to update the detection results and check the most recent information about hosts on which JP1/Software Distribution is not installed.

- A host search was executed.
- JP1/Software Distribution was installed on a host on which JP1/Software Distribution had not already been installed.
- JP1/Software Distribution was uninstalled.
- A host on which JP1/Software Distribution is not installed was added to the network.
- A host was removed from the network.
- System configuration information was created from a file.
- The `dcmhstwo` command was executed to detect hosts on which JP1/Software Distribution is not installed.

This subsection describes how to update the detection results for each case.

(1) When a host search was executed

Click the **Latest information** button to update the information in the Detection of Hosts Not Containing Software Distribution dialog box.

If a host search is executed to detect hosts on which JP1/Software Distribution is not installed, information about the hosts on which JP1/Software Distribution is not installed is updated, but the information in the Detection of Hosts Not Containing Software Distribution dialog box remains unchanged.

(2) When JP1/Software Distribution was installed on a host on which JP1/Software Distribution had not already been installed

Click the **Latest information** button to update the information in the Detection of Hosts Not Containing Software Distribution dialog box.

When the MAC address of the host on which JP1/Software Distribution was installed is registered in the managing server by the *Get system configuration information* or *Get system information from client* job, which are facilities for registering the system configuration automatically, information about the corresponding host is deleted automatically from the existing detection results of hosts on which JP1/Software Distribution is not installed.

If JP1/Software Distribution was installed on a host on which JP1/Software Distribution was not already installed and that host had been set as a non-detection target, the information about the host is not deleted automatically from the existing detection result of hosts on which JP1/Software Distribution is not installed even when the host is reset to being a detection target. In this case, to display the most recent information, set the host as a detection target and then choose the **Detect unintroduced host** menu, which is displayed by clicking the **Search/Detect** button.

(3) When JP1/Software Distribution was uninstalled

From the system configuration information registered in the managing server, delete information about the applicable host, and then choose the **Detect unintroduced host** menu, which is displayed by clicking the **Search/Detect** button.

If you are using a facility for registering system configuration information automatically, you can automatically delete the host from which JP1/Software Distribution has been uninstalled from the system configuration information. In this case, choosing the **Detect unintroduced host** menu, which is displayed by clicking the **Search/Detect** button after uninstalling JP1/Software Distribution, automatically detects the host as one on which JP1/Software Distribution is not installed.

(4) When a host on which JP1/Software Distribution is not installed was added to the network

Execute a host search to detect hosts on which JP1/Software Distribution is not installed.

When the host search is completed, click the **Latest information** button to update the information in the Detection of Hosts Not Containing Software Distribution dialog box.

(5) When a host was removed from the network

Execute a host search to detect hosts on which JP1/Software Distribution is not installed. Note that information about the host that has been removed from the network is deleted if the validity period for its detection results has expired. For details about the validity period of search results, see *9.7.4(5) Settings for the validity period of search results*.

When the host search is completed, click the **Latest information** button to update the information in the Detection of Hosts Not Containing Software Distribution dialog box.

(6) When system configuration information was created from a file

If system configuration information was created from a file, information about hosts on which JP1/Software Distribution is not installed is not updated. Use the following procedure to detect the hosts on which JP1/Software Distribution is not installed:

If a host search in the network has been conducted:

Choose the **Detect unintroduced host** menu, which is displayed by clicking the **Search/Detect** button, and detect the hosts on which JP1/Software Distribution is not installed.

If a host search in the network has not been conducted:

Execute a host search to detect hosts on which JP1/Software Distribution is not installed.

When the host search is completed, click the **Latest information** button to update the information in the Detection of Hosts Not Containing Software Distribution dialog box.

(7) When the dcmhstwo command was executed to detect hosts on which JP1/Software Distribution is not installed

Click the **Latest information** button to update the information in the Detection of Hosts Not Containing Software Distribution dialog box.

When you execute the `dcmhstwo` command to detect hosts on which JP1/Software Distribution is not installed from the network configuration information, the information about hosts on which JP1/Software Distribution is not installed is updated, but the information in the Detection of Hosts Not Containing Software Distribution dialog box remains unchanged.

9.7.6 Setting a host as a non-detection target

If the network contains hosts that need not be managed as hosts on which JP1/Software Distribution is not installed, you can specify such hosts as non-detection targets so that they will no longer be detected. You can also restore such hosts to detection target status.

Note that network devices whose type is not **Computer**, such as routers and printers, are handled automatically as non-detection targets.

If the detection results of hosts on which JP1/Software Distribution is not installed are set to be displayed under the **Hold** icon, you must manually specify the hosts that are to be managed as non-detection targets starting from the next detection.

(1) Setting hosts as non-detection targets

Hosts set as non-detection targets are displayed under the **Non-detection target** icon. Such hosts will not be detected until they are specified as hosts on which JP1/Software Distribution is not installed.

To set a host as a non-detection target:

1. In the left-hand frame of the Detection of Hosts Not Containing Software Distribution dialog box, select a host that you wish to set as non-detection target.

   If you select the **Hold** icon, **Non-JP1/SD host** icon, or a network address, all the hosts displayed under the selected item are selected.
2. Click the **Non-detection target** button.

   The selected hosts are displayed under the **Non-detection target** icon and treated as non-detection targets starting at the next detection of hosts on which JP1/Software Distribution is not installed.

(2) Setting hosts as detection targets

You can specify hosts displayed under the **Hold** icon or specified as non-detection targets as hosts on which JP1/Software Distribution is not installed and handle them as detection targets.

When a host is set as a detection target, its display location changes in the Detection of Hosts Not Containing Software Distribution dialog box, but detection does not take place. To display the most recent information, re-execute detection.

To set a host as a detection target:

1. In the left-hand frame of the Detection of Hosts Not Containing Software Distribution dialog box, select a host that you wish to set as detection target.

   If you select the **Hold** icon, **Non-detection target** icon, or a network address, all the hosts displayed under the selected item are selected.
2. Click the **Non-JP1/SD Host** button.

   The selected hosts are displayed under the **Non-JP1/SD host** icon and treated as detection targets starting at the next detection of hosts on which JP1/Software Distribution is not installed.

   To display the most recent information about hosts on which JP1/Software Distribution is not installed, re-execute detection.

9.7.7 Exporting the detection results to a CSV file

You can export to CSV files the search results of hosts in the network and the detection results of hosts on which JP1/Software Distribution is not installed.

The obtained CSV file can also be used as a network connection information file.

(1) Exporting the search results of hosts in the network

The following information is exported to the CSV file for each host:

IP address, node type, node name, MAC address, subnet mask, network address, last update date and time, description

To export the search results to a CSV file:

1. In the Detection of Hosts Not Containing Software Distribution dialog box, click the **CSV output** button.
2. From the displayed menu, choose **Host search results**.

   A dialog box is displayed to save the CSV file that contains the search results.
3. Specify the storage location and a name for the file and then click the **Save** button.

   The search results are saved in the specified CSV file.

You can also use the `dcmcsvu` command provided by JP1/Software Distribution to export search results to a CSV file. For details about how to use the `dcmcsvu` command to export search results to a CSV file, see *4.5 dcmcsvu.exe (exporting to a CSV-formatted file)* in the manual *Administrator's Guide Volume 2*.

(2) Exporting the detection results of hosts on which JP1/Software Distribution is not installed

The following information is exported to the CSV file for each host except for hosts that are placed on hold or hosts set as non-detection targets:

IP address, node type, node name, MAC address, subnet mask, network address, detection date and time, last update date and time, description

To export the detection results to a CSV file:

1. In the Detection of Hosts Not Containing Software Distribution dialog box, click the **CSV output** button.
2. From the displayed menu, choose **Unintroduced Host Information**.
   A dialog box is displayed to save the CSV file that contains the detection results.
3. Specify the storage location and a name for the file and then click the **Save** button.
   The detection results are saved in the specified CSV file.

You can also use the `dcmcsvu` command provided by JP1/Software Distribution to export detection results to a CSV file. For details about how to use the `dcmcsvu` command to export detection results to a CSV file, see *4.5 dcmcsvu.exe (exporting to a CSV-formatted file)* in the manual *Administrator's Guide Volume 2*.

9.7.8 Creating a network configuration information file

Instead of executing a host search, you can read a CSV file (network configuration information file) the contains network configuration information, such as the MAC addresses and IP addresses of the hosts in the network, to detect hosts on which JP1/Software Distribution is not installed.

There are two ways to create a network configuration information file:

- By exporting the host search results or the detection results of hosts on which JP1/Software Distribution is not installed to a CSV file.
- Manually or by using a desired tool.

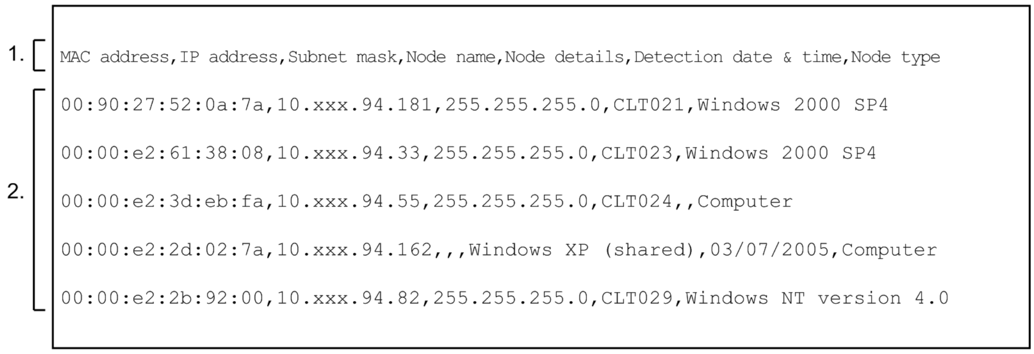
This subsection describes the format of the network configuration information file and the information specified in the file.

(1) Format of network configuration information file

A network configuration information file is specified in CSV format. Line 1 is a title line, and each subsequent line specifies information about a host.

The following figure shows a specification example of a network configuration information file.

Figure 9–46: Specification example of a network configuration information file



```
MAC address,IP address,Subnet mask,Node name,Node details,Detection date & time,Node type
00:90:27:52:0a:7a,10.xxx.94.181,255.255.255.0,CLT021,Windows 2000 SP4
00:00:e2:61:38:08,10.xxx.94.33,255.255.255.0,CLT023,Windows 2000 SP4
00:00:e2:3d:eb:fa,10.xxx.94.55,255.255.255.0,CLT024,,Computer
00:00:e2:2d:02:7a,10.xxx.94.162,,,Windows XP (shared),03/07/2005,Computer
00:00:e2:2b:92:00,10.xxx.94.82,255.255.255.0,CLT029,Windows NT version 4.0
```

1. Title line 2. Host information

The title line defines the order of the items specified as the host information. The title line may contain the items in any order, but the order of specification of the host information items must match the order of the items in the title line.

The following rules apply to specifying a network configuration information file:

- Maximum number of items that can be specified per line: 32
- Maximum amount of data per line: 16 kilobytes

(2) Items in the network configuration information file

This subsection describes the items that can be specified in the title line of the network configuration information file and the items to be specified as host information.

(a) Items specified in the title line

The following describes the items to be specified in the title line and the format of each item.

- `MAC address` (mandatory)
  Specify `MAC` in uppercase alphabetic characters and `address` in lowercase alphabetic characters.
- `IP address` (mandatory)
  Specify `IP` in uppercase alphabetic characters and `address` in lowercase alphabetic characters.
- `Subnet mask`
  Specify all in alphabetic characters as shown above.
- `Node name`
  Specify all in alphabetic characters as shown above.
- `Node details`
  Specify all in alphabetic characters as shown above.
- `Detection date & time`
  Specify all in alphabetic characters as shown above.
- `Node type`
  Specify all in alphabetic characters as shown above.

Do not specify the same item more than once. You can omit all items except `MAC address` and `IP address`.

In the title line, an invalid item or an item in an invalid format is ignored. The corresponding host information item is also ignored. For example, if the third item in the title line is `Device information`, it is invalid; therefore, it will be ignored along with the corresponding host information item, which will be the third item in the network configuration information file.

(b) Items specified as host information

Specify the following items in such a manner that they correspond to the items in the title line in the correct order:

- `MAC address` (mandatory)
  Specify the MAC address of the host, as 12-17 bytes of hexadecimal characters. The MAC address is not case-sensitive. To separate the MAC address into 2-digit segments, use one of the colon (`:`), hyphen (`-`), or space as a delimiter.

  If multiple host information items have the same MAC address, the last applicable host information item specified is subject to detection.
- `IP address` (mandatory)
  Specify the IP address of the host.
- `Subnet mask`
  Specify the subnet mask of the host.
- `Node name`
  Specify the host name, expressed as 1-80 characters. Normally, the computer name is specified as host name.
- `Node details`
  Specify details of the host, as 1-255 characters.
- `Detection date & time`

This is the first date and time the host was detected as a host on which JP1/Software Distribution was not installed. This information is set automatically when a host on which JP1/Software Distribution is not installed is detected for the first time.

To specify the detection date and time, use the format *MM*/*DD*/*YYYY* *hh*:*mm*:*ss*. Place a space between *MM*/*DD*/*YYYY* and *hh*:*mm*:*ss*.

- *MM*: Month (01 to 12)
- *DD*: Date (01 to31)
- *YYYY*: Year (1970 to 2038)
- *hh*: Hour (00 to 23)#
- *mm*: Minute (00 to 59)#
- *ss*: Second (00 to 59)#

#

The item is optional. When it is omitted, all the following items must be omitted. `00` is set in each omitted item.

- `Node type`

Specify the type of host. The supported types are as follows:

- `Computer`
- `Router`
- `Bridge`
- `Repeater`
- `Printer`
- `RMON`

If this item is omitted, `Computer` is set. If any other item is specified, an error occurs during detection of hosts on which JP1/Software Distribution is not installed.

When hosts on which JP1/Software Distribution is not installed are being detected, any host whose type is not `Computer` is set automatically as a non-detection target.

(c) Notes on creation of a network configuration information file

- If the network configuration information file contains any hosts that are outside the management range of JP1/Software Distribution, all such hosts are detected as hosts on which JP1/Software Distribution is not installed.
- If a host information item contains a double quotation mark (`"`) or a comma (`,`), you must specify the item as follows:

Optionally enclose the host information item in double quotation marks (`"`):

Example: Specifying `Windows 2000 Professional`

```
...,"Windows 2000 Professional",...
```

To use a comma (`,`) or double quotation mark (`"`) as part of the host information item, observe the following rules:

When a host information item contains a comma (,):

Enclose the entire item in double quotation marks (`"`).

Example: Specifying `Windows 2000, Professional`

```
...,"Windows 2000, Professional",...
```

When a host information item contains double quotation marks ("):

Specify the double quotation marks as is because they are treated as part of the character string.

Example: Specifying `Windows "2000" Professional`

```
...,Windows "2000" Professional,...
```

To enclose the item in double quotation marks (`"`), specify 2 consecutive double quotation marks inside the item:

Example 1: Specifying `Windows "2000" Professional`

```
...,"Windows ""2000"" Professional",...
```

Example 2: Specifying `"Windows 2000 Professional"`

```
...,"""Windows 2000 Professional""",...
```

When a host information item contains commas (,) and double quotation marks ("):

Enclose the item in double quotation marks (`"`) and specify 2 consecutive double quotation marks inside the item.

Example: Specifying `Windows "2000", Professional`

```
...,"Windows ""2000"", Professional",...
```

10 Settings Required for Using Asset Information Manager Subset

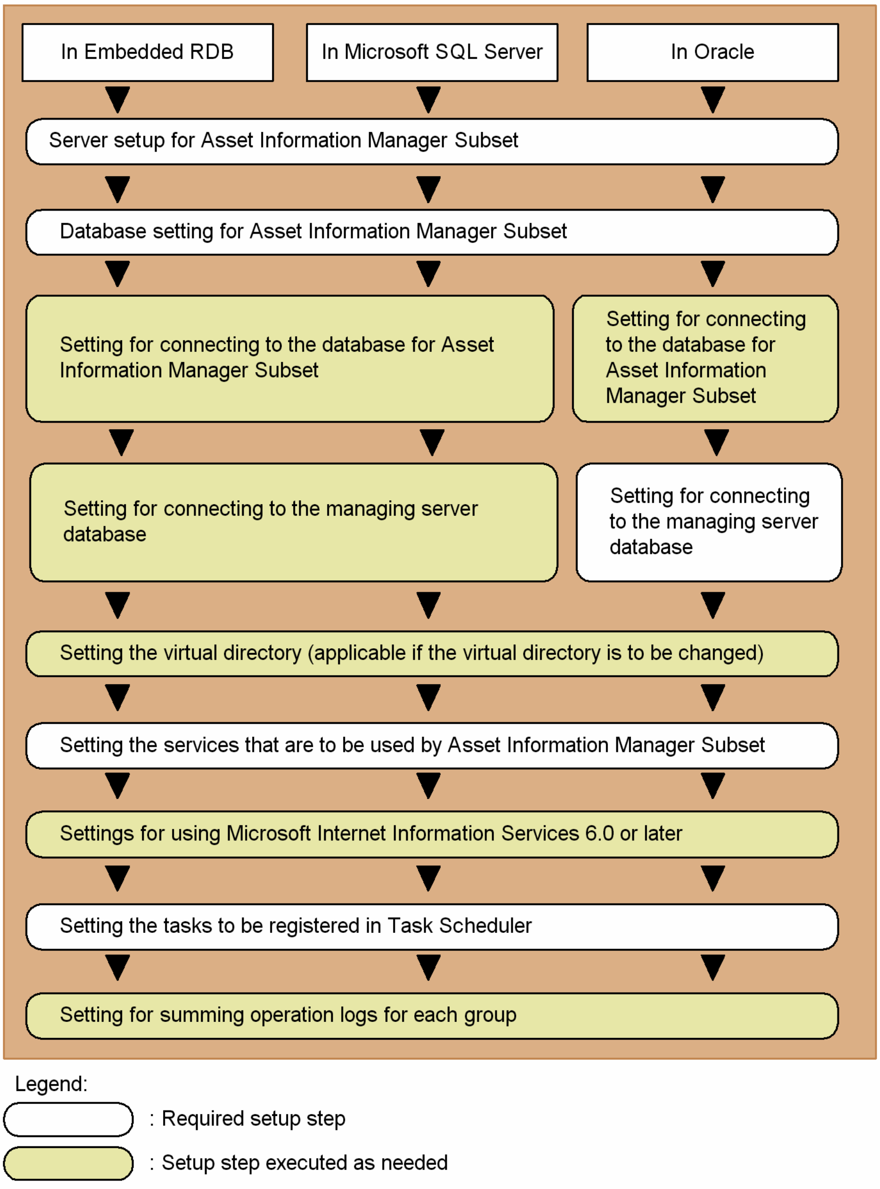
This chapter describes the settings required in order to use Asset Information Manager Subset to total inventory information and operation logs.

10.1 Setting up Asset Information Manager Subset

To use Asset Information Manager Subset to total inventory information and operation logs, you must set up an environment for Asset Information Manager Subset. The environment setup procedure depends on the type of database.

The following figure shows the flow of setting up Asset Information Manager Subset.

Figure 10–1: Flow of setting up Asset Information Manager Subset


In Embedded RDB
In Microsoft SQL Server
In Oracle
Server setup for Asset Information Manager Subset
Database setting for Asset Information Manager Subset
Setting for connecting to the database for Asset Information Manager Subset
Setting for connecting to the database for Asset Information Manager Subset
Setting for connecting to the managing server database
Setting for connecting to the managing server database
Setting the virtual directory (applicable if the virtual directory is to be changed)
Setting the services that are to be used by Asset Information Manager Subset
Settings for using Microsoft Internet Information Services 6.0 or later
Setting the tasks to be registered in Task Scheduler
Setting for summing operation logs for each group
Legend:
: Required setup step
: Setup step executed as needed

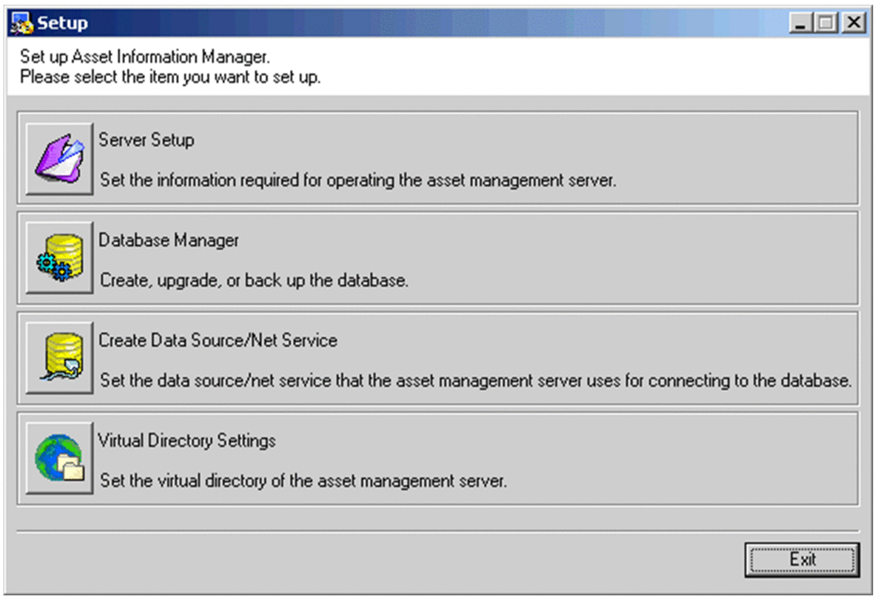
When you set up Asset Information Manager Subset, note the following:

- Terminate all applications that use the database for Asset Information Manager Subset.
- To set up Asset Information Manager Subset, the logon user must have Administrator permissions.

Server setup through the setup of virtual directory is achieved using Asset Information Manager Subset's Setup dialog box.

To display Asset Information Manager Subset's Setup dialog box, from the **Start** menu, choose **Software Distribution Manager**, **Asset Information Manager**, and then **Setup**.

Figure 10–2: Setup dialog box



Set up Asset Information Manager.
Please select the item you want to set up.

Server Setup

Set the information required for operating the asset management server.

Database Manager

Create, upgrade, or back up the database.

Create Data Source/Net Service

Set the data source/net service that the asset management server uses for connecting to the database.

Virtual Directory Settings

Set the virtual directory of the asset management server.

When you click a button for an operation to be performed, the corresponding setup dialog box appears.

Server Setup

Uses the Server Setup dialog box to set the information required for setting up Asset Information Manager Subset. For details about how to set up Asset Information Manager Subset, see *10.2 Setting up the server for Asset Information Manager Subset*.

Database Manager

Uses Database Manager to create an environment for the Asset Information Manager Subset database. For details about how to manipulate Database Manager for Asset Information Manager Subset, see *10.3 Setting up the Asset Information Manager Subset database*.

Create Data Source/Net Service

Creates a data source or a net service for connecting to the managing server database and the Asset Information Manager Subset database.

For details about how to create a data source or a net service, see *10.3.8 Creating a data source or a net service*.

Virtual Directory Settings

Sets the virtual directory for Asset Information Manager Subset to a Web site other than **Default Web Site**.

If Microsoft Internet Information Services 6.0 or later is used, this item is used to create and change an application pool that is to be associated with Asset Information Manager Subset's virtual directory.

For details about how to set the virtual directory and create and change an application pool, see *10.4 Setting the virtual directory*.

The following sections describe each procedure for setting up Asset Information Manager Subset.

10.2 Setting up the server for Asset Information Manager Subset

To set the information needed for setting up the server for Asset Information Manager Subset, use the Server Setup dialog box. The following describes the settings:

- **Database Information**

  Sets the information needed for connecting to the database for Asset Information Manager Subset, such as the login ID and service name.

- **Session Information**

  Sets the time for forcibly logging out from the Asset Information Manager Subset operation window and the Operation Log List, Operation Log Total, and Software Usage Management windows that are started from Remote Installation Manager; also sets the number of users that can log in concurrently.

- **Basic Information**

  Sets the number of search result items to be displayed and the items for managing groups.

- **Link with JP1/SD**

  Sets the information needed for connecting to the managing server database, such as the login ID and service name. This item is also used to set the assignment method for loading inventory information to the Asset Information Manager Subset database.

To set each item in the Server Setup dialog box:

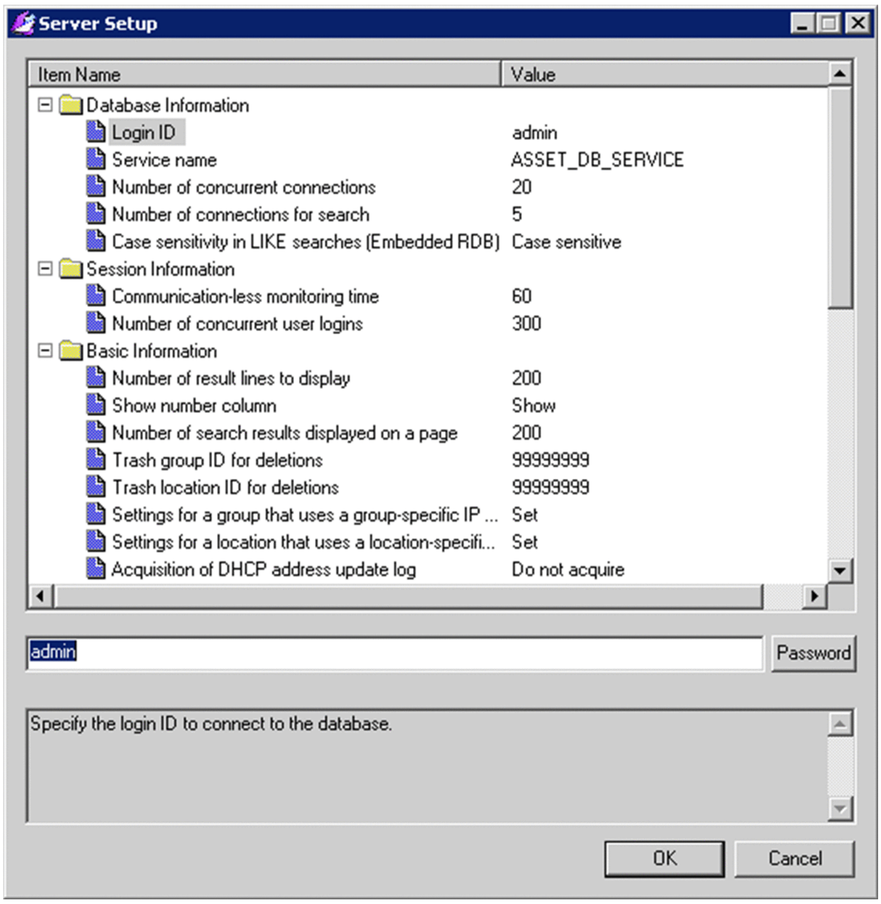
1. From the **Start** menu, choose **Software Distribution Manager**, **Asset Information Manager**, and then **Setup**.

   The Setup dialog box for Asset Information Manager Subset is displayed.

2. Choose **Server Setup**.

   The Server Setup dialog box appears.

Figure 10–3: Server Setup dialog box



Item Name	Value
Database Information	
Login ID	admin
Service name	ASSET_DB_SERVICE
Number of concurrent connections	20
Number of connections for search	5
Case sensitivity in LIKE searches (Embedded RDB)	Case sensitive
Session Information	
Communication-less monitoring time	60
Number of concurrent user logins	300
Basic Information	
Number of result lines to display	200
Show number column	Show
Number of search results displayed on a page	200
Trash group ID for deletions	99999999
Trash location ID for deletions	99999999
Settings for a group that uses a group-specific IP ...	Set
Settings for a location that uses a location-specifi...	Set
Acquisition of DHCP address update log	Do not acquire

admin

Specify the login ID to connect to the database.

3. Set the appropriate values for your environment.

   For details about each setting, see the description of the corresponding item.

   To specify **Login ID** under **Database Information** and **JP1/SD database login ID** under **Link with JP1/SD**, click the **Password** button to display the Set Password dialog box, and then specify the password.

4. Click the **OK** button.

   A server environment is set up for Asset Information Manager Subset based on the specified information, and then the Server Setup dialog box closes.

   To close the Server Setup dialog box without setting up the environment, click the **Cancel** button.

The following subsections provide details of each item.

10.2.1 Setting database information

Sets the information needed for connecting to the database for Asset Information Manager Subset, such as the login ID and service name.

The following describes the items to be set as database information.

(1) Login ID

Login ID specifies the login ID of the user who will be connecting to the database. This is the login user ID that is used when a database is created for Asset Information Manager Subset. For details about how to create a database, see *10.3.1 Creating a new database*.

In the Set Password dialog box, set the password.

This setting is mandatory.

- Permitted value

  From 1 to 29 bytes of characters (**Login ID** and password). In Embedded RDB, specify the **Login ID** as a character string of 1-8 bytes. The default is `admin` for both **Login ID** and the password.

  Depending on the type of DBMS, there are limitations to the values that can be specified for **Login ID** and password. The following table shows the limitations to the values that can be specified in each DBMS.

Table 10–1: Limitations to the values that can be specified for Login ID and password

DBMS type	Limitations to value
Embedded RDB	Only single-byte A to Z, a to z, 0 to 9, # @ and \ can be used. The value must begin with an alphabetic character.
Microsoft SQL Server	!, (,), *, ,, ;, =, ?, @, [,], {, }, and space cannot be used.
Oracle	" cannot be used.

The value set here is applied to **Connection user ID** in the dialog boxes listed below. If you have changed the value after creating a new database, re-create the data source or net service.

- Basic Database Settings dialog box
- Create Data Source/Net Service dialog box

(2) Service name

Service name specifies a service name for the Asset Information Manager Subset database. This is the ODBC data source name (in Embedded RDB or Microsoft SQL Server) or a net service name (in Oracle) that is to be used when a database is created for Asset Information Manager Subset. For details about how to create a database, see *10.3.1 Creating a new database*.

Specification of this item is mandatory.

- Permitted value

  From 1 to 63 bytes of alphanumeric characters and symbols. The default is `ASSET_DB_SERVICE`.

  Depending on the type of DBMS, there are limitations to the value that is specified for **Service name**. The following table shows the limitations to the values that can be specified in each DBMS.

Table 10–2: Limitations to the values that can be specified for Service name

DBMS type	Limitations to value
Embedded RDB or Microsoft SQL Server	!, (,), *, ,, ;, =, ?, @, [,], {, }, and space cannot be used.
Oracle	!, ", #, $, %, &, ', (,), *, +, ,, /, :, ;, <, =, >, ?, @, [, \,], ^, `, {, |, }, ~, and space cannot be used.

The value set here applies to **ODBC data source name** and **Net service name** in the dialog boxes listed below. If you have changed the value after creating a new database, re-create the data source or net service.

- Basic Database Settings dialog box
- Create Data Source/Net Service dialog box

(3) Number of concurrent connections

Number of concurrent connections specifies the number of concurrent database connections.

Specification of this item is optional.

- Permitted value

  From 1 to 64. The default is `20`. Specify a value that is greater than the value of **Number of connections for search** in **Database Information**. If nothing is specified, the default value is used.

(4) Number of connections for search

Number of connections for search specifies the number of processes requiring a long database connection time that can connect to the database concurrently. By specifying this setting, you can prevent the database from being locked by a long-running transaction such as a search request.

Specification of this item is optional.

- Permitted value
  From 1 to 64. The default is `5`. The value of this item must be less than the value of **Number of concurrent connections** in **Database Information**. If nothing is specified, the default value is used.

(5) Case sensitivity in LIKE searches (Embedded RDB)

Case sensitivity in LIKE searches (Embedded RDB) specifies whether or not a search is to be case sensitive when partial match searches including leading and trailing match are performed while Embedded RDB is being used.

- Permitted value
  - **Case sensitive** (default)
    Searches are to be case sensitive.
  - **Case insensitive**
    Searches are not to be case sensitive.

10.2.2 Setting the session information

Sets the time for forcibly logging out from the Operation Log List window and the number of users that can log in concurrently.

The following describes the items that are set as session information.

(1) Communication-less monitoring time

Communication-less monitoring time specifies the length of time Web browser operation can be idle before the user is forcibly logged out.

Specification of this item is optional.

- Permitted value
  5-2,880 minutes. The default is `60` minutes. If nothing is specified, the default value is used.

(2) Number of concurrent user logins

Number of concurrent user logins specifies the number of users that can be logged in concurrently.

This setting is mandatory.

- Permitted value
  From 1 to 100,000. The default is `300`.

10.2.3 Setting the basic information

Basic Information specifies information such as the items that are displayed in windows and the maximum values during operation.

For details about each setting, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

The following describes other items.

(1) Number of result lines to display

Number of result lines to display specifies the number of items to be displayed in the list of search results. This setting is applicable to a window in which the search results are not displayed in pages.

Specification of this item is optional.

- Permitted value

  From 1 to 1,000 items. The default is `200` items. If nothing is specified, the default value is used.

(2) Show number column

Show number column specifies whether or not to display in the operation window the show number column for specifying the number of search result items that are to be displayed per page. This setting is applicable to a window used for executing a search in which the search results are displayed in pages.

- Permitted value
  - **Show** (default)

    Display the show number column.
  - **Hide**

    Do not display the show number column. The number of search results that displays per page becomes the number specified in the Server Setup dialog box, **Basic Information**, **Number of search results displayed on a page**.

(3) Number of search results displayed on a page

Number of search results displayed on a page specifies the number of items to be displayed in the list of search results. This setting is applicable to a window in which the search results are displayed in pages.

Specification of this item can be omitted.

- Permitted value

  From 1 to 1,000 items. The default is `200` items. If nothing is specified, the default value is used.

(4) Trash group ID for deletions

If a group is deleted, a group called **Trash** is automatically created in order to temporarily save the user information that had been registered to the deleted group. In **Trash group ID for deletions**, set the group ID for **Trash**.

Specification of this item is optional.

- Permitted value

  Between 0 and 64 alphanumeric characters. The default is `99999999`. If nothing is specified, the default value is used.

(5) Trash location ID for deletions

When a location is deleted, a location called `Trash` is created automatically to save the deleted location temporarily. **Trash location ID for deletions** specifies the location ID for `Trash`.

The setting for this item can be omitted.

- Permitted value

  Between 0 and 64 alphanumeric characters. The default is `99999999`. If a space is specified, the default value is used.

(6) Settings for a group that uses a group-specific IP group

Setting for a group that uses a group-specific IP group specifies whether or not to set a group that uses devices according to the IP address. To register IP address-specific groups, use the **IP Group** job menu. Groups are set according to the IP addresses of the hardware asset information.

This setting takes effect when the **Asset Information Synchronous Service** service and the **Take inventory** and **Data maintenance** tasks are executed. To enable the setting when executing the **Data maintenance** task, you must modify the settings file (`taskopt.ini`). For details about how to modify the settings file, see *10.7.2(2) Creating a settings file*.

- Permitted value
  - **Do not set**
    Does not set up an IP address-specific device group.
  - **Set**
    Sets up an IP address-specific device group. Even if a value is already specified, it is overwritten with the new group-specific IP group value.
    Specify this value if you need to update groups according to the setting in the **IP Group** job menu.
  - **To only set a group that has not been set** (default)
    Sets up an IP address-specific device group only when no device group has been registered.
    Specify this option mainly when you need to set up a group for a newly registered device.

Note

If **Set** is selected, but the value of user inventory or the value entered in the Device Details dialog box has already been set, the value is not overwritten.

Therefore, to set group-specific IP groups for all devices, first use the **Batch Update** job menu to delete the values for all groups. Also use the **Assign Inventory** job menu to set **Overwrite setting** for **Group information.Local name** to **Overwrite (not overwritten if NULL or N/A)** or use the **Data maintenance** task to overwrite. For details about how to specify settings with the **Data maintenance** task, see *10.7.2 Specifying the work to be performed by the Data maintenance task*.

(7) Settings for a location that uses a location-specific IP group

Settings for a location that uses a location-specific IP group specifies whether to set up IP address-specific locations as device locations. To register IP address-specific locations, use the **IP Group** job menu. Locations are set according to the IP addresses of the hardware asset information.

This setting takes effect when the **Asset Information Synchronous Service** service and the **Take inventory** and **Data maintenance** tasks are executed. To enable the setting when executing the **Data maintenance** task, you must modify the settings file (`taskopt.ini`). For details about how to modify the settings file, see *10.7.2 Specifying the work to be performed by the Data maintenance task*.

- Permitted value
  - **Do not set**
    Does not set up an IP address-specific device location.
  - **Set**
    Sets up an IP address-specific location as the device location. Even if a value is already specified, it is overwritten with the new location-specific IP group value.
    Specify this value if you need to update locations according to the setting in the **IP Group** job menu.
  - **To only set a location that has not been set** (default)
    Sets up an IP address-specific location only when no device location has been registered.
    Specify this option mainly when you need to set up a location for a newly registered device.

Note

If **Set** is selected but the value obtained from the user inventory or the value entered in the Device Details dialog box has already been set, the value is not overwritten. Therefore, to set location-specific IP groups for all devices, first use the **Batch Update** job menu to delete the values for all locations. Also make sure that **Overwrite setting** for *location-information***.***location-name* in the **Assign Inventory** job menu is set to `Overwrite (Not overwritten if NULL or N/A.)`.

Reference note

Even when the value acquired from the user inventory or the value entered in the Device Details dialog box has been set, you can use the **Data maintenance** task to update the location according to the settings specified using the **IP**

Group job menu. For details about how to specify settings with the **Data maintenance** task, see *10.7.2 Specifying the work to be performed by the Data maintenance task.*

---

(8) Number of search results acquired for the operation log

Number of search results acquired for the operation log specifies the number of operation log entries to be searched for each table of the managing server in order to prevent too much time being spent on search processing.

This value cannot be left empty even when operation logs are not managed.

- Permitted value
  Between 1 and 100,000 results. The default is `5000`.

(9) Warning about the operation log list search period

Warning about the operation log list search period specifies a range of time for issuing a warning about the amount of time spent in search processing in the **Operation Log List** job menu and the Operation Log List window in order to prevent too much time from being expended on a search. If the time from **Search period (start)** to **Search period (end)** exceeds the value of this item, a warning is displayed. If `0` is specified in this item, no warning is displayed.

This value cannot be left empty even when operation logs are not managed.

- Permitted value
  Between 0 and 10,080 minutes. The default is `60` minutes.

(10) Hierarchy levels to display when tracing

Hierarchy levels to display when tracing specifies the number of hierarchies to be displayed when the back or forward icon is selected while operations are being traced in the **Operation Log List** job menu and the Operation Log List window.

This value cannot be left empty even when operation logs are not managed.

- Permitted value
  Between 0 and 10 hierarchies. The default is `10` hierarchies. If `0` is specified, all hierarchies are displayed.

(11) Settings for trace time range

Settings for trace time range specifies the range of time that is to be treated as the same time when operations on a client via the network are traced in the **Operation Log List** job menu and the Operation Log List window.

This value cannot be left empty even when operation logs are not managed.

- Permitted value
  Between 0 and 300 seconds. The default is `60` seconds, in which case 60 seconds before and after the reference node are treated as being the same time.

(12) Status to display in device search windows

Status to display in device search windows specifies the device statuses to be displayed in **Status** in the Device Totals window and the Device List window.

- Permitted value
  - **Display only active codes** (default)
    Displays the device statuses with codes in the range from 0 to 499. The default is that **Active** and **Stock** are displayed.
  - **Display all codes**
    Displays the device statuses with codes in the range from 0 to 999. The default is that **Active**, **Stock**, **Restore**, **Scrap**, **Pre-Scrap**, and **Erase** are displayed.

(13) Manage device change log information

Manage device change log information selects how to manage the managed device's initial change log. We recommend selecting **Do not manage** in order to improve performance when acquiring inventory information from JP1/Software Distribution.

- Permitted value
  - **Manage**#
    Retains the initial change log when executing the task *Delete log information*.
  - **Do not manage** (default)#
    Deletes the initial change log when executing the task *Delete log information*.

  #
  When upgrading from version 09-00 or earlier, the default is **Manage**.

10.2.4 Setting the link with Directory Server

The **Link with Directory Server** page is used to specify the settings required for linking to Directory Server to perform login authentication, such as the server name and port number.

The following items are set in **Link with Directory Server**.

(1) Use Directory Server

Use Directory Server specifies whether to use Directory Server to authenticate logins.

Select **Use for authentication** only if using Directory Server to authenticate logins.

- Permitted value
  - **Use for authentication**
    Use Directory Server to authenticate logins.
  - **Do not use** (default)
    Do not use Directory Server to authenticate logins.

(2) Code set

Code set specifies the type of character encoding to use.

- Permitted value
  - **Shift-JIS**
    Sets Shift JIS encoding.
  - **UTF-8** (default)
    Sets UTF-8 encoding.

(3) Server name

Server name specifies the Directory Server host name or IP address.

- Permitted value
  From 1 to 255 bytes of single-byte alphanumeric characters and symbols. The default is `AssetHost`.

(4) Port number

Port No. specifies the Directory Server port number.

- Permitted value
  A number from 1 to 65535. The default is `389`.

(5) Users with access

Users with access specifies the user domain name for accessing Directory Server information entries.

You must first output a list of user information, using Active Directory's `LDIFDE` command, to find the domain names of the users for whom you want to allow access. For details about search methods, see *10.10.1 Login authentication*.

Also set the password in the Set Password dialog box.

- Permitted value

  The permitted value for users with access is 1 to 255 bytes of single-byte alphanumeric characters and symbols, single-byte katakana and kanji. The default is blank.

  The permitted value for the password is 1 to 255 bytes of single-byte alphanumeric characters and symbols, and single-byte katakana. The default is blank.

(6) Response monitoring time

Response monitoring time specifies the time (in seconds) that Directory Server has to respond to a search request. If this amount of time has passed and there is no response from Directory Server, processing is terminated and reported as a communication error. If numerous processes use the Directory Server service and communication errors occur frequently during login authentication, set a longer response wait time.

- Permitted value

  From 1 to 65,535 seconds. The default is `60` (seconds).

(7) User information DN

User information DN specifies the domain name that serves as the basis for user information searches.

You must first output a list of user information, using Active Directory's `LDIFDE` command, to find the domain name of the group to be searched for users during Asset Information Manager Subset login authentication. For more about search methods, see *10.10.1 Login authentication*.

- Permitted value

  From 1 to 255 bytes of single-byte alphanumeric characters, symbols, single-byte katakana, and kanji. The default is `ou=people,o=`*xxxxxxx*`.com`.

(8) User ID attribute name

User ID attribute name specifies the attribute name of the user information to be used as the user ID during Asset Information Manager Subset login.

You must first output a list of user information, using Active Directory's `LDIFDE` command, to find the attribute name to be used as the user ID during Asset Information Manager Subset login authentication. For more about search methods, see *10.10.1 Login authentication*.

- Permitted value

  The permitted value for user ID attribute name is 1 to 255 bytes of single-byte alphanumeric characters, symbols, single-byte katakana, and kanji. The default is `uid`.

  Under Directory Server user object standards, `uid` is not provided as an attribute. Add the attribute `uid` to the Directory Server user objects if necessary, and specify it as the single-byte user ID to be used during login authentication. Also specify an attribute name that stores the single-byte user ID to be used in Asset Information Manager Subset login authentication in place of `uid`.

(9) User name attribute name

User name attribute name specifies the attribute name of the user information to be used as the Asset Information Manager Subset user name.

You must first output a list of user information, using Active Directory's `LDIFDE` command, to find the attribute name to be used as the Asset Information Manager Subset user name. For more about search methods, see *10.10.1 Login authentication*.

- Permitted value

  From 1 to 255 bytes of single-byte alphanumeric characters, symbols, single-byte katakana, and kanji. The default is `cn`.

10.2.5 Setting the link with JP1/SD

Specifies the information needed to connect to the managing server database, such as the login ID, service name, and how to register inventory information in the database.

For details about the settings for assignment between inventory information and Asset Information Manager Subset's asset information in (4) through (9), see *10.2.6 Setting how to assign inventory information*.

The items listed below must be set only when JP1/Client Security Control is linked. If JP1/Client Security Control is not linked, there is no need to specify them.

- **Code specified for deleted assets**
- **Package ID acquisition**
- **Job storage folder name used in JP1/SD**

For details about each setting, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

The following describes other items.

(1) JP1/SD database login ID

JP1/SD database login ID specifies the login ID to be used to connect to the managing server database.

Specify the password in the Set Password dialog box.

Specification of this item is mandatory.

- Permitted value

  From 1 to 29 bytes of characters (**JP1/SD database login ID** and password). In Embedded RDB, specify the **JP1/SD database login ID** as a character string of 1-8 bytes. The default is `admin` for both **JP1/SD database login ID** and the password.

  Depending on the type of DBMS, there are limitations to the values that can be specified for **JP1/SD database login ID** and the password. The following table shows the limitations to the values that can be specified in each DBMS.

Table 10–3: Limitations to the values that can be specified for JP1/SD database login ID and password

DBMS type	Limitations to value
Embedded RDB	The value must begin with an alphabetic character.
Microsoft SQL Server	`!`, `(`, `)`, `*`, `,`, `;`, `=`, `?`, `@`, `[`, `]`, `{`, `}`, and space cannot be used.
Oracle	`"` cannot be used.

The value set here is applied to **Connection user ID** in the Create Data Source/Net Service dialog box.

(2) Connection service for JP1/SD database

Connection service for JP1/SD database specifies the service name to be used to connect to the managing server database. This item specifies an ODBC data source name (in Embedded RDB or Microsoft SQL Server) or a net service name (in Oracle) that is used to connect to the managing server database.

Specification of this item is mandatory.

- Permitted value

  From 1 to 63 bytes of alphanumeric characters and symbols. The default is `NETM_DB_SERVICE`.

  Depending on the type of DBMS, there are limitations to the value that is specified for **Connection service for JP1/SD database**. The following table shows the limitations to the values that can be specified in each DBMS.

Table 10–4: Limitations to the values that can be specified for Connection service for JP1/SD database

DBMS type	Limitations to value
Microsoft SQL Server and Embedded RDB	!, (,), *, ,, ;, =, ?, @, [,], {, }, and space cannot be used.
Oracle	!, ", #, $, %, &, ', (,), *, +, ,, /, :, ;, <, =, >, ?, @, [, \,], ^, `, {, |, }, ~, and space cannot be used.

The value set here is applied to **ODBC data source name** and **Net service name** in the Create Data Source/Net Service dialog box.

(3) Acquire devices on which JP1/SD is not installed

Acquire devices on which JP1/SD is not installed specifies whether to acquire information about devices on which JP1/SD is not installed as part of non Software Distribution host information.

If JP1/Client Security Control is linked, use the settings for linking JP1/Client Security Control.

- Permitted value
  - **Acquire** (default)
    Acquire information on the devices on which JP1/SD is not installed as part of non Software Distribution host information.
  - **Do not acquire**
    Do not acquire information on the devices on which JP1/SD is not installed as part of non Software Distribution host information.

(4) Working key

Working key specifies whether or not a host ID is used for the ID key for operations according to the settings on the managing server. If you have changed the **Use host IDs** setting on the managing server, also change this setting accordingly.

If JP1/Client Security Control is linked, use the settings for linking JP1/Client Security Control.

- Permitted value
  - **Use host ID** (default)
    Use host ID for the ID key for operations on the managing server. When this value is selected, the host ID is used to assign JP1/Software Distribution's inventory information and Asset Information Manager Subset's asset information.
  - **Do not use host ID**
    Do not use host ID as the ID key for operations on the managing server. If **Node identification key** of the system configuration information is `host name working`, assets with matching MAC address and host name are assigned. If the assets cannot be assigned, assets with matching MAC address are assigned. If the assets still cannot be assigned, assets with matching host name are assigned.

    If the node identification key in the system configuration information is `IP address working`, the asset with the same MAC address and IP address is assigned. If no such asset exists, the asset with the same MAC address is assigned. If no asset with the same MAC address exists, the asset with the same IP address is assigned.

(5) Targets for inventory

Targets for inventory specifies whether to acquire information on devices without host IDs or without system information when acquiring inventory information from JP1/Software Distribution.

- Permitted value
  - **Take all** (default)
    Acquire inventory information for all devices regardless of whether they have host IDs or system information.
  - **Only devices with host IDs**

Acquire inventory information only for devices that have host IDs.

- **Only devices with system information**

  Acquire inventory information only for devices that have system information.

(6) Assign key for asset information

Assign key for asset information selects an assignment key for identification purposes when the information collected on the managing server is registered according to Asset Information Manager Subset's asset information.

If JP1/Client Security Control is linked, use the settings for linking JP1/Client Security Control.

- Permitted value
  - **Use working key** (default)

    The value specified in **Working key** is used as the key value to assign JP1/Software Distribution's inventory information to Asset Information Manager Subset's asset information.
  - **Use Asset No.**

    The asset number specified during assignment of inventory information is used as the key. During assignment of inventory information, numbers are assigned automatically by default. Because inventory information cannot be assigned with this default setting, make sure that this setting is changed.

    For details about the settings for assignment of inventory information, see *10.2.6 Setting how to assign inventory information*.

(7) Conditions for assigning asset information 1

Conditions for assigning asset information 1 specifies how to assign Asset Information Manager Subset's asset information when JP1/Software Distribution's inventory information is acquired. This specification is valid when the value of **Assign key for asset information** is **Use working key**, and the value of the **Working key** is **Use host ID**.

If JP1/Client Security Control is linked, use the settings for linking JP1/Client Security Control.

- Permitted value
  - **Machines with only the same Host ID** (default)

    If assets cannot be assigned by the host ID of the JP1/Software Distribution system configuration information, no other value is to be used for assignment.
  - **Machines with the same MAC address**

    If assets cannot be assigned by the host ID of the JP1/Software Distribution system configuration information, the MAC address is to be used for assignment.
  - **According to the JP1/SD definition**

    If assets cannot be assigned by the host ID of the JP1/Software Distribution system configuration information, the MAC address, host name, and IP address are to be used for assignment.

    If assets cannot be assigned, then if the node identification key of the system configuration information is `host name working`, assets with matching MAC address and host name are assigned. If the node identification key of the system configuration information is `IP address working`, assets with matching MAC address and IP address are assigned.

    If assets still cannot be assigned, the MAC address is to be used for assignment.

  Regardless of the selected value, the value of the host ID is registered as **Assignment key** for Asset Information Manager Subset's asset information.

(8) Conditions for assigning asset information 2

Conditions for assigning asset information 2 selects an assignment method to be used when assignment by **Conditions for assigning asset information 1** fails.

If JP1/Client Security Control is linked, use the settings for linking JP1/Client Security Control.

- Permitted value
  - **Use IP address and host name** (default)

Of the devices that could not be assigned by **Conditions for assigning asset information 1**, assign those assets that have matching host name and IP address.

If assets cannot be assigned, then if the node identification key of the system configuration information is `host name working`, assign assets with matching host name; if the node identification key of the system configuration information is `IP address working`, assign assets with matching IP address.

- **Use machine serial number**

  This method assigns asset information to the inventory information with the matching machine serial number. To use this method, "Machine serial number" needs to be specified for the managed item "Hardware information.Serial number" in the Assign Inventory window through the job category "System Definition".

- **Use machine serial number and IP address and host name**

  For a device that has not been assigned to the inventory information by "Conditions for assigning asset information 1", this assigns asset information to the inventory information that has the same machine serial number, IP address, and host name. Otherwise, the asset information is assigned to the inventory information that has the same machine serial number and host name as when "host name working" is specified for the node identification key of the system configuration information, or that has the same machine serial number and IP address when "IP address working" is specified for the node identification key. If the assignment still fails, the asset information is assigned to the inventory information that has the same serial number only. To use this method, "Machine serial number" needs to be specified for the managed item "Hardware information.Serial number" in the Assign Inventory window through the job category "System Definition".

- **Do not assign**

  Do not register unassigned assets.

- **Assignment processing when the specification is Use machine serial number**

  Asset information with a matching machine serial number is assigned.

  When specifying this assignment method, in the system definition job category, you must specify **Machine serial number** for the item to be assigned to **Hardware information.Serial No** in the inventory information assignment window.

- **Assignment processing when the specification is Use machine serial number, IP address, and host name**

  Assignment follows the following procedure:

  Asset information with a matching machine serial number, IP address, and host name is assigned.

1. When the node identification key is **Use host name**, an asset with a matching machine serial number and host name is assigned.
2. When the node identification key is **Use IP address**, an asset with a matching machine serial number and IP address is assigned.
3. Asset information with a matching machine serial number is assigned.

   When specifying this assignment method, in the system definition job category, you must specify **Machine serial number** for the item to be assigned to **Hardware information.Serial No** in the inventory information assignment window.

(9) Perform new registration of unassigned assets

Perform new registration of unassigned assets specifies whether or not an unassigned asset is to be registered as a new asset. This applies to assets that have not been assigned pursuant to **Conditions for assigning asset information 1** and **Conditions for assigning asset information 2** when **Use host ID** is selected as the **Working key**.

If JP1/Client Security Control is linked, use the settings for linking JP1/Client Security Control.

- Permitted value
  - **New registration** (default)

    If there are assets registered in the database for which inventory information has not been assigned, register those assets as new assets.

  - **Do not perform new registration**

    If there are assets registered in the database for which inventory information has not been assigned, do not register those assets.

    Note that when this value is specified, newly added assets might not be registered.

(10) MAC address for dial up connection

MAC address for dial up connection specifies whether or not the MAC address for dial-up connection is to be added to the information used for assigning Asset Information Manager Subset's asset information.

If JP1/Client Security Control is linked, use the settings for linking JP1/Client Security Control.

- Permitted value
  - **Add to the assigned information**
    Use the MAC address for dial-up connection to assign Asset Information Manager Subset's asset information.
  - **Do not add to the assigned information** (default)
    Do not use the MAC address for dial-up connection to assign Asset Information Manager Subset's asset information. Note that if **Machines with the same MAC address** is selected in **Conditions for assigning asset information 1** and **Do not assign** is selected in **Conditions for assigning asset information 2**, Asset Information Manager Subset's asset information that cannot be assigned by host ID will no longer be assigned.

(11) Type of information to acquire

Type of information to acquire specifies the type of information to be imported into the Asset Information Manager Subset database from the managing server.

If you distribute software programs from the Software Applied window, set the Asset Information Manager to acquire software information to search for the target devices.

For details about the information that is updated by importing from the managing server, see *10.9 Inventory information that can be displayed by Asset Information Manager Subset*.

If JP1/Client Security Console is linked, use the settings for linking JP1/Client Security Console.

- Permitted values
  - **Hardware information**
    Registers the hardware information only.
  - **Hardware and software information** (default)
    Registers the hardware and software information. The software information includes all the information that is installed at the clients (information cannot be selected).
  - **Hardware and software inventory information**
    Registers the hardware information and the information about software that is set to be monitored in the software inventory dictionary.
  - **Hardware and software and software inventory information**
    Registers the hardware and software information and the information about software that is set to be monitored in the software inventory dictionary.

(12) Watch interval for update inventory

Watch interval for update inventory specifies an interval at which updating of inventory information is to be monitored. This setting cannot be left blank.

- Permitted value
  From 1 to 429,496 seconds. The default is `60` seconds.

(13) Status of machines deleted with JP1/SD

Status of machines deleted with JP1/SD specifies the device status of devices collected as deleted devices, when inventory information changes are collected in real time.

If JP1/Client Security Control is linked, use the settings for linking JP1/Client Security Control.

- Permitted value
  - **Scrap**
    The status is set to `Scrap` and the **Data Maintenance** task deletes association with other information.

- **Pre-Scrap** (default)
  Handle as inventory information assignment objects. If information is assigned, the status returns to `Active`.
  Furthermore, as with the **Scrap** setting, the **Data Maintenance** task deletes associations with other information.
- **Erase**
  Set to **Erase** so that the **Data Maintenance** task erases the information.
- **Specify code**
  Set to the code status specified in **Code specified for deleted assets**.
- **Ignore**
  Do not change the device status.

(14) CSC notification count

When acquiring inventory information, **CSC notification count** specifies the frequency (in terms of the number of inventory information items acquired from JP1/Software Distribution) at which to determine the status of security measures taken by Job Management Partner 1/Client Security Control. If this item is set to `0`, security status is determined for the whole batch once all acquisition processing is complete. The smaller the value specified here, the faster the status of security measures undertaken by Job Management Partner 1/Client Security Control can be determined. However, too small a value lowers performance when acquiring inventory information.

- Permitted value
  From 0 to 10,000 notifications. The default is `100`.

(15) Inventory acquisition method

Inventory acquisition method specifies whether to use the conventional method or the multithread method when acquiring inventory information from JP1/Software Distribution. If you choose the multithread method, performance when acquiring inventory information increases, and acquisition time decreases.

- Permitted value
  - **Standard method** (default)
    Acquire inventory information using the conventional method.
  - **Multithreading method**
    Acquire inventory information using the multithread method.

Differences between acquisition methods

The following table outlines the differences between the acquisition methods.

Table 10–5: Differences in function between acquisition methods

Function	Conventional method	Multithread method
Take inventory flow	• For Asset Information Synchronous Service Acquired in the order: inventory information, uninstalled equipment, deletion history information. • For the *Take inventory* task Acquired in the order: uninstalled equipment, inventory information.	• For Asset Information Synchronous Service Acquired in the order: inventory information, uninstalled equipment, deletion history information. • For the *Take inventory* task Acquired in the order: inventory information, uninstalled equipment.
Handling when information exceeds the maximum size of a column's data areas in the database	The acquired information is truncated to the column's maximum size. When this causes the end to be half of a double-byte character, it	The acquires information is truncated to the column's maximum size. When this causes the end to be half of a double-byte character, it is deleted. However, for *group-information*.*group-name*, *group-*

Function	Conventional method	Multithread method
Handling when information exceeds the maximum size of a column's data areas in the database	is converted to a single-byte space.	*information*.*group*, *location-information*.*local-name*, and *location-information*.*local-name*, the remainder is converted to a single-byte space.
Handling when a computer name or user inventory is assigned to management item *asset-information*.*asset-number*	If more than 60 bytes of information is acquired, the new asset is not registered and assignment by asset number is not performed.	If more than 60 bytes of information is acquired, only the first 60 bytes of the new asset are registered and use for the assignment by asset number.

Notes on using the multithread method

- If the multiplex level for inventory acquisition is 2 or more, set **Link with JP1/SD** as follows.
  - Set **Working key** to **Use host ID**.
  - Set **Conditions for assigning asset information 1** to **Machines with only the same Host ID**.

  Otherwise, asset registrations may be repeated or assets nay unintentionally be updated when inventory information is acquired.
- The message ID output to the log is `KDAM8C`*nn*-*m*.
- The number of connections to the Asset Information Manager Subset database is the total of the multiplex level for inventory and the number of connections used for search.
- The number of connections to the JP1/Software Distribution database is the multiplex level for inventory.
- If there are multiple assets to be assigned, only the information of the asset with the highest ID is updated.
- If the system information of the node to be acquired from JP1/Software Distribution has no IP address, network information is not saved.

(16) Multiplex level for inventory acquisition

Sets the level of multiplexing when **Multithread method** is selected in **Inventory acquisition method**.

- Permitted value
  From 1 to 16. The default is `4`.

(17) Conditions for assigning asset information "a"

- Permitted value
  - **Use the machine serial number to assign asset information**
    Machine serial number needs to be specified for the managed item **Hardware information.Serial No** in the Assign Inventory window through the job category System Definition.
  - **Do not assign**
    Do not register unassigned assets in the database.

(18) Defining an assignment-exception MAC list

If multiple management-target devices have the same MAC address assigned to them when MAC addresses are set up as the key for Asset Information Manager to assign asset information to the asset management database, you can register these devices as separate assets. To do so, you must create an assignment-exception MAC list (MacListOfOmitMatching.ini). The storage destination, the description method, and a description example of the assignment-exception MAC list are as follows:

- Assignment-exception MAC list storage destination
  Asset-Information-Manager-installation-folder\env
  A sample file of the assignment-exception MAC list (MacListOfOmitMatching.ini.org) is provided in the aforementioned storage destination for use as a reference when creating an assignment-exception MAC list. View this sample when creating an assignment-exception MAC list.

10.2.6 Setting how to assign inventory information

To load inventory information to the Asset Information Manager Subset database and manage it, you must match the client in JP1/Software Distribution and the managed target in Asset Information Manager Subset to avoid registration errors, such as registering information about the same device as for separate devices.

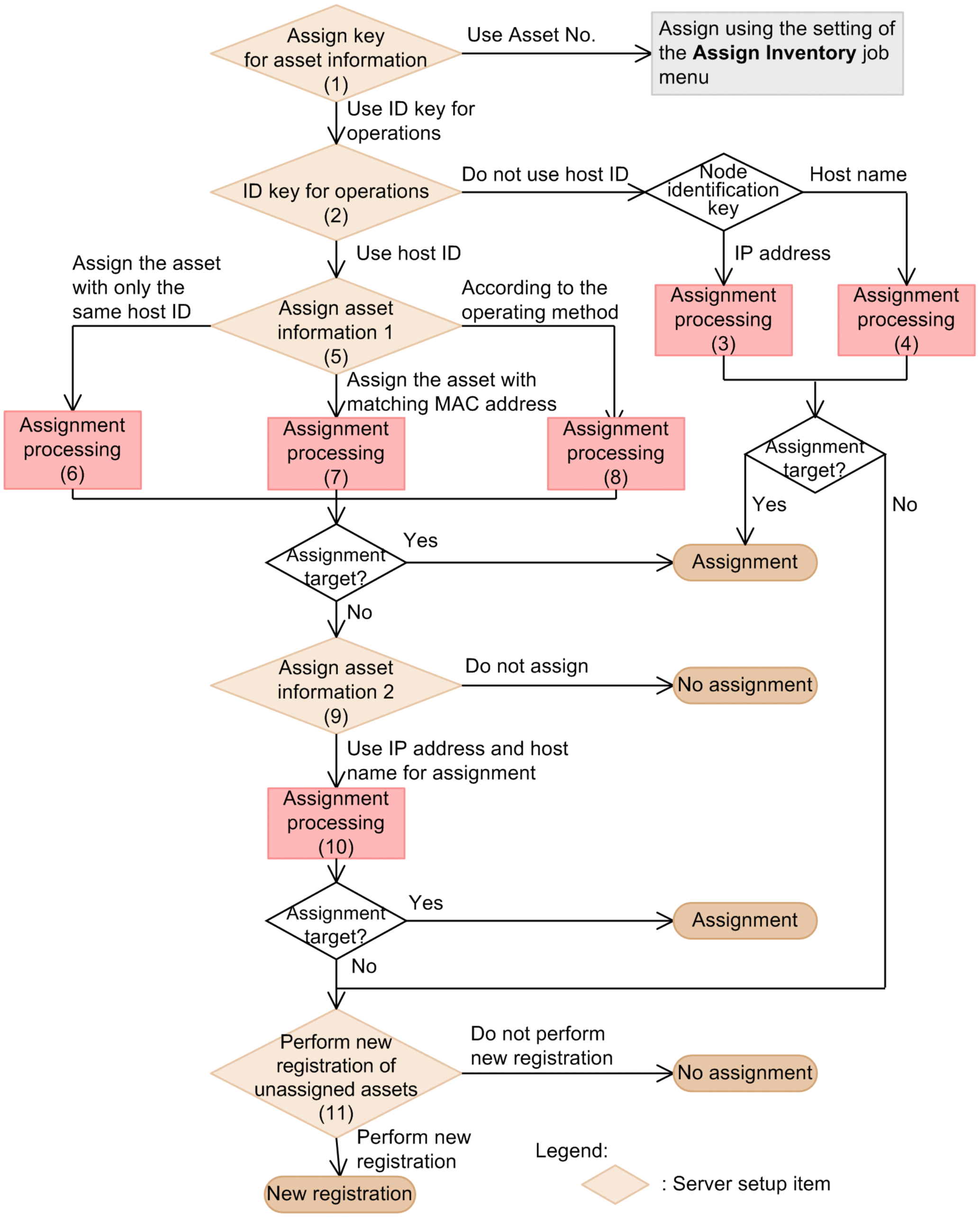
To accurately assign the information collected by JP1/Software Distribution to the asset information in Asset Information Manager Subset, you must specify the information that is to be used as key values for inventory information and Asset Information Manager Subset's asset information.

To specify how to assign inventory information to Asset Information Manager Subset's asset information, use the Server Setup dialog box. For details about the settings, see *10.2.5 Setting the link with JP1/SD*.

This subsection provides a detailed explanation about how inventory information is registered depending on the settings in the Server Setup dialog box.

The following figure shows the flow of settings and assignment in the Server Setup dialog box.

Figure 10–4: Flow of settings and assignment in the Server Setup dialog box


Assign key for asset information (1)
Use Asset No.
Assign using the setting of the **Assign Inventory** job menu
Use ID key for operations
ID key for operations (2)
Do not use host ID
Node identification key
Host name
IP address
Use host ID
Assign the asset with only the same host ID
Assign asset information 1 (5)
According to the operating method
Assignment processing (3)
Assignment processing (4)
Assign the asset with matching MAC address
Assignment processing (6)
Assignment processing (7)
Assignment processing (8)
Assignment target?
Yes
No
Assignment target?
Yes
Assignment
No
Assign asset information 2 (9)
Do not assign
No assignment
Use IP address and host name for assignment
Assignment processing (10)
Assignment target?
Yes
Assignment
No
Perform new registration of unassigned assets (11)
Do not perform new registration
No assignment
Perform new registration
New registration
Legend:
: Server setup item

Numbers (1) through (11) in the figure correspond to the headings for the explanations provided below.

Notes

- If the setting in the Server Setup dialog box is **MAC address for dial up connection** and **Do not add to the assigned information** is specified, devices with a dialup connection are not assigned by MAC address.
- If the device type of the target asset information is not **Computing** (**Device type** code is not in the range from 100 to 199), the asset is registered.

(1) Types of Assign Key for asset information

The two different methods for assigning the inventory information to Asset Information Manager Subset's asset information are the use of JP1/Software Distribution's ID key for operations and the use of asset numbers that have been set by the **Assign Inventory** job menu.

- Using the asset numbers set by the **Assign Inventory** job menu

  The asset number assignment settings specified using the **Assign Inventory** job menu take effect.
- Using the working key

  If the asset number is not managed in the user inventory information, the ID key for operations is used to assign Asset Information Manager Subset's asset information. In this case, the assignment method depends on the ID key for operations used in JP1/Software Distribution.

(2) Details about using working key

The host ID is a special value in the JP1/Software Distribution system; it is key information used to identify each device. The host ID is generated when JP1/Software Distribution Client is installed, and the JP1/Software Distribution server is notified of it automatically. Therefore, the host ID, unlike the node identification key, is not affected by changes to the network configuration.

If the JP1/Software Distribution setting is **Use host ID**, the host ID is used for assignment. If **Use host ID** is not selected, the node identification key is used for assignment.

The host identification key can use the host name or the IP address. The one that is used for management is selected during setup of JP1/Software Distribution; both cannot be used at the same time.

(3) Assignment processing when the node identification key is IP address working

The assignment follows the following procedure:

1. The Asset Information Manager Subset assets with matching MAC address and IP address are assigned.
2. The Asset Information Manager Subset asset information with the matching MAC address is assigned.
3. The Asset Information Manager Subset assets with matching IP address are assigned.

During registration or updating, the IP address is set in **Assignment key** for the Asset Information Manager Subset asset information.

(4) Assignment processing when the node identification key is host name working

The assignment follows the following procedure:

1. The Asset Information Manager Subset asset information with the matching MAC address and host name is assigned.
2. The Asset Information Manager Subset asset information with the matching MAC address is assigned.
3. The Asset Information Manager Subset asset information with the matching host name is assigned.

During registration or updating, the host name is set in **Assignment key** for the Asset Information Manager Subset asset information.

(5) When assignment is not possible by host ID

When assignment cannot be made by the host ID, assignment is made according to the specification of **Conditions for assigning asset information 1** in the Server Setup dialog box.

During registration or updating, the host ID is set in **Assignment key** for the Asset Information Manager Subset asset information.

(6) Assignment processing when the specification is Machines with only the same host ID

The Asset Information Manager Subset asset information with the matching host ID and **Assignment key** value is assigned.

(7) Assignment processing when the specification is Machines with the same MAC address

The assignment follows the following procedure:

1. The Asset Information Manager Subset asset information with the matching host ID and **Assignment key** value is assigned.
2. If there is no corresponding asset information, the Asset Information Manager Subset asset information with the matching MAC address is assigned.

(8) Assignment processing when the specification is According to the JP1/SD definition

The assignment follows the following procedure:

1. The Asset Information Manager Subset asset information with the matching host ID and **Assignment key** value is assigned.
2. The Asset Information Manager Subset asset information with the matching MAC address, IP address, and host name is assigned.
3. If the node ID is `host name working`, the Asset Information Manager Subset asset information with the matching MAC address and host name is assigned.
4. If the node ID is `IP address working`, the Asset Information Manager Subset asset information with the matching MAC address and IP address is assigned.
5. If there is no corresponding asset information in either step 3 or 4, the Asset Information Manager Subset asset information with the matching MAC address is assigned.

(9) If there is no assignment with the Conditions for assigning asset information 1 specification method

If there is no assignment with the **Conditions for assigning asset information 1** specification method (there was no asset information matching the host ID or MAC address), the specification of **Conditions for assigning asset information 2** is followed. If an assignment could not be made by the host ID, it might be that the device was different due to a replacement or due to re-installation of the OS.

(10) Assignment processing when the specification is Use IP address and host name

The assignment follows the following procedure:

1. The Asset Information Manager Subset asset information with the matching IP address and host name is assigned.
2. If the node ID is `host name working`, the Asset Information Manager Subset asset information with the matching host name is assigned.

   If the node ID is `IP address working`, the Asset Information Manager Subset asset information with the matching IP address is assigned.

(11) New registration of unassigned assets

If there is no corresponding asset information in Asset Information Manager Subset, whether or not assets are registered depends on the **Perform new registration of unassigned assets** setting in the Server Setup dialog box. If **New registration** is specified, the asset will be newly registered; if **Do not perform new registration** is specified, the asset will not be registered.

(12) Asset information assignment method by working key

The following table shows the assignment method when **Use working key** is specified for **Assign key for asset information** in the Server Setup dialog box and when the information used as assignment key is updated.

Table 10–6: Assignment method by JP1/Software Distribution's working key

Status in which inventory information is updated (information to be updated)	Host ID	No host ID	
		Host name	IP address
Changing IP address (IP address)	Assign by host ID.	Assign by MAC address and host name.	Assign by MAC address.
Changing host name (host name)	Assign by host ID.	Assign by MAC address.	Assign by MAC address and IP address.
Re-installing OS (host ID)	Assign by one of the following: • MAC address • MAC address, host name, and IP address • MAC address and host name • MAC address and IP address	Assign by MAC address and host name.	Assign by MAC address and IP address.
Replacing (host ID, MAC address)	Assign by one of the following:# • Host name and IP address • Host name • IP address	Assign by host name.	Assign by IP address.

#

This is the assignment method with **Conditions for assigning asset information 2** when **Use IP address and host name** is selected.

This explains the settings in the Server Setup dialog box using an example of replacing. Furthermore, if the **Assign Key for asset information** setting in the Server Setup dialog box is **Use working key**, the **Working key** must be set to **Use host ID**.

When replacing, the host ID and MAC address are different, so assets cannot be assigned by **Conditions for assigning asset information 1**. Therefore, assets are assigned according to the **Conditions for assigning asset information 2** setting.

After a replacement, specify as shown below depending on whether the device after the replacement is to be treated as a new device or as the same device as before the replacement.

When a replaced device is to be registered as a new asset

- With **Conditions for assigning asset information 2**, specify **Do not assign**.
- With **Perform new registration of unassigned assets**, specify **New registration**.

When a replaced device is to be assigned the same as the previous device

- With **Conditions for assigning asset information 2**, specify **Use IP address and Host name**.

If the host name or IP address matches that of the device before replacement, the information on the device before replacement can be assigned.

Notes

- If there is more than one corresponding asset, the information on the asset with the most recent registration date is updated.
- If a mobile network card, such as a PC card, is shared among multiple devices, use **Use host ID** with JP1/Software Distribution.
- If **Use host ID** is used with JP1/Software Distribution, re-installing the OS on the device causes a new **host ID** to be assigned. If this happens, assignment by the assignment key is no longer possible.

  In such a case, assignment conforms to **Conditions for assigning asset information 1** and **Conditions for assigning asset information 2**.
- The values of the MAC address, IP address, and host name of the hardware asset information are used in the assignment.
- If the status of the assigned asset information is **Scrap** (the device status code is 500-699), the information is not changed.

(13) How to define the assignment-exception MAC list

When specifying a MAC address for the key to assign inventory information to the asset information in Asset Information Manager Subset, if you wish to register multiple machines with the same MAC address to identify each machine in the database, create the assignment-exception MAC list (MacListOfOmitMatching.ini). For details on how to define the assignment-exception MAC list, see the description below.

- Location of the assignment-exception MAC list file

The "assignment-exception MAC list" file needs to be placed in the path "Installation folder of Asset Information Manager Subset\env". For reference, see the sample file "MacListOfOmitMatching.ini.org" located in that path. Create the assignment-exception MAC list file based on the sample file.

Note:

Asset Information Manager Subset checks the assignment-exception MAC list file in the above path when assigning the key to the information. If there is no assignment-exception MAC list file, Asset Information Manager Subset will assume that no MAC addresses are specified for exclusion.

- How to create an assignment-exception MAC list

```
; MAC Address List of Omit Matching.
[OMIT_MAC]
OMIT_MAC = 00:11:22:33:44:55
```

[OMIT_MAC]

Specify the MAC addresses you wish to register in the assignment- exception MAC list. Use the format "OMIT_MAC = MAC address" to specify the MAC addresses for exclusion.

Note the following when specifying MAC address to be excluded from assignment:

- Do not use abbreviations.
- Specify MAC addresses separated by colons ":".
- Specify MAC addresses by 17 single-byte characters. These are not case-sensitive.
- Even if the same MAC address is specified more than once, no error will occur.
- A maximum of 1,000 MAC addresses can be specified. However, if many comments, unnecessary key names, or values are entered, an error might occur even if 1,000 or fewer MAC addresses are specified.

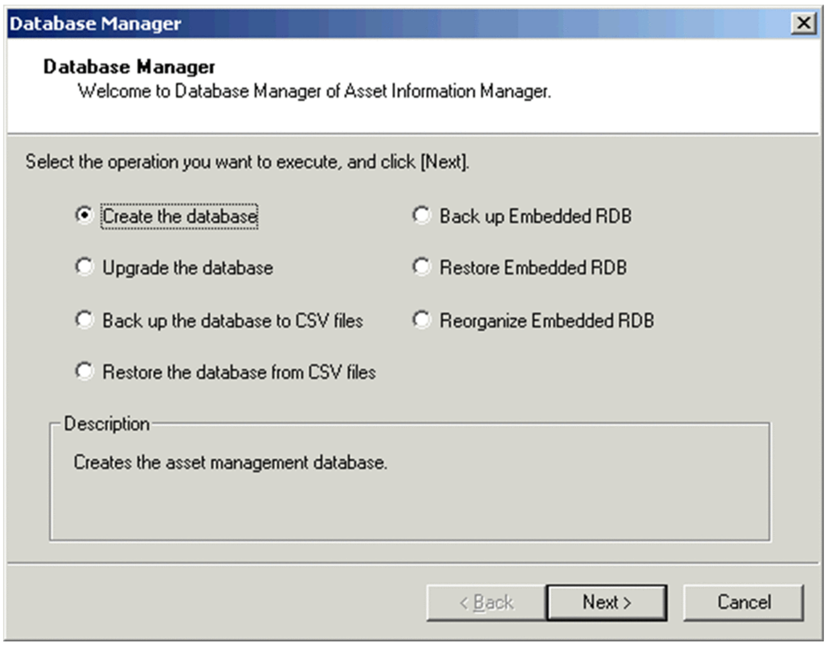
10.3 Setting up the Asset Information Manager Subset database

To create and maintain a database that is used with Asset Information Manager Subset, use Asset Information Manager Subset's *Database Manager*.

To start Asset Information Manager Subset's Database Manager:

1. From the **Start** menu, choose **Software Distribution Manager**, **Asset Information Manager**, and then **Setup**.
   The Setup dialog box for Asset Information Manager Subset is displayed.
2. Choose **Database Manager**.
   The Database Manager dialog box appears.

Figure 10–5: Database Manager dialog box



Database Manager

Database Manager
Welcome to Database Manager of Asset Information Manager.

Select the operation you want to execute, and click [Next].

● Create the database
○ Upgrade the database
○ Back up the database to CSV files
○ Restore the database from CSV files
○ Back up Embedded RDB
○ Restore Embedded RDB
○ Reorganize Embedded RDB

Description
Creates the asset management database.

If the type of database is Microsoft SQL Server or Oracle, the items **Back up Embedded RDB**, **Restore Embedded RDB**, and **Reorganize Embedded RDB** are not displayed.

Select the operation to be executed by Database Manager of Asset Information Manager Subset.

Create the database

Creates a new Asset Information Manager Subset database.

Upgrade the database

Upgrades the Asset Information Manager Subset database. Choose this item when you have upgraded the managing server.

The database upgrade processing is executed on a database that has already been created.

Back up the database to CSV files

Backs up the database by outputting information about the Asset Information Manager Subset database to a CSV file.

Choose this item when you perform a periodic database backup.

Restore the database from CSV files

Restores the Asset Information Manager Subset database from its CSV-format backup files.

Choose this item to restore the backup acquired by **Back up the database to CSV files**.

Back up Embedded RDB

Executes a backup of Asset Information Manager Subset database in an Embedded RDB environment.

Choose this item when you perform a periodic database backup.

This item is displayed when the database type is Embedded RDB.

Restore Embedded RDB

Restores the Asset Information Manager Subset database from the backup files acquired by **Back up Embedded RDB**.

This item is displayed when the database type is Embedded RDB.

Reorganize Embedded RDB

Reorganizes the Asset Information Manager Subset database in an Embedded RDB environment.

This item is displayed when the database type is Embedded RDB.

Note that the Microsoft SQL Server and Oracle databases created by Database Manager of Asset Information Manager Subset are not deleted when Asset Information Manager Subset is uninstalled. To delete the databases, use the RDBMS tools.

The following subsections describe each operation.

10.3.1 Creating a new database

Create a new Asset Information Manager Subset database using Database Manager of Asset Information Manager Subset.

The database creation procedure depends on the type of database. The following describes the procedure for each type of database.

(1) In Embedded RDB

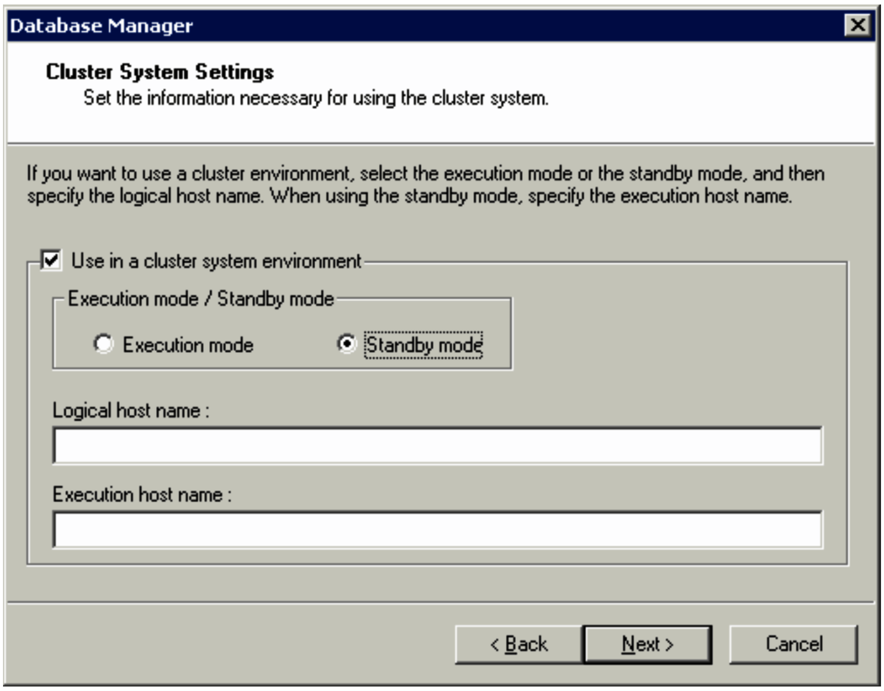
When Database Manager of Asset Information Manager Subset is used, the following processes are executed:

- Creating the service name (ODBC data source name) that was specified at the Asset Information Manager Subset server setup
- Creating a database
- Initializing the database

To create a new Asset Information Manager Subset database in an Embedded RDB environment:

1. In the Database Manager dialog box, choose **Create the database** and then click the **Next** button.
   The Cluster System Settings dialog box appears.
   In this dialog box, set the information required in order to use Asset Information Manager Subset in a cluster system. If you do not use a cluster system, click the **Next** button.

Figure 10–6: Cluster System Settings dialog box



Database Manager

Cluster System Settings

Set the information necessary for using the cluster system.

If you want to use a cluster environment, select the execution mode or the standby mode, and then specify the logical host name. When using the standby mode, specify the execution host name.

☑ Use in a cluster system environment

Execution mode / Standby mode

○ Execution mode ● Standby mode

Logical host name :

Execution host name :

Use in a cluster system environment

If you use Asset Information Manager Subset in a cluster system, select this check box. By default, this check box is not selected. Selecting this check box enables other items to be set.

Execution mode / Standby mode

Select **Execution mode** or **Standby mode** as the type of installation-target cluster node. The default is **Execution mode**.

Logical host name

Specify the name of the logical host created in the cluster system as 1 to 64 bytes of alphanumeric characters and the following symbols: `% - _`

Execution host name

If you have selected **Standby mode** in **Execution mode / Standby mode**, specify the name of the executing host in the cluster system as 1 to 64 bytes of alphanumeric characters and the following symbols:

`% - _`

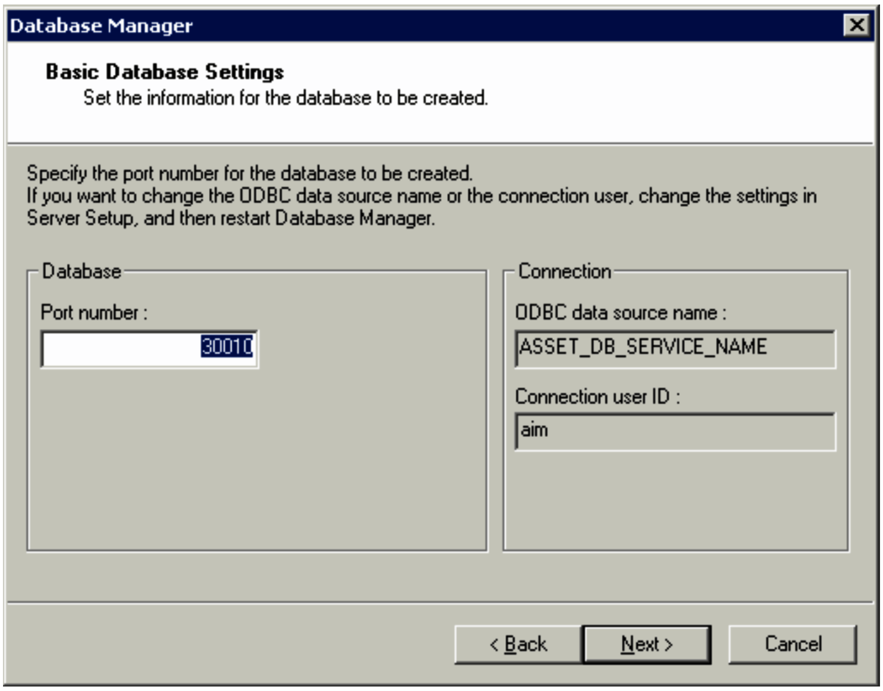
When **Execution mode** is selected in **Execution mode / Standby mode**, this item is disabled.

2. Set the items and then click the **Next** button.

   The Basic Database Settings dialog box appears.

   In this dialog box, set the connection information needed for creating the database that is used by Asset Information Manager Subset.

Figure 10–7: Basic Database Settings dialog box (for Embedded RDB)



Database Manager

Basic Database Settings

Set the information for the database to be created.

Specify the port number for the database to be created.
If you want to change the ODBC data source name or the connection user, change the settings in Server Setup, and then restart Database Manager.

Database

Port number : 30010

Connection

ODBC data source name : ASSET_DB_SERVICE_NAME

Connection user ID : aim

Port number

Specifies the port number used by Asset Information Manager Subset to connect to Embedded RDB. Specify a port number that is not in use. The permitted value is from 5001 to 65535. The default is `30010`.

ODBC data source name

Displays the ODBC data source name.

To change the ODBC data source name, change the **Service name** setting in **Database Information** in the Server Setup dialog box and then restart Database Manager of Asset Information Manager Subset.

Connection user ID

Displays the connection user ID used to log on to the Asset Information Manager Subset database.

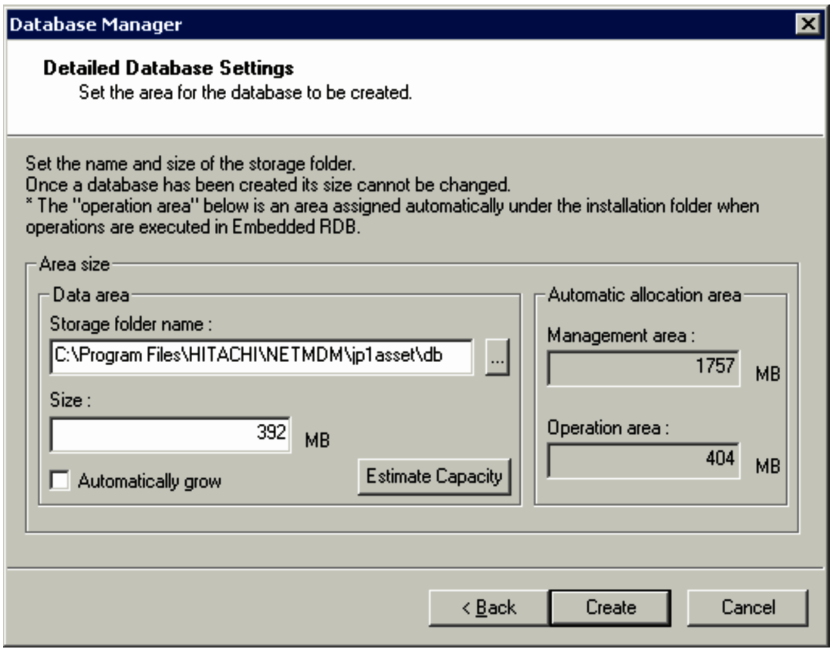
To change the connection user ID, change the **Login ID** setting in **Database Information** in the Server Setup dialog box, and then restart Database Manager of Asset Information Manager Subset.

3. Set the items and then click the **Next** button.

The Detailed Database Settings dialog box appears.

In this dialog box, set the information required in order to create a database that is used by Asset Information Manager Subset.

Figure 10–8: Detailed Database Settings dialog box (for Embedded RDB)



Database Manager

Detailed Database Settings

Set the area for the database to be created.

Set the name and size of the storage folder.
Once a database has been created its size cannot be changed.
* The "operation area" below is an area assigned automatically under the installation folder when operations are executed in Embedded RDB.

Area size

Data area

Storage folder name : C:\Program Files\HITACHI\NETMDM\jp1asset\db

Size : 392 MB

□ Automatically grow

Automatic allocation area

Management area : 1757 MB

Operation area : 404 MB

Storage folder name

Specifies the name of the storage folder for the database used by Asset Information Manager Subset. To change the default database storage folder name, click the `...` button and then specify a desired database storage directory. The default is *JP1/Software-Distribution-Manager-installation-folder*`\jp1asset\db`.

Specify the path of the database area as 1 to 125 bytes of alphanumeric characters, space, and the following symbols:

`_ \ : . ( )`

Size

Specifies the maximum size of the database used by Asset Information Manager Subset. The default is the estimate in the Estimate Capacity dialog box. Specify an integer value of `100` or more.

If the **Automatically grow** check box is selected, the database size is the initial value. Specify an integer between `100` and `65535`.

Note that the size of a created database cannot be changed. To change the size, you must delete the area and then re-create the database.

Estimate Capacity button

You can calculate an estimate of the Asset Information Manager Subset database capacity. The calculated estimate is then entered for **Size**. For more information on estimating database capacity, see *(4) Estimating the database capacity*.

Automatically grow

Select this check box if you want the size of the Asset Information Manager Subset database to be increased automatically. The default is that this check box is cleared. When this check box is selected, the database size can expand automatically to a maximum of 65,535 MB.

Management area

Displays the size required for the Asset Information Manager Subset database management area.

For the management area, the value set in **Size** is automatically assigned and then automatically created under **Storage folder name**.

Operation area

Displays the size required for Embedded RDB operation.

For the operation area, the value required for Embedded RDB operation is automatically assigned and then automatically created under *JP1/Software-Distribution-Manager-installation-folder*`\jp1asset`.

4. Set the items and then click the **Create** button.

The Asset Information Manager Subset database is created.

To change the size of Embedded RDB, if necessary, first back up the database to CSV-format files, and then re-create the database.

(2) In Microsoft SQL Server

When Database Manager of Asset Information Manager Subset is used, the following processes are executed:

- Creating the service name (ODBC data source name) specified during the Asset Information Manager Subset server setup
- Creating a database
- Creating a user for database access
- Initializing the database

Note

When the Asset Information Manager Subset database is created from the Database Manager dialog box, it is created using the collating sequence set during a custom installation of Microsoft SQL Server (or during a standard installation of Microsoft SQL Server 2008 and Microsoft SQL Server 2005).

Therefore, if you want to change the collating sequence to one other than the one set during installation, you will need to create the database manually.

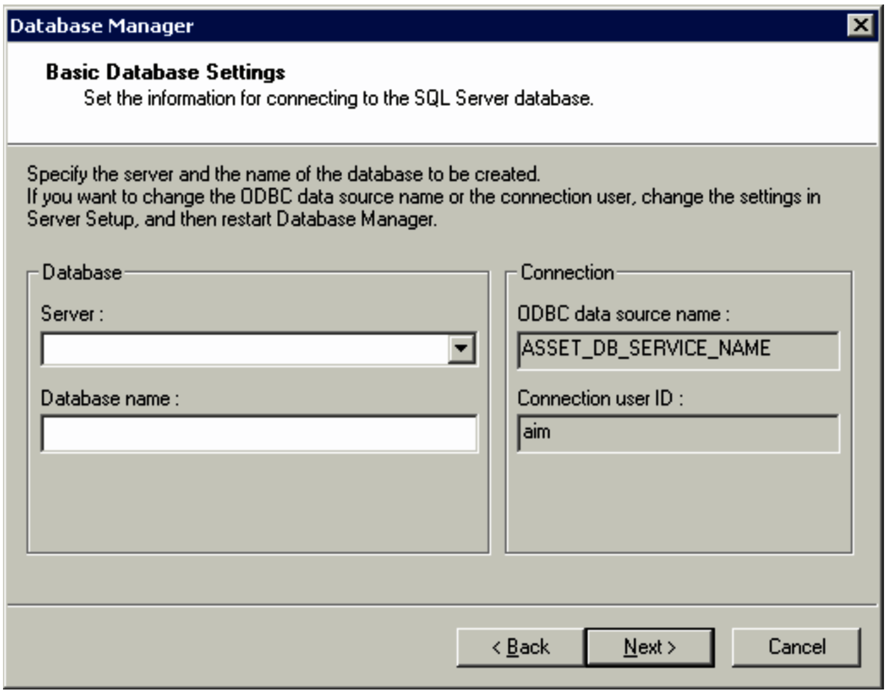
To create a new Asset Information Manager Subset database in a Microsoft SQL Server environment:

1. In the Database Manager dialog box, choose **Create the database** and then click the **Next** button.

   The Basic Database Settings dialog box appears.

   In this dialog box, set the connection information needed for creating the database that is used by Asset Information Manager Subset.

   Figure 10–9: Basic Database Settings dialog box (for Microsoft SQL Server)



Database Manager

Basic Database Settings

Set the information for connecting to the SQL Server database.

Specify the server and the name of the database to be created.
If you want to change the ODBC data source name or the connection user, change the settings in Server Setup, and then restart Database Manager.

Database

Server :

Database name :

Connection

ODBC data source name : ASSET_DB_SERVICE_NAME

Connection user ID : aim

Server

Specifies the server name and IP address of the database that is used by Asset Information Manager Subset. There is no default.

The permitted value is 1 to 63 bytes of characters and the following symbols:

`% ~ - _ . / \`

Database name

Specifies the name of the database used by Asset Information Manager Subset. There is no default.

The permitted value is 1 to 128 bytes of alphanumeric characters and symbols, except the following symbols and the space:

`\ / * " ' | . < > ?`

ODBC data source name

Displays the ODBC data source name.

To change the ODBC data source name, change the **Service name** setting under **Database Information** in the Server Setup dialog box and then restart Database Manager of Asset Information Manager Subset.

Connection user ID

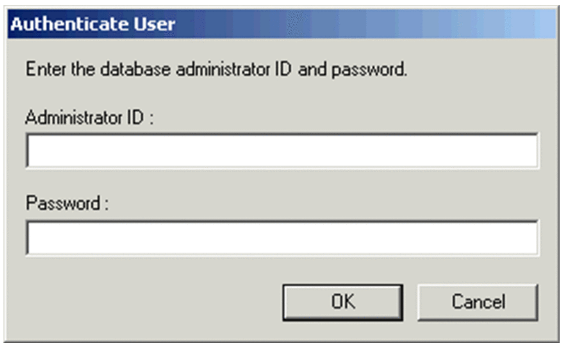
Displays the connection user ID used to log on to the Asset Information Manager Subset database.

To change the connection user ID, change the **Login ID** setting in **Database Information** in the Server Setup dialog box, and then restart Database Manager of Asset Information Manager Subset.

2. Set the items and then click the **Next** button.

   The Authenticate User dialog box appears.

   Figure 10–10: Authenticate User dialog box (for Microsoft SQL Server)



Authenticate User

Enter the database administrator ID and password.

Administrator ID :

Password :

Administrator ID

Specifies the administrator ID of the Asset Information Manager Subset database.

There is no default. The permitted value is 1 to 30 bytes of alphanumeric characters and symbols except \.

Password

Specifies the password for the administrator ID for the Asset Information Manager Subset database.

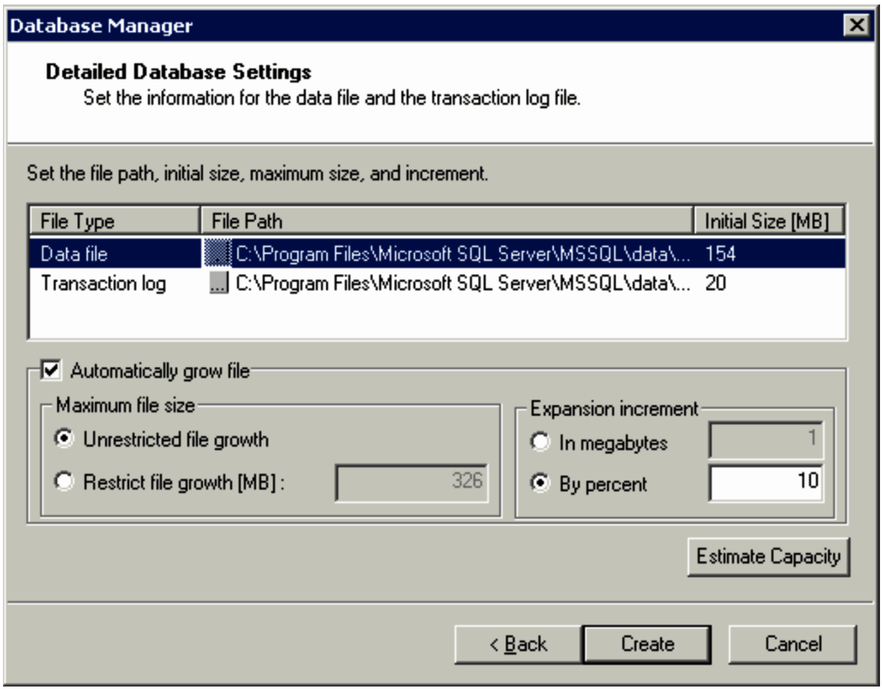
There is no default. The permitted value is 1 to 30 bytes of alphanumeric characters and symbols.

3. Specify the administrator ID and password and then click the **OK** button.

   The Detailed Database Settings dialog box appears.

   In this step, set information about the data file and transaction log file that are required in order to create the database used by Asset Information Manager Subset.

Figure 10–11: Detailed Database Settings dialog box (for Microsoft SQL Server)



Database Manager

Detailed Database Settings

Set the information for the data file and the transaction log file.

Set the file path, initial size, maximum size, and increment.

File Type	File Path	Initial Size [MB]
Data file	C:\Program Files\Microsoft SQL Server\MSSQL\data\...	154
Transaction log	C:\Program Files\Microsoft SQL Server\MSSQL\data\...	20

☑ Automatically grow file

Maximum file size

● Unrestricted file growth

○ Restrict file growth [MB] : 326

Expansion increment

○ In megabytes 1

● By percent 10

File Type

Displays **Data file** and **Transaction log**.

File Path

Specifies the absolute path of the data file and transaction log file. To change the default file path, click the `...` button and then specify a desired file path. Specify the file path as 1 to 255 bytes of alphanumeric characters and space. The following symbols are not permitted:

`" | * < > ? & ^ /`

By default, the path of the data file and transaction log file in the data file storage folder for the connection-target `master` database is specified. The data file name is `AIMDB.mdf` and the transaction log file name is `AIMDB.ldf`.

Initial Size

Specifies the initial size of the data file and transaction log file in megabytes. By default, the value set by the capacity estimation is set for the data file and a value of 20 megabytes is set for the transaction log file.

Automatically grow file

To extend the sizes of data file and transaction log file, select a file type from the area list and then select this check box. By default, this check box is selected. Selecting this check box enables other items to be set.

Maximum file size

Selects one of the following as the maximum file size:

- **Unrestricted file growth**
- **Restrict file growth**

The default is **Unrestricted file growth**.

If you select **Restrict file growth**, specify the maximum file size in megabytes. The default is `1`.

Expansion increment

Selects the unit for expanding file size and then specifies the increment. The default is **By percent** with a value of 10%.

- **In megabytes**

Sets the increment in megabytes. In the input area, specify an integer that is 1 or greater.

- **By percent**

Sets the increment by percent. Specify an integer in the range from 1 to 100. The default value for **By percent** is `10`.

Estimate Capacity button

Enables an estimate of the capacity of the Asset Information Manager Subset database to be obtained. For details about the capacity estimation, see *(4) Estimating the database capacity*.

4. Set the items and then click the **Create** button.

   The Asset Information Manager Subset database is created.

(3) In Oracle

When Database Manager of Asset Information Manager Subset is used, the following processes are executed:

- Creating the service name (net service name) that was specified at the Asset Information Manager Subset server setup
- Creating a database
- Creating a user for database access
- Initializing the database

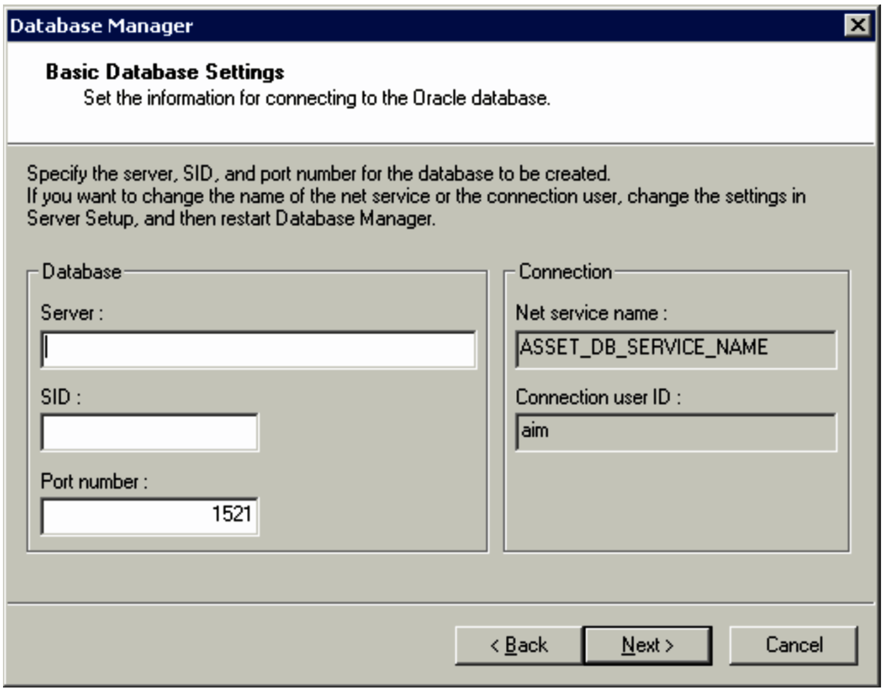
To create a new Asset Information Manager Subset database in an Oracle environment:

1. In the Database Manager dialog box, choose **Create the database** and then click the **Next** button.

   The Basic Database Settings dialog box appears.

   In this dialog box, set the connection information needed for creating the database that is used by Asset Information Manager Subset.

Figure 10–12: Basic Database Settings dialog box (for Oracle)



Database Manager

Basic Database Settings

Set the information for connecting to the Oracle database.

Specify the server, SID, and port number for the database to be created.
If you want to change the name of the net service or the connection user, change the settings in Server Setup, and then restart Database Manager.

Database

Server :

SID :

Port number : 1521

Connection

Net service name : ASSET_DB_SERVICE_NAME

Connection user ID : aim

Server

Specifies the server name and IP address of the database that is used by Asset Information Manager Subset. There is no default.

The permitted value is 1 to 63 bytes of characters and the following symbols:

`% ~ - _ . / \`

SID

In Oracle 8i, this item specifies the SID of the database to be connected. In Oracle 9i, specify the service name of the database to be connected. There is no default.

The permitted value is 1 to 8 bytes of alphanumeric characters.

Port number

Specifies the port number used by Asset Information Manager Subset to connect to Oracle. The permitted value is from 1 to 65535. The default is `1521`.

Net service name

Displays the net service name.

To change the net service name, in the Server Setup dialog box, change the **Service name** setting in **Database Information** and then restart Database Manager of Asset Information Manager Subset.

Connection user ID

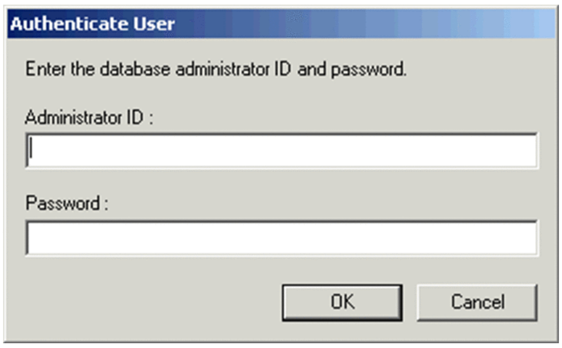
Displays the connection user ID used to log on to the Asset Information Manager Subset database.

To change the connection user ID, change the **Login ID** setting in **Database Information** in the Server Setup dialog box, and then restart Database Manager of Asset Information Manager Subset.

2. Set the items and then click the **Next** button.

The Authenticate User dialog box appears

Figure 10–13: Authenticate User dialog box (for Oracle)



Authenticate User

Enter the database administrator ID and password.

Administrator ID :

Password :

Administrator ID

Specifies the administrator ID of the Asset Information Manager Subset database.

There is no default. The permitted value is 1 to 30 bytes of alphanumeric characters and symbols except \.

Password

Specifies the password for the administrator ID for the Asset Information Manager Subset database.

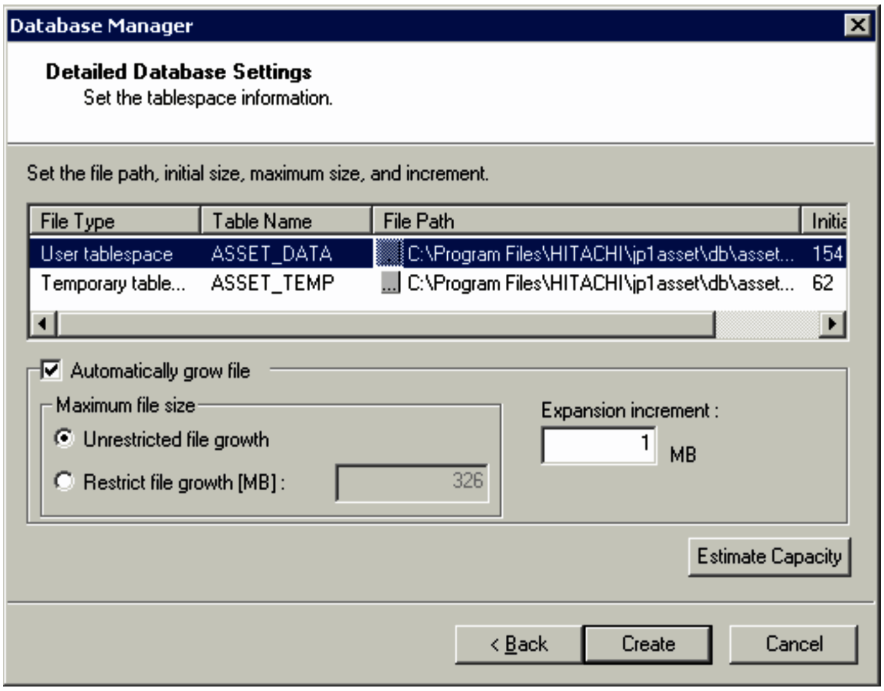
There is no default. The permitted value is 1 to 30 bytes of alphanumeric characters and symbols.

3. Specify the administrator ID and password and then click the **OK** button.

The Detailed Database Settings dialog box appears.

In this step, set information about the tablespace that is required in order to create the database used by Asset Information Manager Subset.

Figure 10–14: Detailed Database Settings dialog box (for Oracle)



Database Manager

Detailed Database Settings

Set the tablespace information.

Set the file path, initial size, maximum size, and increment.

File Type	Table Name	File Path	Initia
User tablespace	ASSET_DATA	C:\Program Files\HITACHI\jp1asset\db\asset...	154
Temporary table...	ASSET_TEMP	C:\Program Files\HITACHI\jp1asset\db\asset...	62

☑ Automatically grow file

Maximum file size

● Unrestricted file growth

○ Restrict file growth [MB] : 326

Expansion increment : 1 MB

File Type

Displays **User tablespace** and **Temporary tablespace**.

Table Name

Specifies a name for the Asset Information Manager Subset database area (1 to 30 bytes of characters). Note that the double-quotation mark (") cannot be used. Specify the table name according to the schema and object naming rules provided in the Oracle SQL reference materials.

File Path

Specifies the absolute path of the user tablespace and temporary tablespace. To change the default file path, click the `...` button and then specify a desired file path. Specify the file path as 1 to 255 bytes of alphanumeric characters and space. The following symbols are not permitted:

`" | * < > ? & ^ /`

By default, *JP1/Software-Distribution-Manager-installation-folder*`\jp1asset\db\asset_db.dbf` is specified as the user tablespace and *JP1/Software-Distribution-Manager-installation-folder*`\jp1asset\db\asset_temp.dbf` as the temporary tablespace.

Initial Size

Specifies the initial size of the user tablespace and temporary tablespace in megabytes. Specify an integer that is 1 or greater. By default, the value set by the capacity estimation is specified.

Automatically grow file

To extend the sizes of user tablespace and temporary tablespace, select a file type from the area list and then select this check box. By default, this check box is selected. Selecting this check box enables other items to be set.

Maximum file size

Selects one of the following as the maximum file size:

- **Unrestricted file growth**
- **Restrict file growth**

The default is **Unrestricted file growth**.

If you select **Restrict file growth**, specify the maximum file size in megabytes. The default is `1`.

Expansion increment

Specifies the expansion increment for file size in megabytes. Specify an integer that is 1 or greater. The default is `1`.

Estimate Capacity button

Enables an estimate of the capacity of the Asset Information Manager Subset database to be obtained. For details about the capacity estimation, see *(4) Estimating the database capacity*.

4. Set the items and then click the **Create** button.

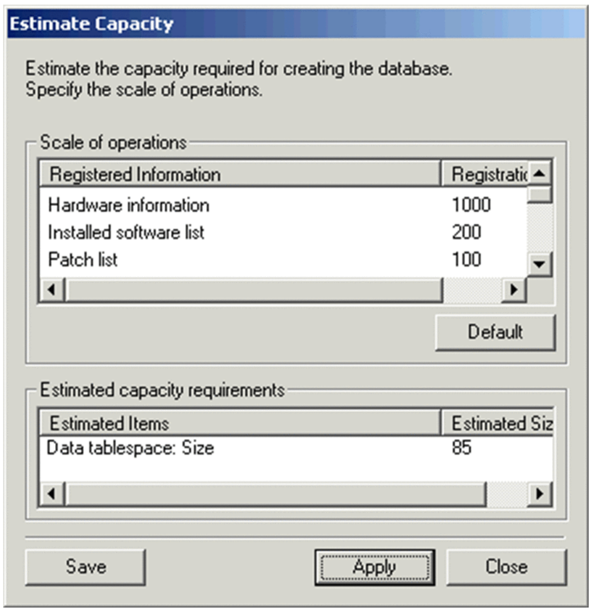
   The Asset Information Manager Subset database is created.

(4) Estimating the database capacity

In the Detailed Database Settings dialog box of the Asset Information Manager Subset database manager, clicking the **Estimate Capacity** button displays the Estimate Capacity dialog box.

In this dialog box, set the information that is required in order to estimate the capacity of the Asset Information Manager Subset database.

Figure 10–15: Estimate Capacity dialog box



Estimate Capacity

Estimate the capacity required for creating the database.
Specify the scale of operations.

Scale of operations

Registered Information	Registratic
Hardware information	1000
Installed software list	200
Patch list	100

Estimated capacity requirements

Estimated Items	Estimated Siz
Data tablespace: Size	85

Scale of operations

Specifies the number of items registered for each information type that is used.

Estimated capacity requirements

Displays the estimated capacity of the Asset Information Manager Subset database.

Default button

Resets each registration count for scale of operations to the default value.

Save button

Saves the registration count specified in **Scale of operations** to a text file.

Apply button

Applies the estimated value to the dialog box used to set the Asset Information Manager Subset database area.

10.3.2 Upgrading the database

Upgrade the Asset Information Manager Subset database. Choose this item when you have upgraded the managing server.

Notes

- Before upgrading the Asset Information Manager Subset database, back up the database.

- When Asset Information Manager Subset is upgraded, the contents of the database are stored in the work folder. Therefore, specify a folder on the drive that has sufficient free space.
- Before you upgrade the Asset Information Manager Subset database, stop the services in the following order.

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before upgrading the database.

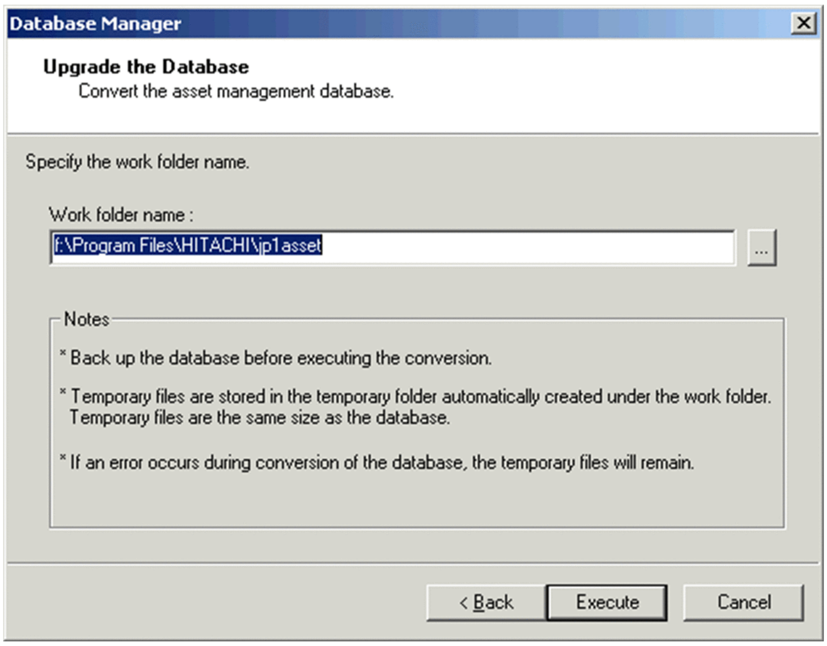
To upgrade the Asset Information Manager Subset database:

1. In the Database Manager dialog box, choose **Upgrade the database** and then click the **Next** button.

   The Upgrade the Database dialog box appears.

   In this dialog box, specify the work folder name information that is required in order to upgrade the Asset Information Manager Subset database.

   Figure 10–16: Upgrade the Database dialog box



Specify the work folder name.

Work folder name : f:\Program Files\HITACHI\jp1asset

Notes

* Back up the database before executing the conversion.

* Temporary files are stored in the temporary folder automatically created under the work folder. Temporary files are the same size as the database.

* If an error occurs during conversion of the database, the temporary files will remain.

   Work folder name

   Specifies the absolute path of the work folder used to update the Asset Information Manager Subset database.

   The default is *JP1/Software-Distribution-Manager-installation-folder*`\jp1asset`. To change the default file path, click the `...` button and then specify a desired file path.

   To directly specify the file path, express it as 1 to 255 bytes of alphanumeric characters and space. The following symbols are not permitted:

   `/ * ? " < > |`

2. Set the work folder name and then click the **Execute** button.

   The Asset Information Manager Subset database is upgraded.

   When upgrade processing is completed, the temporary file used during upgrading is automatically deleted.

10.3.3 Backing up the database as CSV files

There are two ways to back up the Asset Information Manager Subset database as CSV files. One is by using Database Manager of Asset Information Manager Subset, and the other is by using `jamdbexport.bat`.

We recommend that you periodically back up the database so that the database can be recovered in the event of a database failure.

A backup can be used not only for error recovery but also for the following purposes:

- When you upgrade the OS or replace your PC, you can migrate the database by restoring the backup file using Database Manager of Asset Information Manager Subset.
- In the case of an Embedded RDB, to expand the database capacity, use Database Manager of Asset Information Manager Subset to re-create the database and then restore the backup file.

Notes

- Before you back up the Asset Information Manager Subset database, stop the services in the following order:

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from which they were stopped.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before backing up the database.

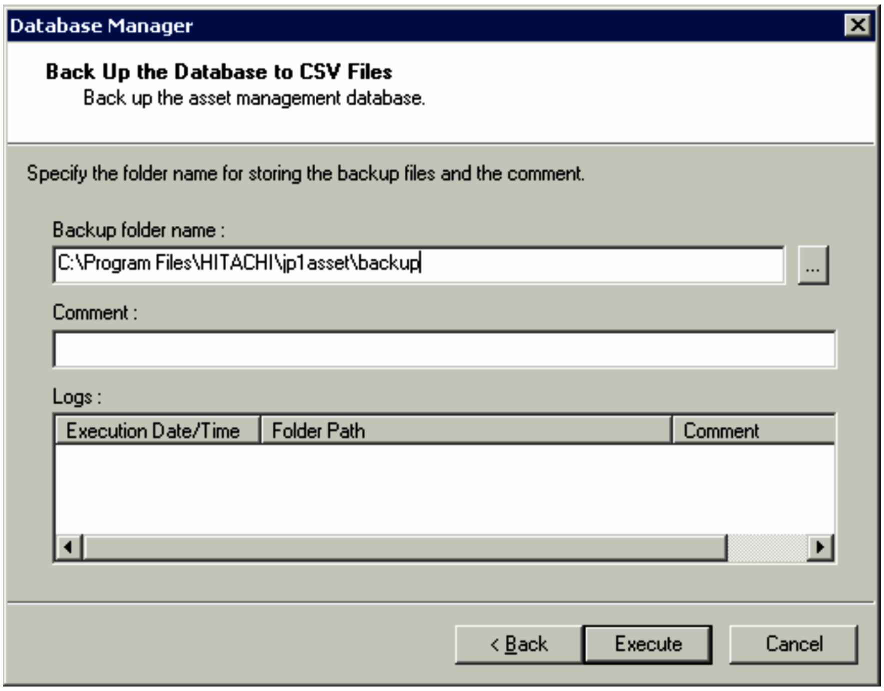
The following describes how to back up the Asset Information Manager Subset database as CSV files.

(1) How to back up the database as CSV files

To back up the Asset Information Manager Subset database as CSV files:

1. In the Database Manager dialog box, choose **Back up the database to CSV files** and then click the **Next** button.
   The Back Up the Database to CSV Files dialog box appears.
   In this dialog box, specify information, such as the folder name for storing backup files and a comment, when the Asset Information Manager Subset database is backed up.

Figure 10–17: Back Up the Database to CSV Files dialog box



Database Manager

Back Up the Database to CSV Files

Back up the asset management database.

Specify the folder name for storing the backup files and the comment.

Backup folder name : C:\Program Files\HITACHI\jp1asset\backup

Comment :

Logs :

Execution Date/Time	Folder Path	Comment

Backup folder name

Specify the absolute path name of the folder that stores the backup files of the Asset Information Manager Subset database.

The default is *JP1/Software-Distribution-Manager-installation-folder*`\jp1asset\backup`. To change the default folder path, click the `...` button and then specify a desired folder path.

To directly specify a folder path, express it as 1 to 223 bytes of alphanumeric characters and space. The following symbols are not permitted:

`" | * < > ? & ^ /`

Comment

Specifies a comment as backup log information.

This item is optional. There is no default. The permitted value is 1 to 64 bytes of characters.

Logs

Displays a maximum of 10 entries of backup log information in chronological order.

Selecting an item in the log list applies the information to **Backup folder name** and **Comment**.

2. Set the items and then click the **Execute** button.

   The Asset Information Manager Subset database is backed up and backup CSV files are created.

(2) Using the command to back up the database as CSV files

This subsection describes the function, format, options, and command execution notes of `jamdbexport.bat`, which executes from the command line at the Asset Information Manager Subset server the same backup as does the method using the Database Manager dialog box.

`jamdbexport.bat` is stored in the following folder:

Asset-Information-Manager-Subset-installation-folder`\exe`

(a) Function

`jamdbexport.bat` makes a backup of the Asset Information Manager Subset database and outputs all data to CSV files. When `jamdbexport.bat` is executed, the contents of the Asset Information Manager Subset database are stored in the backup folder.

(b) Format

```
jamdbexport.bat backup-folder-path [-rp]
```

(c) Options

backup-folder-path

Specifies the full path of the backup folder. Allocate sufficient free space to the drive that is specified for the backup folder. When you specify a path, note the following:

- Do not include any spaces in a folder name.
- Do not enclose the folder name in double-quotation marks (`"`).
- Do not specify an existing folder name.

If the path is omitted, *Asset-Information-Manager-Subset-installation-folder*`\backup` is set.

`-rp`

Specifies that backup processing is to start without waiting for a response from the keyboard.

When this option is omitted, command execution waits for entry of a response from the keyboard. You can cancel execution by pressing the **Ctrl** + **C** keys.

(d) Notes about command execution

- If you specify the `-rp` option, the command prompt closes when processing terminates, making it impossible to determine whether or not an error occurred.
- Do not change the name or contents of the CSV files acquired by `jamdbexport.bat`. If such a change is made, the Asset Information Manager Subset database can no longer be restored.

10.3.4 Restoring the CSV database files

Restore the database using the CSV backup files of the Asset Information Manager Subset database.

When you upgrade the OS or replace your PC, you can also migrate the Asset Information Manager Subset database.

Restoring the CSV-format database files involves the following processing:

- Initializing the database
- Restoring the backup data (database)

Notes

- Before you start restore processing, make sure that the Asset Information Manager Subset database has been created. If no Asset Information Manager Subset database has been created, use the Database Manager dialog box to create a new Asset Information Manager Subset database and then execute the restore processing.
- Before you restore an Asset Information Manager Subset database, stop the services in the following order:

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from which they were stopped.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before restoring the database.

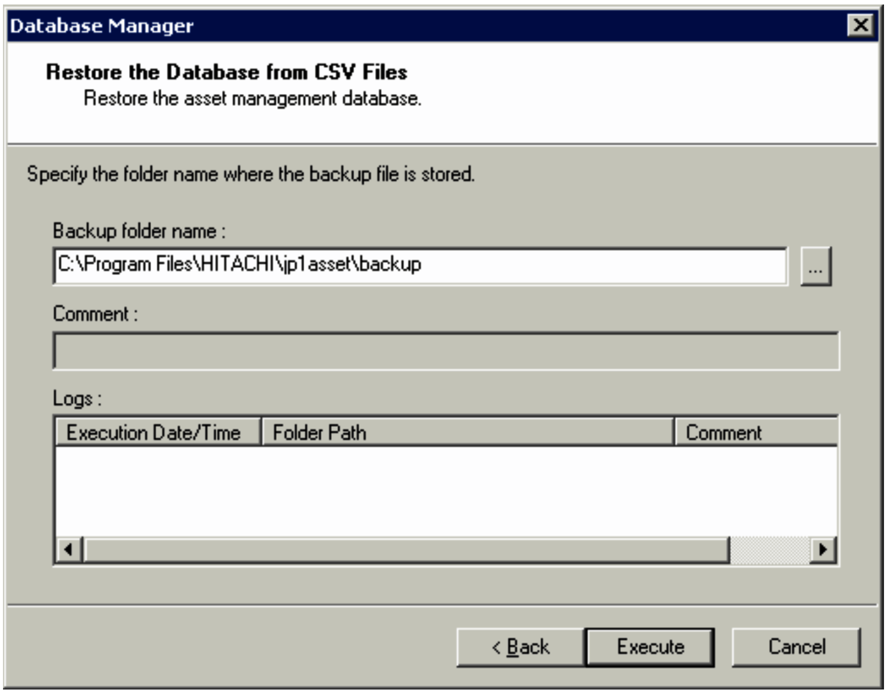
To restore the Asset Information Manager Subset database:

1. In the Database Manager dialog box, choose **Restore the database from CSV files** and then click the **Next** button.

   The Restore the Database from CSV Files dialog box appears.

In this dialog box, specify information such as the name of the folder containing the backup files of the Asset Information Manager Subset database.

Figure 10–18: Restore the Database from CSV Files dialog box



Database Manager

Restore the Database from CSV Files

Restore the asset management database.

Specify the folder name where the backup file is stored.

Backup folder name : C:\Program Files\HITACHI\jp1asset\backup

Comment :

Logs :

Execution Date/Time	Folder Path	Comment

Backup folder name

Specifies the absolute path name of the folder that stores the backup files of the Asset Information Manager Subset database.

The default is *JP1/Software-Distribution-Manager-installation-folder*`\jp1asset\backup`. To change the default folder path, click the `...` button and then specify a desired folder path.

To directly specify a folder path, express it as 1 to 255 bytes of alphanumeric characters and space. The following symbols are not permitted:

`/ * ? " < > | & ^`

Comment

Displays the comment that was specified as log information during backup processing.

Logs

Displays a maximum of 10 entries of backup log information in chronological order.

Selecting an item in the log list applies the information to **Backup folder name** and **Comment**.

2. Set the items and then click the **Execute** button.

   The backup files are restored and the Asset Information Manager Subset database is recovered.

10.3.5 Backing up the database in an Embedded RDB environment

There are two ways to back up the Asset Information Manager Subset database in an Embedded RDB environment. One is by using Database Manager of Asset Information Manager Subset, and the other is by using `jamemb_backup.bat`.

We recommend that you periodically back up the database so that the database can be recovered in the event of a database failure.

Notes

- Before you back up the Asset Information Manager Subset database, stop the services in the following order:

  1. World Wide Web Publishing Service or World Wide Web Publishing

2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from which they were stopped.

- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before backing up the database.

The following describes how to back up the Asset Information Manager Subset database in an Embedded RDB environment.

(1) How to back up the database in an Embedded RDB environment

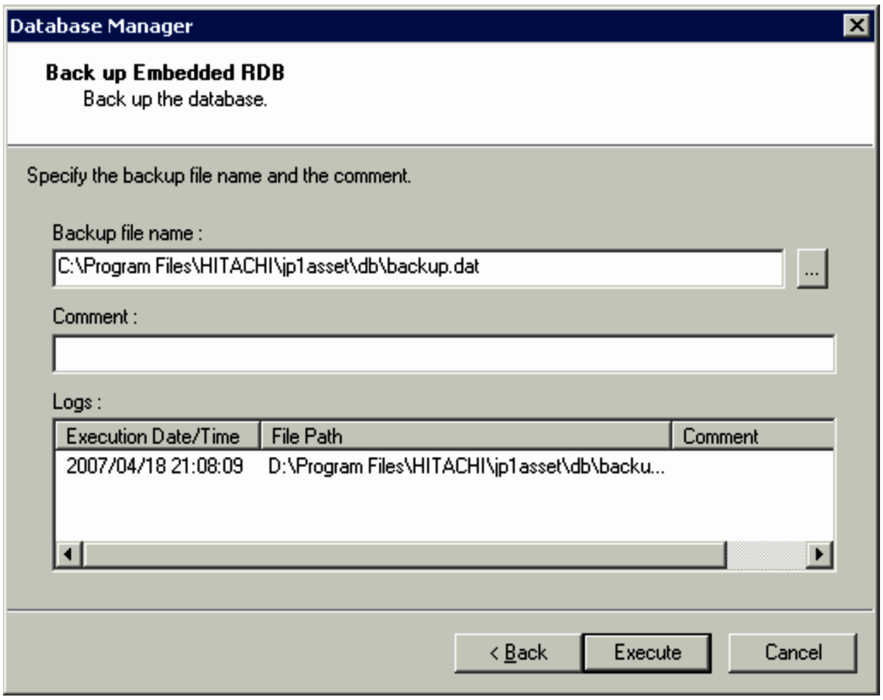
To back up the Asset Information Manager Subset database in an Embedded RDB environment:

1. In the Database Manager dialog box, choose **Back up Embedded RDB** and the click the **Next** button.

   The Back up Embedded RDB dialog box appears.

   In this dialog box, specify information, such as the backup file name and comment, for the Asset Information Manager Subset database.

   Figure 10–19: Back up Embedded RDB dialog box



Database Manager

Back up Embedded RDB

Back up the database.

Specify the backup file name and the comment.

Backup file name : C:\Program Files\HITACHI\jp1asset\db\backup.dat

Comment :

Logs :

Execution Date/Time	File Path	Comment
2007/04/18 21:08:09	D:\Program Files\HITACHI\jp1asset\db\backu...	

Backup file name

Specifies the absolute path name of the backup files of the Asset Information Manager Subset database.

The default is *JP1/Software-Distribution-Manager-installation-folder*`\jp1asset\db\backup.dat`. To change the default file path, click the `...` button and then specify a desired file path.

To directly specify the file path, express it as 1 to 255 bytes of alphanumeric characters and space. The following symbols are not permitted:

`" | * < > ? & ^ /`

Comment

Specifies a comment as backup log information.

This item is optional. There is no default setting. The permitted value is 1 to 64 bytes of characters.

Logs

Displays a maximum of 10 entries of backup log information in chronological order.

Selecting an item in the log list applies the information to **Backup file name** and **Comment**.

2. Set the items and then click the **Execute** button.

   The Asset Information Manager Subset database is backed up and the backup files are created.

Note

To restore the backup files created here, the environment must be the same as when the Asset Information Manager Subset database was created (such as the port number and database storage).

If you want to change the environment used to create the Asset Information Manager Subset database and restore the backup files, use **Back up the database to CSV files** to make a backup. For details about how to back up data using **Back up the database to CSV files**, see *10.3.3 Backing up the database as CSV files*.

(2) Using the command to back up the database in an Embedded RDB environment

This subsection describes the function, format, options, return values, and command execution notes of `jamemb_backup.bat`, which makes a backup of the Asset Information Manager Subset database in an Embedded RDB environment. Note that `jamemb_backup.bat` is applicable only to Embedded RDB.

`jamemb_backup.bat` is stored in the following folder:

Asset-Information-Manager-Subset-installation-folder`\exe`

(a) Function

`jamemb_backup.bat` backs up the Asset Information Manager Subset database.

(b) Format

```
jamemb_backup.bat -b backup-file-path -o result-file-path [-y]
```

(c) Options

`-b` *backup-file-path*

Specifies the full path of the file to which the backup is to be made. Specification of this option is mandatory.

`-o` *result-file-path*

Specifies the full path of the file to which the execution results are to be output. Specification of this option is mandatory.

`-y`

Specifies that backup processing is to start without waiting for a response from the keyboard.

When this option is omitted, command execution waits for entry of a response from the keyboard. You can cancel execution by pressing the **Ctrl** + **C** keys.

(d) Return value

Returns one of the following return values:

Return value	Description
`0`	Normal termination. You can check the results files for the backup details.
`11`	Invalid option specification.
`101` or greater	Terminated with another error.

(e) Notes about command execution

Execute `jamemb_backup.bat` as a user with administrator permissions.

(f) Execution example

```
jamemb_backup.bat -b C:\temp\backup\Backup.dat -o C:\temp\backup\kekka.log -y
```

10.3.6 Restoring the database in an Embedded RDB environment

In an Embedded RDB environment, you use the Database Manager of Asset Information Manager Subset to restore an Asset Information Manager Subset database that was created.

Notes

- Before you restore the Asset Information Manager Subset database, stop the services in the following order.

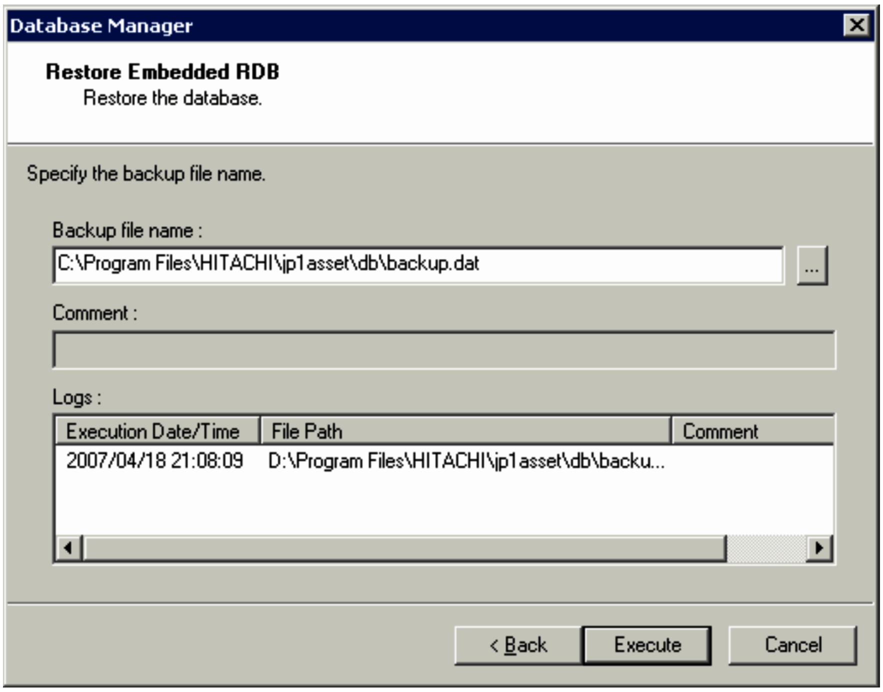
  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before restoring the database.

To restore the Asset Information Manager Subset database:

1. In the Database Manager dialog box, choose **Restore Embedded RDB** and then click the **Next** button.
   The Restore Embedded RDB dialog box appears.
   In this dialog box, specify the name of the Asset Information Manager Subset database backup file.

   Figure 10–20: Restore Embedded RDB dialog box



Backup file name: C:\Program Files\HITACHI\jp1asset\db\backup.dat

Execution Date/Time	File Path	Comment
2007/04/18 21:08:09	D:\Program Files\HITACHI\jp1asset\db\backu...	

Backup file name

Specifies the absolute path name for the backup file that was specified when the Asset Information Manager Subset database was backed up.

The default is *JP1/Software-Distribution-Manager-installation-folder*`\jp1asset\db\backup.dat`. To change the default file path, click the `...` button and then specify a desired file path.

Note that if the storage location of the backup file that was specified when the Asset Information Manager Subset database was backed up has changed, the Asset Information Manager Subset database cannot be restored. Change the backup file storage to the initial location and then specify **Backup file name**.

Comment

Displays the comment that was specified as log information during backup processing.

Logs

Displays a maximum of 10 entries of backup log information in chronological order.

Selecting an item in the log list applies the information to **Backup file name** and **Comment**.

2. Set the items and then click the **Execute** button.

   The backup files are restored and the Asset Information Manager Subset database is recovered.

10.3.7 Reorganizing the database in an Embedded RDB environment

Reorganizing the database is a maintenance task performed as part of regular operations. For more information about when to reorganized the database, see *5.2.3(2) Reorganizing the database* in the manual *Administrator's Guide Volume 2*.

Notes

- Before you reorganize the Asset Information Manager Subset database, stop the services in the following order.

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before reorganizing the database.
- If database capacity is still insufficient after reorganizing the Asset Information Manager Subset database, expand the database capacity.

There are two ways to reorganize the Asset Information Manager Subset database in an Embedded RDB environment. One is by using Database Manager of Asset Information Manager Subset, and the other is by using `jamemb_reorganization.bat`.

The following subsections explain these methods.

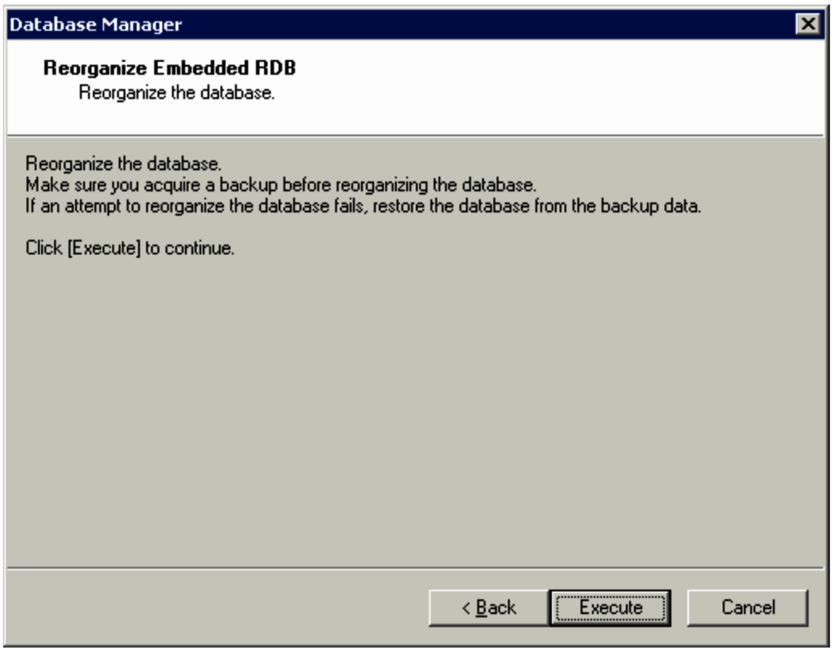
(1) How to reorganize the database in an Embedded RDB environment

To reorganize the Asset Information Manager Subset database in an Embedded RDB environment:

1. In the Database Manager dialog box, choose **Reorganize Embedded RDB** and then click the **Next** button.

   The Reorganize Embedded RDB dialog box appears.

Figure 10–21: Reorganize Embedded RDB dialog box



Database Manager

Reorganize Embedded RDB
Reorganize the database.

Reorganize the database.
Make sure you acquire a backup before reorganizing the database.
If an attempt to reorganize the database fails, restore the database from the backup data.

Click [Execute] to continue.

2. Click the **Execute** button.

   The Asset Information Manager Subset database is reorganized.

(2) Using the command to reorganize the database in an Embedded RDB environment

This subsection describes the function, format, options, return values, and command execution notes of `jamemb_reorganization.bat`, which reorganizes the Asset Information Manager Subset database in an Embedded RDB environment.

`jamemb_reorganization.bat` is stored in the following folder:

Asset-Information-Manager-Subset-installation-folder`\exe`

If reorganization fails, the Asset Information Manager Subset database can no longer be used. In such a case, you must restore the backup data and recover the Asset Information Manager Subset database.

(a) Function

`jamemb_reorganization.bat` reorganizes the Asset Information Manager Subset database.

(b) Format

```
jamemb_reorganization.bat port-number user-ID password -o result-file-path [-y]
```

(c) Options

port-number

Specifies the database connection port number that was specified when Asset Information Manager Subset was installed. To determine the port number that was set, check `PDNAMEPORT` in the `HiRDB.ini` file, which is stored in *Asset-Information-Manager-Subset-installation-folder*`\aimdb\conf\emb`. Specification of this option is mandatory.

user-ID, *password*

Specifies the values that were set in **Login ID** in **Database Information** in the Server Setup dialog box. Specification of this option is mandatory.

`-o` *result-file-path*

Specifies the full path of the files to which the execution results are to be output. Specification of this option is mandatory.

`-y`

Specifies that reorganization processing is to start without waiting for a response from the keyboard.

When this option is omitted, command execution waits for entry of a response from the keyboard. You can cancel execution by pressing the **Ctrl** + **C** keys.

(d) Return value

Returns one of the following return values:

Return value	Description
0	Normal termination. You can check the results files for the reorganization details.
11	Invalid option specification.
`101` or greater	Terminated with another error.

(e) Notes about command execution

- Before you execute `jamemb_reorganization.bat`, stop all Asset Information Manager Subset services in the following order:
  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

  To use Asset Information Manager Subset after you have executed `jamemb_reorganization.bat`, start the services in the reverse order from which they were stopped.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before reorganizing the database.
- Execute `jamemb_reorganization.bat` as a user with administrator permissions.

(f) Execution example

```
jamemb_reorganization.bat 30010 admin admin -o C:\temp\backup\kekka.log -y
```

(3) Releasing area whose size was increased automatically in an Embedded RDB work file

When a new Asset Information Manager Subset database is created in an Embedded RDB environment and the automatically grow option is enabled, free space may decrease dramatically on the drive where the database is created.

This may be caused by automatic size increase of Embedded RDB work files (files for temporary storage of information needed when SQL statements execute).

The size for work files is increased automatically when a large amount of search results is output. If there is not enough space on the drive where the Asset Information Manager Subset database has been created, you can release the automatically increased area for work files by executing `jamemb_workcomp.exe`.

This subsection describes the function, format, return values, and command execution notes of `jamemb_workcomp.exe`, which releases the automatically increased area for Embedded RDB work files.

`jamemb_workcomp.exe` is stored in the following folder:

Asset-Information-Manager-installation-folder`\exe`

(a) Function

`jamemb_workcomp.exe` releases the automatically increased area for Embedded RDB work files.

(b) Format

```
jamemb_workcomp.exe
```

(c) Return value

Returns one of the following return values:

Return value	Description
0	Normal termination.
11	Invalid option specification.
`101` or greater	Terminated with another error.

(d) Notes about command execution

Execute `jamemb_workcomp.exe` as a user with administrator permissions.

(4) Setting an execution timeout for reorganizing Embedded RDB

While you are reorganizing Embedded RDB, if an error (such as a communication error or disk error) occurs, the reorganization process might not respond.

If you cannot forcibly terminate the reorganization process that does not respond because, for example, Embedded RDB was reorganized automatically by the Windows task feature or by JP1/AJS, perform the following steps to set an execution timeout for the reorganization process.

Notes

- Before you set an execution timeout for reorganizing Embedded RDB, stop all the services, commands, and tasks of Asset Information Manager on the asset management server.
- Stop the services of Asset Information Manager in the following order.

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Asset Information Synchronous Service, and Asset Information Manager Subset commands and tasks
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

  To use Asset Information Manager Subset after you have changed an execution timeout for reorganizing Embedded RDB, start the services in the reverse order from that listed above.

1. To terminate Embedded RDB, execute the jamemb_dbstop.bat command that is stored in *JP1/Software-Distribution -installation-directory*`\jp1asset\exe`.

   Check the message to make sure that Embedded RDB has terminated.
2. Use a text editor to open the `pdsys` file that is stored in *JP1/Software-Distribution-installation-directory*\jp1asset \jp1asset\aimdb\conf.
3. Add a line for set pd_utl_exec_time = execution timeout for reorganizing Embedded RDB in the `pdsys` file. #1
4. Execute the jamemb_dbstart.bat command that is stored in *JP1/Software-Distribution -installation-directory* `\jp1asset\exe` to start the Embedded RDB.

#1

pd_utl_exec_time = execution timeout for reorganizing Embedded RDB To set an execution timeout for a command to manipulate the Embedded RDB, specify an execution timeout in the range from 0 to 35791394 (minutes) for the command. If you do not specify a value, or specify 0, the execution timeout will not be set.

If the command does not complete after the time specified for the execution timeout has elapsed, the command being executed will be abnormally terminated.

For this operand, specify a value that allows for some extra time compared to the actual time that the command requires for execution.

For example, if reorganizing the database requires a maximum of approximately 90 minutes, specify `pd_utl_exec_time=120` for the timeout, just in case. This is because if a process that normally finishes in 90 minutes has not responded after 120 minutes, we can assume that an error causing the command not to respond has occurred.

Sample

```
#
#------------------------------------------------------------------
# set form
#
:

:
set pd_utl_exec_time = 120
#
#------------------------------------------------------------------
# putenv form
#
```

10.3.8 Creating a data source or a net service

Create a data source (in Embedded RDB and Microsoft SQL Server) or a net service (in Oracle) in order to connect to the managing server and the Asset Information Manager Subset database created for the managing server.

Notes

- Before you create a database or net service for connecting to the Asset Information Manager Subset database, stop the services in the following order.

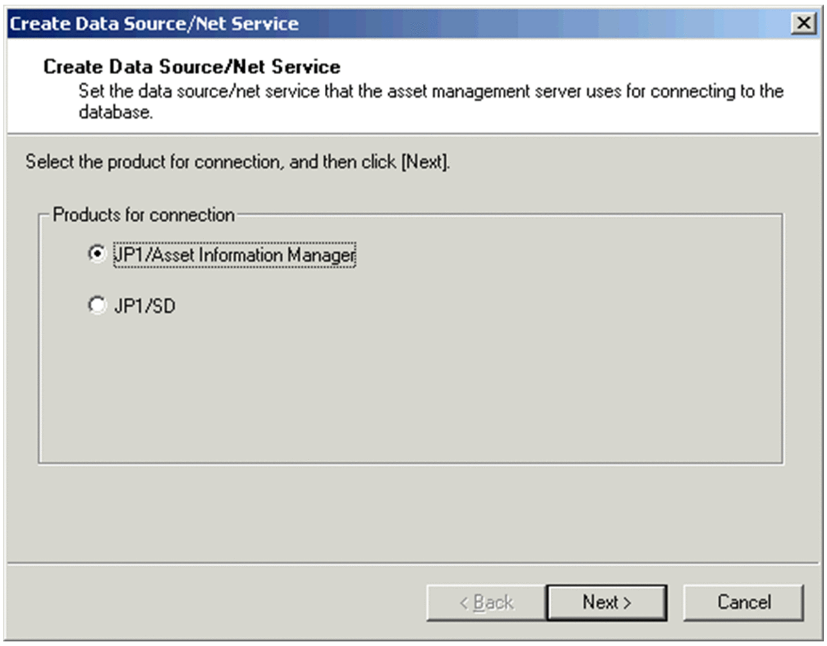
  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before creating the database or net service.

To create a data source or a net service in order to connect to the database:

1. From the **Start** menu, choose **Software Distribution Manager**, **Asset Information Manager**, and then **Setup**.
   The Setup dialog box for Asset Information Manager Subset is displayed.
2. Choose **Create Data Source/Net Service**.
   The Create Data Source/Net Service dialog box appears.

Figure 10–22: Create Data Source/Net Service dialog box



Create Data Source/Net Service

Create Data Source/Net Service

Set the data source/net service that the asset management server uses for connecting to the database.

Select the product for connection, and then click [Next].

Products for connection

● JP1/Asset Information Manager

○ JP1/SD

JP1/Asset Information Manager

Creates a data source (in Embedded RDB and Microsoft SQL Server) or a net service (in Oracle) to connect to the Asset Information Manager Subset database.

Select this item to connect to the existing Asset Information Manager Subset database. If you use the Database Manager of Asset Information Manager Subset to create a database, there is no need to select this item because a data source (in Embedded RDB and Microsoft SQL Server) or a net service (in Oracle) is created when the database is created.

JP1/SD

Creates a data source (in Embedded RDB and Microsoft SQL Server) or a net service (in Oracle) to connect to the managing server database.

Select this item if the database type is Oracle. In Embedded RDB or Microsoft SQL Server, there is no need to select this item because a data source is created during installation.

If you have changed the database environment for the managing server, or the managing server cannot be connected (for reasons such as specification of an invalid value during installation of Asset Information Manager Subset), change the setting.

3. From **Products for connection**, select the name of the database product to be connected, and then click the **Next** button.

   The Create Data Source dialog box appears.

The Create Data Source dialog box depends on the type of database. The following provides a description for each type.

(1) In Embedded RDB

Create a data source in order to connect to the database specified in **Products for connection**.

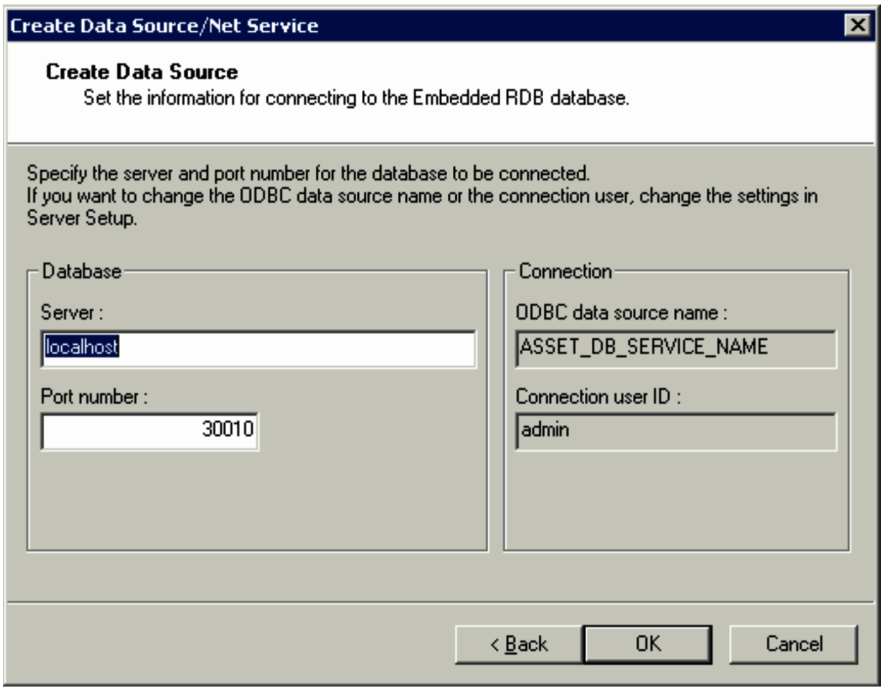
To create a data source for Embedded RDB:

1. In the Create Data Source/Net Service dialog box, select the name of the database product to be connected from **Products for connection**, and then click the **Next** button.

   The Create Data Source dialog box appears.

   In this dialog box, specify the server and port number required in order to create a data source.

Figure 10–23: Create Data Source dialog box (for Embedded RDB)


Create Data Source/Net Service
Create Data Source
Set the information for connecting to the Embedded RDB database.
Specify the server and port number for the database to be connected.
If you want to change the ODBC data source name or the connection user, change the settings in Server Setup.
Database
Server :
localhost
Port number :
30010
Connection
ODBC data source name :
ASSET_DB_SERVICE_NAME
Connection user ID :
admin
< Back
OK
Cancel

Server

Specifies the server name or IP address of the connection-target database. The default depends on the item selected in **Products for connection** in the Create Data Source/Net Service dialog box.

- For **JP1/Asset Information Manager**: `local host`
- For **JP1/SD**: Space

The permitted value is 1 to 63 bytes of characters and the following symbols:

`% ~ - _ . / \`

Port number

Specifies the port number of the connection-target database server. The permitted value is from 5001 to 65535. The default depends on the item selected in **Products for connection** in the Create Data Source/Net Service dialog box.

- For **JP1/Asset Information Manager**: `30010`
- For **JP1/SD**: `30008`

ODBC data source name

Displays the name of the database connection service as the ODBC data source name, according to the selected connection target.

To change the ODBC data source name, do the following:

If you have selected **JP1/Asset Information Manager** from **Products for connection**, change the **Service name** setting in **Database Information** in the Server Setup dialog box.

If you have selected **JP1/SD** from **Products for connection**, change the **Connection service for JP1/SD database** setting in **Link with JP1/SD** in the Server Setup dialog box.

Connection user ID

Displays the database login ID that was specified at setup as the connection user ID used to log on to the database.

To change the connection user ID, do the following:

If you have selected **JP1/Asset Information Manager** from **Products for connection**, change the **Login ID** setting in **Database Information** in the Server Setup dialog box.

If you have selected **JP1/SD** from **Products for connection**, change the **JP1/SD database login ID** setting in **Link with JP1/SD** in the Server Setup dialog box.

2. Set the items and then click the **OK** button.

The data source is created.

(2) In Microsoft SQL Server

Create a data source in order to connect to the database specified in **Products for connection**.

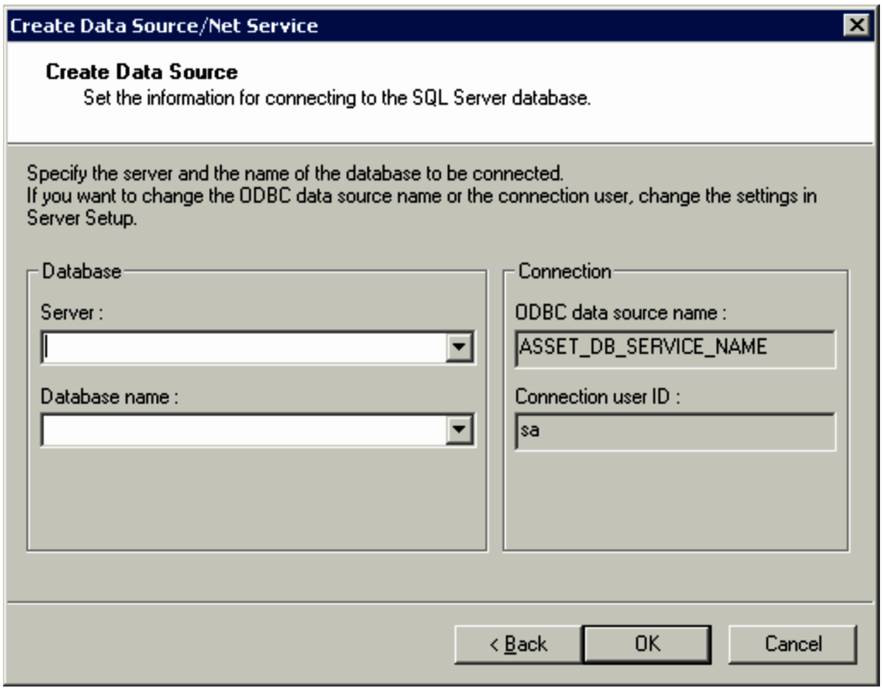
To create a data source for Microsoft SQL Server:

1. In the Create Data Source/Net Service dialog box, select the name of the database product to be connected from **Products for connection**, and then click the **Next** button.

   The Create Data Source dialog box appears.

   In this dialog box, set information about the server and the database name that are required in order to create a data source.

   Figure 10–24: Create Data Source dialog box (for Microsoft SQL Server)

   Create Data Source/Net Service

   Create Data Source

   Set the information for connecting to the SQL Server database.

   Specify the server and the name of the database to be connected.
   If you want to change the ODBC data source name or the connection user, change the settings in Server Setup.

   Database

   Server :

   Database name :

   Connection

   ODBC data source name : ASSET_DB_SERVICE_NAME

   Connection user ID : sa

   Server

   Specifies the server name or IP address of the connection-target database. There is no default.

   The permitted value is 1 to 63 bytes of characters and the following symbols:

   % ~ - _ . / \

   Database name

   Specifies the name of the connection-target database. There is no default.

   The permitted value is 1 to 128 bytes of alphanumeric characters and symbols, except the following symbols and the space:

   \ / * " ' | . < > ?

   ODBC data source name

   Displays the name of the database connection service as the ODBC data source name according to the selected connection target.

   To change the ODBC data source name, do the following:

   If you have selected **JP1/Asset Information Manager** from **Products for connection**, change the **Service name** setting in **Database Information** in the Server Setup dialog box.

   If you have selected **JP1/SD** from **Products for connection**, change the **Connection service for JP1/SD database** setting in **Link with JP1/SD** in the Server Setup dialog box.

   Connection user ID

   Displays the database login ID that was specified at setup as the connection user ID used to log on to the database.

   To change the connection user ID, do the following:

If you have selected **JP1/Asset Information Manager** from **Products for connection**, change the **Login ID** setting in **Database Information** in the Server Setup dialog box.

If you have selected **JP1/SD** from **Products for connection**, change the **JP1/SD database login ID** setting in **Link with JP1/SD** in the Server Setup dialog box.

2. Set the items and then click the **OK** button.

   The data source is created.

(3) In Oracle

Create an Oracle net service to connect to the database specified in **Products for connection**.

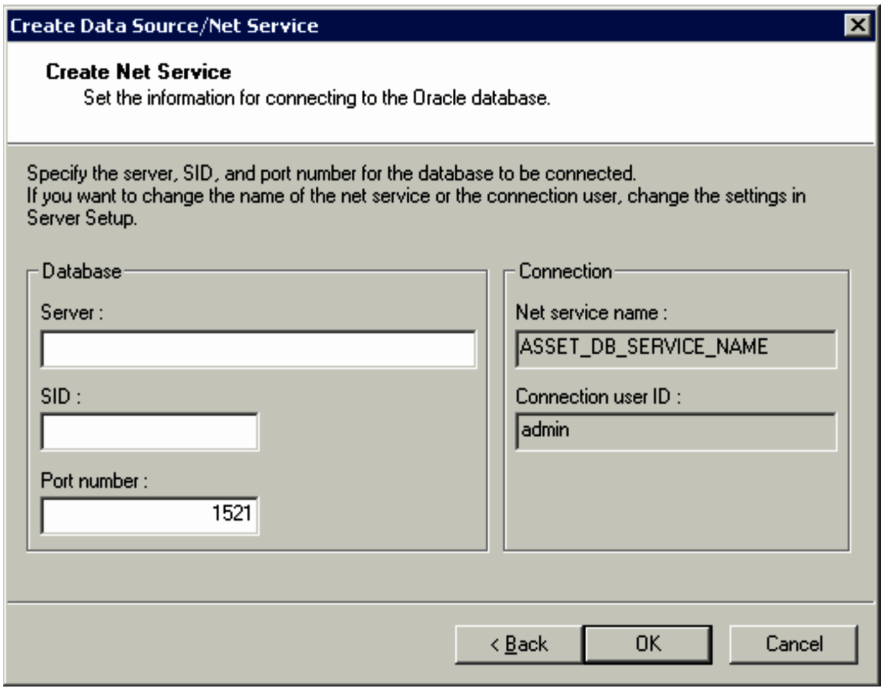
To create an Oracle net service:

1. In the Create Data Source/Net Service dialog box, select the name of the database product to be connected from **Products for connection**, and then click the **Next** button.

   The Create Net Service dialog box appears.

   In this dialog box, specify information about the server and database name required in order to create a net service.

Figure 10–25: Create Net Service dialog box (for Oracle)



Create Data Source/Net Service

Create Net Service

Set the information for connecting to the Oracle database.

Specify the server, SID, and port number for the database to be connected.
If you want to change the name of the net service or the connection user, change the settings in Server Setup.

Database

Server :

SID :

Port number : 1521

Connection

Net service name : ASSET_DB_SERVICE_NAME

Connection user ID : admin

Server

Specifies the server name and IP address of the connection-target database.

There is no default. The permitted value is 1 to 63 bytes of characters and the following symbols:

`% ~ - _ . / \`

SID

In Oracle 8i, specify the SID of the database to be connected. In Oracle 9i, specify the service name.

There is no default. The permitted value is 1 to 8 bytes of alphanumeric characters.

Port number

Specifies the port number of the target database server. The permitted value is from 1 to 65535. The default is `1521`.

Net service name

Displays the database connection service name as the net service name according to the selected connection target.

To change the net service name, do the following:

If you have selected **JP1/Asset Information Manager** from **Products for connection**, change the **Service name** setting in **Database Information** in the Server Setup dialog box.

If you have selected **JP1/SD** from **Products for connection**, change the **Connection service for JP1/SD database** setting in **Link with JP1/SD** in the Server Setup dialog box.

Connection user ID

Displays the connection user ID used to log on to the database.

To change the connection user ID, do the following:

If you have selected **JP1/Asset Information Manager** from **Products for connection**, change the **Login ID** setting in **Database Information** in the Server Setup dialog box.

If you have selected **JP1/SD** from **Products for connection**, change the **JP1/SD database login ID** setting in **Link with JP1/SD** in the Server Setup dialog box.

2. Set the items and then click the **OK** button.

   The data source is created.

10.4 Setting the virtual directory

In Microsoft Internet Information Services, set the virtual directory of Asset Information Manager Subset.

If you are using Microsoft Internet Information Services 6.0 or later, you can create and change application pools.

Note

- If you install Asset Information Manager Subset on a Windows Server 2003 system, you must set an application pool in Microsoft Internet Information Services after the installation is finished. If you use an existing application pool, you must use the same settings as described in *10.6.1(1) Creating an application pool*.
- Before you set the Asset Information Manager Subset virtual directory, stop the services in the following order.

  1. World Wide Web Publishing Service or World Wide Web Publishing
  2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
  3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

  To use Asset Information Manager Subset after you have used the Database Manager, start the services in the reverse order from that listed above.
- If a connection pool has been set up in the ODBC database, the connected status will not change from the time that the Asset Information Manager Subset job was stopped until the timeout time set in the connection pool elapses. Therefore, wait for the connected status to change before setting the virtual directory.

You can use the Virtual Directory Settings dialog box to set application pools only if you are using Microsoft Internet Information Services 6.0 or later.

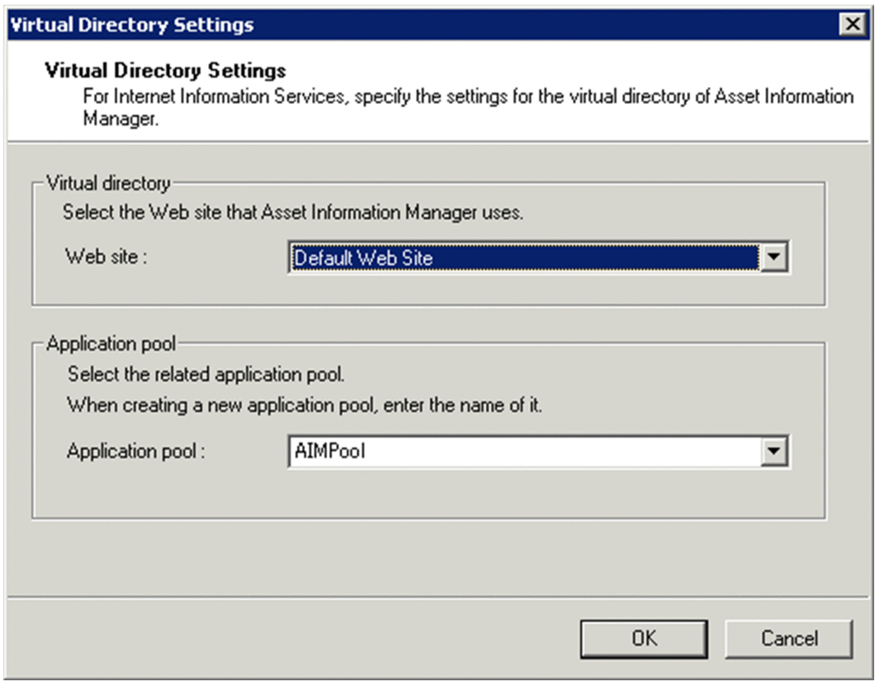
To change the Web site used by Asset Information Manager Subset and to create and change an application pool:

1. From the **Start** menu, choose **Software Distribution Manager**, **Asset Information Manager**, and then **Setup**.

   The Setup dialog box for Asset Information Manager Subset is displayed.
2. Choose **Virtual Directory Settings**.

   The Virtual Directory Settings dialog box appears. Set the virtual directory for Asset Information Manager Subset that is used to store information such as the data required during execution of Asset Information Manager Subset and log files.

Figure 10–26: Virtual Directory Settings dialog box



Virtual Directory Settings

Virtual Directory Settings

For Internet Information Services, specify the settings for the virtual directory of Asset Information Manager.

Virtual directory

Select the Web site that Asset Information Manager uses.

Web site : Default Web Site

Application pool

Select the related application pool.

When creating a new application pool, enter the name of it.

Application pool : AIMPool

If the installed version of Microsoft Internet Information Services is 5.1 or earlier, the application pool items are not displayed.

Web site

Specifies the Web site at which the virtual directory of Asset Information Manager Subset is to be registered. From the pull-down menu, select **Web site**. Direct entry is not permitted. By default, the Web site displaying the virtual directory of Asset Information Manager Subset is specified. If no virtual directory has been registered, **Default Web Site** is specified. If no Web site has been registered, nothing is specified.

Application pool

Specifies the application pool to be associated with the virtual directory of Asset Information Manager Subset. From the combo box, select **Application pool**. By default, the application pool associated with the virtual directory of Asset Information Manager Subset is displayed.

If the name of an application pool registered by the Internet Information Service Manager contains any of the characters =, :, or ,, the name is not displayed in the combo box.

To create a new application pool, enter the name of the new application pool as 1 to 255 bytes of characters. Note that the characters /, \, =, :, and , cannot be used. Application pools are created with the same settings as in *10.6.1(1) Creating an application pool* or *10.6.2(2) Creating an application pool*.

3. Set the items and then click the **OK** button.

   This action causes the virtual directory to be changed and an application pool to be created and changed. Once the changes are complete, a message indicating that the virtual directory setting is completed is displayed.

4. Click the **OK** button.

   The Virtual Directory Settings dialog box closes.

To associate an existing application pool with the virtual directory of Asset Information Manager Subset, use the Internet Information Service Manager to set **Application pool**. For details about the settings for **Application pool**, see the following subsections:

- When using Microsoft Internet Information Services 6.0

  10.6.1(1) Creating an application pool

- When using Microsoft Internet Information Services 7.0

  10.6.2(2) Creating an application pool

10.5 Setting the services used by Asset Information Manager Subset

Asset Information Manager Subset uses the following services:

- IIS Admin Services
- World Wide Web Publishing Service or World Wide Web Publishing
- Asset Information Synchronous Service
  You need these services to acquire updates of inventory information in real time. They are created if you select the component **Asset Information Manager Subset** when you install JP1/Software Distribution Manager.

Set the services used by Asset Information Manager Subset to start automatically. After you install Asset Information Manager Subset, Asset Information Synchronous Service is not set to start automatically.

To set Asset Information Synchronous Service to start automatically:

1. In the Services window, choose **Asset Information Synchronous Service**.
2. From the **Action** menu, choose **Properties**.
   The Properties dialog box appears.
3. On the **General** page, change the setting for **Startup type** to **Automatic**.
4. Click the **OK** button.
   The Properties dialog box closes and Asset Information Synchronous Service is set to start automatically.
5. Start Asset Information Synchronous Service.

Check the properties of other services that are used by the Asset Information Manager Subset server. If they are not set to be started automatically, change the settings so that they will be started automatically in the same manner.

10.6 Settings for using Microsoft Internet Information Services 6.0 or later

This section describes the required settings and provides notes about using Microsoft Internet Information Services 6.0 when Asset Information Manager Subset is installed.

If you are using Microsoft Internet Information Services 5.1 or earlier, there is no need to specify the settings described here.

10.6.1 Setting the Web server (for Microsoft Internet Information Services 6.0)

This subsection describes the required settings and provides notes about using Microsoft Internet Information Services 6.0 when Asset Information Manager Subset is installed.

(1) Creating an application pool

To associate an existing application pool with the virtual directory for Asset Information Manager Subset, use the settings described here. These settings are not required if you create a new application pool from the Asset Information Manager Subset setup.

To set **Application pool** using Internet Information Service Manager:

1. Start Internet Information Service Manager.
2. Select **Application pool** for the Asset Information Manager Subset server.
3. From the **Action** menu, choose **New**, then **Application pool**.
   The Add New Application Pool dialog box opens.
4. Enter an application pool ID in **Application pool ID** and click the **OK** button.
   The characters =, **:**, and **,** cannot be used in the application pool ID. If any of these characters is used, the application pool ID will not be displayed in the combo box in the Virtual Directory Settings dialog box.
5. Display the properties of the created application pool.
6. On the **Recycling**, **Performance,** and **Health** pages, clear all options.
7. On the **Identity** page, choose **Predefined** and then choose **Local System** for **Application pool ID**.
8. For Asset Information Manager Subset's **Web site**, choose **Default Web Site**, then **jp1asset** to display the properties.
9. Select the application pool created in step 4 and click the **OK** button.
10. Restart World Wide Web Publishing Service.

In the virtual directory specified in **Web site** in the Virtual Directory Settings dialog box, do not create a Web site in which work processes are recycled.

(2) Adding a site for Asset Information Manager

When Microsoft Internet Information Services 6.0 is used, in order to use Asset Information Manager Subset from Microsoft Internet Explorer, you must add a site for Asset Information Manager Subset.

To add the Asset Information Manager Subset site:

1. In Microsoft Internet Explorer, choose **Tools** and then choose **Internet Options**.
   The Internet Options dialog box opens.
2. On the **Security** page, choose the **Intranet** icon and click the **Site** button.
3. In the displayed dialog box, add the Asset Information Manager Subset site and click the **Close** button.

(3) Notes on creating a site

If you use Microsoft Internet Information Services 6.0 and have installed Asset Information Manager Subset, do not create a Web site in which work processes are recycled in the virtual directory that was specified in **Web site** in the Virtual Directory Settings dialog box. By default, **Default Web Site** is set in **Web site**.

10.6.2 Setting the Web server (for Microsoft Internet Information Services 7.0)

This subsection describes the required settings and provides notes about using Microsoft Internet Information Services 7.0 when Asset Information Manager Subset is installed.

(1) Installing the role services

When you use Microsoft Internet Information Services 7.0, you must install the role services appropriate to your purpose.

To install role services for Microsoft Internet Information Services 7.0:

1. From **Server Manager**, choose **Roles**, and then **Add Roles Service**.
   A dialog box for selecting role services is displayed.
2. Select the role services suitable for the purpose, and then click the **Next** button.
   A dialog box for confirming the installation options is displayed.
   The following table lists and describes the role services that can be selected when the Asset Information Manager Subset server and the WSUS server are configured.

Table 10–7: Role services that can be selected when the Asset Information Manager Subset server and the WSUS server are configured

Item	Role service	AIM Subset# server	WSUS server
Common HTTP Features	Static Content	S	S
	Default Document	R	--
	Directory Browse	S	--
	HTTP Errors	R	R
Application Development	ASP.NET	--	S
	ISAPI Extensions	S	--
	ISAPI Filters	S	--
Performance	Static Content Compression	R	--
IIS Management Console		S	S
IIS 6 Management Compatibility	IIS 6 Metabase Compatibility	S	S

Legend:
S: Role service must be selected.
R: Selection of the role service is recommended.
--: Not applicable.

#: AIM Subset: Asset Information Manager Subset

3. Make sure that the role services selected in step 2 are displayed, and then click the **Install** button.
   When installation is completed, a dialog box indicating the installation result is displayed.
4. Click the **Close** button.

(2) Creating an application pool

You use the settings described here to associate an existing application pool with the virtual directory for Asset Information Manager Subset. These settings are not required when you create a new application pool from the Asset Information Manager Subset setup.

To set **Application pool** using Internet Information Service Manager:

1. Start Internet Information Service Manager.
2. Select **Application pool** for Asset Information Manager Subset.
3. From the **Action** menu, choose **Add Application Pool**.
   The Add Application Pool dialog box appears.
4. In **Name**, enter a desired application pool name, set **Managed pipeline mode** to **Classic**, then click the **OK** button.
   The characters =, `:`, and `,` cannot be used in the application pool ID. If any of these characters is used, the application pool ID will not be displayed in the combo box in the Virtual Directory Settings dialog box.
5. Select the created application pool, and then from the **Action** menu, choose **Advanced Settings**.
   The Advanced Settings dialog box appears
6. Specify the necessary settings, and then click the **OK** button.
   In the Advanced Settings dialog box, specify the settings as shown below. The other items may be set to their defaults.

   General

   Queue Length: `4000`

   Enable 32-Bit Applications: `True` (applicable only in the case of a 64-bit version of Windows Server 2012, or Windows Server 2008 (x64))

   Process Model

   Identity: `LocalSystem`

   Ping Enabled: `False`

   Idle Time-out (minutes): `0`

   Rapid-Fail Protection

   Enabled: `False`

   Recycling

   Isapi Reported Unhealthy: `True`

   Manual Recycle: `True`

   Specific Time: `True`

   Application Pool Configuration Changed: `True`

   Request Limit Exceeded: `True`

   Disable Recycling for Configuration Changes: `True`

   Regular Time Interval (minutes): `0`
7. From the **Action** menu, choose **Recycling**.
   The Edit Application Pool Recycling Settings dialog box appears.
8. Clear all the recycle condition check boxes and then click the **Next** button.
9. Of the recycle events that are to be logged, select the check boxes for the recycle events that are to be logged during recycling of application pools, then click the **Finish** button.
   It is recommended that you select all the enabled check boxes. If there is any recycle event that is not to be logged during recycling of application pools, clear its check box, and then click the **Finish** button.
10. Restart the World Wide Web Publishing Service.

Note that a Web site that recycles worker processes must not be created in the virtual directory specified in **Web site** in the Virtual Directory Settings dialog box.

(3) Setting an application (virtual directory)

If you added the **IIS 6 Metabase Compatibility** role service after you installed Asset Information Manager Subset, you must set the application (virtual directory) with Internet Information Service Manager.

To create a new application (virtual directory):

1. From the Asset Information Manager Subset server's **Sites**, right-click **Default Web Site**, then choose **Add Application**.
   The Add Application dialog box appears.
2. Click the **Select** button to specify the application pool that has been created in **Application Pools**.
3. In **Physical path**, specify the virtual directory of the Asset Information Manager Subset server, then click the **OK** button.
   The default virtual directory of the Asset Information Manager Subset server is *Asset-Information-Manager-Subset-installation-folder*`\wwwroot`.

The following describes how to change the settings when the application (virtual directory) already exists:

1. From the Asset Information Manager Subset server's **Sites**, choose **Default Web Site**, **jp1asset**, then choose **Advanced Settings**.
   The Advanced Settings dialog box appears.
2. Specify the created application pool in **Application Pools** and the virtual directory of the Asset Information Manager Subset server in **Physical path**, then click the **OK** button.
   The default virtual directory of the Asset Information Manager Subset server is *Asset-Information-Manager-Subset-installation-folder*`\wwwroot`.

(4) Setting ISAPI restrictions

If you added the **IIS 6 Metabase Compatibility** and **ISAPI Extensions** role services after you installed Asset Information Manager Subset, you must set ISAPI restrictions with Internet Information Service Manager.

To set ISAPI restrictions:

1. Select the Asset Information Manager Subset server and then choose **ISAPI and CGI Restrictions**.
2. From the **Action** menu, choose **Add**.
   The Add ISAPI or CGI Restriction dialog box appears.
3. In **ISAPI or CGI path**, specify the file path, select the **Allow extension path to execute** check box, then click the **OK** button.
   In **ISAPI or CGI path**, specify the path to each of the following files, which are stored in the virtual directory of the Asset Information Manager Subset server:
   - `jamwscript.dll`
   - `bin\jamlogin.dll`
   - `jamenter.dll`
   - `jamfile.dll`
   - `jamhtmlfile.dll`

   Add all these files by repeating steps 1 through 3 for each file.
   The default virtual directory of the Asset Information Manager Subset server is *Asset-Information-Manager-Subset-installation-folder*`\wwwroot`.

(5) Setting ISAPI filters

If you added the **IIS 6 Metabase Compatibility** and **ISAPI Filters** role services after you installed Asset Information Manager Subset, you must set ISAPI filters with Internet Information Service Manager.

To set ISAPI filters:

1. From the Asset Information Manager Subset server's **Sites**, choose **Default Web Site**, then choose **ISAPI Filters**.
2. From the **Action** menu, choose **Add**.
   The Add ISAPI Filter dialog box appears.
3. In **Executable**, specify the file path, and then click the **OK** button.
   In **Executable**, specify the path to `bin\jamssessionfilter.dll` that is stored in the Asset Information Manager Subset installation folder.
   There is no need to change **Filter name**.

(6) Setting the handler mappings

If you added the **IIS 6 Metabase Compatibility** role service after you installed Asset Information Manager Subset, you must set the handler mappings with Internet Information Service Manager.

To set the handler mappings:

1. From the Asset Information Manager Subset server's **Sites**, choose **Default Web Site**, **jp1asset**, and then choose **Handler Mappings**.
2. From the **Action** menu, choose **Edit Feature Permissions**.
   The Edit Feature Permissions dialog box appears.
3. Select all check boxes (**Read**, **Script**, and **Execute**), and then click the **OK** button.

(7) Setting directory browsing

If you added the **IIS 6 Metabase Compatibility** and **Directory Browse** role services after you installed Asset Information Manager Subset, you must set directory browsing with Internet Information Service Manager.

To set directory browsing:

1. From the Asset Information Manager Subset server's **Sites**, choose **Default Web Site**, **jp1asset**, **log**, and then choose **Directory Browse**.
2. From the **Action** menu, choose **enable**.

(8) Adding a site for Asset Information Manager Subset

When Microsoft Internet Information Services 7.0 is used, in order to use Asset Information Manager Subset from Microsoft Internet Explorer, you must add a site for Asset Information Manager Subset.

To add the Asset Information Manager Subset site:

1. In Microsoft Internet Explorer, choose **Tools** and then choose **Internet Options**.
   The Internet Options dialog box opens.
2. On the **Security** page, select the **Local intranet** icon, and then click the **Sites** button.
3. In the displayed dialog box, add the Asset Information Manager Subset site and click the **Close** button.

(9) Notes on creating a site

For notes on installing Asset Information Manager Subset on a 64-bit OS, see *10.11(1) Notes on installing Asset Information Manager Subset on a 64-bit OS*.

- If you use Microsoft Internet Information Services 7.0 and have installed Asset Information Manager Subset, do not create a Web site in which work processes are recycled in the virtual directory that was specified in **Web site** in the Virtual Directory Settings dialog box. By default, **Default Web Site** is set in **Web site**.

10.7 Setting the tasks that are registered in Task Scheduler

Asset Information Manager Subset enables you to use Windows Task Scheduler to automatically maintain and monitor asset information that is created by daily asset management jobs.

When you install Asset Information Manager Subset, tasks are created in Windows Task Scheduler. You can modify this task schedule and settings for enabling or disabling tasks as appropriate for how you handle asset information.

Note that when Asset Information Manager Subset is first installed, all tasks are disabled.

This section provides the details of the tasks and describes each task's setup procedure.

Note

- A user with Administrator permissions must execute task scheduling.
- If you use Windows XP Professional, you must execute task schedules in an environment in which Windows XP Professional's login user and password have been set. Task schedules will not execute in an environment in which the user and password have not been set.
- When executing Asset Information Manager Subset tasks in a 64-bit OS, tasks must be executed from a 32-bit command prompt. For details about execution procedure, see *10.11(2) Notes on executing commands and tasks on a 64-bit OS*.

10.7.1 Types of tasks

This subsection describes the tasks, the details of each task, and the default when each task is enabled that are set in Windows Task Scheduler.

(1) Name and details of tasks

Do not change the files that are used by a task.

The following describes the name and details of each task:

- Data maintenance

  To maintain data integrity between the managing server database and the Asset Information Manager Subset database, this task updates related information according to the updated information. This task also deletes unneeded information.

  Make sure that you enable this task after you have finished setting up Asset Information Manager Subset.

  For details about how to specify the tasks to be executed in **Data maintenance**, see *10.7.2 Specifying the work to be performed by the Data maintenance task*.

- Delete change log

  Deletes all the asset information logs and change logs except for the information for a specified period.

  In the default setting, the **Delete change log** task deletes the history information of asset information that is more than six months old at 6:30 a.m. on the first day of every month. For details about the procedure for changing the date and time and the frequency of task execution, see *10.7.3 Specifying the types of history information to be deleted and the deletion timing*.

- Take inventory

  Imports inventory information into the Asset Information Manager Subset database. When you acquire updated inventory information in real time, there is no need to use this task.

  For the procedure for specifying an option to re-acquire all inventory information, see *10.7.4 Acquiring all inventory information*.

  For details about the inventory information that can be acquired, see *10.9 Inventory information that can be displayed by Asset Information Manager Subset*.

- Acquiring directory information

  Imports group and user information into the Asset Information Manager Subset database from the directory information. It is recommended that you execute this task after directory information has been updated.

You should not acquire directory information together with user inventory information because the group and user information may be duplicated.

For details about how to acquire directory information, see *10.7.6 Acquiring directory information*.

Note

When you acquire directory information, you cannot select whether or not the existing data is to be overwritten. The assigned group or user names will be overwritten by the corresponding directory information.

(2) Default settings for the tasks

The following table lists the default schedule settings that take effect when the various tasks are enabled.

Table 10–8: Default settings when tasks are enabled

Task name	Default schedule setting
Data maintenance	5:00 a.m. every day
Delete change log	6:00 a.m. on the first of every month
Take inventory	5:30 a.m. every Wednesday
Acquiring directory information	Midnight every Sunday

10.7.2 Specifying the work to be performed by the Data maintenance task

When you execute the **Data maintenance** task, all related information is updated according to the updated information in order to maintain data integrity between the managing server database and the Asset Information Manager Subset database. Unneeded information is deleted.

For details about how to specify the data maintenance process, see *(2) Creating a settings file*.

When you execute the **Data maintenance** task, you should stop Asset Information Manager Subset services in the following order:

1. World Wide Web Publishing Service or World Wide Web Publishing
2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
3. JP1/Client Security Control - Manager (applicable if JP1/CSC is linked)

To use Asset Information Manager Subset after you have executed the *Data maintenance* task, start the services in the reverse order from which they were stopped.

This subsection describes the work that is performed by the **Data maintenance** task and how to create the settings file.

(1) Work performed by the Data maintenance task

Using the **Data maintenance** task, you can perform the following:

- Deleting the asset information in the Erase status
  When asset information is deleted, the following related information is also deleted:
  Hardware information, network information, installed software information, patch information, virus definition information, transfer log, component information
- Deleting information related to asset information in `Restore`, `Scrap`, or `Pre-Scrap` status
  The following information is deleted:
  Installed software information, patch information, virus definition information, software usage information, component information, and network information#
  #: Only the IP address is deleted as network information.

- Changing the group names, location names, and user names registered in the existing asset information according to the changes made to them in windows.

  Group, location, and user names that have been changed by window operations are applied to the asset information by this task, and change logs are acquired in the transfer logs.

- Setting the groups, locations, and user names corresponding to IDs in the asset information.

  If the asset information contains group IDs, location IDs, user IDs, administrator IDs, and administrator group IDs, but no corresponding groups, locations, user names, administrators, or administrator groups are set, the corresponding names are set.

- Deleting unneeded IP address control information.

  The IP address control information of an unused IP address outside the range of IP group information is deleted.

- Deleting installed software information for which no installed software name is registered.
- Deleting the installed software information of the software whose management level is set to **Unused**.
- Deleting group- or location-specific IP groups from which the corresponding groups or locations have been deleted.
- Registering the group that corresponds to the IP address in the hardware asset information in **Group** in the asset information.

  For the correspondence between IP addresses and groups, the IP group settings created by the **IP Group** job menu are used. In the default, this task is not set to be executed.

- Registering the location that corresponds to the IP address in the hardware asset information in **Location** in the asset information.

  For the correspondence between IP addresses and locations, the IP group settings created by the **IP Group** job menu are used. In the default, this task is not set to be executed.

- Deleting attached files for which there is no corresponding information (hardware asset information).
- Deleting division information specified in groups that no longer exist.

(2) Creating a settings file

Specify the work performed by the **Data maintenance** task in the settings file (`taskopt.ini`).

`taskopt.ini` is stored in *Asset-Information-Manager-Subset-installation-folder*`\env`. When you create `taskopt.ini`, you should use `taskopt.org` that is stored in the same folder for convenience.

Create `taskopt.ini` with the following contents:

```
[DATAMAINTENANCE]
ASSET_ERASE_DEL              = YES
ASSET_ASSOC_DEL              = YES
SOFTINFO_ERASE_DEL           = NO
SOFTINFO_ASSOC_DEL           = NO
CONTRACT_ERASE_DEL           = NO
VOLUME_ERASE_DEL             = NO
USER_ASSOC_UPD               = YES
GROUP_ASSOC_UPD              = YES
LOCATION_ASSOC_UPD           = YES
IP_UNNECESSARY_DEL           = YES
INSTINFO_NOLIST_DEL          = YES
LICENSELINK_UNNECESSARY_DEL  = NO
SOFTINFO_CONSOLIDATE         = NO
INSTINFO_UNMANAGED_DEL       = YES
IPGROUP_NOOBJECT_DEL         = YES
IP_GROUP_ASSOC               = OVERWRITE
IP_LOCATION_ASSOC            = OVERWRITE
ATTACHFILE_DEL               = NO
```

`IP_GROUP_ASSOC` is overwritten even when user inventory values have been set. To update **Group name** for all assets according to the setting in the **IP Group** job menu, specify `OVERWRITE`. If you do not use the **IP Group** job menu to manage groups, specify `NO`.

10.7.3 Specifying the types of history information to be deleted and the deletion timing

This subsection describes how to specify the types of history information to be deleted and the deletion timing.

(1) Specifying the types of history information to be deleted

On the **Task** page, in **Run**, specify `-s TARGET=(`*change-log-code-to-be-deleted*`)` following the file name. You can specify multiple codes.

If nothing is specified, the task deletes only the change log for asset information.

Codes for the change log that can be deleted are as follows:

- `A`
  Asset information history. The affected class is `AssetUpdateRecord`.
- `U`
  Update history. The affected classes are `UpdateRecord` and `InstalledUpdateRecord`.

If you specify multiple codes, specify them consecutively, such as `-s TARGET=AU`.

(2) Specifying the duration for retaining history information

On the **Task** page, in **Run**, specify the value following the file name in the format shown below:

- Change log for asset information
  `-s TARGET=A -s MONTH=(`*retention-period*`)`
  Specify the retention period in number of months (0-120). Specifying 0 deletes all change log information.
  If nothing is specified, the task deletes all change log data that is at least six months old.
- Device change log
  `-s TARGET=U -s UMONTH=(`*retention-period*`)`
  Specify the retention period in number of months (0-120). Specifying 0 deletes all change log information.
  If nothing is specified, the task deletes all change log data.

Specification example

This example deletes the logs of asset information that were acquired more than 3 months ago.

```
"C:\netmdm\jp1asset\exe\jamscript.exe"
-f "C:\jp1asset\scriptbatch\RemoveRecord.txt"
-s TARGET=A -s MONTH=3
```

Here, `C:\netmdm\`*jp1asset* refers to the Asset Information Manager Subset installation folder.

10.7.4 Acquiring all inventory information

This option updates all information, including information for which the update date has not changed.

Specify **ALL** after a file name in **Run** on the **Task** page. If this option is omitted, only updated inventory information is acquired.

The following is a specification example:

```
"C:\netmdm\jp1asset\exe\jamTakeDMInventory.bat" ALL
```

Here, `C:\netmdm\`*jp1asset* refers to the Asset Information Manager Subset installation folder.

Notes

If `ALL` is not specified, inventory information is not collected if the inventory information update date has not changed. Therefore, even if the collected inventory information operates over JP1/Software Distribution, the JP1/Software Distribution update date is not changed and it is not collected.

10.7.5 Task setup procedure

This subsection describes the procedures for using Windows Task Scheduler to enable and disable tasks, change a task execution schedule, and delete tasks.

(1) Enabling a task

A task for Asset Information Manager Subset that has been created in Windows Task Scheduler is disabled by default. To use the task, you must enable it.

Also, for details about running tasks in a 64-bit OS, see *10.11(2) Notes on executing commands and tasks on a 64-bit OS*.

To enable or disable a task registered in Task Scheduler:

1. On Windows **Control Panel**, double-click the **Scheduled Tasks** icon.
   The Scheduled Tasks window appears.
2. Select the task that you want to enable (or disable) and display its properties.
   The selected task's Properties dialog box appears.
3. On the **Task** page, select the **Enabled [scheduled task runs at specified time]** check box.
   To disable the task, clear this check box.
4. If you are using Windows Server 2003(x64), you need to change the file specified in **Run**.
5. Click the **OK** button.
   The task is enabled (or disabled), and the task's Properties dialog box closes.
   The results of task execution are confirmed from the Scheduled Tasks window, which is started by double clicking the **Scheduled Tasks** icon in the Windows control panel.
   Switch the Scheduled Tasks window to detailed display, then confirm the return value displayed for **Last Result**. For details, see the file `ASTMES`*`n`*`.log`.

The table below shows the **Run** setting for each task.

In the table, *AIM* indicates the Asset Information Manager Subset installation folder.

Table 10–9: Run setting for each task

Task name	Run setting
Data maintenance	`"`*`AIM`*`\exe\jamscript.exe" -f "`*`AIM`*`\scriptbatch\DataMaintenance.txt"`
Delete change log	`"`*`AIM`*`\exe\jamscript.exe" -f "`*`AIM`*`\scriptbatch\RemoveRecord.txt" -s TARGET=A -s MONTH=6`
Take inventory	`"`*`AIM`*`\exe\jamTakeDMInventory.bat"`
Acquiring directory information	`"`*`AIM`*`\exe\jamscript.exe" -f "`*`AIM`*`\scriptbatch\DMDirectory.txt"`

(2) Changing a task schedule

You can change a task's execution date and time. You can also add a schedule.

- Changing the execution date and time
  To change a task execution date and time:
  1. On the Windows **Control Panel**, double-click the **Scheduled Tasks** icon.
     The Scheduled Tasks window appears.
  2. Select the task whose execution date and time are to be changed and display its properties.
     The selected task's Properties dialog box appears.
  3. On the **Schedule** page, change **Schedule Task** and **Start time**.
  4. Click the **OK** button.

The task is modified to the specified schedule, and the task's Properties dialog box closes.

- Adding an execution schedule
  To add a task execution schedule:
  1. On the Windows **Control Panel**, double-click the **Scheduled Tasks** icon.
     The Scheduled Tasks window appears.
  2. Select the task for which a schedule is to be added and display its properties.
     The selected task's Properties dialog box appears.
  3. On the **Schedule** page, select the **Show multiple schedules** check box.
     At the top of the **Schedule** page, a pull-down list of schedules and the **New** and **Delete** buttons appear.
  4. Click the **New** button.
     The schedule is added to the pull-down list.
  5. Set **Schedule Task** and **Start time** for the new schedule.
  6. Click the **OK** button.
     The new schedule is added to the task, and the task's Properties dialog box closes.

(3) Deleting a task

To delete an unneeded task:

1. On the Windows **Control Panel**, double-click the **Scheduled Tasks** icon.
   The Scheduled Tasks window appears.
2. Select the task you wish to delete, and then from the **File** menu, choose **Delete**.
   The selected task is deleted.

(4) Task execution results

You can check the execution results of a task in the Scheduled Tasks window that is displayed when the **Scheduled Tasks** icon is double-clicked.

Set the Scheduled Tasks window to the detail view and check the return value that is displayed in **Last Result**. For details about the displayed information, see `ASTMES`***n***`.log`.

The following table describes the return values.

Return value	Description
`0x0`	Normal end.
`0x1`	No corresponding data was found.
`0x2` or greater	Terminated with some other error.

10.7.6 Acquiring directory information

You can choose to acquire only group information or both group and user information from the directory information.

The acquired information is group information that is defined in `OU ou` *name*, and user information in `USR cn` *full-name* of the sample definition file (map file) provided in JP1/Software Distribution.

On the **Task** page, specify the information to be acquired in **Run** following the file name in the following format:

Format

`-s OPT=`*processing-type*

For the processing type, specify one of the following as a numeric character:

- `1`: Acquire only group information from the directory information (default).
  Creates GroupInfo from the acquired group information.

- 2: Acquire both group and user information from the directory information and assigns them to the asset information.

  GroupInfo is created from the acquired group information, and is assigned to the managed item, *AssetInfo* **.** *GroupName*.

  Also, the acquired user information is assigned to *AssetInfo* **.** *UserName*. However, UserInfo is not created from the acquired user information.

Specification example

```
"C:\jp1asset\exe\jamscript.exe"
-f "C:\jp1asset\scriptbatch\DMDirectory.txt"
-s OPT=1
```

`C:\jp1asset` indicates the Asset Information Manager Subset installation folder.

Notes

- When group information is to be acquired from the directory information and there are multiple groups with the same name in the same hierarchy, the task acquires only one of them.
- If group information was not assigned using **Local name** and **ADGUID** of the group information in the Asset Information Manager Subset database, the group information is registered as new information. In such a case, a **Group ID** is assigned automatically.

10.8 Setting for summing the operation logs by group

In the Operation Log Total window, you can sum up the operation logs collected from the managed devices for each group. To do this, you must manage group information separately from the operation logs.

This section describes how to manage group information.

Device groups are managed as one of the device attributes in the Asset Information Manager Subset database. There are three ways to register group information to device attributes:

1. Using IP addresses to register applicable groups in the batch mode
2. Using the user inventory information to register groups in the batch mode
3. Registering groups individually

You can combine all three methods. The following subsections describe how to register group information with each method.

10.8.1 Using IP addresses

This method creates groups by defining a range of IP addresses to be used by each group and then registering managed device groups on the basis of the IP address value.

To register managed device groups using the IP addresses in the inventory information:

1. Log in to Asset Information Manager Subset.

   Start the Web browser and specify `http://`*host-name*`/jp1asset/login.htm` as the URL. For **Host name**, specify the host name of the server where Asset Information Manager Subset has been installed.

   For **User ID** and **Password**, specify `dm_admin`.
2. Create groups.

   Create groups according to the group hierarchies. To create groups, use the **Group and User** job menu. For details about how to create groups, see *10.7.1 Changing user and group information (Group and User)* in the manual *Administrator's Guide Volume 1*.
3. Group IP addresses for each group.

   For each group created in step 2, define the range of IP addresses and create a group. To define a group of IP addresses, use the **IP Group** job menu. For details about how to define a group of IP addresses for each group, see *10.7.4 Changing IP group information (IP Group)* in the manual *Administrator's Guide Volume 1*.

By creating groups and then a group of IP addresses for each group, you can register information about the managed groups in each device when the inventory information is loaded to the Asset Information Manager Subset database.

10.8.2 Using the user inventory information

If you have defined user inventory to collect information about groups, you can use the user inventory information to register a corresponding group.

To register a corresponding group using the user inventory information:

1. Log in to Asset Information Manager Subset.

   Start the Web browser and specify `http://`*host-name*`/jp1asset/login.htm` as the URL. For **Host name**, specify the host name of the server where Asset Information Manager Subset has been installed.

   For **User ID** and **Password**, specify `dm_admin`.
2. Assign user inventory information to the item that manages group attributes.

   Assign a group name for the user inventory information to the item that manages group information in Asset Information Manager Subset (**Group information.Local name**). To assign user inventory information, use the **Assign Inventory** job menu. For details about how to assign user inventory information, see *10.8.5 Setting assigned items (Assign Inventory)* in the manual *Administrator's Guide Volume 1*.

By assigning user inventory information to managed items, you can register information about managed groups in each device when the inventory information is loaded to the Asset Information Manager Subset database.

10.8.3 Setting a group name to a device

You can register groups by editing information about the devices registered in Asset Information Manager Subset. Because this method sets information about managed devices individually, use it for a device for which the IP address or user inventory information cannot be registered.

To set a group name for each device:

1. Log in to Asset Information Manager Subset.

   Start the Web browser and specify `http://`*host-name*`/jp1asset/login.htm` as the URL. For **Host name**, specify the host name of the server where Asset Information Manager Subset has been installed.

   For **User ID** and **Password**, specify `dm_admin`.

2. Search for a device for which a group is to be set.

   To search devices, use the **Device List** job menu. For details about how to search devices, see *10.2.2 Searching for devices (Device List)* in the manual *Administrator's Guide Volume 1*.

3. Set a device group.

   From the list of search results, display the Device Details dialog box and set a group. For details about how to edit information in the Device Details dialog box, see *10.2.6 Management of detailed information about a device* in the manual *Administrator's Guide Volume 1*.

10.9 Inventory information that can be displayed by Asset Information Manager Subset

The information supported by Asset Information Manager Subset is created and updated on the basis of inventory information.

If information is to be collected also from devices on which JP1/Software Distribution Client has not been installed, the available information is limited. For details about the information that can be acquired from a machine on which JP1/Software Distribution is not installed, see *10.9.1(1) Asset information that can be acquired from a machine on which JP1/Software Distribution is not installed* and *10.9.2(1) Hardware information that can be acquired from a machine on which JP1/Software Distribution is not installed*.

The following table describes the correspondence between the information that is created and updated, and the inventory information that is assigned.

Table 10–10: Correspondence between information that is created and updated and the inventory information that is assigned

Information in AIM Subset	JP1/Software Distribution inventory information							
	Sys cnfg	Sys#1	Inst pckg	SW inv	MS Office	Virus def	User inv	Rgstr
Asset information	Y	Y	N	N	N	N	Y	Y
Hardware information	Y	Y	N	N	N	N	Y	Y
Network information	Y	Y	N	N	N	N	Y	Y
Installed software information#2	N	Y	Y	Y	N	N	Y	N
Installed software list#2	N	Y	Y	Y	N	N	Y	N
Component information#2	N	N	N	N	Y	N	N	N
Software list	N	N	Y	Y	N	N	N	N
Patch information#3	N	Y	Y	N	N	N	N	N
Patch name list	N	Y	Y	N	N	N	N	N
Virus definition information	N	N	N	N	N	Y	N	N
Group information#4	N	N	N	N	N	N	Y	N
Location information#4	N	N	N	N	N	N	Y	N
IP address	N	Y	N	N	N	N	N	N
Device change log information	Y	Y	N	N	N	N	Y	Y
Software update log information	N	N	Y	Y	N	N	N	N

Legend:

Information in AIM Subset: Information in Asset Information Manager Subset

Sys cnfg: System-configuration information

Sys: System information

Inst pckg: Installed package information

SW inv: Software inventory information

MS Office: Microsoft Office information

Virus def: Virus definition information

User inv: User inventory information

Rgstr: Registry information

Y: Can be assigned

N: Cannot be assigned

#1

Some JP1/Software Distribution system information (security information, domain type, AMT firmware version, and printer server name) cannot be assigned.

#2

This information is not created or updated if the system is set to acquire only hardware-related information.

For details about how to specify the types of information acquired from JP1/Software Distribution, see *10.2.5 Setting the link with JP1/SD*.

#3

If unapplied patch information is set to be acquired, information about patches requiring installation can also be acquired. For details about how to specify the settings to acquire unapplied patch information, see *7.2 Detecting client patch information* in the manual *Administrator's Guide Volume 1*.

#4

This information is created or updated if the system is set to register the group names and location information of the user inventory information during inventory information assignment.

Note

- When system information and system configuration information are assigned, if the source value is null, Asset Information Manager Subset's information is not updated.
- Information is updated when the status is `Active`, `Stock`, `Pre-Scrap`, or `Erase`. If the status of an assigned device is `Stock`, `Pre-Scrap`, or `Erase`, it is changed to `Active`.

The following provides the details of each type of information that is created and updated.

10.9.1 Inventory information that can be acquired as asset information

The table below lists and describes the asset information in Asset Information Manager Subset that is created and updated on the basis of the inventory information stored in the managing server database.

For details about the inventory information assignment settings, see *10.8.5 Setting assigned items (Assign Inventory)* in the manual *Administrator's Guide Volume 1*.

Table 10–11: Details of asset information that is created and updated on the basis of the inventory information

Item name	Value to be set	Whether or not the value is updated when there is existing data
Asset ID	The value is assigned automatically during creation.	N
Asset type	**Hardware**	N
Asset number	One of the following assigned items selected by **Assign Inventory**: • **Auto** • **Get from the user inventory** • **Host name (with domain name)** • **Host name (without domain name)** • **Working key** • **IP address** • **MAC address** • **Computer name** The default is **Auto**. **Working key** is a host ID or a node identification key.	Y

Item name	Value to be set	Whether or not the value is updated when there is existing data
Group ID	ID corresponding to the group specified in **Group**	Y
Group	One of the following assigned items selected by **Assign Inventory**: • **Do not set** • **Enter the group to which the user belongs** • **Get from the user inventory** The default is **Do not set**.	Y
User ID	The ID corresponding to the user name set in **User name** is set.	Y
User name	One of the following assigned items selected by **Assign Inventory**: • **Do not set** • **User ID** (user inventory information) • **E-mail** (user inventory information) • **User name** (user inventory information) • **System Configuration Information** The default is **Do not set**.	Y
Location ID	ID corresponding to the location set in **Location**	Y
Location name	One of the following assigned items selected by **Assign Inventory**: • **Do not set** • **Get from the user inventory** The default is **Do not set**.	Y
Status	Among the values of the `AssetStatus` code ID, the item selected by **Assign Inventory** is set. The default is `Active`.	Y
Registration date	Date and time the new asset information was created by acquisition of inventory information	N
SD installed status	**Installed** is set	Y
Modification date of system configuration information	Acquired from **System configuration information last update date** in system configuration information.	Y
Modification date of system information	Acquired from **Last time system information was updated** in system configuration information.	Y
Modification date of software inventory information	Acquired from **Last time software inventory information was updated** in system configuration information.	Y
Modification date of installed package information	**Installed package information last update date** in system configuration information	Y
Modification date of user inventory information	**User inventory information last update date** in system configuration information	Y
Modification date of registry information	Acquired from **Registry information last update date** in system configuration information.	Y
last modification date of the inventory	**Final update date/time** for system configuration information or for deletion history information is set, whichever is more recent	Y

Item name	Value to be set	Whether or not the value is updated when there is existing data
Assigned key	**Node name** in system configuration information	Y
Usage management	Among the values of the `AssetWorkKind` code ID, the item selected by **Assign Inventory** is set. The default is **Used**.	Y
User property	One of the following assigned items selected by **Assign Inventory**: • **Do not set** • **System Configuration Information** • **Code** (code ID `AssetProperty1` to `AssetProperty6`) • **Get from the user inventory** • **Get from the registry** • **Constant value** The default is **Do not set**.	Y

Legend:
Y: Updated
N: Not updated

Note

If **Use asset number** is selected for **Assign key for asset information** in the Server Setup dialog box, the asset number cannot be updated.

If **Use working key** is selected for **Assign key for asset information** in the Server Setup dialog box, and a value other than **Auto** is selected for **Asset No.** in the Assign Inventory window, and the value of the inventory information corresponding to the selected assigned item changes, the asset number also changes. However, the asset number does not change in the following cases:

- The new value duplicates the asset number that was registered in the Asset Information Manager Subset database.
  Duplication of values may occur if **host name**, **IP address**, **MAC address**, or **Computer name** is selected as the assigned item for asset number.
- The most recent information has not been collected by the managing server.

(1) Asset information that can be acquired from a machine on which JP1/Software Distribution is not installed

The following table provides details of Asset Information Manager Subset's asset information that is created and updated on the basis of information acquired from a machine on which JP1/Software Distribution is not installed.

Table 10–12: Details of asset information that can be acquired from a machine on which JP1/Software Distribution is not installed

Item name	Value to be set	Whether or not the value is updated when there is existing data
Asset ID	The value is assigned automatically during creation.	N
Asset type	**Hardware** is set.	N
Asset No.	The value is assigned automatically.	N
Status	If the attribute of the non-Software Distribution host table is `Target`, the `Active` status is set; if it is `Non-target` or `Remove`, the `Erase` status is set.	Y[#]

Item name	Value to be set	Whether or not the value is updated when there is existing data
Registration date	Date and time the new asset information was created by acquisition of inventory information.	N
SD installed status	**Not installed** is set.	Y
Inventory last update date/time	**Final update date/time** is set for machine on which JP1/Software Distribution is not installed.	Y
Usage management	**Unused** is set.	N

Legend:

Y: Updated

N: Not updated

#

The attribute is set to **Erase** only when existing asset information is assigned. If the attribute of a non-Software Distribution host table is `Non-target` or `Remove`, and the item cannot be assigned to an existing device, it will not be registered.

10.9.2 Inventory information that can be acquired as hardware information

The following table lists and describes the hardware information in Asset Information Manager Subset that is created and updated on the basis of the inventory information.

Table 10–13: Details of hardware information that is created and updated on the basis of the inventory information

Item name	Value to be set	Whether or not the value is updated when there is existing data
Asset ID	**Asset ID** of the corresponding asset information	N
Device type	One of the following assigned items selected by **Assign Inventory**: • **OS** in system information • **Code** (system device category code of the `MachineKind` code ID) • **Get from the user inventory** By default, **OS** in the system information is acquired and one of the following values is set according to the type of OS: • **PC** • **UNIX**	Y#
Developer	One of the following assigned items selected by **Assign Inventory**: • **System Configuration Information** • **Get from the user inventory** • **Constant value** By default, the system information **Maker name** is acquired.	Y
Serial number	One of the following assigned items selected by **Assign Inventory**: • **System Configuration Information** • **Get from the user inventory** • **Constant value**	Y

Item name	Value to be set	Whether or not the value is updated when there is existing data
Serial number	By default, JP1/Software Distribution's (06-71 or later) system information **Machine serial number** is acquired.	Y
Device name	One of the following assigned items selected by **Assign Inventory**: • **System Configuration Information** • **Get from the user inventory** • **Constant value** By default, the system information **Model** is acquired.	Y
Processor	**CPU type** in system information	Y
Processor speed	**Processor speed** in system information	Y
Number of processors	**Number of processors** in system information	Y
Memory	**Installed RAM** in system information	Y
Hard disk sizes	**Partition size** in system information	Y
Hard disk free space	**Free space** in system information	Y
Monitor resolution	**Horizontal resolution** and **Vertical resolution** in system information	Y
IP address	**IP address** in system configuration information	Y
MAC address	**MAC address** in system configuration information	Y
Host name	**Host name** in system configuration information	Y
MBSA version	**MBSA** in system configuration information	Y
OS	**Name of OS family** in system information, or **OS** if there is no OS family name	Y
OS version	**OS version** in system information for device type **PC**, and **UNIX OS version** in system information for device type **UNIX**	Y
Computer ID	Acquired from **Computer ID** in system information.	Y
User property	One of the following assigned items selected by **Assign Inventory**: • **Do not set** • **System Configuration Information** • **Code** (`HardwareProperty1` to `HardwareProperty12` code ID) • **Get from the user inventory** • **Get from the registry** • **Constant value** The default is **Do not set**.	Y

Legend:

Y: Updated

N: Not updated

#

Depends on the **Assign Inventory** settings.

(1) Hardware information that can be acquired from a machine on which JP1/Software Distribution is not installed

The following table provides details of Asset Information Manager Subset's hardware information that is created and updated on the basis of information acquired from a machine on which JP1/Software Distribution is not installed.

Table 10–14: Details of hardware information that can be acquired from a machine on which Software Distribution is not installed

Item name	Value to be set	Whether or not the value is updated when there is existing data
Asset ID	**Asset ID** of the corresponding asset information	N
Device type	**PC**	N
IP address	**IP address** in system configuration information	Y
MAC address	**MAC address** in system configuration information	Y
Host name	**Host name** in system configuration information	Y

Legend:

Y: Updated

N: Not updated

10.9.3 Inventory information that can be acquired as network information

The following table lists and describes the network information in Asset Information Manager Subset that is created and updated on the basis of the inventory information.

Table 10–15: Details of network information that is created and updated on the basis of the inventory information

Item name	Value to be set	Whether or not the value is updated when there is existing data
Asset ID	**Asset ID** of the corresponding asset information	N
Network information ID	The value is assigned automatically during creation.	N
IP address[#1]	JP1/Software Distribution's (06-71 or later) system information **IP address** or JP1/Software Distribution's (06-70 or earlier) system configuration information **IP address**	Y
Subnet mask[#2]	**Subnet mask** in system information	Y
IP type	**IPv4**	Y
MAC address	**MAC address** in system information	Y
Node name (host name)	**Host name** in system configuration information	Y
DHCP server name	Corresponding IP group's DHCP server name	Y
Default gateway[#2]	**Default router address** in system information	Y
Computer name	**Computer name** in system information	Y
User property	One of the following assigned items selected by **Assign Inventory**: • **Do not set** • **System Configuration Information** • **System Information**	Y

Item name	Value to be set	Whether or not the value is updated when there is existing data
User property	• **Code** (`NetworkProperty1` to `NetworkProperty2` code ID) • **Get from the user inventory** • **Get from the registry** • **Constant value** The default is **Do not set**.	Y

Legend:

Y: Updated

N: Not updated

#1

The inventory information and network information are assigned by the MAC address. If the IP address corresponding to the MAC address that was acquired from the managing server is different from the existing network information, the IP address is updated by the value acquired from the managing server.

#2

If value acquisition from the managing server fails, the value is acquired from the IP group to which the IP address belongs. If a DHCP server name has been set for the IP group to which the IP address belongs, the value acquired from the IP group takes effect even when the DHCP server name is acquired from the managing server.

10.9.4 Inventory information that can be acquired as installed software information

The following table provides the details of the installed software information in Asset Information Manager Subset that is created on the basis of the inventory information.

Table 10–16: Details of the installed software information that is created on the basis of the inventory information

Item name	Value to be set	Whether or not the value is updated when there is existing data
Asset ID	**Asset ID** of the corresponding asset information	N
Installed software ID	Installed software ID corresponding to the installed package information, software inventory information is acquired from the installed software list.	N
Product ID	**Product ID** in Microsoft Office information. For an OS, **OS serial number** in the system information is acquired. If the software asset does not have a product ID, this information is not acquired.	N
Install date	One of the following information is set according to the type of acquired inventory information: • **Installation date/time** in the installed package information • **OS installation date/time** in the system information • **Installation date/time** in the Microsoft Office information For software inventory information, this information is not acquired.	N
User property	One of the following assigned items selected by **Assign Inventory**: • **Do not set** • **Installed Package Information** • **Software Inventory Information**	Y

Item name	Value to be set	Whether or not the value is updated when there is existing data
User property	• **Code** (`InstalledInfoProperty1` to `InstalledInfoProperty2` code ID) • **Get from the user inventory** • **Constant value** The default is **Do not set**.	Y

Legend:

Y: Updated

N: Not updated

10.9.5 Inventory information that can be acquired as installed software list

The table below provides details of the Asset Information Manager Subset's installed software list that is created and updated on the basis of the inventory information. When an inventory is imported, the installed software list is searched for the corresponding software name and version. If the list contains no corresponding information, the imported information is added to the installed software list.

Table 10–17: Details of the installed software list that is created on the basis of the inventory information

Item name	Value to be set	Whether or not the value is updated when there is existing data
Installed software ID	The value is assigned automatically during creation.	N
Installed software name#1	One of the values according to the type of acquired inventory information: • **Package name** in the installed package information • **Software name** in the software inventory information • **Software name** in Microsoft Office information	N
Installed software version#2	One of the values according to the type of acquired inventory information: • **Package version** in the installed package information • **Software version** in the software inventory information • **Software version** in Microsoft Office information	N
File name	**File names constituting the target software** in software inventory information	N
File size	**Target software creation date/time** in software inventory information	N
File date	**File size of target software** in software inventory information	N
Package former attribute	Acquired from **Packager type** in JP1/Software Distribution installed package information.	U
Package ID	Acquired from **Package ID** in JP1/Software Distribution installed package information.	Y
Managed level	Among the values of the `InstalledInd` code ID, one of the following items is set according to the type of inventory in information: • **Managed object** in the installed package information, software inventory information, Microsoft Office information, or OS information • **Managed object not in license count** in the IE patch information	N

Item name	Value to be set	Whether or not the value is updated when there is existing data
Permission	Among the values of the `Permit` code ID, the item selected by **Assign Inventory** is set. The default is **Permit**.	N
Type	One of the following assigned items selected by **Assign Inventory**: • **Set according to acquired information** • **Code** (`InstalledKind` code ID) By default, **Set according to acquired information** is set, and one of the following values is set according to the acquired installed software information: • **Normally** • **Office products** • **Operating system**	N

Legend:

Y: Updated

U: Updated only when a value is not registered

N: Not updated

#1

For OS information, **Installed software name** is acquired from **Name of OS family** in the system information. If there is no value for **Name of OS family**, **OS sub-version** is acquired. If there is no value for **OS sub-version**, **OS** is acquired.

For patch information for Microsoft Internet Explorer, **Microsoft Internet Explorer Patch** is set.

#2

For OS information, **Installed software version** is acquired from **OS** version in the system information.

Information about Microsoft Internet Explorer patches is acquired from the **IE Patch** system information.

10.9.6 Inventory information that can be acquired as component information

The table below provides details of the Asset Information Manager Subset's component information that is created and updated on the basis of the inventory information. A Microsoft Office information component is registered. If there is no corresponding software component in the asset information, the imported component information is added. Any information that is not in the acquired component information is deleted.

Table 10–18: Details of component information that is created and updated on the basis of the inventory information

Item name	Value to be set	Whether or not the value is updated when there is existing data
Asset ID	**Asset ID** of the corresponding asset information	N
Installed software ID	Installed software ID that corresponds to the **Package name** and **package version** in the installed package information is acquired from the installed software list.	N
Component name	**Software display name** in component information	Y
Component version	**Display version** in component information	Y
Installed parent software ID	**Software indicator ID** in the Microsoft Office information	N

Legend:

Y: Updated

N: Not updated

10.9.7 Inventory information that can be acquired as patch information

The following table provides details of Asset Information Manager Subset's patch information that is created and updated on the basis of the inventory information.

Table 10–19: Details of patch information that is created and updated on the basis of the inventory information

Item name	Value to be set	Whether or not the value is updated when there is existing data
Asset ID	**Asset ID** of the corresponding asset information	N
Patch ID	The patch ID corresponding to **IE Patch** in system information or **Installed name** in installed package information is acquired from the patch name list	N
Installed date	**Installed date** only for installed package information	Y
Applied status	If the information is acquired from system information, **Apply** is set. If the information is acquired from the installed package information and **Package ID** begins with `SUP` or `WUA-SUP`, **Apply** is set; if **Package ID** begins with `BSA`, **Not applied** is set. Note that `BSD` is not supported.	Y

Legend:

Y: Updated

N: Not updated

10.9.8 Inventory information that can be acquired as a patch list

The following table provides details of Asset Information Manager Subset's patch name list that is created and updated on the basis of the inventory information.

Table 10–20: Details of the patch name list that is created and updated on the basis of the inventory information

Item name	Value to be set	Whether or not the value is updated when there is existing data
Patch ID	New numbers are assigned	N
Patch name	**Microsoft Internet Explorer Patch** or **Installed name** in installed package information	N
Version	**IE Patch** in system information or **Installed version** in installed package information	N

Legend:

N: Not updated

10.9.9 Inventory information that can be acquired as virus definition information

The following table provides details of the Asset Information Manager Subset's virus definition information that is created and updated on the basis of the inventory information.

Table 10–21: Details of virus definition information that is created and updated on the basis of the inventory information

Item name	Value to be set	Whether or not the value is updated when there is existing data
Asset ID	**Asset ID** of the corresponding asset information	N
Anti-virus product name	**Software name (only display)** in anti-virus product information	N
Anti-virus product version	**Software version** in anti-virus product information	N
Engine version	**Engine version** in anti-virus product information	Y
Resident/nonresident	**Virus detection resident/nonresident setup** in anti-virus product information	Y
Installation date	**Installed date** in anti-virus product information	Y
Virus definition version	**Virus definition version** in anti-virus product information	N

Legend:

Y: Updated

N: Not updated

10.9.10 Inventory information that can be acquired as group information

If no corresponding group has been registered, the imported inventory information is added to the group information. You can use **Assign Inventory** to specify whether or not to add imported inventory information to group information. For details about the inventory information assignment settings, see *10.8.5 Setting assigned items (Assign Inventory)* in the manual *Administrator's Guide Volume 1*.

The following table provides details of the Asset Information Manager Subset's group information that is created on the basis of the inventory information.

Table 10–22: Details of the group information that is created on the basis of the inventory information

Item name	Value to be set	Whether or not the value is updated when there is existing data
Group ID	The value is assigned automatically.	N
Upper group ID	If there is an upper group, **Group ID** of the upper group	N
Group	Group information indicating the entire hierarchy from the top	N
Group name	Group name acquired from the user inventory information	N

Legend:

N: Not updated

10.9.11 Inventory information that can be acquired as location information

If no corresponding location has been registered, imported inventory information is added to the location information. You can use **Assign Inventory** to specify whether or not to add the imported inventory information to location information. For details about the inventory information assignment settings, see *10.8.5 Setting assigned items (Assign Inventory)* in the manual *Administrator's Guide Volume 1*.

The following table provides details of the Asset Information Manager Subset's location information that is created on the basis of the inventory information.

Table 10–23: Details of the location information that is created on the basis of the inventory information

Item name	Value to be set	Whether or not the value is updated when there is existing data
Location ID	The value is assigned automatically.	N
Upper location ID	If there is an upper location, **Location ID** of the upper location	N
Location	Location information indicating the entire hierarchy from the top	N
Location name	Location name acquired from the user inventory information	N
Attribute	**Area**	N

Legend:

N: Not updated

10.10 Link to Active Directory

Logins to Asset Information Manager Subset can be authenticated, and user information being administered by Active Directory can be stored into the asset management database, by linking to Active Directory.

Active Directory can be linked to if it is running on one of the following operating systems.

- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003

We recommend that the asset management server and Directory Server be run on separate machines.

The following subsections describe the settings required to link to Active Directory.

10.10.1 Login authentication

Directory server usage in the Server Setup dialog box must be selected when authenticating Asset Information Manager Subset logins by linking to Active Directory. For details about the settings in the Server Setup dialog box, see *10.2.4 Setting the link with Directory Server*.

Setting the link with Directory Server

You must look up the information you need to enter in the Server Setup dialog box before you begin.

Reference note

Finding the information you will need to enter is discussed below.

1. Log into the computer running Active Directory as a user with administrator permission.
2. Execute the Active Directory `LDIFDE` command to output the DN information showing the users who can login.
   The command to execute is shown below.
   ```
   ldifde -u -p Subtree -r "objectclass=user" -l dn -f out11.txt
   ```
   Information is written to `out11.txt` as follows.
   ```
   dn: CN=Administrator,CN=Users,DC=Sample,DC=co,DC=jp
   changetype: add
   dn: CN=Guest,CN=Users,CN=Users,DC=Sample,DC=co,DC=jp
   changetype: add
        :
   ```
   Using this information, specify the domain names of the users who will use the Asset Information Manager Subset connection in the Server Setup dialog box's **Access user** field.
3. Execute the Active Directory `LDIFDE` command to output the domain name information of the group to be searched for users when the Asset Information Manager Subset login is authenticated.
   The command to execute is shown below.
   ```
   ldifde -u -p SUBTree -r "(objectclass=organizationalUnit)" -l dn -f out22.txt
   ```
   Information is written to `out22.txt` as follows.
   ```
   dn: OU=Domain Controllers, DC=Sample,DC=co,DC=jp
   changetype: add
   dn: OU=people, DC=Sample,DC=co,DC=jp
   changetype: add
   dn: OU=hitachi,OU=people, DC=Sample,DC=co,DC=jp
   changetype: add
        :
   ```
   Using this information, specify the domain name of the group to be searched for users when authenticating Asset Information Manager Subset login in the Server Setup dialog box's **User information DN** field.
4. Execute the Active Directory `LDIFDE` command to output the attribute information of the user information to be used for authenticating Asset Information Manager Subset login.
   The command to execute is shown below.
   ```
   ldifde -u -p Subtree -r "cn=Administrator" -f out33.txt
   ```

Information is written to `out33.txt` as follows.

```
dn: CN=user1,OU=design3,OU=hitachi,OU=people, DC=Sample,DC=co,DC=jp
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: user1
sn: customerA
telephoneNumber: 030303
givenName: user1
distinguishedName:
CN=user1,OU=design3,OU=hitachi,OU=people, DC=Sample,DC=co,DC=jp
instanceType: 4
    :
displayName: customerA user1
uSNCreated: 376915
uSNChanged: 487476
name: user1
uid: user1
mail: a-user1@sample.co.jp
    :
```

Using this information, specify the attribute name to be used as the user ID when authenticating Asset Information Manager Subset login in the Server Setup dialog box's **User ID attribute name** field. Also specify the attribute name to be recognized as the user name by Asset Information Manager Subset in the Server Setup dialog box's **User name attribute name** field.

Note

The only item that can be provided when authenticating login using Active Directory is the password. User group information must be managed in the Asset Information Manager Subset user information.

10.11 Notes on using Asset Information Manager Subset on a 64-bit OS

(1) Notes on installing Asset Information Manager Subset on a 64-bit OS

Microsoft Internet Information Services must be set up when installing Asset Information Manager Subset on a 64-bit OS.

(a) Using Microsoft Internet Information Services 6.0

To install Asset Information Manager Subset on Windows Server 2003(x64), you must set it so that 32-bit applications can run.

At the command prompt, move the current directory to `%windir%\Inetpub\AdminScripts`, and then execute the following command.

```
cscript.exe adsutil.vbs set W3SVC/AppPools/Enable32BitAppOnWin64 "true"
```

(b) Using Microsoft Internet Information Services 7.0 or 7.5

When installing Asset Information Manager Subset on 64-bit Windows Server 2012, Windows Server 2008 or Windows Server 2008 R2, set **Enable 32-bit Applications** to `True` in the application pool settings that will be used by Web sites that register the Asset Information Manager Subset virtual directory. For details about setting the application pool, see *10.6.2(2) Creating an application pool*.

(2) Notes on executing commands and tasks on a 64-bit OS

To execute Asset Information Manager Subset commands or tasks on a 64-bit OS, the procedure outlined below must be followed.

(a) Executing batch or VBScript

To execute batch or VBScript:

1. Execute the command shown below.

   ```
   %windir%\syswow64\cmd.exe
   ```

   This starts the 32-bit command prompt.
2. At the 32-bit command prompt, execute the Asset Information Manager Subset batch or VBScript.

(b) Registering a task

To register a task:

1. Register a task using the following format.

   `%windir%\syswow64\cmd.exe /c "`*`program-to-be-executed`*`"`

   Examples of this are shown below.

   - `%windir%\syswow64\cmd.exe /c ""C:\Program Files (x86)\HITACHI\jp1asset\exe\jamTakeDMInventory.bat" ALL"`
   - `%windir%\syswow64\cmd.exe /c "cscript.exe "C:\Program Files (x86)\HITACHI\jp1asset\exe\jamSoftwareAddUp.vbs" GENERATION=1"`

11 Configuring a JP1/Software Distribution Cluster System

This chapter describes how to configure an environment for a JP1/Software Distribution cluster system.

11.1 Constructing a JP1/Software Distribution Cluster System

You can use Server and Asset Information Manager Subset of JP1/Software Distribution Manager in a cluster system environment. This section describes how to build an environment when you create a cluster system using JP1/Software Distribution; it also discusses important points that you should take into consideration.

When Embedded RDB is used as the relational database, a configuration that allows mutual monitoring of server and database cannot be achieved because the server facility and the database server cannot be placed on separate PCs.

11.1.1 Programs necessary for creating a cluster system

The following table shows the programs necessary for creating a cluster system.

Table 11–1: Programs necessary for creating a cluster system

Item	Necessary programs
Operating system	Windows Server 2012 Datacenter, Windows Server 2012 Standard, Windows Server 2008 Enterprise, Windows Server 2008 Standard, Windows Server 2003, Enterprise Edition, Windows 2000 Datacenter Server, Windows 2000 Advanced Server
Cluster software	Microsoft Cluster Service, Windows Server Failover Cluster
Management database	• Embedded RDB • Microsoft SQL Server Microsoft SQL Server 2012 Enterprise Microsoft SQL Server 2012 Business Intelligence Microsoft SQL Server 2012 Standard Microsoft SQL Server 2008 Standard#, Microsoft SQL Server 2008 Enterprise#, Microsoft SQL Server 2005 Standard Edition, Microsoft SQL Server 2005 Standard x64 Edition, Microsoft SQL Server 2005 Enterprise Edition, Microsoft SQL Server 2005 Enterprise x64 Edition, Microsoft SQL Server 2000 Enterprise Edition, Microsoft SQL Server 7.0 Enterprise Edition, Microsoft SQL Server 7.0 #: Supports x64 and x86. • Oracle Oracle9i Enterprise Edition, Oracle8i Enterprise Edition To use the failover function, you must have Oracle Fail Safe. Use the same version as the Oracle you are using.
When using Oracle as a management database in a Solaris cluster system environment	Solaris 7 + VERITAS Cluster Server 1.1

11.1.2 Creating an environment that enables failover of JP1/Software Distribution

The following shows how to create an environment in which failover of JP1/Software Distribution is enabled.

If the OS is Windows Server 2008, replace *Cluster Administrator* with *Failover Cluster management*. If the OS is Windows Server 2012, replace *Cluster Administrator* with *Failover Cluster Manager*.

(1) Using Cluster Administrator of Microsoft Cluster Service or Windows Server Failover Cluster to create a group resource

Create a group for JP1/Software Distribution and register the IP address resource, network name resource, and shared disk (physical disk) resource.

The first time Microsoft Cluster Service or Windows Server Failover Cluster is installed, a group named `Cluster Group` is created. Create a new group separately from `Cluster Group`. Also, set the server that is running as the executing server as the primary server.

For details about creating a group resource, see the Microsoft Cluster Service or Windows Server Failover Cluster documentation.

(2) Creating a cluster environment for applying a failover facility to the database server

When using Microsoft SQL Server 2012 or Microsoft SQL Server 2008 in a cluster system

You must use the Microsoft SQL Server installation wizard to set up the failover cluster.

Install Microsoft SQL Server on the local disk of the executing server that is part of the cluster. Then, use the failover cluster wizard to set up the clustering service. For details about installing and setting up Microsoft SQL Server, see the manual for the Microsoft SQL Server. To start installation of the failover cluster, choose **New SQL Server failover cluster installation** at the SQL Server Installation Center. After that, choose **Add node to a SQL Server failover cluster** to add a standby server.

For details about how to install and set up Microsoft SQL Server, see the Microsoft SQL Server documentation.

When using Microsoft SQL Server 2005 in a cluster system

You must use the installation wizard of Microsoft SQL Server to set up the failover cluster.

Install Microsoft SQL Server on the local disk of the executing server that is part of the cluster. The failover cluster setup is started by selecting the **Create a SQL Server failover cluster** check box in the Components to Install dialog box. After the failover cluster setup has executed, add the standby server to **Selected Nodes** in the Cluster Node Configuration dialog box.

For details about how to install and set up Microsoft SQL Server, see the Microsoft SQL Server documentation.

When using Microsoft SQL Server 2000 in a cluster system

You must use the installation wizard of Microsoft SQL Server to set up the failover cluster.

Install Microsoft SQL Server in the local disk of the executing server that is part of the cluster. The failover cluster setup is started by choosing **Virtual Server** and specifying the name of the virtual server. After the failover cluster setup has executed, use **Add Node** to install Microsoft SQL Server in the local disk of the standby server. For details about installing and setting up Microsoft SQL Server, see the manual for the Microsoft SQL Server.

When you use Microsoft SQL Server in a cluster system environment, we recommend that you use TCP/IP for communication between Microsoft SQL Server and clients.

When using Microsoft SQL Server 7.0 in a cluster system

You must use the failover cluster wizard of Microsoft SQL Server to set up the clustering service.

Install Microsoft SQL Server in the local disk of the executing server that is part of the cluster. Then, use the failover cluster wizard to set up the clustering service. For details about installing and setting up Microsoft SQL Server, see the manual for the Microsoft SQL Server.

When using Oracle in a cluster system

Install Oracle Fail Safe Server and other software for configuring an Oracle server in the local disks of the executing server and standby server for which a cluster system is being created. Then, use Oracle Fail Safe Manager to set up the clustering service. Be sure to create an instance of an Oracle database on a shared disk. For details about setting up an Oracle cluster environment, see the manual for Oracle Fail Safe.

(3) Creating an environment for using a failover facility

This subsection describes how to create an environment for using the failover facility of JP1/Software Distribution.

(a) Install JP1/Software Distribution Manager on the executing server

Be sure to install and set up JP1/Software Distribution Manager and then set up Database Manager.

Some settings are not displayed, depending on the components to be installed. For the settings that are not listed in the tables below, set them as usual. For details about the installation, setup, and Database Manager settings, see the following chapters:

- *2. Installing JP1/Software Distribution Manager*
- *4. Setting Up JP1/Software Distribution Manager*
- *7. Setting Up a Relational Database*

The following table shows the settings required when Server and Asset Information Manager Subset of JP1/Software Distribution Manager are installed:

Table 11–2: How to set up JP1/Software Distribution Manager

Program	Item	Setting	Server	AIM Setup#
Installation	Type of JP1/Software Distribution Manager	Choose **Central manager**.	Y	Y
	Components to be installed	Choose **Server** or **Asset Information Manager Subset**, whichever you will be using.	Y	Y
	Installation directory setting	Specify the local drive.	Y	Y
	Database settings (when Microsoft SQL Server is used)	If you have configured Microsoft SQL Server in a cluster system, specify the logical host name or logical IP address as the host name of the database server.	Y	Y
	Database settings (when Oracle is used)	If you have configured Oracle on a failover cluster system, specify the logical host name or logical IP address as the host name of the database server.	Y	Y
	Package storage directory setting	Specify a shared disk.	Y	--
	Software operation history storage directory setting	Specify a shared disk or network drive.	Y	--
	Service setting (for new installation only)	In **Startup type**, select **Manual**.	Y	--
	Connection destination setting (Remote Installation Manager)	Specify a logical host name or logical IP address.	--	Y
	Virtual directory setting for Asset Information Manager Subset	Specify a shared disk.	--	Y
Setup	**Cluster Settings** page	• Select the **Use in a cluster system environment** check box. • Specify JP1/Software Distribution Manager's logical host name with domain name.	Y	--
	Operation Monitoring page	If you select the **Compress and move the operation history to the storage directory** radio button, specify a shared directory under **Storage directory**.	Y	--
	Audit Log page	If you select the **Output audit logs** check box, specify the local disk in **Output directory for audit logs**.	Y	--
SQL Server client network utility	Network library settings	When connecting Microsoft SQL Server in a cluster system, use TCP/IP as the network library	Y	Y

Program	Item	Setting	Server	AIM Setup#
(when Microsoft SQL Server is used)	Network library settings	for connection. Use the SQL client setup utility to add an entry that uses the logical host name for Microsoft SQL Server.	Y	Y
Oracle Net8 Assistant or Net Manager (when Oracle is used)	Create a net service name	Create a net service name in the format `NETM_`*logical-host-name*. If you have configured Oracle on a failover cluster system, specify the logical host name for the destination Oracle as the host name used in the address configuration.	Y	--
Database Manager (for executing system only)	Detailed database settings (for Microsoft SQL Server)	Specify a shared disk for all database files.	Y	--
	Detailed tablespace settings (for Oracle)		Y	--
Database Manager (for Embedded RDB)	Edit HiRDB.ini (Computer on which Server Core facility is installed has more than one NIC)	Specify a logical IP address as the client environment variable PDCLTRCVADDR in the files listed below. JP1/Software-Distribution-installation-directory \Setup_Input\ini\HiRDB.ini JP1/Software-Distribution-installation-directory \Setup_Input_HA\ini\HiRDB.ini	Y	--
	Cluster system environment settings	Select the **Use in a cluster system environment** option, and then select **Execution mode** or **Standby mode**. Specify the logical host name and executing host name.	Y	--
	Management database settings	Specify a shared disk for the management database area path. Specify a local disk for the work table area path. Use the same **Automatically increase the size** check box setting for both active and standby servers.	Y	--
	Detailed database settings	Specify a shared disk for all database files.	Y	--
Asset Information Manager Subset environment setting (creation of data source or net service) (when Oracle is used)	Net service creation	If you have configured Oracle on a failover cluster system, specify the logical host name of the target Oracle for **Server**.	--	Y
Asset Information Manager Subset environment setting (Database Manager) (execution mode only when Microsoft SQL Server or Oracle is used)	Detailed database settings	Specify a shared disk for all database files.	--	Y
Asset Information Manager Subset environment setting (Database Manager) (when Embedded RDB is used)	Cluster system settings	Select the **Use in a cluster system environment** option, and then select **Execution mode** or **Standby mode**. Specify the logical host name and executing host name. Specify the same port number for both active and standby servers.	--	Y
	Detailed database settings	Specify a shared disk for the storage folder name. Specify the same **Storage folder name** and **Size** for both active and standby servers.	--	Y

Legend:

Y: Item that requires setting when the component is selected.

--: Item that does not require setting when the component is selected.

#: AIM Subset: Asset Information Manager Subset

If you have already constructed an environment for JP1/Software Distribution Manager for a configuration in which failover does not occur, open **Control Panel**, choose **Administrative Tools**, and **Services**, double-click the service **Remote Install Server**, and then change the startup type from **Automatic** to **Manual**.

If system restart is requested at the end of the installation procedure for JP1/Software Distribution Manager, restart the computer.

(b) Use Cluster Administrator to move the group.

The standby server becomes the owner of the group.

(c) Install JP1/Software Distribution Manager on the standby server

Construct an environment for the standby server. For details about the installation procedure and settings, see *(a) Install JP1/Software Distribution Manager on the executing server*.

(d) Use Cluster Administrator to move the group.

The standby server becomes the active of the group.

(e) Use Cluster Administrator to create a new JP1/Software Distribution Manager resource.

Tables 11-3 through 11-8 list and describe the settings.

Table 11–3: Resource settings when Server is used

Registered resource	Item	Setting
Remote Install Server	Name	Specify any name.
	Resource type	Set **Generic Service**.
	Group	Set the group name that was created by Cluster Administrator of Microsoft Cluster Service or Windows Server Failover Cluster.
	Executable owner	Set the running system and standby system nodes.
	Dependency	• Set the network name and physical disk that were registered by Cluster Administrator of Microsoft Cluster Service or Windows Server Failover Cluster. • If Microsoft SQL Server or Oracle is used and RDBMS is set to the same group, set the resources for RDBMS. • If Embedded RDB is used, set the resources for HiRDBClusterService_JN1 presented in Table 11-4.
	Generic service parameter	Remote Install Server

	Registry copy#	**For 32-bit OSs**
		`SOFTWARE\HITACHI\NETM/DM`
		For 64-bit OSs
		`SOFTWARE\Wow6432Node\Hitachi\NETM/DM`

#

The *Failover Cluster Manager of* Windows Server 2012 cannot perform the registry copy. In Windows Server 2012, use the Windows PowerShell commandlet. The following shows examples if you specify Remote Install Server for the generic service name.

To add the settings:

Add-ClusterCheckpoint -ResourceName "Remote Install Server" -RegistryCheckpoint SOFTWARE\Wow6432Node\Hitachi\NETM/DM

To check the settings:

```
Get-ClusterCheckpoint -ResourceName "Remote Install Server" -RegistryCheckpoint
```

To delete the settings:

```
Remove-ClusterCheckpoint -ResourceName "Remote Install Server" -RegistryCheckpoint
```

Table 11–4: Resource settings for HiRDB/ClusterService_JN1 when Embedded RDB is used

Registered resource	Item	Setting
HiRDBClusterService_JN1	Name	Specify any name.
	Resource type	Set **Generic Service**.
	Group	Set the group name that was created by Cluster Administrator of Microsoft Cluster Service or Windows Server Failover Cluster.
	Executable owner	Set the running system and standby system nodes.
	Dependency	Set the network name and physical disk that were registered by Cluster Administrator of Microsoft Cluster Service or Windows Server Failover Cluster.
	Generic service parameter	HiRDBClusterService_JN1
	Registry copy	Not specified

Use Cluster Administrator to set the generic-service resource Remote Install Server to online. Thereafter, to stop and start the Remote Install Server service, use Cluster Administrator to set it to offline or online.

Table 11–5: Resource settings when Asset Information Manager Subset is used

Registered resource	Item	Setting
Asset Information Synchronous Service	Name	Specify any name.
	Resource type	Set **Generic Service**.
	Group	Set the group name that was created by Cluster Administrator of Microsoft Cluster Service or Windows Server Failover Cluster.
	Executable owner	Set the running system and standby system nodes.
	Dependency	• Set the network name and physical disk that were registered by Cluster Administrator of Microsoft Cluster Service or Windows Server Failover Cluster. • If Microsoft SQL Server or Oracle is used and RDBMS is set to the same group, set the resources for RDBMS. • If Embedded RDB is used, set the resources for HiRDBClusterService_AM1 presented in Table 11-6.
	Generic service parameter	AssetInformationSynchronousService
	Registry copy	Not specified

Table 11–6: Resource settings for HiRDB/ClusterService_AM1 when Embedded RDB is used

Registered resource	Item	Setting
HiRDBClusterService_AM1	Name	Specify any name.
	Resource type	Set **Generic Service**.

Registered resource	Item	Setting
HiRDBClusterService_AM1	Group	Set the group name that was created by Cluster Administrator of Microsoft Cluster Service or Windows Server Failover Cluster.
	Executable owner	Set the running system and standby system nodes.
	Dependency	Set the network name and physical disk that were registered by Cluster Administrator of Microsoft Cluster Service or Windows Server Failover Cluster.
	Generic service parameter	HiRDBClusterService_AM1
	Registry copy	Not specified

Table 11–7: Resource settings for Microsoft Internet Information Services when Asset Information Manager Subset is used (for Windows 2000 and Windows Server 2003)

Registered resource	Item	Setting
Microsoft Internet Information Services	Name	Specify any name.
	Resource type	Set the following value: **For Windows 2000** IIS Server Instance **Windows Server 2003** General-purpose script
	Group	Set the group name created by Microsoft Cluster Service's Cluster Administrator.
	Executable owner	Set the running system and standby system nodes.
	Dependency	Set the network name and physical disk registered by Microsoft Cluster Service's Cluster Administrator.
	Parameter (for Windows 2000)	Set to the service that is used for failover. In **IIS**, select the **WWW** radio button, and then select **Default Web Site** in the **IIS Server** combination box.
	Script file path (for Windows Server 2003)	Set the following value: `%systemroot%\System32\Inetsrv\Clusweb.vbs`

Table 11–8: Resource settings for Microsoft Internet Information Services when Asset Information Manager Subset is used (for Windows 2008)

Resource type	Content input to script file path	Dependency
Generic script	`%systemroot%\System32\Inetsrv\Clusweb.vbs`	Set the **Shared disk** and **Client access point** resources.

#

By default, the script file (`Clusweb.vbs`) for setting resources in the Windows Server 2008 cluster environment is not installed. If the IIS6 Management Compatibility IIS script tool is installed by execution of a Microsoft Internet Information Services 7.0 role service, the script file is stored in the prescribed path (`%systemroot%\System32\Inetsrv`).

Therefore, the IIS script tool should be installed before setting resources in a cluster environment. For details about installation methods, see the Microsoft Internet Information Services manual. If you use Microsoft Internet Information Services 7.5 and install the IIS script tool of IIS 6 Management Compatibility, Clusweb.vbs will not be created. Refer to the Microsoft support information KB97059 on the web, and obtain the generic sample script.

(4) Creating an environment for a system directly under JP1/Software Distribution Manager

To set up an environment for a relay system or client immediately below JP1/Software Distribution Manager:

1. In the TCP/IP definition, set the logical host name or IP address for JP1/Software Distribution Manager.
2. Perform the setup.
   Specify the logical host name and logical IP address in the settings for the higher server at the connection destination.

(5) Specifying the connection destinations for using components

When you want to use the facilities of JP1/Software Distribution, specify the logical host name or logical IP address of the connection destination during installation.

The following table shows how to specify the connection destination for each component you use.

Table 11–9: Specifying the connection destinations for using components

Component	Name of dialog box	Setting
Server core facility	Server Setup (**AIM** page)	If you have constructed Asset Information Manager Subset on a failover cluster system, specify the connection-target logical host name or logical IP address in **URL for Asset Information Manager**.
Remote Installation Manager	Specify Connection Destination (installer)	For the connection destination of Remote Installation Manager, specify the logical host name or logical IP address.
	Software Distribution Manager Logon (Logon window)	
Packager	Specify Connection Destination	Specify a logical host name or logical IP address for Packager's connection destination.

(6) Settings for an environment containing a firewall

When you use JP1/Software Distribution Manager in a cluster system configuration containing a firewall, specify the logical and physical addresses for the nodes that data passes through.

(7) Actions to be taken after a failover

The table below shows the actions that should be taken by the user in the event of a failover. If you use an Oracle cluster environment as a relational database environment, you can continue the application without re-connection due to a communication error.

Table 11–10: Actions to be taken by the user after a failover

No.	When failover occurred	Action to be taken after the failover
1	While starting the Inventory Viewer of Remote Installation Manager	After a dialog box appears indicating a communication error or a database access error, reconnect to the JP1/Software Distribution server.
2	While registering a job	After a dialog box appears indicating a communication error or a database access error, re-register the job.
3	While a job was waiting for execution	Re-execute the job.
4	While a job was being executed (20%)	Re-execute only the failed job (you do not need to take any action for a job waiting for execution, a job resulting in a startup error, a suspended job, a job placed in installation-rejecting status, a completed job, or a normally terminated job)
5	While re-executing a job that was executed at least 20%	For jobs contained in the job execution status folder *RETRY_RELAY_SYSTEM*, perform steps 3 and 4.

No.	When failover occurred	Action to be taken after the failover
6	After editing an ID group (adding/deleting the relay managing the ID, adding/deleting clients, or changing the password)	For the jobs contained in the job execution status folder *Edit ID Group*, perform steps 3 and 4.
7	When the options that are enabled on the **System Configuration** page in JP1/Software Distribution Manager's Server Setup dialog box are **Apply the system configuration information automatically** and **Linkage when system configuration is changed**	For jobs contained in the job execution status folder *Edit System Configuration Information*, perform steps 3 and 4.
8	While editing a job definition	After a dialog box appears indicating a communication error or a database access error, re-create a new job definition. The job definition you were editing is invalid, so delete it.
9	While executing the CSV output utility	After a dialog box appears indicating a communication error or a database access error, re-execute the job.
10	While executing Database Manager	After a dialog box appears indicating a database access error, take appropriate action for the situation. • When a new database is being created: Delete the database and then re-execute the job. • While management files are being moved: Delete the database, re-create it, and then re-execute the job. • While the database is being restored: Restore the database from its backup and then re-execute the job. • While the database is being upgraded: Restore the database from its backup and then re-execute the job. • When a resource is being moved to a file system: Delete all the files from the package storage directory and then re-execute the job. • For other cases: Restart Database Manager.
11	While executing a command	Re-execute the command that returned the communication error or connection error.
12	While the packager was packaging software	After a dialog box appears indicating a communication error, use Remote Installation Manager to delete the failed packages and then re-execute packaging.
13	While a client was being registered into an ID group or being deleted from an ID group	After a dialog box appears indicating a communication error, re-execute registration into the ID group or deletion from the ID group.
14	While Package Setup Manager was installing a package	After the error is detected, reinstall the package.
15	While the Operation Log List window is displayed	Close the Operation Log List window, and then re-display it.
16	While *Data maintenance* and *Take operation history* tasks are executing	The tasks are cancelled. Re-execute the tasks.

11.1.3 Disabling failover of JP1/Software Distribution

If failover of JP1/Software Distribution is disabled, use the normal procedures to install and set up the central manager, relay managers, relay systems, and clients.

Note the following about creating a cluster system that does not use a failover facility:

- As the installation directory and the directories for various settings, specify the local disk.

- In an environment that does not use a failover facility, specify the physical host name or physical IP address of the cluster server as the connection destination for a system to which the central manager, relay managers, and relay systems are connected.

11.1.4 Notes on using a cluster system

When using a failover facility, note the following:

- If JP1/Base is linked to manage JP1/Software Distribution users, register JP1/Software Distribution Manager in the same cluster groups as for JP1/Base. For the logical host name of JP1/Software Distribution Manager, specify the same logical host name as for JP1/Base.
- When an application error occurs and an error message is notified from Dr. Watson, failover may fail. You can prevent this by suppressing notification of error messages. For details about how to suppress error message notification, see the OS manual.

  Note that if you suppress error message notification, information acquisition in the event of an application error may be adversely affected.
- If an application error occurs when the OS being used is Windows Server 2003, a dialog box reporting the error to Microsoft is displayed. When this dialog box is displayed, failover may fail. You can prevent this by suppressing reporting of errors. For details about how to suppress error reporting, see the OS manual.
- When you stop or start a service, use Cluster Administrator to place the generic-service resource Remote Install Server offline or online. If you stop or start the service by choosing **Control Panel**, **Administrative Tools**, and then **Services**, a failover may occur depending on the resource settings.
- When the generic-service resource Remote Install Server is offline, any change to the registry information may not be applied. Therefore, note the following points:

  When installing or uninstalling JP1/Software Distribution Manager (for Embedded RDB)

  You must place the generic-service resources Remote Install Server, HiRDB/ClusterService_JN1, and HiRDB/ClusterService_AM1 offline.#

  Before you place HiRDB/ClusterService_JN1 offline, execute the netmdb_stop.bat command that is stored in *JP1/Software-Distribution-Manager-installation-directory*`\BIN` to terminate the Embedded database. Before you place HiRDB/ClusterService_AM1 offline, execute the jamemb_dbstop.bat command that is stored in *JP1/Software-Distribution-installation-directory*\jp1asset\exe to terminate the Embedded database.

  Check the message to make sure that each Embedded RDB has terminated.

  #: Required when Asset Information Manager Subset is used.

  Additionally, delete the **Registry Copy** settings in the generic-service resource Remote Install Server. After installing or uninstalling JP1/Software Distribution Manager, add the settings again according to the description in *11.1.2 Creating an environment that enables failover of JP1/Software Distribution*.

  If you perform the installation without deleting those settings, the installed component may not function correctly.

  When installing or uninstalling JP1/Software Distribution Manager (for Microsoft SQL Server or Oracle)

  You must place the generic-service resource Remote Install Server offline. If you start the installer or uninstaller when the generic-service resource is online, a failover may occur or the installer or uninstaller may fail (freeze or terminate abnormally) depending on the resource settings.

  Also, delete the Registry Copy entry for the generic-service resource Remote Install Server. After installing or uninstalling JP1/Software Distribution Manager, add the settings again according to the description in *11.1.2 Creating an environment that enables failover of JP1/Software Distribution*. If you perform the installation without deleting that entry, the installation component may not work correctly.
- The *registry copy* of Cluster Administrator does not support the window size, arrangement pattern, and other display information for the Remote Installation Manager at the execution server. Therefore, the Remote Installation Manager at the standby server does not inherit this information.
- If a failover occurs, the relational database server automatically restores the database. While the relational database server is restoring the database, you cannot connect the database. Therefore, wait a while and then re-connect the database.
- If you have installed only Remote Installation Manager in the cluster system and a failover occurs during execution of *Define User Inventory* or *Define Registry Collection*, it may not be possible any longer to execute *Define User Inventory* or *Define Registry Collection* from a machine other than the executing server.

In such a case, perform recovery and then execute *Define User Inventory* or *Define Registry Collection* from the executing server. Alternatively, restart JP1/Software Distribution Manager (Remote Install Server service) to which the Remote Installation Manager is connected.

- When you set up the system directly below the cluster system, specify the settings in such a manner that the total amount of time required for retries in the event of a communication error (retry interval **x** retry count) is greater than the time required for failover.

  If the time required for failover is greater than the total amount of time required for retries and failover occurs during job execution (execution status: 20%), the maximum retries may be reached during failover processing, in which case the job may not be restarted after failover.
- If you have constructed Asset Information Manager Subset on a failover cluster system in a Windows Server 2003 environment, and if control is passed from the executing system to the standby system due to failover, and then passed again from the standby system back to the executing system due to another failover, you must restart the World Wide Web Publishing Service.

11.1.5 How to reconfigure a cluster system environment

This subsection describes how to perform overwrite installation and reinstallation of JP1/Software Distribution Manager in a cluster system environment.

(1) How to perform overwrite installation of JP1/Software Distribution Manager in a cluster system environment

If you use an Embedded RDB relational database, you must overwrite the database in both the active and standby servers to upgrade JP1/Software Distribution Manager in a cluster system environment.

To perform overwrite installation of JP1/Software Distribution Manager:

1. Delete the **Registry Copy** settings in the generic-service resource Remote Install Server.

   If you perform overwrite installation without deleting the **Registry Copy** settings, the installed components may not function correctly.
2. Place the generic-service resource Remote Install Server offline.
3. Place the generic-service resource Asset Information Synchronous Service offline.
4. Execute the `netmdb_stop.bat` command stored in *JP1/Software-Distribution Manager-installation-directory* `\BIN`.

   Check the message to make sure that Embedded RDB has stopped.
5. Place the generic-service resource HiRDB/ClusterService_JN1 offline.
6. Execute the `jamemb_dbstop.bat` command stored in *JP1/Software-Distribution-installation-directory* `\jp1asset\exe`.

   Check the message to make sure that Embedded RDB has stopped.
7. Place the generic-service resource HiRDB/ClusterService_AM1 offline.#
8. Install JP1/Software Distribution Manager on the executing server by overwriting.
9. Place the generic-service resource HiRDB/ClusterService_JN1 online.
10. Use Database Manager to upgrade the database from **Upgrade database**.

    In the Cluster System Environment Settings dialog box, specify the settings in the same manner as when a new database is created.
11. Place the generic-service resource HiRDB/ClusterService_AM1 online.#
12. From the **Start** menu, choose **Software Distribution Manager**, **Asset Information Manager**, **Setup**, and then **Database Manager** to upgrade the database by using **Upgrade the database**.#
13. Execute the netmdb_stop.bat command that is stored in *JP1/Software-Distribution-Manager-installation-directory* `\BIN` to terminate the database. Check the message to make sure that Embedded RDB has terminated.
14. Place the generic-service resource HiRDB/ClusterService_JN1 offline.

15. Execute the jamemb_dbstop.bat command that is stored in *JP1/Software-Distribution-installation-directory* \jp1asset\exe to terminate the database. Check the message to make sure that Embedded RDB has terminated.#
16. Place the generic-service resource HiRDB/ClusterService_AM1 offline.#
17. As the cluster system administrator, move the group and set the owner to the standby server.
18. Install JP1/Software Distribution Manager by overwriting at the standby server.
19. Execute steps 9 and 16 at the standby server.
20. As the cluster system administrator, move the group and set the owner to the executing server.
21. Enter the **Registry Copy** settings for the generic-service resource Remote Install Server.

    Enter the settings according to the information provided in *11.1.2 Creating an environment that enables failover of JP1/Software Distribution*.
22. Place the generic-service resource Remote Install Server online.
23. Place the generic-service resource Asset Information Synchronous Service online.#

#: Required when Asset Information Manager Subset is used.

(2) How to reinstall JP1/Software Distribution Manager in a cluster system environment

If you re-install JP1/Software Distribution Manager at the active and standby servers after you have configured a cluster system environment, you must follow the procedure below:

1. Use the `netmdb_unload.bat` command to make a backup of the database.
2. Uninstall JP1/Software Distribution Manager from the active and standby servers.
3. Install JP1/Software Distribution Manager and configure a cluster system environment.
4. Use the `netmdb_reload.bat` command to restore the database from the backup.

Appendixes

A. How to Upgrade and Migrate JP1/Software Distribution

This appendix describes how to upgrade JP1/Software Distribution, how to migrate data when you change the type of database and when you replace a PC, and how to migrate the JP1/Software Distribution environment.

A.1 Upgrading JP1/Software Distribution

This appendix describes how to upgrade JP1/Software Distribution and provides notes on upgrading.

To upgrade an entire JP1/Software Distribution system, you begin with the higher system programs in the sequence indicated below.

To upgrade JP1/Software Distribution:

1. Upgrade the central manager and relay managers
2. Upgrade the database
3. Upgrade the relay systems
4. Upgrade the clients

Settings that were applicable before upgrading are inherited by the upgraded programs. During installation, each dialog box displays the existing settings before upgrading; you can change settings as necessary.

For the notes on upgrading JP1/Software Distribution, see *(5) Notes about upgrading*.

(1) Upgrading the central manager and relay managers

You upgrade JP1/Software Distribution Manager at the central manager and at the relay manager computers.

If you are using a basic database with JP1 Version 7i or earlier, you must create a relational database.

(2) Upgrading the database

After upgrading JP1/Software Distribution Manager, you must use Database Manager to upgrade the relational database.

It is strongly recommended that you make a backup of your relational database before upgrading it. For details about making a backup, see *5.3 Backing up and restoring the system* in the manual *Administrator's Guide Volume 2*.

If you are using a basic database with JP1 Version 7i or earlier, use Database Manager to migrate data from the basic database to the relational database created in (1).

For details about how to use Database Manager, see *7.4 How to use Database Manager (for Embedded RDB)* or *7.5 How to use Database Manager (for Microsoft SQL Server or Oracle)*.

If you have upgraded the Asset Information Manager Subset component, you must use Database Manager of Asset Information Manager Subset to upgrade the Asset Information Manager Subset relational database. For details about how to upgrade the database, see *10.3.2 Upgrading the database*.

(3) Upgrading the relay systems

You upgrade JP1/Software Distribution on the relay system computers.

If you are using JP1/Software Distribution SubManager JP1 Version 7i or earlier, upgrade it to JP1/Software Distribution Client (relay system). You can use the remote installation facility to distribute JP1/Software Distribution Client (relay system) from JP1/Software Distribution Manager.

If you are using JP1/Software Distribution SubManager JP1 Version 7i or earlier, and you are upgrading the product and replacing the PC at the same time, you should first upgrade the relay system to JP1/Software Distribution Client (relay system) and then replace the PC according to the procedure described in *A.4 Migrating data when replacing a PC*. JP1/Software Distribution Client (relay system) JP1 Version 8 or later cannot restore data from a backup acquired by JP1/Software Distribution SubManager JP1 Version 7i or earlier.

(4) Upgrading the clients

You upgrade JP1/Software Distribution Client on the client computers. You can use the remote installation facility to distribute JP1/Software Distribution Client from JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system)

(5) Notes about upgrading

You should note the following points about upgrading JP1/Software Distribution:

- If you upgrade a machine on which both JP1/Software Distribution Manager and JP1/Software Distribution SubManager are installed from a version earlier than JP1 Version 7i to JP1 Version 8 or later, you must uninstall JP1/Software Distribution Manager or JP1/Software Distribution SubManager.

  JP1 Version 8 or later does not allow JP1/Software Distribution Manager and JP1/Software Distribution Client (relay system) to be installed on the same machine.
- If you upgrade from JP1/Software Distribution 08-10 or earlier to version 08-51 or later, some job menus will not be displayed in the GUI of Asset Information Manager Subset. To display all available job menus, follow the steps below after you have upgraded the database:
  1. Log on to Asset Information Manager Subset.
  2. From the job category **System Definition**, click the job menu **Customize Job Menu**.
     The Customize Job Menu window appears.
  3. Select the **Software Applied Management**, **Software Applied Status**, and **Distribution Status** check boxes.
  4. Click the **Update** button.
- If you install JP1/Software Distribution Client (relay manager) JP1 Version 8 or later by overwriting a JP1/Software Distribution SubManager JP1 Version 7i or earlier in which Remote Control Manager was installed, your Remote Control Manager will be deleted.
- If you are using any of the following relational databases with JP1/Software Distribution JP1 Version 7i or earlier, you will also need to upgrade the relational database when you upgrade JP1/Software Distribution:
  - Oracle8i R8.1.5 or R8.1.6
  - Oracle8
  - Microsoft SQL Server 6.5

  When you upgrade your relational database because you have upgraded your JP1/Software Distribution to JP1 Version 7i or later, make sure that you follow the steps below:
  1. Make a backup of JP1/Software Distribution database.
  2. Upgrade the relational database to a version supported by JP1 Version 7i or later.
  3. Upgrade JP1/Software Distribution Manager.
  4. Use Database Manager to upgrade the JP1/Software Distribution database.
     For details about how to upgrade the JP1/Software Distribution database using Database Manager, see *7.5.4 Upgrading the database*.
- If you are migrating from an environment that uses a basic database for JP1 Version 7i or earlier to an environment for JP1 Version 8 or later and changing the ID key for operations during installation, you must first delete some information. For details about the information to be deleted, see *4.2.8(2) Notes on changing the node identification key*.
- If you are upgrading from JP1/Software Distribution Manager JP1 Version 7i or earlier, make sure that a job executing split package distribution has terminated before you start the upgrade process. If upgrading is attempted while a split distribution job is executing, there may be no display of the split distribution progress, or the progress display may not be correct. Note that this has no effect on the distribution processing itself.
- If you have upgraded a JP1/Software Distribution Client version earlier than 05-24 to version 06-00 or later, registry information may no longer be acquired. Before you acquire registry information, re-transfer the registry items to be acquired.
- If you are using the operation monitoring function, you must restart the computer after upgrading JP1/Software Distribution Client (relay system) or JP1/Software Distribution Client (client).

- If you have upgraded JP1/Software Distribution, you may need to execute a *Get software information from client*. For notes on on upgrading JP1/Software Distribution, see *3.2.3 Notes on collecting software information* in the manual *Administrator's Guide Volume 1*.

A.2 Changing the database type

This section describes how to migrate data and the types of data that can be migrated when you change the type of relational database used in your JP1/Software Distribution system.

You must use the procedure described here in the following cases:

- When you change from Embedded RDB to Microsoft SQL Server
- When you change from Microsoft SQL Server to Oracle
- When you change from Oracle to Embedded RDB
- When you change from Microsoft SQL Server 2000 or earlier to Microsoft SQL Server 2012#
  #: This change must be preceded by OS upgrading or migration to another machine. If you are upgrading the OS, see *A.3 Migrating data during OS upgrading*. If you are migrating data to another machine, see *A.4 Migrating data when replacing a PC*. In this case, replace the term *database backup and restore* with *data migration*.

You should note the following when you are using Asset Information Manager Subset:

- In Embedded RDB and Oracle, searches are case sensitive as the default. If you are migrating from Embedded RDB and Oracle to Microsoft SQL Server, set **Binary** as the database matching sequence so that upper-case letters can be distinguished from lower-case letters.
- If you are migrating from Microsoft SQL Server to Embedded RDB and Oracle, upper-case letters are distinguished from lower-case letters during searches after the migration. However, if you are using Embedded RDB, you can also set the searches to not be case sensitive by specifying the server setup setting **Case sensitivity in LIKE searches (Embedded RDB)**.

(1) How to migrate a database

To migrate a relational database:

1. Export the data that is to be transferred from JP1/Software Distribution Manager.
   For details about the data to be transferred, see *(2) Transferable data*.
2. Uninstall JP1/Software Distribution Manager.
3. Install JP1/Software Distribution Manager Embedded RDB Edition.
   Use the installer to set up the database after the change.
4. Create a database for JP1/Software Distribution Manager Embedded RDB Edition.
5. Import the data that was exported in step 1.

(2) Transferable data

The following table describes the data that can be transferred to JP1/Software Distribution Manager Embedded RDB Edition and the methods for importing and exporting each type of data:

Transferable data	Export method	Import method
System configuration information#1	In the System Configuration window, choose **File**, and then **Save to File**.	In the System Configuration window, choose **File**, and then **Create from File**.
Host group	In the Destination window, choose **File**, and then **Save to File**.	• In the Destination window, choose **File**, and then **Create from File**. • In the Destination window, choose **File**, and then **Add from File**.#2

Transferable data	Export method	Import method
ID group	In the Destination window, choose **File**, and then **Save ID Hosts to File**.	In the Destination window, choose **File**, and then **Use File for ID Registration**.
Policies for host groups and ID groups	In the Policy Setup dialog box, click the **Output File** button.	In the Policy Setup dialog box, click the **Add from File** button.
Package	Execute the `dcmpkget` command.	Execute the `dcmpkput` command.
Software search list	In the List of Software Information window, choose **File**, and then **Save to File**.	In the List of Software Information window, choose **File**, and then **Create from File**.
List of user inventory items	In the Define User Inventory dialog box, click the **Export** button.	In the Define User Inventory dialog box, click the **Import** button.
User inventory information	Use the CSV output utility to output the template of user asset information to a CSV file.	In the System Information or Destination window, choose **File**, and then **Input from CSV File**.
Software inventory	Execute the `dcmdice` command.	Execute the `dcmdici` command.

#1

If managing servers are configured in a hierarchy, the file output at the central manager does not include system configuration information about hosts under relay managers. To obtain system configuration information about hosts under relay managers, output system configuration information to a file at each relay manager.

To restore the system configuration information, import the system configuration information from the relay managers, and then execute a *Get system configuration information* job from the central manager to the relay managers.

#2

This menu is displayed only in Remote Installation Manager of JP1/Software Distribution Manager.

A.3 Migrating data during OS upgrading

This section describes how to upgrade the OS in a computer where JP1/Software Distribution is installed.

To upgrade the OS in a computer where JP1/Software Distribution Manager or JP1/Software Distribution Client is installed, you must first make a backup and then uninstall JP1/Software Distribution Manager and JP1/Software Distribution Client.

If you use AMT Linkage with JP1/Software Distribution Manager (relay manager) or JP1/Software Distribution Client to store host IDs, the assets are treated as being the same as before migration by the higher system because the host IDs can be restored after data migration. For details about how to store clients' host IDs, see *6.5.1 Storing the client's host ID* in the manual *Description and Planning Guide*.

When you make the backup and when you restore from the backup, you must stop the JP1/Software Distribution services. In the case of JP1/Software Distribution Manager, you must stop the Remote Install Server service. In the case of JP1/Software Distribution Client, you must stop the client from the client manager.

To upgrade the OS:

1. Make a backup of JP1/Software Distribution Manager and JP1/Software Distribution Client.

   For details about the data to be backed up, see *5.3 Backing up and restoring the system* in the manual *Administrator's Guide Volume 2*.

2. Uninstall JP1/Software Distribution Manager and JP1/Software Distribution Client.

   For details about how to uninstall, see *1.4 Uninstalling JP1/Software Distribution*.

3. Upgrade the OS.

4. Install a new JP1/Software Distribution Manager and JP1/Software Distribution Client.

   If you are using AMT Linkage with JP1/Software Distribution Manager (relay manager) or JP1/Software Distribution Client to store host IDs, the host IDs that were used prior to uninstallation are restored.

5. Restore from the backup.

A.4 Migrating data when replacing a PC

This section describes how to migrate current data for JP1/Software Distribution Manager and JP1/Software Distribution Client when a PC is replaced.

When you make a backup and when you restore from the backup, you must stop the JP1/Software Distribution services. For details about the services to be stopped, see *5.3 Backing up and restoring the system* in the manual *Administrator's Guide Volume 2*.

If an information file for higher connection destinations has been distributed to the clients and the IP address of a PC set as the connection destination has been changed, delete the information file for higher connection destinations from the clients. Automatic change of connection destination occurs when the IP address is changed.

(1) Migrating data for JP1/Software Distribution Manager

To migrate data when a PC used as JP1/Software Distribution Manager (central manager or relay manager) is replaced:

1. Make a backup from the PC before you replace the PC.

   For details about the data to be backed up, see *5.3.1 Manually backing up JP1/Software Distribution Manager* in the manual *Administrator's Guide Volume 2*.

   If you use an Embedded RDB relational database, use the command for data migration (`netmdb_unload.bat`) when you back up the database.
2. Copy the host ID management file acquired in step 1 (`netmdmp.hid`) to the Windows installation target directory on the new PC (for a relay manager).
3. After replacement of the PC, install JP1/Software Distribution Manager on the new PC.

   If you are using Asset Information Manager Subset, select **Asset Information Manager Subset** as an installed component before you start installation of JP1/Software Distribution Manager.
4. Use the Database Manager to create a new database (applicable to Embedded RDB).

   For details about how to use the Database Manager, see *7.4 How to use Database Manager (for Embedded RDB)*.
5. Restore the backup obtained in step 1.

   For details about how to restore a backup, see *5.3.5 Restoring JP1/Software Distribution Manager* in the manual *Administrator's Guide Volume 2*.

   If you use an Embedded RDB relational database, use the command for data migration (`netmdb_reload.bat`) when you restore the database.

(2) Migrating data for JP1/Software Distribution Client

To migrate data when the PC for JP1/Software Distribution Client (relay system or client) is replaced:

1. Make a backup from the PC before you replace the PC.

   For details about the information that must be backed up for JP1/Software Distribution Client (relay system), see *5.3.3 Backing up JP1/Software Distribution Client (relay system)* in the manual *Administrator's Guide Volume 2*.

   For details about the information that must be backed up for JP1/Software Distribution Client (client), see *5.3.4 Backing up JP1/Software Distribution Client (client)* in the manual *Administrator's Guide Volume 2*.
2. Copy the host ID management file acquired in step 1 (`netmdmp.hid`) to the Windows installation target directory in the new.
3. After replacement of the PC, install JP1/Software Distribution Client on the new PC.
4. Restore from the backup made in step 1 to the installation destination in step 3.

   For details about how to restore JP1/Software Distribution Client (relay system), see *5.3.6 Restoring JP1/Software Distribution Client (relay system)* in the manual *Administrator's Guide Volume 2*.

   For details about how to restore JP1/Software Distribution Client (client), see *5.3.7 Restoring JP1/Software Distribution Client (client)* in the manual *Administrator's Guide Volume 2*.

(3) Data migration using Asset Information Manager Subset

To migrate data when a PC that uses Asset Information Manager Subset is to be replaced:

1. Make a backup on the PC that is to be replaced.

   With the Asset Information Manager Subset database manager, make a backup from the **Back up the database to CSV files** menu. For details about how to operate the database manager, see *10.3.3 Backing up the database as CSV files*.
2. Install JP1/Software Distribution Manager on the new PC.

   Select **Asset Information Manager Subset** as the component to be installed and then install JP1/Software Distribution Manager.
3. At the server setup of Asset Information Manager Subset, set **Login ID** and **Service name** in **Database Information**.
4. Create a new Asset Information Manager Subset database.
5. Restore the database from the backup.

   With the Asset Information Manager Subset database manager, restore the database from the backup using the **Restore the database from CSV files** menu. For details about how to operate the database manager, see *10.3.4 Restoring the CSV database files*.

If you use Asset Information Manager Subset after you have restored the backup, start the services in the following order:

1. JP1/Client Security Control - Manager services (applicable if JP1/Client Security Control is linked)
2. Commands and tasks of the Asset Information Synchronous Service and Asset Information Manager Subset
3. World Wide Web Publishing Service or World Wide Web Publishing
4. IIS Admin Service or IIS Admin

A.5 Upgrading the version in a cluster system environment

This section describes the procedures for upgrading JP1/Software Distribution Manager in a cluster system environment. When upgrading JP1/Software Distribution added to a new version, the settings displayed in the dialog boxes are inherited from the previous version. Change these settings, as necessary.

(1) If using Embedded RDB

If you are using Embedded RDB, the databases being used by the running system and the standby system must be overwritten when upgrading the cluster system environment JP1/Software Distribution to a new version. The procedure to do this is outlined below.

To upgrade the version when using Embedded RDB:

1. Place the following generic service resources in offline status.#
   - Asset Information Synchronous Service
   - Microsoft Internet Information Services
2. Delete the settings for Registry Copy, a generic service resource of Remote Install Server.
3. Place Remote Install Server generic service resources in offline status.
4. Execute the command `netmdb_stop.bat` in the JP1/Software Distribution Manager installation target directory `\BIN`.

   Check the message to confirm that Embedded RDB has stopped.
5. Place HiRDB/ClusterService_JN1 generic service resources in offline status.
6. Execute the `jamemb_dbstop.bat` command in the JP1/Software Distribution installation target directory `\jp1asset\exe`.#

   Check the message to confirm that Embedded RDB has stopped.

7. Place HiRDB/ClusterService_AM1 generic service resources in offline status.#
8. Perform an overwrite installation of JP1/Software Distribution Manager in the running system server.
9. Place HiRDB/ClusterService_JN1 generic service resources in online status.
10. In Database Manager, execute the database upgrade from **Upgrade database**.

    In the Cluster system environment settings dialog box, enter the same values as you would when creating a new database.
11. Place HiRDB/ClusterService_AM1 generic service resources in online status.#
12. From the **Start** menu, choose **Software Distribution Manager**, **Asset Information Manager**, **Setup**, and then **Database Manager**. Then, execute the database upgrade from **Upgrade the database**.#
13. Execute the command `netmdb_stop.bat` in the JP1/Software Distribution Manager installation target directory `\BIN`.

    Check the message to confirm that Embedded RDB has stopped.
14. Place HiRDB/ClusterService_JN1 generic service resources in offline status.#
15. Execute the `jamemb_dbstop.bat` command in the JP1/Software Distribution installation target directory `\jp1asset\exe`.#

    Check the message to confirm that Embedded RDB has stopped.
16. Place HiRDB/ClusterService_AM1 generic service resources in offline status.#
17. Working as the cluster system administrator, move the group and make its owner the standby system server.
18. Perform an overwrite installation of JP1/Software Distribution Manager in the standby system server.
19. Repeat steps 9 through 16 in the standby system.
20. Working as the cluster system administrator, move the group and make its owner the running system server.
21. Place the following generic service resources in offline status.
    - HiRDB/ClusterService_AM1#
    - HiRDB/ClusterService_JN1
    - Remote Install Server
22. Enter the appropriate settings into the Remote Install Server generic service resource Registry Copy.

    Enter the settings as instructed in *11.1.2 Creating an environment that enables failover of JP1/Software Distribution*.
23. Place the following generic service resources in online status.#
    - Microsoft Internet Information Services
    - Asset Information Synchronous Service

#: These tasks are required if you are using Asset Information Manager Subset.

A.6 Transferring data in a cluster system environment

This section describes how to transfer JP1/Software Distribution Manager data when replacing the cluster system environment server.

Tasks to execute on the server prior to replacement

1. Place the following generic service resources in offline status.
    - Asset Information Synchronous Service#
    - Microsoft Internet Information Services#
    - Remote Install Server
2. Create a backup.

For details about the content that that needs to be backed up, see *5.3.1 Manually backing up JP1/Software Distribution Manager* in the manual *Administrator's Guide Volume 2*. If you are using Embedded RDB as the relational database, use the migration command (`netmdb_unload.bat`) to back up the database.

Tasks to execute on the server after replacement

1. Install JP1/Software Distribution Manager and create the cluster system environment.

   If you are using Asset Information Manager Subset, choose **Asset Information Manager Subset** as an installed component before you start installation of JP1/Software Distribution Manager.#

   For details about creating a cluster system environment, see *11.1.2 Creating an environment that enables failover of JP1/Software Distribution*.
2. Place the following generic service resources in offline status.
   - Asset Information Synchronous Service#
   - Microsoft Internet Information Services#
   - Remote Install Server
3. Restore the backup from step 2 of the tasks you executed on the server prior to replacement.

   For details about methods for restoring a database, see *5.3.5 Restoring JP1/Software Distribution Manager* in the manual *Administrator's Guide Volume 2*.

   If you are using Embedded RDB as the relational database, use the migration command (`netmdb_unload.bat`) to back up the database.

#: These tasks are required when using Asset Information Manager Subset.

B. Using JP1/Software Distribution Client (Client) on a Terminal Server

JP1/Software Distribution Client (client) can be installed and run on the following terminal servers.

- Windows Server 2012 and Windows Server 2008 R2 where a Remote Desktop session host is running
- Windows Server 2008 and Windows Server 2003 where the terminal server is running
- Windows 2000 Server, or Windows 2000 Advanced Server where the terminal service created in the application server mode is running

When using JP1/Software Distribution Client (client) on a terminal server, there are restrictions on how to install and operate the software, and on certain functions. In order to remote install the software, the terminal server mode must be changed.

This appendix describes how to use JP1/Software Distribution Client (client) on a terminal server. It also describes the limitations that occur when using JP1/Software Distribution Client (client) in a Citrix XenApp environment.

B.1 Limitations when using JP1/Software Distribution Client (client) on a terminal server

The following limitations apply when using JP1/Software Distribution Client (client) on a terminal server.

Installation restrictions

- An installation set cannot be used to install JP1/Software Distribution Client (client).
- Install the JP1/Software Distribution Client (client) in the same way you would install any application on a terminal server.

Operation restrictions

- You cannot do offline installations.
- If you log on with non-Administrator user permissions, you cannot install packages in the following cases:
  - The client was stopped by the Client Manager.
  - The **Client starts automatically at system boot** check box on the **Default Running Status/Polling** page and the **Use the Package Setup Manager or Execute Job Backlog command when a client is not resident** check box on the **Security** page are both cleared.
- Even if the **Prompt users before deletion whenever a shortcut in Software Distribution Client startup fails** check box is selected on the **Notification Dialog Box** page during client setup, a dialog box that asks whether or not unexecutable icons and shortcuts are to be deleted is not displayed.
- JP1/Software Distribution Client (client) applications cannot be used as the terminal service RemoteApp program.

B.2 Remotely installing software on a terminal server

If you are installing software on a terminal server, change the terminal service mode to installation mode before you install and return it to execution mode after installation is finished.

! Important note

Perform remote installation carefully, because mode change affects the entire terminal service.

The remote installation method depends on the software package type and installation method, as described below:

- When another company's software or a Hitachi program product is installed remotely
- When JP1/Software Distribution Client (client) is installed remotely

- When software is installed from Package Setup Manager

The following describes the installation method for each case:

(1) When another company's software or a Hitachi program product is installed remotely

When you remotely install another company's software or a Hitachi program product, specify appropriate information during packaging so that the terminal service mode changes before and after the installation.

To remotely install another company's software or a Hitachi program product:

1. In the Software Distribution Package dialog box, on the **External Program** page, specify the following commands:
   - Immediately before installation: `change user /install`
   - Immediately after installation: `change user /execute`
2. In the External Program Options dialog box, which is displayed by clicking the **Details** button on the **External Program** page, specify the following settings:
   - **End status is notified by**: **Exit code**
   - **When an external program error occurs, the job**: **Continues**
3. Specify other applicable items and then execute packaging.
   The software is packaged.
4. Remotely install the package created in step 3.
   Before installation, the terminal service is placed in the application installation mode and the software is installed. When installation is complete, the terminal service is placed back in the application execution mode.

(2) When JP1/Software Distribution Client (client) is installed remotely

When you remotely install JP1/Software Distribution Client (client), specify the appropriate information during packaging so that the terminal service mode changes before installation. Separately from the job for installing JP1/Software Distribution Client(client), execute a job to change the terminal service mode after installation. To do this, you must install the appropriate files.

To remotely install JP1/Software Distribution Client(client):

1. In the Software Distribution Package dialog box, on the **External Program** page, specify the following command:
   - Immediately before installation: `change user /install`

   When JP1/Software Distribution Client (client) is installed remotely, the system ignores specification of a command that is to be executed immediately after installation.
2. In the External Program Options dialog box, which is displayed by clicking the **Details** button on the **External Program** page, specify the following settings:
   - **End status is notified by**: **Exit code**
   - **When an external program error occurs, the job**: **Continues**
3. Specify other applicable items, and then execute packaging.
   JP1/Software Distribution Client (client) is packaged.
4. Remote install the package created in step 3.
   Before installation, the terminal service is placed in the application installation mode and JP1/Software Distribution Client (client) is installed.
   Next, create a job for placing the terminal service back in the previous mode after installation.
5. In the Software Distribution Packager window, select desired files, and then from the **Run** menu, choose **Packaging**.
   Make sure that the selected files can be safely installed on the JP1/Software Distribution Client (client). Choosing **Packaging** displays the Software Distribution Package dialog box.

6. In the Software Distribution Package dialog box, on the **External Program** page, specify the following commands:
   - Immediately after installation: `change user /execute`
7. In the External Program Options dialog box, which is displayed by clicking the **Details** button on the **External Program** page, specify the following settings:
   - **End status is notified by**: **Exit code**
   - **When an external program error occurs, the job**: **Continues**
8. Specify other applicable items, and then execute packaging.
   The files are packaged.
9. Confirm that the remote install from step 4 has terminated, and then remote install the package created in step 8.
   The files are installed and the terminal service is placed back in the application execution mode.

(3) When software is installed from Package Setup Manager

When you install a package from Package Setup Manager, change the terminal service mode directly at the PC that executes installation.

To install software from Package Setup Manager:

1. At the command prompt, enter `change user /install` and execute.
   The terminal service is placed in the application installation mode.
2. Use the Package Setup Manager to select a package, and then execute installation.
   The selected software is installed.
3. After installation is complete, at the command prompt, enter `change user /execute`, and then execute.
   The terminal service is placed back in the application execution mode.

B.3 Limitations on using JP1/Software Distribution Client (client) in a Citrix XenApp environment

JP1/Software Distribution Client (client) can be installed in the following OS machines with Citrix XenApp (open-source desktop):

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003

Note that Citrix XenApp open-source applications are not supported.

Set up a JP1/Software Distribution Client (client) to be used on a Windows Server 2003 Citrix XenApp environment (open-source desktop) as follows. JP1/Software Distribution Client (client) will stop functioning if these settings are changed.

- On the **Default Running Status/Polling** page of the client setup, select the **Client starts automatically at system boot** check box.
- On the **Permissions** page of the client setup, select the **Run the client with non-Administrator user permissions** check box.
- Create the registry value shown below in registry key `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hitachi\NETM/DM/P` (for 32-bit operating systems, use registry key `HKEY_LOCAL_MACHINE\SOFTWARE\HITACHI\NETM/DM/P).`

  Name

  `EnableRDP`

  Type

  `REG_SZ`

Data

```
YES
```

C. Using JP1/Software Distribution Client (Client) in a Windows XP Mode Environment

The following products can be installed and used in a Windows XP Mode environment.

- JP1/Software Distribution Client 09-50 or later (client)

The following limitations on installation, setup, and functionality apply when using JP1/Software Distribution Client (client) in a Windows XP Mode environment.

This appendix describes how to operate JP1/Software Distribution Client (client) in a Windows XP Mode environment.

JP1/Software Distribution Client (client) operation when using virtual applications

If JP1/Software Distribution Client (client), installed in a Windows XP Mode environment, is set up to be resident, starting a virtual application also starts JP1/Software Distribution Client (client).

C.1 Notes on installation and setup of JP1/Software Distribution Client (client) in a Windows XP Mode environment

(1) Notes on installation

Installation procedure

JP1/Software Distribution Client (client) is installed in a Windows XP Mode environment following the same procedure as for a normal installation. For details about the JP1/Software Distribution Client (client) installation procedure, see *3. Installing JP1/Software Distribution Client*.

Components that can be used

There are limitations on the JP1/Software Distribution Client (client) components that can be used in a Windows XP Mode environment. Therefore, when the Select Components dialog box is displayed during the installation, only select components that can be used in a Windows XP Mode environment. Other components can be selected, but they may not operate correctly, so it is not safe to select them.

JP1/Software Distribution Client (client) components that can be used in a Windows XP Mode environment are listed in *Tables C-1* to *C-3*.

Table C–1: Components that can be used in a Windows XP Mode environment (JP1/Software Distribution Client)

Component		Usable?
Client	Client	Y
	Additional facilities	Y
	Package Setup Manager	Y
	Distribution facility using Visual Test 6.0	Y
	AMT Linkage	N
Relay System		N
Package		Y
Remote Control Agent#	Remote control agent	N
	Chart	N
Automatic Installation Tool		Y

Component	Usable?
Startup Kit Support Tool	N
Online Help	Y

Legend:

Y: Usable

N: Not usable

--: Not Applicable

#

To perform remote operations in a Windows XP Mode environment, install a remote control agent in the host OS (Windows 7), and then perform operations through the host OS (Windows 7).

(2) Notes on client setup

The Client resident/polling page

When using virtual applications, startup requests may not be accepted and polling may not always be performed even if the **Client resident** check box and **Polling** check box have been selected.

The reason for this is that when the virtual application terminates, Windows XP Mode goes into sleep status and the JP1/Software Distribution Client (client) running in Windows XP Mode environment stops. If instructions requesting execution arrive from a managing server when Windows XP Mode is asleep, they will be executed when the virtual application starts. Therefore, the execution interval and execution date/time you set for the job are ignored.

The Dial-up page

JP1/Software Distribution Client (client) running in the Windows XP Mode environment does not support dialup connections. Do not select the **Dial-up connection** check box.

C.2 Notes on using JP1/Software Distribution Client (client) in a Windows XP Mode environment

(1) Before starting operation

Network configuration

Manage JP1/Software Distribution Client (client) installed in a Windows XP Mode environment in accordance with the network settings as shown below.

Shared networks (NAT) or bridge mode

Manage as usual.

Internal networks

Use one of the following methods.

- Managed as an offline machine.
- A managing server and a host operating system capable of communication (Windows 7) can be managed as relay systems via the host OS (Windows 7).

Not connected to a network

Manage as an offline machine.

Windows XP Mode environment settings

When using JP1/Software Distribution Client (client) in a Windows XP Mode environment, make sure the following check boxes are cleared in **User Accounts** under the Control Panel.

- **Use Welcome Screen** check box
- **Use Fast User Switching** check box

Selecting these check boxes may make JP1/Software Distribution Client (client) unusable.

(2) Notes on job management

Timing of job execution

When executing a job from JP1/Software Distribution Client (client) installed in a Windows XP Mode environment, setting the job execution timing to **When client starts** may result in the job not being executed at the intended time.

For example, if a virtual application is started while Windows XP Mode is being used, Windows XP Mode will be restarted. This results in Windows XP Mode being restarted without the JP1/Software Distribution Client (client) user being aware of the fact.

Client control

If the Windows XP Mode combine facility is enabled or virtual applications are in use, the computer cannot be shut down automatically after job execution.

(3) Notes on software distribution (remote installation)

Recording of AIT files

If virtual applications are in use, AIT files cannot be recorded in the Windows XP Mode environment.

Installer displays

If virtual applications are in use, the installer is displayed full screen on the host OS (Windows 7) when remote installing JP1/Software Distribution Client (client) in a Windows XP Mode environment.

(4) Notes on managing inventory information

To identify JP1/Software Distribution Client (client) installed in a Windows XP Mode environment from acquired inventory information, check the system information items OS and owner. In the Windows XP Mode environment, the following values are displayed for these items.

Table C–2: Values displayed for system information items

System information item	Value displayed
OS	Windows XP Professional
Owner	Windows XP Mode

(5) Notes on operation monitoring functions

Operation monitoring policy settings

To monitor operation of JP1/Software Distribution Client (client) installed in a Windows XP Mode environment, apply the operation monitoring policy not just to the host OS (Windows 7) but to the Windows XP Mode environment as well.

Acquiring operating information

Acquire operating information not just from the host OS (Windows 7) but from the Windows XP Mode environment as well.

Note also that Windows XP Mode information, not Windows 7 information, will be used for the logon users and accounts in the operation history and suppression history acquired from the JP1/Software Distribution Client (client) installed in a Windows XP Mode environment.

Note that running virtual applications will be seen as use of software in the Windows XP Mode environment.

D. Installing and Setting Up HP-UX JP1/Software Distribution Network Node Manager Linkage

To link with the HP-UX version of HP NNM version 7.5 or earlier, the HP network administration manager requires JP1/SD Network Node Manager Linkage. This appendix describes how to install and set up JP1/Software Distribution Network Node Manager Linkage.

D.1 Installing the JP1/Software Distribution Network Node Manager Linkage

To run the JP1/Software Distribution Network Node Manager Linkage, use Hitachi Program Product Installer. The superuser privilege is required to run Hitachi Program Product Installer.

(1) Installing Hitachi Program Product Installer

If Hitachi Program Product Installer is not installed, you must set the provided media in your drive and execute the following command. If Hitachi Program Product Installer is installed, you do not need to perform these operations.

`tar xf` *device-file-name*

For *device-file-name*, specify a file name that is appropriate in your environment. Also, specify a device file that does not have rewind capability.

(2) Running Hitachi Program Product Installer

Ensure that the provided media is set in the drive, and then execute the following command.

When a list of products that can be installed is displayed, select **JP1/Software Distribution Linkage** and start installation.

`/etc/hitachi_setup -i` *device-file-name*

For *device-file-name*, specify a file name that is appropriate in your environment. Also, specify a device file the does not have rewind capability.

D.2 Uninstalling the JP1/Software Distribution Network Node Manager Linkage

To uninstall the JP1/Software Distribution Network Node Manager Linkage, use Hitachi Program Product Installer. The superuser privilege is required to run Hitachi Program Product Installer.

Make sure that the background process of HP NNM version 7.5 or earlier is started when you uninstall this facility.

D.3 Setting up the JP1/Software Distribution Network Node Manager Linkage

To set up the JP1/Software Distribution Network Node Manager Linkage:

1. Log in as a superuser.
   Make sure that the background process of HP NNM version 7.5 or earlier is started.
2. Execute the `/opt/NETMDM_NNM/bin/dmnnm_install` command.
   This command registers files required for registering JP1/Software Distribution symbols and menus in HP NNM.
3. Execute the `/opt/NETMDM_NNM/bin/dmnnm_setup -s` command.
   The following screen appears. Choose **(2) Setup**.

```
# dmnnm_setup -s
```

```
** JP1/Software Distribution NNM Linkage Setup **
The host name or IP address of the OpenView Linkage Gateway Server to be connected
Current setting: [ ]
1)*Next
2) Setup
3) Cancel
- > 2
Specify the host name or IP address of the OpenView Linkage Gateway Serve to be
connected.
- > dmp195
```

4. Specify the host name or IP address of the OpenView Gateway Server.

   Specify the host name or the IP address of the OpenView Gateway Server to be connected to HP NNM, then press the **Enter** key. The following screen appears.

```
The port number used to connect the OpenView Linkage Gateway Server
1)*Next
2) Setup
3) Cancel
- > 2
Specify the port number used to connect with the OpenView Linkage Gateway Server.
- > 20049
```

5. Specify the port number that should be used for communication with the OpenView Gateway Server.

   Specify the port number that should be used when an attempt to access JP1/Software Distribution management information is made from HP NNM. Use the port number that should be set during setup for the OpenView Gateway Server. When you press the **Enter** key, the following screen appears.

```
* Set the following items. *
The host name or IP address of the OpenView Linkage Gateway Server to be connected:
[ dmp195 ]
The port number used to connect with the OpenView Linkage Gateway Server:
[ 20049 ]
1)*Apply the Setup
2) Cancel
- > 1
Setup completed.
#
```

6. Confirm the specified values.

   When you choose **Apply the Setup**, the specified values will be applied to the configuration file.

E. Using Internet Options to Install JP1/Software Distribution

Internet Options is a facility that converts the JP1/Software Distribution's protocol to HTTP, making it possible to use JP1/Software Distribution over the Internet. Internet Options consists of Internet Gateway and HTTP Gateway.

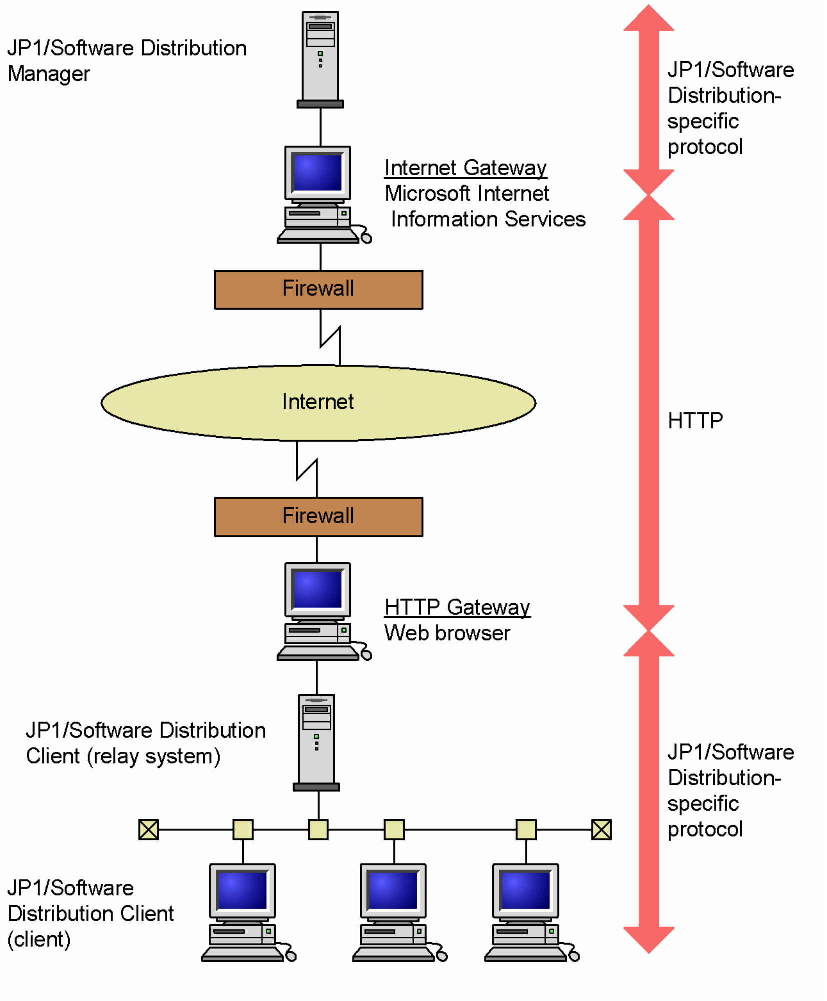
E.1 Overview of Internet Options

(1) HTTP Gateway

You can place Internet Gateway and HTTP Gateway between any JP1/Software Distribution nodes to convert the communications protocol between those nodes from the JP1/Software Distribution-specific protocol to HTTP. Therefore, if your environment is Web-enabled, JP1/Software Distribution can be used over the Internet without the need for complex setup. If HTTP is already enabled through a firewall and if you use the Internet option, you do not need to perform the firewall setup described in *6.1.5 Using JP1/Software Distribution in a firewall environment* in the manual *Description and Planning Guide*.

The following figure shows protocol conversion using Internet Options.

Figure E–1: Protocol conversion using Internet Options


JP1/Software Distribution Manager
Internet Gateway
Microsoft Internet Information Services
Firewall
Internet
Firewall
HTTP Gateway
Web browser
JP1/Software Distribution Client (relay system)
JP1/Software Distribution Client (client)
JP1/Software Distribution-specific protocol
HTTP
JP1/Software Distribution-specific protocol

(2) Secure communications using SSL

Internet Options support HTTPS using SSL, so the security level is therefore maintained.

(3) Splitting transfer data

Depending on your proxy server and the Web server, the maximum data size that can be sent at one time may be limited. In such a case, the Internet Options can split a file to be sent by JP1/Software Distribution into smaller sizes.

(4) Auto-dialing

When HTTP Gateway and client are installed on a notebook computer and you connect to the Internet with a dial-up connection, you can use the auto-dialing facility to establish connection.

E.2 Job flow via Internet Options

Normally, the client executes a job on receipt of a job execution request from the managing server. However, in an Internet environment, job execution requests from the managing server cannot reach the clients because the internal network is concealed or the NAT facility is used to translate addresses for security purposes. Communication using Internet Options is performed at the following times:

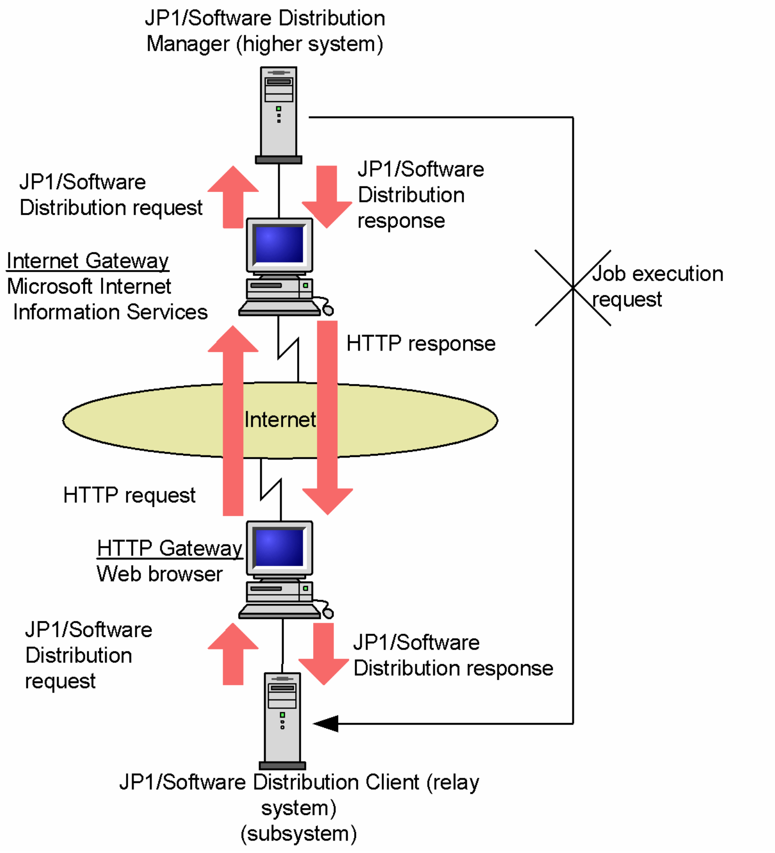
- At periodic polling by a relay manager/system or client
- On execution of the Package Setup Manager at a client
- When a user chooses the **Execute Job Backlog** icon at a client

Jobs are executed as a result of requests from these lower systems.

HTTP Gateway converts JP1/Software Distribution requests from lower systems to HTTP and sends the request to the specified Internet Gateway. Internet Gateway extracts the JP1/Software Distribution message from the HTTP request and sends it to the higher system. It also converts the response from the higher system into an HTTP response and sends it to the request source. The Web server (Microsoft Internet Information Services) is used for processing HTTP.

The following figure shows the job flow via Internet Options.

Figure E–2: Job flow via Internet Options


JP1/Software Distribution Manager (higher system)
JP1/Software Distribution request
JP1/Software Distribution response
Internet Gateway
Microsoft Internet Information Services
Job execution request
HTTP response
Internet
HTTP request
HTTP Gateway
Web browser
JP1/Software Distribution request
JP1/Software Distribution response
JP1/Software Distribution Client (relay system) (subsystem)

Note that job execution requests from the higher system are not received by the lower system. You must therefore set 0 in **Max. number of subsystems in which jobs can execute concurrently** in the setup for the higher system. Also, because jobs are executed only when there is a request from a lower system, you must set up polling for the lower system.

For details about setting up the higher and lower systems, see *E.5(5) Setting up the higher system*, and *E.6(5) Setting up the lower system*.

E.3 Notes on using Internet Options

Observe the following notes on the use of JP1/Software Distribution when using Internet Options:

- You cannot use packaging with HTTP Gateway.
- JP1/Software Distribution uses host names, IP addresses, and host IDs as the ID key for operations (key information for identifying nodes). JP1/Software Distribution compares the created job with the key for operations. If the NAT facility is used, the address is converted and the job is not given to the appropriate client. This is because the IP address of the JP1/Software Distribution Client (client) for the JP1/Software Distribution Manager differs, due to the NAT facility, from the actual IP address of the JP1/Software Distribution Client (client). In an environment using the NAT facility, you cannot therefore use IP addresses as the key for operations. We recommend using host IDs.
- When you use IP addressing, the IP address is used in the protocol and may be leaked. Therefore, if you are using a firewall, we recommend not using IP addresses.
- The automatic registration facility for the system configuration in JP1/Software Distribution uses the IP address in the protocol regardless of what key is used for operations. Therefore, there is a risk of the IP address used in the protocol being leaked if you use the automatic registration facility for the system configuration. If you are using a firewall, we recommend not using the automatic registration facility for the system configuration.
- To improve security with a basic firewall configuration, the general recommendation is a network configuration that separates the segment with the external public server (unprotected segment) from the private network. In most such configurations, communication is limited between the unprotected segment and the private network. To enable communication between the Web server and JP1/Software Distribution, set the filtering table of the firewall product as follows:

  IP address of sender: IP address of Microsoft Internet Information Services

  Sending port: 1024-65535

  IP address of receiver: IP address of JP1/Software Distribution higher system

  Receiving port: NETMDM

  Protocol: TCPEST

  Direction: in
- You cannot use the remote control facility via Internet Options.

E.4 System configuration

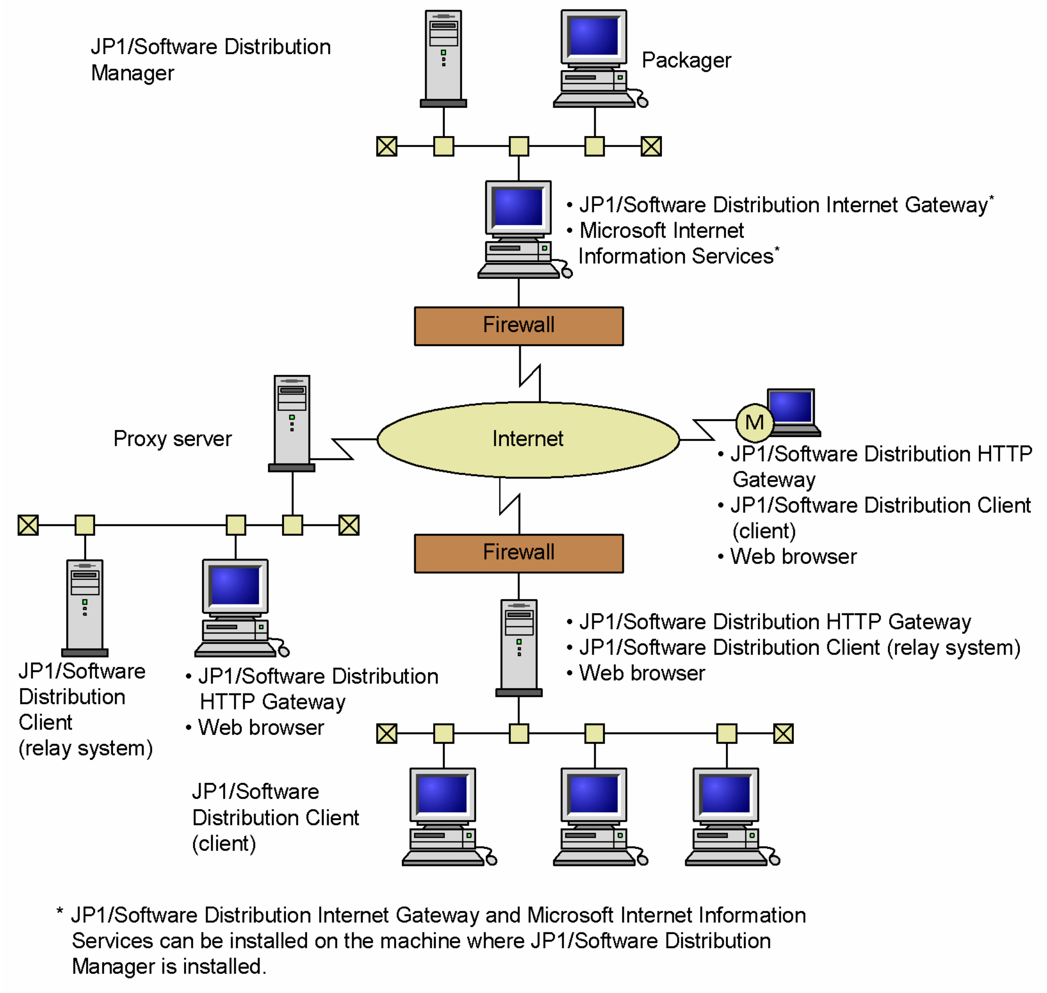
To convert JP1/Software Distribution's protocol to HTTP, place Internet Gateway and HTTP Gateway between the JP1/Software Distribution nodes where you want to use HTTP. Place Internet Gateway at the higher system on the route using HTTP, and place HTTP Gateway at the lower system.

Once you have installed Internet Gateway and HTTP Gateway, they are handled transparently without being recognized by the managing server as a level in the hierarchy.

Note that the higher system directly connected to Internet Gateway must be running JP1/Software Distribution version 06-71 or later. Similarly, the lower system directly connected to HTTP Gateway must be running JP1/Software Distribution version 06-71 or later.

The following figure shows the JP1/Software Distribution system configuration when using Internet Options.

Figure E–3: JP1/Software Distribution system configuration when using Internet Options


JP1/Software Distribution Manager
Packager
• JP1/Software Distribution Internet Gateway*
• Microsoft Internet Information Services*
Firewall
Proxy server
Internet
M
• JP1/Software Distribution HTTP Gateway
• JP1/Software Distribution Client (client)
• Web browser
Firewall
• JP1/Software Distribution HTTP Gateway
• JP1/Software Distribution Client (relay system)
• Web browser
JP1/Software Distribution Client (relay system)
• JP1/Software Distribution HTTP Gateway
• Web browser
JP1/Software Distribution Client (client)

* JP1/Software Distribution Internet Gateway and Microsoft Internet Information Services can be installed on the machine where JP1/Software Distribution Manager is installed.

(1) Internet Gateway

The number of HTTP Gateways that can be connected to an Internet Gateway depends on the higher system connected to Internet Gateway. When the higher system is a central manager, we recommend between 50 and 100. When the higher system is a SubManager, we recommend between 20 and 50.

Internet Gateway can be installed on the same machine as the higher system.

(a) Minimum system requirements

Resource	Requirement
CPU	At least 1 GHz (2 GHz or more recommended)
Memory	1,000 + 50 **x** number of simultaneous HTTP Gateway connections (KB unit: kilobytes)
Disk space	5 megabytes + number of simultaneous HTTP Gateway connections x size of packages to be distributed However, when using split distribution, calculate the required disk space using the following formula: 5 megabytes + number of simultaneous HTTP Gateway connections **x** size package is split into

(b) Operating system

Windows Server 2003, Windows XP Professional, Windows 2000, or Windows NT Server 4.0

(c) Required software

Microsoft Internet Information Services 5.0 or later, or Microsoft Internet Information Server 4.0 or later must be installed.

In this appendix, Microsoft Internet Information Services 5.0 and later and Microsoft Internet Information Server 4.0 and later are referred to collectively as Microsoft Internet Information Services, unless otherwise noted.

(2) HTTP Gateway

You must have HTTP Gateway on each directly connected lower system. If there are multiple clients, place a relay system directly under HTTP Gateway.

HTTP Gateway can be installed on the same machine as the lower system.

(a) Minimum system requirements

Resource	Requirement
CPU	At least 1 GHz (2 GHz or more recommended)
Memory	3,000 kilobytes
Disk space	5 megabytes + size of package to be distributed However, when using split distribution, calculate the required disk space using the following formula: 5 megabytes + size package is split into

(b) Operating system

Windows Server 2003, Windows XP, Windows 2000, Windows NT 4.0, Windows Me, or Windows 98

(c) Required software

Microsoft Internet Explorer 5.01 or later must be installed.

(3) Proxies and firewalls

You can use transparent proxies compatible with HTTP 1.0 and later. Transparent proxies are proxies that require authentication for access and certification of the client itself. Transparent proxies do not make any changes to requests and responses. You can also use packet filtering firewalls that allow HTTP to pass through, and application gateway firewalls.

Internet Options is compatible with proxies and firewalls that do not require settings at the client.

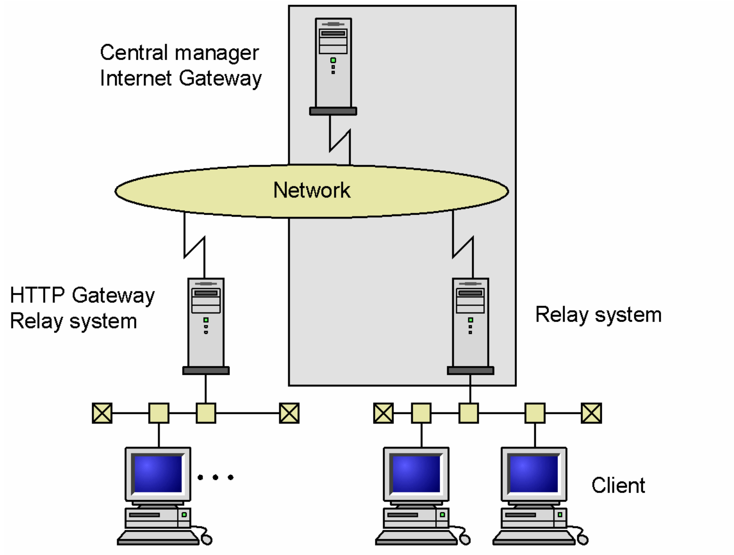
The following are representative of products with applicable proxies:

- Microsoft Proxy Server 2.0
- Sun ONE Web Proxy Server

(4) Notes on system configuration

When you use Internet Options, job execution requests from a higher system are not received by the lower system. Jobs are executed only in response to requests from a lower system. Therefore, as shown in the figure below, when the system is configured so that only some of the lower systems use HTTP Gateway, jobs are executed only in response to requests from a lower system even between the relay systems that do not use HTTP Gateway and the central manager (shaded area in the figure).

Figure E–4: System configuration in which HTTP Gateway is used solely in some lower systems



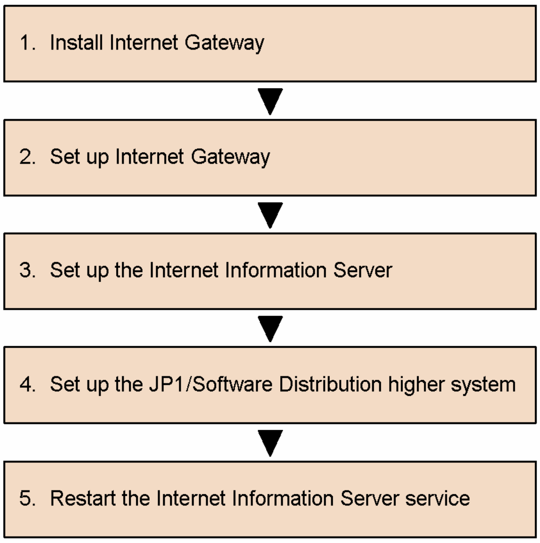
E.5 Setting up Internet Gateway

To run Internet Gateway on your system, you must install Internet Gateway and set it up. You must also set up the Microsoft Internet Information Services and the higher system.

(1) Setup procedure

The following figure shows the procedures for setting up Internet Gateway, Microsoft Information Services, and higher systems.

Figure E–5: Internet Gateway setup procedures


1. Install Internet Gateway
2. Set up Internet Gateway
3. Set up the Internet Information Server
4. Set up the JP1/Software Distribution higher system
5. Restart the Internet Information Server service

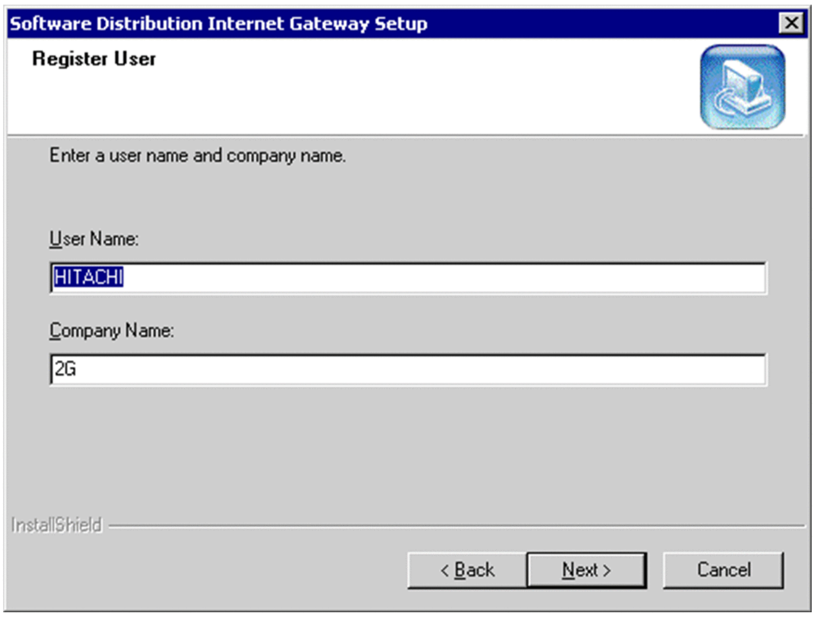
(2) Installing Internet Gateway

Because Internet Options is a background service that converts protocols, no icon is added to the **Start** menu when Internet Gateway is installed. After Internet Gateway is installed, use **Control Panel** to make the required settings. When installed, Internet Gateway functions as an ISAPI.

To install Internet Gateway:

1. Insert the Internet Gateway installation medium into the CD-ROM drive.
   The Software Distribution Internet Gateway Setup dialog box appears.
2. Choose the **Next** button.
   The Register User dialog box appears.

Figure E–6: Register User dialog box



Software Distribution Internet Gateway Setup

Register User

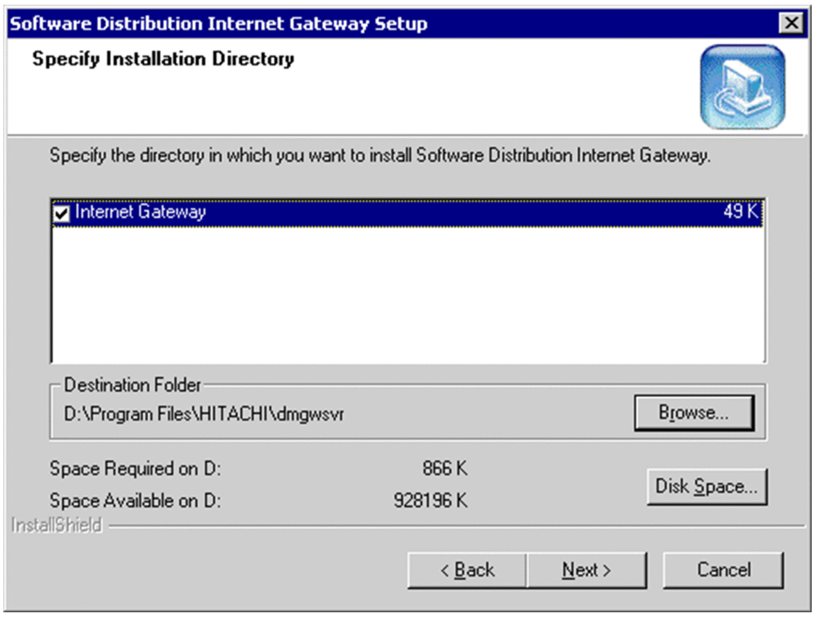
Enter a user name and company name.

User Name: HITACHI

Company Name: 2G

3. Enter the user name and company name, then choose the **Next** button.
   The Specify Installation Directory dialog box appears.

Figure E–7: Specify Installation Directory dialog box



Software Distribution Internet Gateway Setup

Specify Installation Directory

Specify the directory in which you want to install Software Distribution Internet Gateway.

☑ Internet Gateway 49 K

Destination Folder
D:\Program Files\HITACHI\dmgwsvr

Space Required on D: 866 K
Space Available on D: 928196 K

4. Specify the directory in which Internet Gateway is to be installed.
   The default directory for installation is *system-drive*`\Program Files\HITACHI\dmgwsvr`.
   If the OS being used is Windows Server 2003 (x64), the default directory is *system-drive*`\Program Files (x86)\HITACHI\dmgwsvr`.

5. Choose the **Next** button.

   The Confirm Installation dialog box appears.

6. Review the installation, then choose the **Next** button.

   Installation starts. When installation is completed, the Installation Complete dialog box appears.

7. Choose **Finish**.

   If you selected **Start Setup** in the Installation Complete dialog box, the Software Distribution Internet Gateway Settings dialog box appears and you can continue with setup.

(3) Setting up Internet Gateway

Set up Internet Gateway from **Control Panel**.

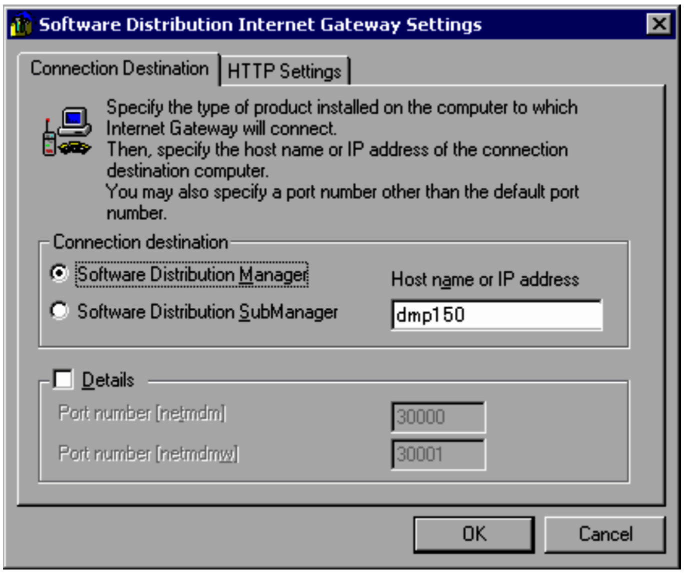
Open **Control Panel** and double-click **SD Internet Gateway Settings** to display the Software Distribution Internet Gateway Settings dialog box. In this dialog box, specify the higher connection destination for Internet Gateway and the maximum data size for downloads.

You must have Administrator rights to set up Internet Gateway.

(a) Connection Destination

Specify the JP1/Software Distribution higher system to which Internet Gateway connects, as well as the port number.

Figure E–8: Connection Destination page



Software Distribution Internet Gateway Settings

Specify the type of product installed on the computer to which Internet Gateway will connect.
Then, specify the host name or IP address of the connection destination computer.
You may also specify a port number other than the default port number.

Connection destination

● Software Distribution Manager

○ Software Distribution SubManager

Host name or IP address: dmp150

□ Details

Port number [netmdm]: 30000

Port number [netmdmw]: 30001

Connection Destination

Select whether the JP1/Software Distribution higher system to which Internet Gateway connects is a central manager or submanager. Also specify the address of the higher system to which Internet Gateway connects using the ID key for operations (host name or IP address) of the higher system. This setting is mandatory

Details

You can specify the port number that Internet Gateway uses for communications. The default port numbers are `30000` for the `netmdm` port and `30001` for the `netmdmw` port. If there is a possibility that another program uses the same port number, choose **Details** and change the port number. When the higher system is JP1/Software Distribution Manager, the `netmdm` port value is used. When the higher system is JP1/Software Distribution Client (relay system), the `netmdmw` port value is used.

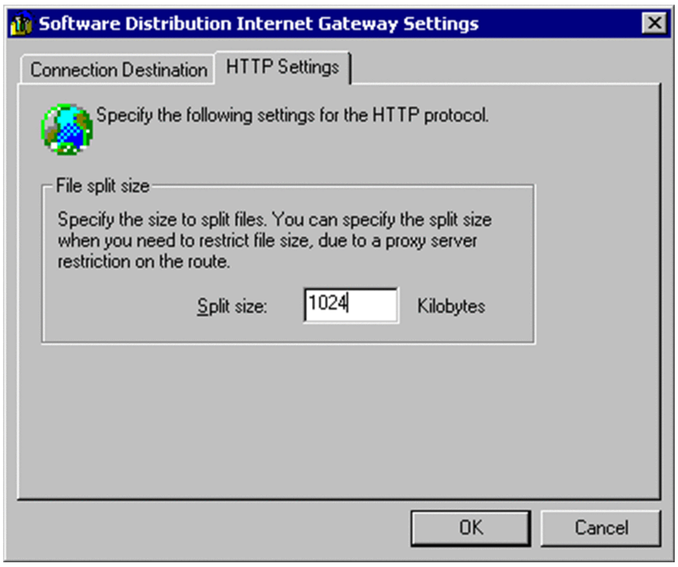
(b) HTTP settings

You can specify the file split size for file data that is sent from JP1/Software Distribution.

The proxy server or Web server that you are using may limit the maximum data size that you can send (download). If so, split the JP1/Software Distribution file data for sending. The default file split size is 1,024 KB.

Note that the specified file split size affects the memory allocation performance of Microsoft Internet Information Services and the number of frame transfers in the file transfer protocol. For details, see the Microsoft Internet Information Services documentation.

Figure E–9: HTTP Settings page



Software Distribution Internet Gateway Settings

Specify the following settings for the HTTP protocol.

File split size

Specify the size to split files. You can specify the split size when you need to restrict file size, due to a proxy server restriction on the route.

Split size: 1024 Kilobytes

(4) Notes on the Microsoft Internet Information Services settings

In the Microsoft Internet Information Services, you must use **Internet Service Manager** to create a virtual directory for Internet Gateway and to specify whether access permission and log file output are required. You may also need to set up SSL.

This subsection provides notes on making these settings. For details about **Internet Service Manager**, see the Microsoft Internet Information Services documentation.

- You should note the following about setting up the virtual directory for Internet Gateway:
  - For the physical path, specify the `bin` subdirectory of the directory in which you installed Internet Gateway.
  - When using Microsoft Internet Information Server 4.0, enable **Allow Read Access**, **Allow Script Access**, and **Allow Execute Access (includes Script Access)**. When using Microsoft Internet Information Services 5.0, enable **Read**, **Run scripts [such as ASP]**, and **Execute [such as ISAPI applications or CGI]**.
- If you change the default installation destination and install Internet Gateway directly in `wwwroot` (the default for storing Web pages), you must also apply read/write permissions for the `log` and `work` directories.

  If you are using Windows NT 4.0, the `log` and `work` directories are created as subdirectories of the directory in which you install Internet Gateway. If you are using Windows 2000, the `log` and `work` directories are created in `\Documents and Settings\All Users\Application Data\hitachi\dmgwsvr` on the drive in which the OS is installed.
- Normally, the status of both HTTP requests and responses are output to the log file. If you do not require a log, clear the **Log visits** check box in the Properties dialog box in the Internet Gateway virtual directory.
- If you are using SSL, open the Default Web Site Properties dialog box, select **Secure communications** on the **Directory security** tab, then install a server certificate verified by the certifying organization. If required, then set the **SSL Port** in the **Web site** tab.
- If you are using Microsoft Internet Information Services 6.0, use **Web Service Extensions** to set **Allowed** for **Server Side Includes**. Also, use **Web Service Extensions** to add a **New Web Service Extension** with the following settings:
  - **Extension name**

    Any name
  - **Required files**

    `C:\Program Files\HITACHI\dmgwsvr\BIN\dmgwsvr.dll`

(Applicable if Internet Gateway is installed in `C:\Program Files\HITACHI\dmgwsvr`)

- **Set extension status to Allowed**
  Selected

(5) Setting up the higher system

This subsection describes which of the setup items of the higher system to which Internet Gateway connects require attention when you use Internet Options. For details about the setup procedure and the settings, see *4. Setting Up JP1/ Software Distribution Manager* or *5. Setting Up JP1/Software Distribution Client (relay system)*.

Page	Item	Setting	Description
Server Customization[#1]	Max. number of subsystems in which jobs can execute concurrently[#2]	0	Jobs distributed via Internet Options are executed in response to a request from a lower system. To block job execution requests from higher systems, set 0. For details about the job flow, see *E.2 Job flow via Internet Options*.
	Monitor startup of subsystems	OFF	Monitoring is not required because Internet Options blocks job execution requests from higher systems.
ID Key for Operations	How to resolve IP addresses	Use the system configuration of Software Distribution Manager	Use JP1/Software Distribution system configuration information because address resolution may fail in a network environment via the Internet.
	When resolution of IP address fails	The job starts.	Set the item in such a manner that the job will not result in an error even if address resolution fails because address resolution may fail in a network environment via the Internet.
	Use host IDs[#3]	Yes	Use of host IDs is recommended.

#1

Relay System Customization in the Relay System Setup.

#2

Max. number of relays or clients in which jobs can execute concurrently in the Relay System setup.

#3

This item does not exist in the Relay System Setup.

E.6 Setting up HTTP Gateway

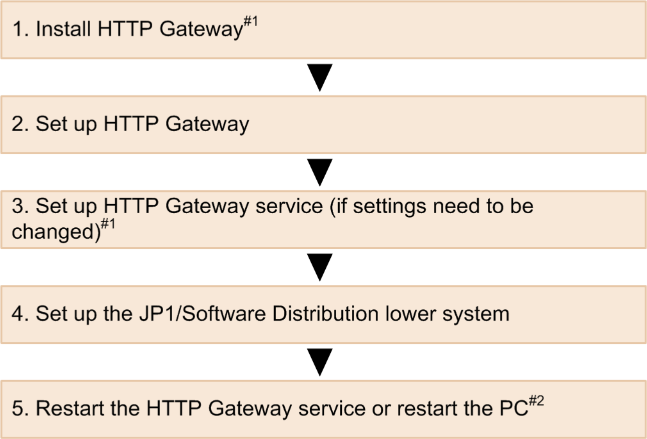
To run HTTP Gateway on your system, you must install HTTP Gateway and set it up. You must also set up the lower system.

In Windows NT, you must do the setup so that HTTP Gateway is registered as a Windows service. After installation, you can change the HTTP Gateway service settings as required.

(1) Setup procedure

The figure below shows the procedures for setting up HTTP Gateway, the HTTP Gateway service, and the lower system. The HTTP Gateway service should be set up only under Windows NT.

Figure E–10: HTTP Gateway setup procedures



1. Install HTTP Gateway[#1]

2. Set up HTTP Gateway

3. Set up HTTP Gateway service (if settings need to be changed)[#1]

4. Set up the JP1/Software Distribution lower system

5. Restart the HTTP Gateway service or restart the PC[#2]

[#1] If you have created a new user account that is used when the HTTP Gateway service logs on, log off from the desktop and then log on again using the created user account.

[#2] If you are using Windows NT, restart the HTTP Gateway service. If you are using Windows Me or Windows 98, restart the PC.

(2) Installing HTTP Gateway

Because Internet Options is a background service that converts protocols, no icon is registered in the **Start** menu when you install HTTP Gateway. After installing the software, make the necessary settings from the **Control Panel**.

In Windows NT, you must also make the required settings so that HTTP Gateway is registered as a Windows service. The HTTP Gateway service settings can be changed as required after installation. After installed, HTTP Gateway functions as a Windows service named Software Distribution HTTP Gateway Service.

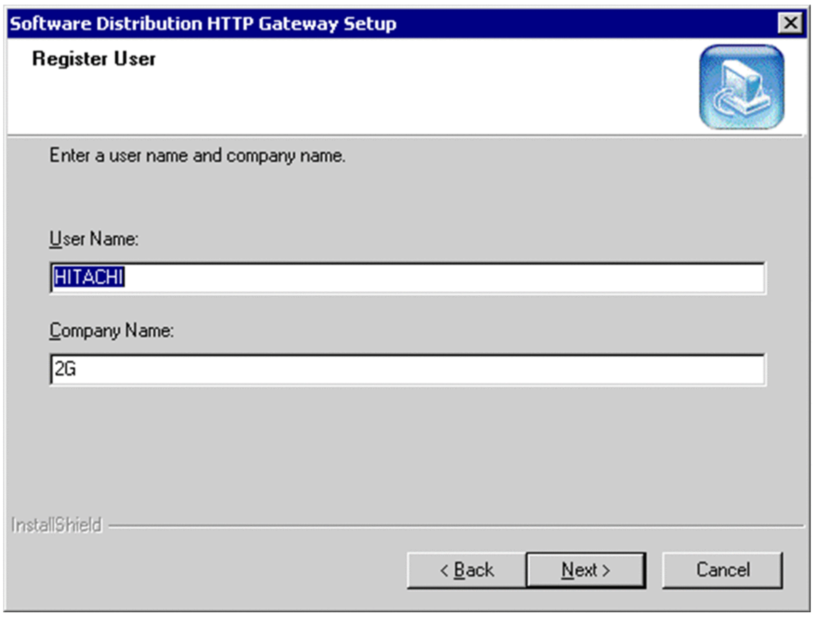
In Windows Me and Windows 98, HTTP Gateway is a resident program.

Note that you cannot use the remote installation facility of JP1/Software Distribution to install HTTP Gateway. However, you can use this facility to reinstall this product.

To install HTTP Gateway:

1. Insert the HTTP Gateway installation medium into the CD-ROM drive.
   The Software Distribution HTTP Gateway Setup dialog box appears.
2. Choose the **Next** button.
   The Register User dialog box appears.

Figure E–11: Register User dialog box



Software Distribution HTTP Gateway Setup

Register User

Enter a user name and company name.

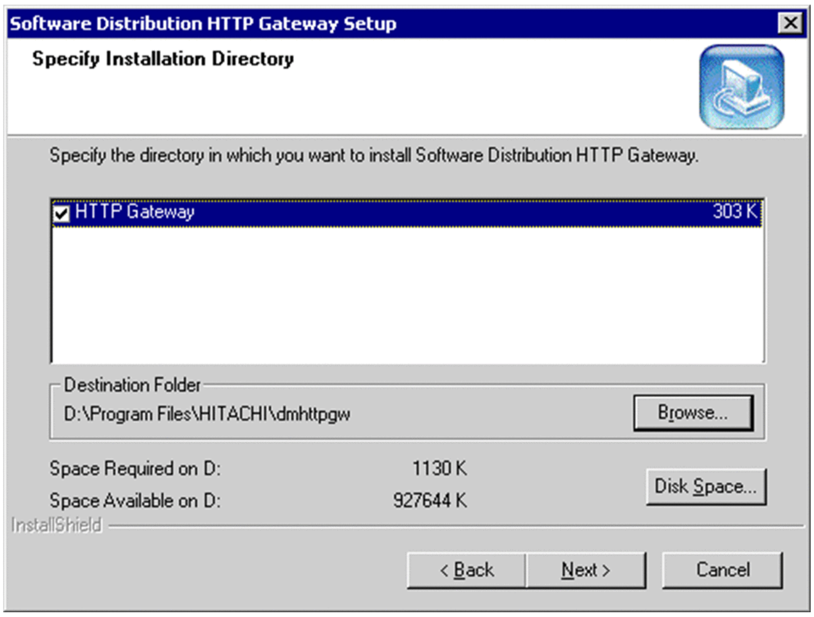
User Name: HITACHI

Company Name: 2G

3. Enter the user name and company name, then choose the **Next** button.

   The Specify Installation Directory dialog box appears.

Figure E–12: Specify Installation Directory dialog box



Software Distribution HTTP Gateway Setup

Specify Installation Directory

Specify the directory in which you want to install Software Distribution HTTP Gateway.

☑ HTTP Gateway 303 K

Destination Folder
D:\Program Files\HITACHI\dmhttpgw

Space Required on D: 1130 K

Space Available on D: 927644 K

4. Specify the directory in which **HTTP Gateway** is to be installed.

   The default directory for installation is *system-drive*`\Program Files\hitachi\dmhttpgw`.

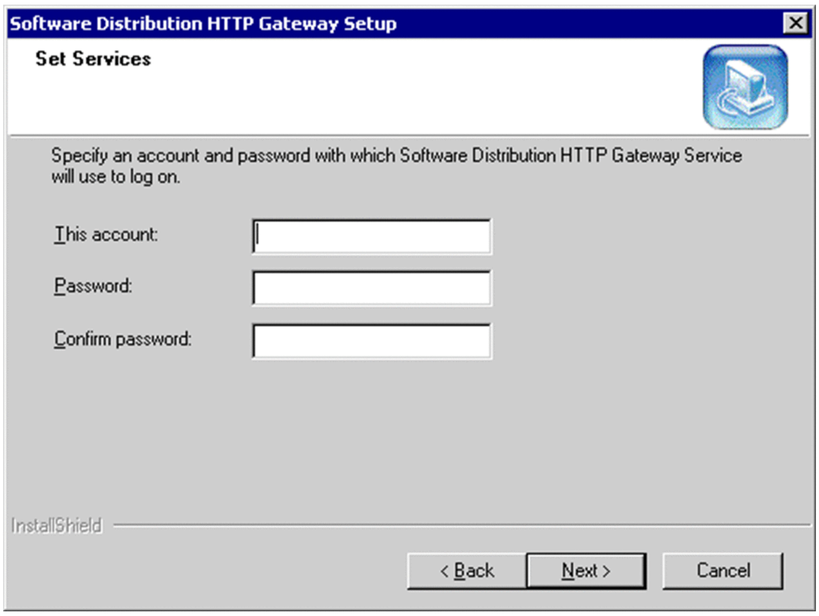
   If the OS being used is Windows Server 2003 (x64), the default directory is *system-drive*`\Program Files (x86)\HITACHI\dmhttpgw`.

5. Choose the **Next** button.

   In Windows NT, the Set Services dialog box appears when you first install HTTP Gateway. When you reinstall HTTP Gateway, this dialog box is not displayed and installation advances to step 8.

   In Windows Me and Windows 98, this dialog box is not displayed and installation advances to step 8.

Figure E–13: Set Services dialog box


Software Distribution HTTP Gateway Setup

Set Services

Specify an account and password with which Software Distribution HTTP Gateway Service will use to log on.

This account:

Password:

Confirm password:

6. Complete the settings for registering HTTP Gateway as a Windows service.

   Set the user account and password to be used when the HTTP Gateway service logs on. HTTP Gateway uses the settings in the Windows Internet Options setup for the specified account user.

   Note the following about setting up the user account:

   - Account users must have Users rights. However, when Secure Socket Client is installed on the machine on which HTTP Gateway is installed, Power Users rights or higher are required.
   - In Windows NT 4.0, you must give read/write permission to the account user for the directory in which HTTP Gateway is being installed.
   - When you create a new user account, after installing HTTP Gateway, log off from the desktop and then log on again using the new user account.

   Note that the **Startup Type** for the HTTP Gateway service is registered as **Automatic**.

7. Choose the **Next** button.

   The Confirm Installation dialog box appears.

8. Review the installation, then choose the **Next** button.

   Installation starts. When installation is completed, the Installation Complete dialog box appears.

9. Choose **Finish**.

   If you selected **Start Setup** in the Installation Complete dialog box, the Software Distribution HTTP Gateway Settings dialog box appears and you can continue with the setup.

(3) Setting up HTTP Gateway

You set up HTTP Gateway from the **Control Panel**.

Open **Control Panel** and double-click **SD HTTP Gateway Settings** to display the Software Distribution HTTP Gateway Settings dialog box. In this dialog box, specify the following settings, then make a test connection to the Web server:

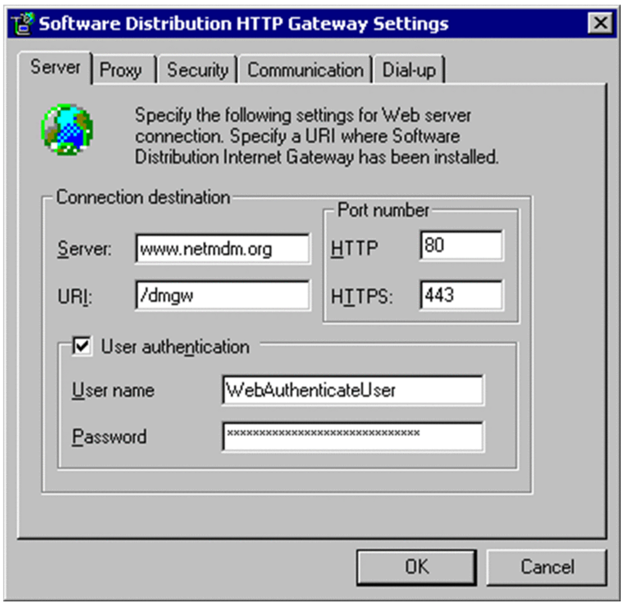
- Server
- Proxy
- Security
- Communication
- Dial-up

If you change the settings after you begin using Internet Options, you must restart the HTTP Gateway service in order for those changes to take effect. If you are running Windows Me or Windows 98, you must restart the PC.

(a) Server

Specify the Web server and Internet Gateway to which HTTP Gateway connects. You can also specify the port number for HTTP and HTTPS communications.

Figure E–14: Server page


Software Distribution HTTP Gateway Settings

Specify the following settings for Web server connection. Specify a URI where Software Distribution Internet Gateway has been installed.

Connection destination

Server: www.netmdm.org

URI: /dmgw

Port number

HTTP: 80

HTTPS: 443

☑ User authentication

User name: WebAuthenticateUser

Password: ******************************

Server

Specify the address of the Web server to which HTTP Gateway connects. This setting is required.

URI

Specify the alias specified at the time of creation of the virtual directory for Internet Gateway using the Microsoft Internet Information Services. This setting is required.

Port number

You can specify the port numbers used for HTTP and HTTPS communications. The defaults are 80 and 443, respectively. If there is a possibility that another program uses the same port number, change the port number.

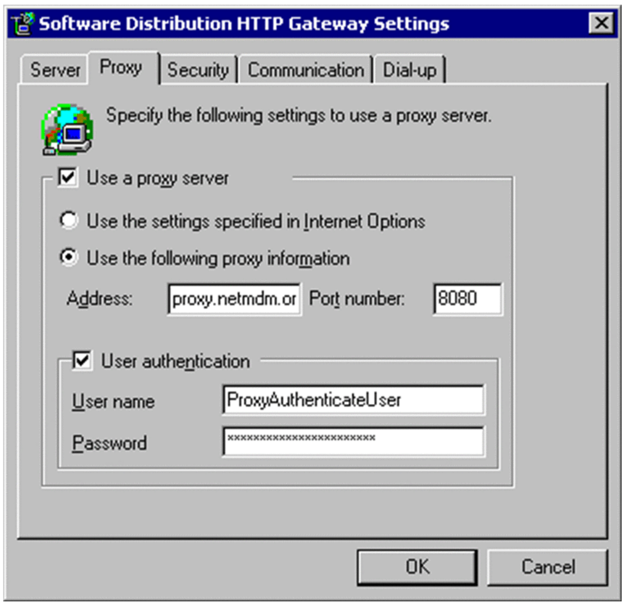
User Authentication

If the Web server requires user authentication, specify the user name and password.

(b) Proxy

When you use a proxy server, select **Use a proxy server** and complete the various settings.

Figure E–15: Proxy page



Specify the following settings to use a proxy server.

☑ Use a proxy server

○ Use the settings specified in Internet Options

● Use the following proxy information

Address: proxy.netmdm.or Port number: 8080

☑ User authentication

User name: ProxyAuthenticateUser

Password: ************************

Use the settings specified in Internet Options

Select this option to use the proxy-related information set in the Windows Internet Options. Windows NT uses the Windows Internet Options settings for account users registered in the HTTP Gateway service.

Use the following proxy information

Select this option to use the proxy information set in **Address** and **Port number**.

Address

Specify the address of the proxy server.

Port number

You can specify the port number to be used when communicating with the proxy server. The default value is 8080. If there is a possibility that another program uses the same port number, change the port number.

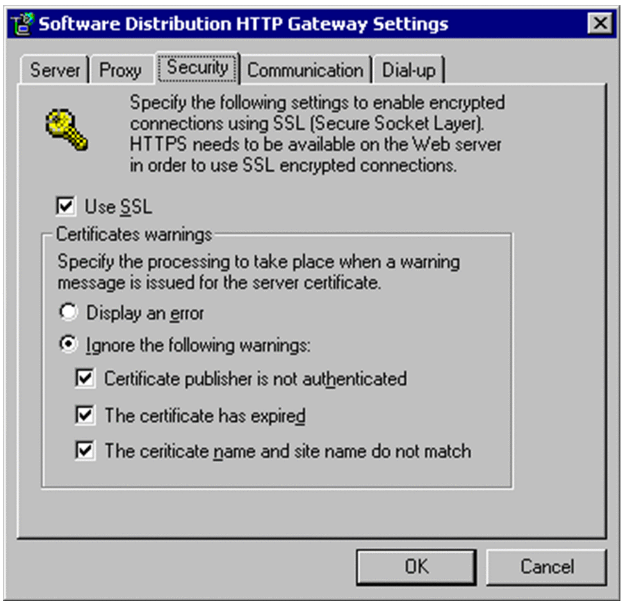
User authentication

If the proxy server requires user authentication, specify the user name and password.

(c) Security

Implement the settings required for HTTPS communications using SSL.

Figure E–16: Security page



Software Distribution HTTP Gateway Settings

Specify the following settings to enable encrypted connections using SSL (Secure Socket Layer). HTTPS needs to be available on the Web server in order to use SSL encrypted connections.

☑ Use SSL

Certificates warnings

Specify the processing to take place when a warning message is issued for the server certificate.

○ Display an error

● Ignore the following warnings:

☑ Certificate publisher is not authenticated

☑ The certificate has expired

☑ The ceriticate name and site name do not match

Use SSL

Select this option for HTTPS communications. Note that you must have already installed the certificate in the Web server.

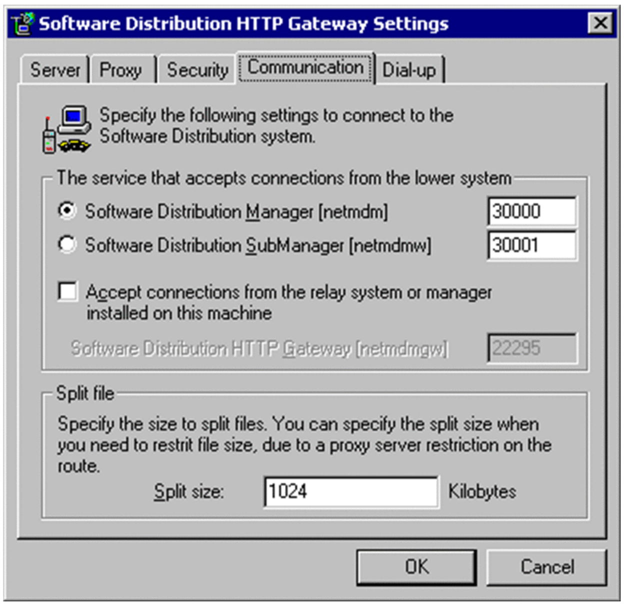
Certificates warnings

Select whether an error results when a certificate-related warning occurs or the warning is ignored and HTTPS communication is performed. If you choose to ignore warnings, specify the types of warnings.

(d) Communication

Specify the service that accepts connection from the JP1/Software Distribution lower system and the maximum data size per upload.

Figure E–17: Communication page



Software Distribution HTTP Gateway Settings

Specify the following settings to connect to the Software Distribution system.

The service that accepts connections from the lower system

● Software Distribution Manager [netmdm] 30000

○ Software Distribution SubManager [netmdmw] 30001

□ Accept connections from the relay system or manager installed on this machine

Software Distribution HTTP Gateway [netmdmgw] 22295

Split file

Specify the size to split files. You can specify the split size when you need to restrit file size, due to a proxy server restriction on the route.

Split size: 1024 Kilobytes

The service that accepts connections from the lower system

Select the service that accepts a connection from the JP1/Software Distribution lower system. When the lower system is a relay manager or relay system and HTTP Gateway is installed on the same machine, select **Accept connections from the relay system or manager installed on this machine**. When HTTP Gateway is installed on a different machine, select **Software Distribution Manager** if the higher connection destination for Internet Gateway is a central manager, and select **Software Distribution SubManager** if the connection destination for Internet Gateway is a relay system.

You can also specify the port number used for each service. The default port numbers are shown below. If there is a possibility that another program uses the same port number, change the port number.

- JP1/Software Distribution Manager: `30000`
- JP1/Software Distribution SubManager: `30001`
- JP1/Software Distribution HTTP Gateway: `22295`

Split file

Specify the file split size for file data sent from JP1/Software Distribution.

Depending on your proxy server and on the Web server, the maximum data size that can be sent (uploaded) at one time may be limited. In such a case, split JP1/Software Distribution file data for sending. The default file split size is 1,024 kilobytes.

(e) Dial-up

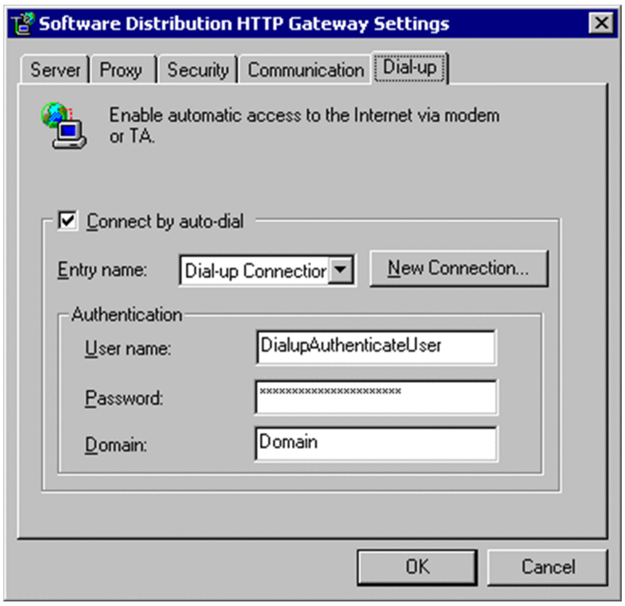
When you install HTTP Gateway and client on a notebook computer and connect to the Internet using a dial-up connection, the dial-up connection can be automated using the *auto-dialing facility*, which is set up on the **Dial-up** page. The **Dial-up** page is displayed only when the remote access service is installed.

The auto-dialing facility connects and disconnects at the following times:

- When an HTTP request is generated, the facility checks whether or not a connection has been established using the specified dial-up entry; if there is no connection, it initiates auto dialing.
- Only when auto dialing has been performed by HTTP Gateway, the facility disconnects at the end of the session.
- When multiple sessions are in progress simultaneously, the facility maintains the connection until all sessions have terminated.

Before using the HTTP Gateway auto-dialing facility, you must clear the **Dial-up connection** in the lower system setup. However, when HTTP Gateway is installed on the same computer as the lower system, the same function can be achieved by selecting **Dial-up connection** at the lower system and setting the auto-dialing facility in HTTP Gateway off.

Figure E–18: Dial-up page



Enable automatic access to the Internet via modem or TA.

☑ Connect by auto-dial

Entry name: Dial-up Connectior

Authentication

User name: DialupAuthenticateUser

Password: **********************

Domain: Domain

Connect by auto-dial

Select this box to use the HTTP Gateway auto-dialing facility. When you select this box, you must clear the **Dial-up connection** in the setup of the lower system.

Entry name

Select the dial-up entry to be used. To create a new dial-up entry, choose the **New connection** button.

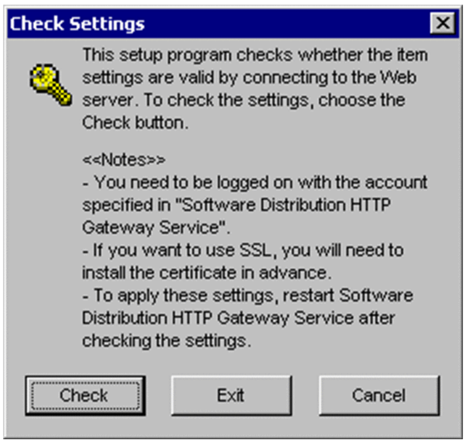
Authentication

Enter the user name, password, and domain to be used for the dial-up connection.

(f) Checking settings

When you have completed all settings in the Software Distribution HTTP Gateway Settings dialog box, choose the **OK** button to display the confirmation dialog box shown below. Choose the **Check** button to make a test connection to the Web server.

Figure E–19: Check Settings dialog box



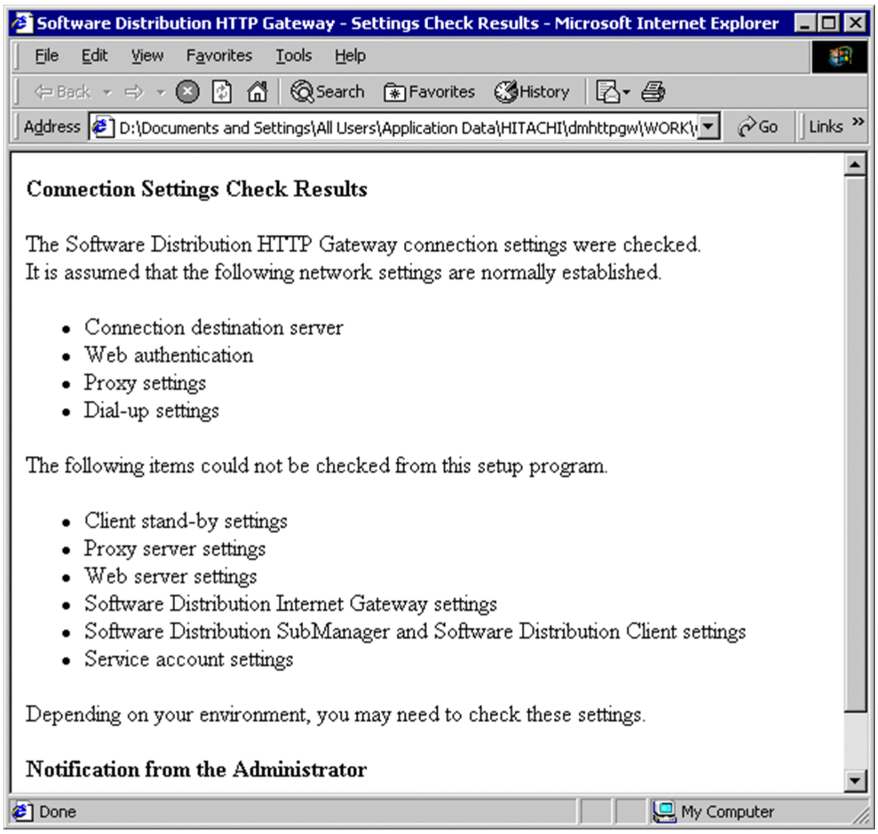
Check Settings

This setup program checks whether the item settings are valid by connecting to the Web server. To check the settings, choose the Check button.

<<Notes>>
- You need to be logged on with the account specified in "Software Distribution HTTP Gateway Service".
- If you want to use SSL, you will need to install the certificate in advance.
- To apply these settings, restart Software Distribution HTTP Gateway Service after checking the settings.

When connection is established successfully, the Software Distribution HTTP Gateway - Settings Check Results page is displayed.

Figure E–20: Software Distribution HTTP Gateway - Settings Check Results page


Software Distribution HTTP Gateway - Settings Check Results - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address D:\Documents and Settings\All Users\Application Data\HITACHI\dmhttpgw\WORK\
Go Links
Done
My Computer

Connection Settings Check Results

The Software Distribution HTTP Gateway connection settings were checked.
It is assumed that the following network settings are normally established.

- Connection destination server
- Web authentication
- Proxy settings
- Dial-up settings

The following items could not be checked from this setup program.

- Client stand-by settings
- Proxy server settings
- Web server settings
- Software Distribution Internet Gateway settings
- Software Distribution SubManager and Software Distribution Client settings
- Service account settings

Depending on your environment, you may need to check these settings.

Notification from the Administrator

If this Web page is not displayed, connection has not been established. Check the setup. If you are using SSL, make sure that the certificate is installed on the Web server.

(4) Setting up the service

In Windows NT, HTTP Gateway is registered automatically as a Windows service upon completion of installation of HTTP Gateway. The registration items are as follows:

- Service name: Software Distribution HTTP Gateway Service
- Startup type: Automatic
- Logon: Account specified at HTTP Gateway installation

You can change the HTTP Gateway service settings as necessary.

In the account, specify the user account and password to be used when the HTTP Gateway service logs on. HTTP Gateway uses the settings in the Windows Internet Options for the specified account user.

You should note the following about setting up a user account:

- Account users must have Users rights. However, when Secure Socket Client is installed on the PC on which HTTP Gateway is installed, Power Users rights or higher are required.
- In Windows NT 4.0, the account user must have read/write permission for the directory in which HTTP Gateway is being installed.
- When you create a new user account, after installing HTTP Gateway, log off from the desktop and then log on again using the new user account.

Use the following procedure to change the service setup. For details about services, see the Windows manual or online help.

■ For Windows Server 2003, Windows XP, and Windows 2000

1. From the **Program** menu, select **Settings**, **Control Panel**, **Administrative Tools**, then **Computer management**.
   The Computer Management window appears.
2. In the left pane of the window, select **Services** under **Services and Applications**.
3. In the right pane of the window, right-click on **Software Distribution HTTP Gateway Service**, then select **Properties** from the menu that is displayed.
   The Software Distribution HTTP Gateway Service Properties dialog box appears.
4. Change the HTTP Gateway Service settings as required.

■ For Windows NT 4.0

1. From **Control Panel**, choose **Services**.
   The Services dialog box appears.
2. From the list box, select **Software Distribution HTTP Gateway Service**, then choose the **Startup** button.
   The HTTP Gateway service settings are displayed.
3. Change the HTTP Gateway Service settings as required.

(5) Setting up the lower system

This subsection describes the setup items of the lower system to which HTTP Gateway connects that require attention when Internet Options is used. For details about the setup procedure and the settings, see *4. Setting Up JP1/Software Distribution Manager*, *5. Setting Up JP1/Software Distribution Client (relay system)*, or *6. Setting Up JP1/Software Distribution Client (client)*.

(a) For relay manager

Page	Item	Description
Connection destination	Higher connection destination host name or IP address	When HTTP Gateway is installed on the same machine as the relay manager, specify the host name or IP address of the higher system connected via HTTP Gateway and Internet Gateway. When HTTP Gateway and the relay manager are installed on different machines, specify the host name or IP address of the machine on which HTTP Gateway is installed.
	Connect using the HTTP Gateway installed on this relay manager	Select this item when HTTP Gateway is installed on the same machine as the relay manager.
Communication	Port number Software Distribution HTTP Gateway [`netmdmgw`]	When HTTP Gateway is installed on the same machine as the relay manager, you can specify the port number to be used when communicating with HTTP Gateway. The default is `22295`. Change the port number if the default port number is used by another program. Note that the `netmdmgw` port can also be set on the **Communication** tab in the Server setup.
	Wait for response	Communications via Internet Gateway, HTTP Gateway, and the Internet are slower than when there is a direct connection with the managing server. This is particularly so for file transfers with a low bandwidth Internet connection. In some cases, the lower system may determine that there is no response and a communication error may result. In this item, set a time that takes into account the scale of the system, the lines, and the sizes of the files to be transferred. Use the following formula to calculate the timeout value, then check operations and adjust the setting if required: Timeout value = T1 **x** Sp#
Default Running Status/ Polling	Client will poll the managing server	When using Internet Options, job execution requests from the higher system are not received by the lower system. Jobs are executed only in response to requests from a lower system. Taking the job flow into account, select the **Client will poll the managing server** option and set the polling timing

Page	Item	Description
Default Running Status/ Polling	Client will poll the managing server	according to the operating environment and conditions. For details about the job flow, see *E.2 Job flow via Internet Options*.

#

T1: Time (in seconds) required to send a 1-megabyte file by FTP, etc.

Sp: Maximum size (in megabytes) of packages to be distributed or files to be collected.

(b) For relay system

Page	Item	Description
Connection destination	Higher system	Specify the product type (Software Distribution Manager or Software Distribution SubManager) of the higher system connecting via HTTP Gateway and Internet Gateway.
	Host name or IP address	When HTTP Gateway is installed on the same machine as the relay system, specify the host name or IP address of the higher system connecting via HTTP Gateway and Internet Gateway. When HTTP Gateway is installed on a different machine from the relay system, specify the host name or IP address of the machine on which HTTP Gateway is installed.
	Poll multiple higher systems	When you select this item, you must specify the following machine as first priority: • When HTTP Gateway is installed on the same machine as the relay system, specify the higher system connecting via HTTP Gateway and Internet Gateway. • When HTTP Gateway is installed on a different machine from the relay system, specify the machine on which HTTP Gateway is installed. Note that when HTTP Gateway and the relay system are installed on the same machine, machines set as second priority and lower are ignored.
	Connect using the HTTP Gateway installed on this relay system	Select this item when HTTP Gateway is installed on the same machine as the relay system.
Communication	Port number Software Distribution HTTP Gateway [`netmdmgw`]	When HTTP Gateway is installed on the same machine as the relay system, you can specify the port number to be used when communicating with HTTP Gateway. The default is `22295`. Change the port number if the default port number may be in use by another program.
	Wait for response	Communications via Internet Gateway, HTTP Gateway, and the Internet are slower than when there is a direct connection with the managing server. This is particularly so for file transfers with a low bandwidth Internet connection. In some cases, the lower system may determine that there is no response and a communication error may result. In this item, set a time that takes into account the scale of the system, the lines, and the sizes of the files to be transferred. Use the following formula to calculate the timeout value, then check operations and adjust the setting if required: Timeout value = T1 **x** Sp#
Default Running Status/ Polling	Client will poll the managing server	When using Internet Options, job execution requests from the higher system are not received by the lower system. Jobs are executed only in response to requests from a lower system. Taking the job flow into account, select the **Client will poll the managing server** option and set the polling timing according to the operating environment and conditions. For details about the job flow, see *E.2 Job flow via Internet Options*.

#

T1: Time (in seconds) required to send a 1-megabyte file by FTP, etc.

Sp: Maximum size (in megabytes) of packages to be distributed or files to be collected.

(c) For client

Page	Item	Description
Connection destination	Connection destination	Specify the product type (Software Distribution Manager or Software Distribution SubManager) of the higher system connecting via HTTP Gateway and Internet Gateway.
	Host name or IP address	Specify the host name or IP address of the machine on which HTTP Gateway is installed.
	Automatically register this computer in the system configuration	In an environment via the Internet, we recommend the operation mode in which the system configuration is not automatically registered. For details, see *E.3 Notes on using Internet Options*.
Communication	Wait for response	Communications via Internet Gateway, HTTP Gateway, and the Internet are slower than when there is a direct connection with the managing server. This is particularly so for file transfers with a low bandwidth Internet connection. In some cases, the lower system may determine that there is no response and a communication error may result. In this item, set a time that takes into account the scale of the system, the lines, and the sizes of the files to be transferred. Use the following formula to calculate the timeout value, then check operations and adjust the setting if required: Timeout value = T1 **x** Sp#
Default Running Status/ Polling	Client starts automatically at system boot	When using Internet Options, job execution requests are blocked. It is, therefore, not necessary for the client to start automatically.
	Client will poll the managing server	When using Internet Options, job execution requests from the higher system are not received by the lower system. Jobs are executed only in response to requests from a lower system. Taking the job flow into account, select the **Client will poll the managing server** option and set the polling timing according to the operating environment and conditions. To save money when using a dial-up connection, make use of the **Specify the time to execute polling** option. You can also unselect the **Client will poll the managing server** option and make a connection only when executing the **Package Setup Manager** of the client or when choosing the **Execute Job Backlog** icon. For details about the job flow, see *E.2 Job flow via Internet Options*.
Dial-up	Dial-up connection	Do not select this item when using the auto-dialing facility in HTTP Gateway. However, when HTTP Gateway is installed on the same machine as the client, you can also unselect the auto-dialing facility in HTTP Gateway and use the client settings.

#

T1: Time (in seconds) required to send a 1-megabyte file by FTP, etc.

Sp: Maximum size (in megabytes) of packages to be distributed or files to be collected.

E.7 Stopping Internet Gateway and HTTP Gateway

(1) Stopping Internet Gateway

There are two methods of stopping Internet Gateway, both of which use Microsoft Internet Information Services.

■ Stopping the Microsoft Internet Information Services

Use the Internet Service Manager to stop the Web site of the Microsoft Internet Information Services. In addition to Internet Gateway, other sites stored in virtual directories, if any, will also stop.

■ Limiting access to the Internet Gateway virtual directory

Execute the following operations in the Properties dialog box for the virtual directory of Internet Gateway to stop Internet Gateway. This method does not affect other virtual directories.

To limit access to the Internet Gateway virtual directory:

1. In the **Directory security** page, choose the **Edit** button in **IP address and domain name restrictions**.
   The IP Address and Domain Name Restrictions dialog box appears.
2. For **By default, all computers will be**, choose **Denied Access**.

(2) Stopping HTTP Gateway

If you need to stop HTTP Gateway, move to the directory in which HTTP Gateway is installed and then enter the following command on the command line (`STOP` must be entered in uppercase letters):

```
dmhttpgw.exe /STOP
```

F. Query Scripts for Data Partitions

This appendix provides samples of query scripts that can be used to store operation monitoring histories when using data partitions, which is a functionality of Microsoft SQL Server 2012, Microsoft SQL Server 2008 and Microsoft SQL Server 2005.

Note that these samples were created using the following assumptions.

- The storage destination is the JP1/Software Distribution installation target directory `\SAMPLE\MSSQL`.
- The database name specified is `NETMDM_SAMPLE`.
- The query scripts conform to the syntax in Microsoft's Transact-SQL reference.
  For details about this syntax, see Microsoft's Transact-SQL Reference.

F.1 DropTable.sql query script

```
USE [NETMDM_SAMPLE]
GO

DROP INDEX [netmdm_metsec_index1] ON [dbo].[netmdm_monitoring_security]
GO

DROP INDEX [netmdm_metsec_index2] ON [dbo].[netmdm_monitoring_security]
GO

DROP INDEX [netmdm_metsec_index3] ON [dbo].[netmdm_monitoring_security]
GO

DROP TABLE [dbo].[netmdm_monitoring_security]
GO
```

F.2 AddFilegroup.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0001]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0002]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0003]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0004]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0005]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0006]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0007]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0008]
GO
```

F.3 AddFiletoEdrive.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0001',
        FILENAME = N'E:\NETMDP\MONITOR_DP_0001.ndf',
        SIZE = 80GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0001]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0002',
        FILENAME = N'E:\NETMDP\MONITOR_DP_0002.ndf',
        SIZE = 80GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0002]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0003',
        FILENAME = N'E:\NETMDP\MONITOR_DP_0003.ndf',
        SIZE = 80GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0003]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0004',
        FILENAME = N'E:\NETMDP\MONITOR_DP_0004.ndf',
        SIZE = 80GB,MAXSIZE = UNLIMITED,FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0004]
GO
```

F.4 AddFiletoFdrive.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0005',
        FILENAME = N'F:\NETMDP\MONITOR_DP_0005.ndf',
        SIZE = 80GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0005]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0006',
        FILENAME = N'F:\NETMDP\MONITOR_DP_0006.ndf',
        SIZE = 80GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0006]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0007',
        FILENAME = N'F:\NETMDP\MONITOR_DP_0007.ndf',
        SIZE = 80GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0007]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0008',
        FILENAME = N'F:\NETMDP\MONITOR_DP_0008.ndf',
        SIZE = 80GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0008]
GO
```

F.5 CreatePartition.sql query script

```
USE [NETMDM_SAMPLE]
GO

CREATE PARTITION FUNCTION netmdm_monitoring_security_pf (datetime) AS RANGE RIGHT FOR
VALUES (
        '20110101',
        '20110201',
        '20110301',
        '20110401',
        '20110501',
        '20110601',
        '20110701',
        '20110801'
)
GO

CREATE PARTITION SCHEME netmdm_monitoring_security_ps AS PARTITION
netmdm_monitoring_security_pf TO (
        [netmdm_moni_seg],
        [netmdm_moni_dp_0001],
        [netmdm_moni_dp_0002],
        [netmdm_moni_dp_0003],
        [netmdm_moni_dp_0004],
        [netmdm_moni_dp_0005],
        [netmdm_moni_dp_0006],
        [netmdm_moni_dp_0007],
        [netmdm_moni_dp_0008]
)
GO
```

F.6 CreateTable.sql query script

```
USE [NETMDM_SAMPLE]
GO

SET ANSI_DEFAULTS OFF
SET ANSI_NULLS OFF
SET ANSI_PADDING OFF
SET ANSI_WARNINGS OFF
SET ARITHABORT OFF
SET QUOTED_IDENTIFIER ON
SET CONCAT_NULL_YIELDS_NULL OFF
SET ANSI_NULL_DFLT_ON OFF
SET STATISTICS TIME OFF
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[netmdm_monitoring_security] (
        [dm_nodename] [varchar](64) NOT NULL,
        [dm_hostname] [varchar](64) NULL DEFAULT (NULL),
        [dm_ipaddress] [varchar](15) NULL DEFAULT (NULL),
        [dm_startdate] [datetime] NOT NULL,
        [dm_enddate] [datetime] NULL DEFAULT (NULL),
        [dm_eventtype] [int] NOT NULL,
        [dm_filename] [varchar](520) NULL DEFAULT (NULL),
        [dm_filenamenew] [varchar](520) NULL DEFAULT (NULL),
        [dm_productname] [varchar](50) NULL DEFAULT (NULL),
        [dm_productversion] [varchar](50) NULL DEFAULT (NULL),
        [dm_productlanguage] [int] NULL DEFAULT (NULL),
        [dm_fileversion] [varchar](50) NULL DEFAULT (NULL),
        [dm_filelanguage] [int] NULL DEFAULT (NULL),
        [dm_logonuser] [varchar](128) NULL DEFAULT (NULL),
        [dm_execaccount] [varchar](128) NULL DEFAULT (NULL),
        [dm_caption] [varchar](520) NULL DEFAULT (NULL),
        [dm_processname] [varchar](520) NULL DEFAULT (NULL),
        [dm_drivetypeold] [int] NULL DEFAULT (NULL),
        [dm_drivetypenew] [int] NULL DEFAULT (NULL),
        [dm_documentname] [varchar](260) NULL,
        [dm_printername] [varchar](484) NULL,
        [dm_printingresult] [tinyint] NULL,
        [dm_url] [varchar](2083) NULL,
        [dm_drivetype] [int] NULL,
        [dm_drivename] [char](2) NULL,
        [dm_usbconnectname] [varchar](1024) NULL,
        [dm_usbdiskdrive] [varchar](2048) NULL,
        [dm_usbcontroller] [varchar](2048) NULL,
        [dm_usballowedcondition] [varchar](2069) NULL,
        [dm_devicetype] [int] NULL DEFAULT (NULL)
) ON netmdm_monitoring_security_ps(dm_startdate)
GO
CREATE INDEX [netmdm_metsec_index1] ON [dbo].[netmdm_monitoring_security] (
        [dm_nodename],
        [dm_startdate]
) ON netmdm_monitoring_security_ps(dm_startdate)
GO

CREATE INDEX [netmdm_metsec_index2] ON [dbo].[netmdm_monitoring_security] (
        [dm_startdate],
        [dm_eventtype]
) ON netmdm_monitoring_security_ps(dm_startdate)
GO

CREATE INDEX [netmdm_metsec_index3] ON [dbo].[netmdm_monitoring_security] (
        [dm_hostname]
) ON netmdm_monitoring_security_ps(dm_startdate)
GO
```

F.7 AddFilegroup2nd.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0009]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0010]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0011]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0012]
GO
```

F.8 AddFiletoGdrive.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0009',
        FILENAME = N'G:\NETMDP\MONITOR_DP_0009.ndf',
        SIZE = 80GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0009]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0010',
        FILENAME = N'G:\NETMDP\MONITOR_DP_0010.ndf',
        SIZE = 80GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0010]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0011',
        FILENAME = N'G:\NETMDP\MONITOR_DP_0011.ndf',
        SIZE = 80GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0011]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0012',
        FILENAME = N'G:\NETMDP\MONITOR_DP_0012.ndf',
        SIZE = 80GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0012]
GO
```

F.9 AlterPartition.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0009]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110901')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0010]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20111001')
GO
```

```
ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0011]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20111101')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0012]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20111201')
GO
```

F.10 CreateArchTable.sql query script

```
USE [NETMDM_SAMPLE]
GO

SET ANSI_DEFAULTS OFF
SET ANSI_NULLS OFF
SET ANSI_PADDING OFF
SET ANSI_WARNINGS OFF
SET ARITHABORT OFF
SET QUOTED_IDENTIFIER ON
SET CONCAT_NULL_YIELDS_NULL OFF
SET ANSI_NULL_DFLT_ON OFF
SET STATISTICS TIME OFF
SET QUOTED_IDENTIFIER ON
GO
CREATE TABLE [dbo].[netmdm_monitoring_security_arch] (
        [dm_nodename] [varchar](64) NOT NULL,
        [dm_hostname] [varchar](64) NULL DEFAULT (NULL),
        [dm_ipaddress] [varchar](15) NULL DEFAULT (NULL),
        [dm_startdate] [datetime] NOT NULL,
        [dm_enddate] [datetime] NULL DEFAULT (NULL),
        [dm_eventtype] [int] NOT NULL,
        [dm_filename] [varchar](520) NULL DEFAULT (NULL),
        [dm_filenamenew] [varchar](520) NULL DEFAULT (NULL),
        [dm_productname] [varchar](50) NULL DEFAULT (NULL),
        [dm_productversion] [varchar](50) NULL DEFAULT (NULL),
        [dm_productlanguage] [int] NULL DEFAULT (NULL),
        [dm_fileversion] [varchar](50) NULL DEFAULT (NULL),
        [dm_filelanguage] [int] NULL DEFAULT (NULL),
        [dm_logonuser] [varchar](128) NULL DEFAULT (NULL),
        [dm_execaccount] [varchar](128) NULL DEFAULT (NULL),
        [dm_caption] [varchar](520) NULL DEFAULT (NULL),
        [dm_processname] [varchar](520) NULL DEFAULT (NULL),
        [dm_drivetypeold] [int] NULL DEFAULT (NULL),
        [dm_drivetypenew] [int] NULL DEFAULT (NULL),
        [dm_documentname] [varchar](260) NULL,
        [dm_printername] [varchar](484) NULL,
        [dm_printingresult] [tinyint] NULL,
        [dm_url] [varchar](2083) NULL,
        [dm_drivetype] [int] NULL,
        [dm_drivename] [char](2) NULL,
        [dm_usbconnectname] [varchar](1024) NULL,
        [dm_usbdiskdrive] [varchar](2048) NULL,
        [dm_usbcontroller] [varchar](2048) NULL,
        [dm_usballowedcondition] [varchar](2069) NULL,
        [dm_devicetype] [int] NULL DEFAULT (NULL)
) ON netmdm_monitoring_security_ps(dm_startdate)
GO
CREATE INDEX [netmdm_metsec_index1] ON [dbo].[netmdm_monitoring_security_arch] (
        [dm_nodename],
        [dm_startdate]
) ON netmdm_monitoring_security_ps(dm_startdate)
GO

CREATE INDEX [netmdm_metsec_index2] ON [dbo].[netmdm_monitoring_security_arch] (
        [dm_startdate],
        [dm_eventtype]
) ON netmdm_monitoring_security_ps(dm_startdate)
GO

CREATE INDEX [netmdm_metsec_index3] ON [dbo].[netmdm_monitoring_security_arch] (
        [dm_hostname]
) ON netmdm_monitoring_security_ps(dm_startdate)
GO
```

F.11 SwitchPartition.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 1 TO
netmdm_monitoring_security_arch PARTITION 1
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 2 TO
netmdm_monitoring_security_arch PARTITION 2
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 3 TO
netmdm_monitoring_security_arch PARTITION 3
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 4 TO
netmdm_monitoring_security_arch PARTITION 4
GO
```

F.12 DropArchTable.sql query script

```
USE [NETMDM_SAMPLE]
GO

DROP INDEX [netmdm_metsec_index1] ON [dbo].[netmdm_monitoring_security_arch]
GO

DROP INDEX [netmdm_metsec_index2] ON [dbo].[netmdm_monitoring_security_arch]
GO

DROP INDEX [netmdm_metsec_index3] ON [dbo].[netmdm_monitoring_security_arch]
GO

DROP TABLE [dbo].[netmdm_monitoring_security_arch]
GO
```

F.13 MergeRange.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110101')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110201')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110301')
GO
```

F.14 AlterPartition2nd.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20120101')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0002]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20120201')
GO
```

```
ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0003]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20120301')
GO
```

F.15 LargeAddFilegroup.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0001]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0002]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0003]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0004]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0005]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0006]
GO
```

F.16 LargeAddFile.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0001',
        FILENAME = N'E:\NETMDP\MONITOR_DP_0001.ndf',
        SIZE = 800GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0001]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0002',
        FILENAME = N'F:\NETMDP\MONITOR_DP_0002.ndf',
        SIZE = 800GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0002]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0003',
        FILENAME = N'G:\NETMDP\MONITOR_DP_0003.ndf',
        SIZE = 800GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0003]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0004',
        FILENAME = N'H:\NETMDP\MONITOR_DP_0004.ndf',
        SIZE = 800GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0004]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0005',
        FILENAME = N'I:\NETMDP\MONITOR_DP_0005.ndf',
        SIZE = 800GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0005]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0006',
        FILENAME = N'J:\NETMDP\MONITOR_DP_0006.ndf',
        SIZE = 800GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0006]
GO
```

F.17 LargeCreatePartition.sql query script

```
USE [NETMDM_SAMPLE]
GO

CREATE PARTITION FUNCTION netmdm_monitoring_security_pf (datetime)
AS RANGE RIGHT FOR VALUES (
 '20110101','20110102','20110103','20110104','20110105','20110106'
,'20110107','20110108','20110109','20110110','20110111','20110112'
,'20110113','20110114','20110115','20110116','20110117','20110118'
,'20110119','20110120','20110121','20110122','20110123','20110124'
,'20110125','20110126','20110127','20110128','20110129','20110130'
,'20110131'
,'20110201','20110202','20110203','20110204','20110205','20110206'
,'20110207','20110208','20110209','20110210','20110211','20110212'
,'20110213','20110214','20110215','20110216','20110217','20110218'
,'20110219','20110220','20110221','20110222','20110223','20110224'
,'20110225','20110226','20110227','20110228'
,'20110301','20110302','20110303','20110304','20110305','20110306'
,'20110307','20110308','20110309','20110310','20110311','20110312'
,'20110313','20110314','20110315','20110316','20110317','20110318'
,'20110319','20110320','20110321','20110322','20110323','20110324'
,'20110325','20110326','20110327','20110328','20110329','20110330'
,'20110331'
,'20110401','20110402','20110403','20110404','20110405','20110406'
,'20110407','20110408','20110409','20110410','20110411','20110412'
,'20110413','20110414','20110415','20110416','20110417','20110418'
,'20110419','20110420','20110421','20110422','20110423','20110424'
,'20110425','20110426','20110427','20110428','20110429','20110430'
,'20110501','20110502','20110503','20110504','20110505','20110506'
,'20110507','20110508','20110509','20110510','20110511','20110512'
,'20110513','20110514','20110515','20110516','20110517','20110518'
,'20110519','20110520','20110521','20110522','20110523','20110524'
,'20110525','20110526','20110527','20110528','20110529','20110530'
,'20110531'
,'20110601','20110602','20110603','20110604','20110605','20110606'
,'20110607','20110608','20110609','20110610','20110611','20110612'
,'20110613','20110614','20110615','20110616','20110617','20110618'
,'20110619','20110620','20110621','20110622','20110623','20110624'
,'20110625','20110626','20110627','20110628','20110629','20110630'
)
GO
CREATE PARTITION SCHEME netmdm_monitoring_security_ps AS PARTITION
netmdm_monitoring_security_pf TO (
 [netmdm_moni_seg]
,[netmdm_moni_dp_0001],[netmdm_moni_dp_0001],[netmdm_moni_dp_0001]
,[netmdm_moni_dp_0001],[netmdm_moni_dp_0001],[netmdm_moni_dp_0001]
,[netmdm_moni_dp_0001],[netmdm_moni_dp_0001],[netmdm_moni_dp_0001]
,[netmdm_moni_dp_0001],[netmdm_moni_dp_0001],[netmdm_moni_dp_0001]
,[netmdm_moni_dp_0001],[netmdm_moni_dp_0001],[netmdm_moni_dp_0001]
,[netmdm_moni_dp_0001],[netmdm_moni_dp_0001],[netmdm_moni_dp_0001]
,[netmdm_moni_dp_0001],[netmdm_moni_dp_0001],[netmdm_moni_dp_0001]
,[netmdm_moni_dp_0001],[netmdm_moni_dp_0001],[netmdm_moni_dp_0001]
,[netmdm_moni_dp_0001],[netmdm_moni_dp_0001],[netmdm_moni_dp_0001]
,[netmdm_moni_dp_0001],[netmdm_moni_dp_0001],[netmdm_moni_dp_0001]
,[netmdm_moni_dp_0001]
,[netmdm_moni_dp_0002],[netmdm_moni_dp_0002],[netmdm_moni_dp_0002]
,[netmdm_moni_dp_0002],[netmdm_moni_dp_0002],[netmdm_moni_dp_0002]
,[netmdm_moni_dp_0002],[netmdm_moni_dp_0002],[netmdm_moni_dp_0002]
,[netmdm_moni_dp_0002],[netmdm_moni_dp_0002],[netmdm_moni_dp_0002]
,[netmdm_moni_dp_0002],[netmdm_moni_dp_0002],[netmdm_moni_dp_0002]
,[netmdm_moni_dp_0002],[netmdm_moni_dp_0002],[netmdm_moni_dp_0002]
,[netmdm_moni_dp_0002],[netmdm_moni_dp_0002],[netmdm_moni_dp_0002]
,[netmdm_moni_dp_0002],[netmdm_moni_dp_0002],[netmdm_moni_dp_0002]
,[netmdm_moni_dp_0002],[netmdm_moni_dp_0002],[netmdm_moni_dp_0002]
,[netmdm_moni_dp_0002]
,[netmdm_moni_dp_0003],[netmdm_moni_dp_0003],[netmdm_moni_dp_0003]
,[netmdm_moni_dp_0003],[netmdm_moni_dp_0003],[netmdm_moni_dp_0003]
,[netmdm_moni_dp_0003],[netmdm_moni_dp_0003],[netmdm_moni_dp_0003]
,[netmdm_moni_dp_0003],[netmdm_moni_dp_0003],[netmdm_moni_dp_0003]
,[netmdm_moni_dp_0003],[netmdm_moni_dp_0003],[netmdm_moni_dp_0003]
,[netmdm_moni_dp_0003],[netmdm_moni_dp_0003],[netmdm_moni_dp_0003]
,[netmdm_moni_dp_0003],[netmdm_moni_dp_0003],[netmdm_moni_dp_0003]
,[netmdm_moni_dp_0003],[netmdm_moni_dp_0003],[netmdm_moni_dp_0003]
,[netmdm_moni_dp_0003],[netmdm_moni_dp_0003],[netmdm_moni_dp_0003]
,[netmdm_moni_dp_0003],[netmdm_moni_dp_0003],[netmdm_moni_dp_0003]
,[netmdm_moni_dp_0003]
,[netmdm_moni_dp_0004],[netmdm_moni_dp_0004],[netmdm_moni_dp_0004]
,[netmdm_moni_dp_0004],[netmdm_moni_dp_0004],[netmdm_moni_dp_0004]
,[netmdm_moni_dp_0004],[netmdm_moni_dp_0004],[netmdm_moni_dp_0004]
,[netmdm_moni_dp_0004],[netmdm_moni_dp_0004],[netmdm_moni_dp_0004]
,[netmdm_moni_dp_0004],[netmdm_moni_dp_0004],[netmdm_moni_dp_0004]
,[netmdm_moni_dp_0004],[netmdm_moni_dp_0004],[netmdm_moni_dp_0004]
,[netmdm_moni_dp_0004],[netmdm_moni_dp_0004],[netmdm_moni_dp_0004]
,[netmdm_moni_dp_0004],[netmdm_moni_dp_0004],[netmdm_moni_dp_0004]
,[netmdm_moni_dp_0004],[netmdm_moni_dp_0004],[netmdm_moni_dp_0004]
,[netmdm_moni_dp_0004],[netmdm_moni_dp_0004],[netmdm_moni_dp_0004]
,[netmdm_moni_dp_0005],[netmdm_moni_dp_0005],[netmdm_moni_dp_0005]
,[netmdm_moni_dp_0005],[netmdm_moni_dp_0005],[netmdm_moni_dp_0005]
,[netmdm_moni_dp_0005],[netmdm_moni_dp_0005],[netmdm_moni_dp_0005]
,[netmdm_moni_dp_0005],[netmdm_moni_dp_0005],[netmdm_moni_dp_0005]
,[netmdm_moni_dp_0005],[netmdm_moni_dp_0005],[netmdm_moni_dp_0005]
,[netmdm_moni_dp_0005],[netmdm_moni_dp_0005],[netmdm_moni_dp_0005]
,[netmdm_moni_dp_0005],[netmdm_moni_dp_0005],[netmdm_moni_dp_0005]
,[netmdm_moni_dp_0005],[netmdm_moni_dp_0005],[netmdm_moni_dp_0005]
,[netmdm_moni_dp_0005],[netmdm_moni_dp_0005],[netmdm_moni_dp_0005]
,[netmdm_moni_dp_0005],[netmdm_moni_dp_0005],[netmdm_moni_dp_0005]
,[netmdm_moni_dp_0005]
,[netmdm_moni_dp_0006],[netmdm_moni_dp_0006],[netmdm_moni_dp_0006]
,[netmdm_moni_dp_0006],[netmdm_moni_dp_0006],[netmdm_moni_dp_0006]
,[netmdm_moni_dp_0006],[netmdm_moni_dp_0006],[netmdm_moni_dp_0006]
,[netmdm_moni_dp_0006],[netmdm_moni_dp_0006],[netmdm_moni_dp_0006]
,[netmdm_moni_dp_0006],[netmdm_moni_dp_0006],[netmdm_moni_dp_0006]
,[netmdm_moni_dp_0006],[netmdm_moni_dp_0006],[netmdm_moni_dp_0006]
,[netmdm_moni_dp_0006],[netmdm_moni_dp_0006],[netmdm_moni_dp_0006]
,[netmdm_moni_dp_0006],[netmdm_moni_dp_0006],[netmdm_moni_dp_0006]
,[netmdm_moni_dp_0006],[netmdm_moni_dp_0006],[netmdm_moni_dp_0006]
,[netmdm_moni_dp_0006],[netmdm_moni_dp_0006],[netmdm_moni_dp_0006]
)
GO
```

F.18 LargeAddFilegroup2nd.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILEGROUP [netmdm_moni_dp_0007]
GO
```

F.19 LargeAddFiletoKdrive.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER DATABASE NETMDM_SAMPLE ADD FILE (
        NAME = N'NETMDM_DP_0007',
        FILENAME = N'K:\NETMDP\MONITOR_DP_0007.ndf',
        SIZE = 800GB, MAXSIZE = UNLIMITED, FILEGROWTH = 10%
) TO FILEGROUP [netmdm_moni_dp_0007]
GO
```

F.20 LargeAlterPartition.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110701')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110702')
```

```
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110703')
GO
ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110704')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110705')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110706')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO
ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110707')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110708')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110709')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110710')
GO
ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110711')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110712')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110713')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO
ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110714')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110715')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110716')
GO
```

```
ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110717')
GO
ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110718')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110719')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110720')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO
ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110721')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110722')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110723')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110724')
GO
ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110725')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110726')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110727')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO
ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110728')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110729')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110730')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0007]
GO
```

```
ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110731')
GO
```

F.21 LargeSwitchPartition.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 1 TO
netmdm_monitoring_security_arch PARTITION 1
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 2 TO
netmdm_monitoring_security_arch PARTITION 2
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 3 TO
netmdm_monitoring_security_arch PARTITION 3
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 4 TO
netmdm_monitoring_security_arch PARTITION 4
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 5 TO
netmdm_monitoring_security_arch PARTITION 5
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 6 TO
netmdm_monitoring_security_arch PARTITION 6
GO
ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 7 TO
netmdm_monitoring_security_arch PARTITION 7
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 8 TO
netmdm_monitoring_security_arch PARTITION 8
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 9 TO
netmdm_monitoring_security_arch PARTITION 9
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 10 TO
netmdm_monitoring_security_arch PARTITION 10
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 11 TO
netmdm_monitoring_security_arch PARTITION 11
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 12 TO
netmdm_monitoring_security_arch PARTITION 12
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 13 TO
netmdm_monitoring_security_arch PARTITION 13
GO
ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 14 TO
netmdm_monitoring_security_arch PARTITION 14
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 15 TO
netmdm_monitoring_security_arch PARTITION 15
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 16 TO
netmdm_monitoring_security_arch PARTITION 16
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 17 TO
netmdm_monitoring_security_arch PARTITION 17
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 18 TO
netmdm_monitoring_security_arch PARTITION 18
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 19 TO
```

```
netmdm_monitoring_security_arch PARTITION 19
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 20 TO
netmdm_monitoring_security_arch PARTITION 20
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 21 TO
netmdm_monitoring_security_arch PARTITION 21
GO
ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 22 TO
netmdm_monitoring_security_arch PARTITION 22
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 23 TO
netmdm_monitoring_security_arch PARTITION 23
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 24 TO
netmdm_monitoring_security_arch PARTITION 24
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 25 TO
netmdm_monitoring_security_arch PARTITION 25
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 26 TO
netmdm_monitoring_security_arch PARTITION 26
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 27 TO
netmdm_monitoring_security_arch PARTITION 27
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 28 TO
netmdm_monitoring_security_arch PARTITION 28
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 29 TO
netmdm_monitoring_security_arch PARTITION 29
GO
ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 30 TO
netmdm_monitoring_security_arch PARTITION 30
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 31 TO
netmdm_monitoring_security_arch PARTITION 31
GO

ALTER TABLE netmdm_monitoring_security SWITCH PARTITION 32 TO
netmdm_monitoring_security_arch PARTITION 32
GO
```

F.22 LargeMergeRange.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110101')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110102')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110103')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110104')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110105')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110106')
GO
ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110107')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110108')
```

```
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110109')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110110')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110111')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110112')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110113')
GO
ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110114')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110115')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110116')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110117')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110118')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110119')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110120')
GO
ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110121')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110122')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110123')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110124')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110125')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110126')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110127')
GO
ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110128')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110129')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110130')
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() MERGE RANGE ('20110131')
GO
```

F.23 LargeAlterPartition2nd.sql query script

```
USE [NETMDM_SAMPLE]
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110801')
GO
```

```
ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110802')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110803')
GO
ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110804')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110805')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110806')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO
ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110807')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110808')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110809')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110810')
GO
ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110811')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110812')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110813')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO
ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110814')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110815')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO
```

```
ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110816')
GO


ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110817')
GO
ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110818')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110819')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110820')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO
ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110821')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110822')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110823')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110824')
GO
ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110825')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110826')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110827')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO
ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110828')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110829')
GO

ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110830')
GO
```

```
ALTER PARTITION SCHEME netmdm_monitoring_security_ps NEXT USED [netmdm_moni_dp_0001]
GO

ALTER PARTITION FUNCTION netmdm_monitoring_security_pf() SPLIT RANGE ('20110831')
GO
```

G. Version Changes

(1) Changes in version 09-50

- Windows 7 and Windows Server 2008 R2 are now supported.
- If remote installation of JP1/Software Distribution Client (relay system) is performed on a JP1/Software Distribution (relay system) in which Automatic Installation Tool is installed, all components other than Automatic Installation Tool are now updated.
- The user can now set as system information that password protection for screen saver information is to be acquired even if the screen saver is disabled.
- The following inventory information (system information) can now be collected:
    - Encryption information set by BitLocker
    - Drive (hard drive) encryption information set by HIBUN FDE
    - Linux distribution
- Software information can now be collected for additional Microsoft Office products. In addition, greater detail about Microsoft Office products is now provided.
- Software information can now be collected for additional anti-virus products.
- Directory information about groups can now be acquired from Active Directory. In addition, the argument `/d` has been added to the command for acquiring directory information (`dcmadsync.exe`), which enables the user to delete directory information that has already been acquired.
- The operation status of virtual environments can now be monitored.
- Use of the devices listed below can now be suppressed. In addition, their connection history, disconnection history, connection permission logs, and connection suppression logs can now be acquired.
    - Bluetooth devices
    - Imaging devices
- If suppression exclusion conditions are set when access to USB media is suppressed, the following logs can now be acquired:
    - Connection permission log
    - Connection suppression log
- Writing can now be suppressed individually for the following devices, and their connection suppression logs can now be acquired:
    - Internal CD/DVD drives
    - Internal floppy disk drives
    - IEEE 1394 connection devices
    - Internal SD card readers
- Operation of JP1/Software Distribution Client (client) is now supported in Windows XP Mode environments.
- The facilities for acquiring print logs and for suppressing printing can now be used when a shared network printer is being used in Windows Vista or Windows Server 2008.
- In the event that a USB media device for which operations have been suppressed is connected to a client PC, the corresponding JP1 event can now be reported as an alert.
- If one of the devices listed below is connected to a client PC when its use is suppressed, a message indicating that use of that device is suppressed can be displayed on the client PC. In addition, the corresponding JP1 event can be reported to JP1/IM as an alert.
    - Internal CD/DVD drives
    - Internal floppy disk drives
    - IEEE 1394 connection devices
    - Internal SD card readers

  - Bluetooth devices
  - Imaging devices
- If startup of a software program is suppressed, the corresponding JP1 event can be reported as an alert.
- If printing is suppressed, the corresponding JP1 event can be reported as an alert.
- Content on the following pages in the server setup process has been modified:
  - **Operation Monitoring** page
  - **AIM** page
- Operation monitoring history can now be stored using the data partitioning facility provided in Microsoft SQL Server 2008 and Microsoft SQL Server 2005.
- An explanation has been added about the relationship between directory information and system configuration information.
- By assigning divisions to users when inventory information is being managed with Asset Information Manager Subset, a single user can manage information about multiple groups.
- The minimum and recommended CPU performance specifications needed to run products and components of JP1/Software Distribution have been changed.
- An explanation has been added about the memory requirements on a managing server when Embedded RDB is used as the relational database.
- The formulas used to estimate the disk capacity needed for Microsoft SQL Server and Oracle databases have been revised.
- If operation monitoring logs are set on the **Report To Higher System** page to be relayed to a higher system, the user can now select which information is sent to the higher system.
- The firewall data pass-through direction can now be changed when the port number and protocol are set to 30002/udp.
- The CPU type can now be acquired as system information.
- The sizes of the following columns in the netmdm_ospatch_patchinf relational database table have been changed:
  - `dm_title`
  - `dm_kbarticle`
- When Embedded RDB is used as the database, a maximum of 1,840 megabytes of patch data can now be stored in the netmdm_ospatch_patchinf relational database table.
- The maximum number of characters that can be used in a collection path name has been increased from 63 half-width characters to 256 half-width characters.
- Explanations have been added about the correspondences between the settings in the Windows and UNIX editions of JP1/Software Distribution.
- A checkbox labeled **Do not repeat package IDs when collecting software information** has been added to the client setup **Job Options** page to allow suppression of duplicate package IDs.
- The following explanation has been moved to the chapter on setting up JP1/Software Distribution Manager:
  - Registry setting for displaying the OS name
- By specification of a registry setting, command processing can now be set to continue even after the user has logged off of Windows.
- By specification of the argument /LC in a command, command processing can now be set to continue even after the user has logged off of Windows.
- Unicode CSV files can now be output using the CSV output utility or the CSV output command (`dcmcsvu.exe`).
- During the client setup process, the user can now select on the **Error Handling** page whether to output messages to the event viewer.
- The following log files can now be output:
  - `DPTExpt.log`
  - `DPTInpt.log`

- The number of log entries has been changed by moving INVENTRY.LOG to the FUNC log.
- The argument `/n` has been added to the command (`dcmmonrst.exe`) that stores operating information in a database; this argument enables the user to check the status of a store process. A log file for checking the store process status has also been added (`MONRST.LOG`).
- The minimum size of the security update management file has been changed to 130 megabytes.
- When upgrading Embedded RDB, the user can now select whether to migrate patches acquired by the security update management facility.
- The command DPTInpt.exe (store patches in database) has been added, which enables the user to migrate patches acquired by the security update management facility.
- An explanation of possible corrective actions to take in order to handle delays in automatic notifications from the relay managing the ID has been added.
- The setting **Manage device change log information** has been added under **Basic Information** in the Server Setup dialog box of Asset Information Manager Subset. This setting allows the user to select whether to manage the initial change history of a device to be managed when the *Delete change log* task is performed.
- Login authentication can now be performed by linking Asset Information Manager Subset to Active Directory. In addition, Active Directory user information can now be acquired.
- The setting **Targets for inventory** has been added under **Link with JP1/SD** in the Server Setup dialog box of Asset Information Manager Subset. This setting allows the user to acquire inventory information from all devices, or only from devices with host IDs, or only from devices with system information.
- The setting **CSC notification count** has been added under **Link with JP1/SD** in the Server Setup dialog box of Asset Information Manager Subset. This setting allows the user to set the timing for reporting acquisition of JP1/Software Distribution inventory information to JP1/Client Security Control.
- The setting **Inventory acquisition method** has been added under **Link with JP1/SD** in the Server Setup dialog box of Asset Information Manager Subset. This setting allows the user to select **Multithreading method** as the method for acquiring inventory information.
- The setting **Multiplex level for inventory** has been added under **Link with JP1/SD** in the Server Setup dialog box of Asset Information Manager Subset. This setting allows the user to specify the multiplex level when inventory information is collected using the multithread method.
- Modification date of system configuration information and modification date of registry information can now be managed as asset information.
- Explanations have been added about upgrading the program version and migrating data in a cluster system environment.
- JP1/Software Distribution Client (client) is now supported for Citrix XenApp (public desktop) running on a terminal server.
- Explanations about starting and stopping the managing server have been added.

  The following explanation has also been included:

  System shutdown procedure when using Embedded RDB as the relational database.
- A facility has been added for backing up operation monitoring results. With this addition, the dmTRUtil.exe command can now be used to output a backup of the operation monitoring results to a CSV file.
- The following capabilities have been added for using device instance IDs to set exclusion conditions for suppressing connection of USB media:
  - The device instance ID of a USB controller can be set as an exclusion condition.
  - A comparison method can be selected for comparing device instance IDs against a specified condition character string.
- A note has been added in the Software Operation Information window stating that software operation history is not displayed for clients if more than 560,000 operation history entries have been stored.
- Explanations have been added about environment variables that cannot be set and other items that are not available when offline installation is performed.
- The dcmstdiv.exe command has been added to enable command-initiated entry of information about offline machines.
- The following items have been added as information that can be output to a CSV file by the CSV output utility or the dcmscvu command:

    - Registry path (registry collection items template)
    - Software indicator ID (Microsoft Office products template)
    - Software indicator ID (anti-virus products template)
- Client configuration settings can now be changed when remote installation of JP1/Software Distribution Client (client) is used.
- The following settings have been added for remote setup of clients:
    - **Host name or IP address**
    - **Product type**
    - **When the system is changed, inventory information is notified to Higher System**
- If operation history on a client is lost, the corresponding JP1 event can now be reported as an alert.
- Descriptions have been added about system maintenance operations that need to be performed. In addition, explanations about the following items have been included:
    - How to change the JP1/Software Distribution Manager settings in a cluster system environment
    - Recommended intervals for performing various database maintenance operations
    - Procedures for backing up and restoring the system
- WMI information can now be collected.
- Messages have been added for the following event IDs:
    - `1081`
    - `1082`
    - `1083`
    - `1084`
    - `1085`
    - `1086`
    - `2021`
    - `11029`
    - `16031`
- A JP1/Software Distribution Client (client) event log message is no longer output for event ID 7009.
- Messages with the following IDs have been added to the section about event log messages for which monitoring is recommended (including the causes and the corrective actions to be taken):
    - `16023`
    - `16024`
    - `16031`
- The basic client log messages KDSF0055-W and KDSF0123-E have been added.
- The contents of the basic client log messages KDSF0010-I and KDSF0020-I have been changed.

(2) Changes in version 09-00

- Microsoft SQL Server 2008 can now be used as a relational database program.
- Additional anti-virus products can now be acquired as software information.
- Specific USB media can now be excluded from being suppressed. In addition, if USB media connected to a client PC is being suppressed, a message indicating that fact can now be displayed.
- When automatic storage of operation information is not being performed, the information can now be manually stored in a database by executing the `dcmmonrst` command with the `/x` argument specified.
- Hitachi bundle-named (name created from multiple products) products stored on Hitachi bundled-product CD-ROMs can now be packaged.

- Output of messages to the event log by Embedded RDB that are not required for operations can now be suppressed.
- Hosts can now be deleted from system configuration information by removing the host from the ID group.
- Remote Installation Manager of JP1/Software Distribution Manager can now be used to add a host group or a host from a file.
- The following items have been changed in the Server Setup dialog box of Asset Information Manager Subset.
    - The minimum value that can be specified for the **Communication-less monitoring time** setting under **Session Information** has been changed to 5 minutes.
    - The **Status to display in device search windows** setting has been added under **Basic Information**, allowing the user to choose the device statuses to display as **Status** search conditions in the Device Totals and Device List windows.
- If **Scheduled Tasks** is used to automatically obtain patches, the following functions can now be used:
    - Deletion of security updates after packaging
    - Non-downloading of packaged security updates
- The user name, host name, and IP address can now be specified as search conditions in the Batch Update window of Asset Information Manager Subset.
- The `Text_Title` (text for dialog box titles) item has been added to the Asset Information Manager Subset `VariousInfo` management class, allowing the user to change the title of operation windows.
- Information about the cause and handling of the `3000AF008300` maintenance code has been added to the event log message.
- Commands for backing up and restoring package files and operation history files have been added when Microsoft SQL Server or Oracle is being used as the relational database:
    - `netmfile_backup.bat`
    - `netmfile_restore.bat`
- The following inventory information items can now be acquired:
    - Turn off hard disks (AC)
    - Turn off hard disks (DC)
    - System standby/Sleep (AC)
    - System standby/Sleep (DC)
    - System hibernates (AC)
    - System hibernates (DC)

  Additionally, operation examples of dealing with clients whose power-save setting is not configured and of shutting down clients have been added.
- The operation monitoring function can now be applied to offline machines through the use of media.
- The maximum size of the management file cache can now be specified during setup of relay systems, so that decreases in job processing throughput can be avoided, even if the number of jobs managed by the relay system increases.
- Re-installation is now performed automatically if the initial installation of JP1/Software Distribution Client fails. In addition, the location of the InstallShield environment deletion tool, which is executed if re-installation of JP1/Software Distribution Client fails, is now noted.
- Procedures have been added describing how to perform an overwrite installation or a re-installation of JP1/Software Distribution Manager in a cluster system.
- Job execution results are now recorded, regardless of the setting specified for the **Record the results of ID group jobs** during setup of the relay system, so that relay system ID group jobs can be re-executed by default.
- If Embedded RDB is used for the JP1/Software Distribution Manager database, the size of the operation table area can now be increased automatically.
- If Embedded RDB is used to create an Asset Information Manager Subset database, the size of the database can be expanded automatically.

- A CSV-format backup of Asset Information Manager Subset databases can now be obtained by executing `jamdbexport.bat`.
- An explanation has been added about `jamemb_backup.bat`, which is used to obtain backup files of Asset Information Manager Subset databases in an Embedded RDB environment.
- An explanation has been added about `jamemb_reorganization.bat`, which is used to re-organize Asset Information Manager Subset databases in an Embedded RDB environment.
- As an option for `jamTakeOperationLog.bat`, the group, user name, and location information can now be output to a CSV file when a search pattern is used to output all items in an operation log.
- Event log messages have been added for the following event IDs:
  - `8060`
  - `8061`
  - `8064`
  - `8065`
  - `8066`
  - `8067`
  - `8068`
  - `8069`

(3) Changes in version 08-51

- WUA 3.0 can now be used to acquire client patch information.
- Active Directory information can now be collected on managing servers, specified for job destinations, and viewed in Inventory Viewer.
- Asset Information Manager Subset can now be used to count inventory information items based on job purpose.
- Web access logs, and the logs of print operations and operations to and from external media, can now be acquired as software operation information. Also, printing and operations to and from external media can now be suppressed.
- When a computer that supports AMT is used as a client, the client's BIOS can now be controlled remotely. Also, a diagnostic program on a floppy disk in the managing server can now be used to perform checks on clients.
- Through the use of Microsoft .NET Framework 3.0, AMT Linkage can now be used for clients in a wireless LAN environment.
- Some JP1/Software Distribution Manager components can now be used on Windows Vista.
- Windows Server 2008 is now supported.
- Security-related items can now be acquired as system information.
- The following power management information can now be acquired as system information:
  - Turn off monitor (AC)
  - Turn off monitor (DC)
  - Processor throttle (AC)
  - Processor throttle (DC)
- Software information can now be acquired for additional anti-virus products. A description has also been added about the ability to determine the resident/nonresident status of various anti-virus products.
- Software information on Hitachi program products can now be acquired by using **Search software listed in "Add/Remove Programs"**.
- Whether to save operation information reported to a central manager or relay manager from lower-level systems is now selectable. Whether or not to report operation information received by a relay manager from a lower-level system to a higher-level system can now be selected as well.
- Operation monitoring policies can now be output to a file. Operation monitoring policies can also now be added by importing these output files.

- Operation monitoring functions can now be used for clients running the 64-bit version of Windows Vista.
- File operation history can now be acquired from clients running Windows Server 2008 or Windows Vista.
- Network drives can now be used as directories for storing operation history and backups.
- Database Manager can now be used to create a database area for acquired patches. Windows Mail has also been added as a program type for which patches can be acquired.
- JP1/Software Distribution can now link to WSUS 3.0. When linked to a hierarchically-configured WSUS system, downstream WSUS servers can now be synchronized with the top-level WSUS server, and clients can now be registered to computer groups of downstream WSUS servers.
- Windows Remote Desktop operations are now supported.
- Software inventory information can now be managed under Coordinated Universal Time (UTC).
- The default, minimum, and maximum sizes of the Embedded RDB database area have been changed. The size of the Embedded RDB work table area can also now be specified with Database Manager.
- A formula for calculating the size of the operation monitoring logs has been added to the formulas for estimating the area required for the Embedded RDB database.
- A formula for calculating the size of the registry acquisition items has been added to the formulas for estimating the area required for the Microsoft SQL Server database.
- The Windows Server 2008 and Windows Vista versions of JP1/Software Distribution Client can now be used for relay systems.
- The check box for displaying the Readme file when installation finishes has been removed.
- A description has been added about the log files in which the number of managed log generations and entries cannot be set.
- The following Embedded RDB commands now output return codes:
  - netmdb_backup.bat
  - netmdb_reload.bat
  - netmdb_reorganization.bat
  - netmdb_unload.bat
- A description of the backup procedure for Asset Information Manager Subset has been added.
- The date and time that software registered in **Add/Remove Programs** is installed can now be acquired along with other software information.
- When automatic host group maintenance is used to create a host group based on user inventory information, the maximum number of characters that can be used in the host group name has been changed to 32.
- The `JOB_DESTINATION_ID` tag used by the command parameter file can now be used to specify a relay managing the ID on which to execute the job.
- A command can now be used to acquire information about problems that occur in JP1/Software Distribution.
- Event log messages assigned the following event IDs have been added:
  - `11026`
  - `11027`
  - `11028`
  - `16029`
  - `16030`

  Also, it is now recommended to monitor for event ID `16030` event log messages.

(4) Changes in version 08-10

- Functionality has been added to enable management of users of JP1/Software Distribution when linked to JP1/Base.
- The following functionalities can now be used when computers that support AMT are used as clients:
  - Control of clients that use the AMT power control feature

  - Storing of host IDs in nonvolatile memory provided by AMT
- Software operation time at clients can now be acquired by the function for monitoring software operation status. In addition, a function has been added that totals the acquired operation times in the Software Operation Status window.
- Operation logs can now be traced by using the File Operation Trace window.
- A function has been added that obtains security updates, service packs, and other patches provided by Microsoft.
- A function has been added that provides HTML message notifications to clients.
- Operation logs can now be totaled by group using the Operation Log Total window.
- Support for Windows Vista has been added in the following program product:
  - JP1/Software Distribution Client
- Anti-virus products for which software information can be acquired have been added.
- Version and generation numbers have been added to operation monitoring policies, to make it easier to understand which operation monitoring policy is being applied.
- Text-format files that contain policy information for automatic maintenance of host groups and ID groups can now be imported and exported.
- A user inventory item has been added as a policy type for automatic maintenance of ID groups.
- The description of the number of clients that can be connected directly to a relay system has been modified.
- The data types of some database items in Embedded RDB have been changed, and the size of the database that is created has been reduced.
- The descriptions of the formulas for estimating database size have been improved by clarifying the items targeted by the calculations.
- Functionality has been added so that clients using the host name as the ID key for operations and which are unable to resolve the name of the connection-target higher system through normal means can perform name resolution and connect to the higher system based on the IP address received in the execution request information.
- A function has been added for output of JP1/Software Distribution's operation as audit logs.
- The method of setting up Asset Information Manager Subset and creating a database has been changed.
- A setting has been added to disable display of dialogs while JP1/Software Distribution Client is being installed remotely.
- An additional facility has been added as a JP1/Software Distribution Client component.
- The function that detects hosts on which JP1/Software Distribution is not installed can now detect hosts in a VPN environment with routers that do not support SNMP in the search path.
- The apostrophe (`'`) can now be entered in text-entry user inventory items.
- The basic log message at the client (`KDSF0096-W`) has been changed.
- A program product ID file can now be created from the Package Information tool when an AIT file is created.
- The following messages about editing AIT files have been added: `AITG123-E`, `AITG124-E`, `AITG125-E`

(5) Changes in version 08-00

- Microsoft SQL Server 2005 is now supported as a relational database program.
- Embedded RDB is supported as the standard relational database provided by JP1/Software Distribution Manager. Basic databases are no longer supported.
- In the Find dialog box, hosts can now be searched by using the host name or IP address as the key value.
- The automatic host group maintenance facility enables hosts to be grouped by the client's OS sub-version.
- The software operation monitoring facility enables the user to select whether or not startup of specified software and path is to be permitted. It also enables the user to select whether or not startup of all software other than specified items is to be permitted.
- The software operation monitoring facility can acquire a file manipulation log.
- Client operation information can now be viewed in the Operation Log List window.

- WUA can be used to acquire information on installed patches.
- Anti-virus products that can be acquired as software information have been added.
- The Add Destination, Add Package, and Save Job dialog boxes can now be resized.
- The maximum number of user inventory items that can be selected has been changed from 255 items to a total size of 51,254 bytes. For hierarchized user inventory items, a maximum size of 102,509 bytes, including the higher items, has been added.
- In split package distribution, the status of execution from relay system to lower system can now be checked at the higher system.
- Polling has been added as a timing for automatically changing a client's connection destination.
- A function for setting client security management has been added for use when JP1/Client Security Control is linked.
- The JP1/Software Distribution management facility and the client installation facility are no longer supported for Web browsers.
- The differing-components distribution facility is no longer supported.
- WUA can be used to acquire information on uninstalled patches.
- WSUS can be linked to manage security updates.
- Windows Server 2003 (x64) is now supported.
- Parentheses (`(` and `)`) are now permitted in installation and work directory names.
- The system configuration information can be searched for duplicate hosts and the hosts with the older update dates/times can be deleted.
- An option for delaying a client's polling start time has been added.
- A description of Embedded RDB settings in a firewall environment has been added.
- CPU types have been added to the system information that can be acquired.
- The user can now select whether or not to use the standard retrieve list when software information is acquired.
- When a package is distributed to a UNIX client and an external program is started, the external program's termination code can now be referenced by the server.
- JP1/Software Distribution can now install security update data on the security PC.
- Additional anti-virus products for which information can be acquired have been added.
- Descriptions of environment variables that can be specified in **Skip directory** on the **Options** page and in **File name by full path** on the **Collect File** page of the Create Job dialog box have been added.
- Name of a hotfix whose format is changed when it is displayed as software information by Remote Installation Manager has been added.
- Contents of client's basic log messages `KDSF0060-I` and `KDSF0090-I` have been changed.
- `KDSF0097-I`, `KDSF0098-W`, and `KDSF0099-E` have been added to client's basic log messages.
- In Remote Installation Manager's Job Status window, a folder is now created to store the *Report message* job executed from JP1/Client Security Control.
- During host search, the user can now select whether or not host names are to be acquired. The user can also select the range of host information to be acquired.
- Inventory information for Microsoft Office products and anti-virus products can now be acquired from offline machines.
- A description of how to make a backup of suppress history and operation history has been added.
- Event log message with event ID `19003` has been added.
- System security measures can now be enhanced by linking to JP1/Client Security Control.

(6) Changes in version 07-50

- The *Get software information from client* job now provides capability to acquire information about patches that have not been installed on a computer. This also allows Remote Installation Manager to display information on patches that have not been installed on a computer.

An event log message maintenance code (`3000EF300000`) has also been added.

- Capabilities to monitor the operating status of client software, suppress startup of software, and obtain the operation history of software are now provided. Remote Installation Manager can now also display suppression logs and operation logs.

  Event IDs 16016 and 16020 messages have also been added.
- An administrator can now send messages to clients.
- Notification of event information that has been updated on a client can now be reported automatically to the higher system.
- A facility for automatic maintenance of ID groups has been added, which provides capability to register automatically new clients added to an ID group by setting a policy for that ID group.
- JP1/Software Distribution Manager Embedded RDB Edition has been added.
- Capability to search hosts that exist on a network and to detect hosts on which JP1/Software Distribution is not installed is now provided.
- Information that enables JP1/Asset Information Manager to monitor updating of inventory information has been added to several tables in the database.
- Causes and actions to take for event log messages that recommend monitoring have been added.
- Client's basic log message `KDSF0103-I` has been added.
- Contents of client's basic log messages `KDSF0060-I` and `KDSF0092-E` have been changed.
- AIT files provided by JP1/Software Distribution have been added.
- Capability to install software on a PC on which JP1/Software Distribution Client is installed without using a network has been added.
- Because an installation set can now be used to overwrite a previous installation of JP1/Software Distribution Client, the overwrite installation item has been deleted from the table that indicates differences between using an installation set and installing from a Web browser.

  Descriptions of the use of an installation set when performing an overwrite installation have also been added to the procedure for configuring JP1/Software Distribution Client setup information.
- Hosts on which JP1/Software Distribution is not installed (hosts without JP1/Software Distribution installed) can now be detected by reading a CSV file containing information about the hosts in the network.
- CPU types have been added as system information that can be acquired.
- A description of operating JP1/Software Distribution in the terminal service environment has been added.
- Support has been added for running Microsoft Windows Server 2003, Enterprise Edition, as a cluster system OS for JP1/Software Distribution.
- The *Get software information from client* job now provides capability to acquire information about patches that have been installed on a computer. The acquired patch information can also be displayed by Remote Installation Manager and Package Setup Manager.
- Anti-virus products have been added as system information that can be acquired.
- When user inventory items are being created, the only characters that cannot be used in a comment field now are the semicolon (;) and percent sign (%).
- When a *Transfer user inventory schema to client* job is being created, whether or not to allow the user to cancel user inventory items in the dialog box and for the client to specify an action after the user inventory has been set has been added.
- Acquired Microsoft Office product and anti-virus product information can now be output to a CSV-format file.
- Notes about creating and using AIT files have been added.
- Capability to distribute software and check distribution status from operation windows of JP1/Asset Information Manager has been added.
- JP1/Software Distribution Client can no longer be installed on PCs on which Client Installation by Web and the Startup Kit Support Tool are installed.
- JP1/Software Distribution SubManager can now be used by a user logged on without Administrator permissions to perform remote installation.

- If an error occurs while an overwrite installation is being performed, information on the previously installed package can now be retained.
- By setting a priority for use of network adapters, a client's IP address can now be reported to the higher system.
- Host inventory information not included in the system configuration can now be deleted.
- *Windows Installer* has been added to system information to maintain Windows Installer version information. *Windows Installer* can now be counted in Inventory Viewer as well.
- Registered tools can now be started from Remote Installation Manager.
- Silent installation of programs can now be performed using Windows Installer.
- For the UNIX version of JP1/Software Distribution Client 07-50 and later, whether or not to restart the client machine automatically after a package has been installed can now be specified.
- When in the Job Definition window a job selected with the **F5** key is executed, a confirmation dialog box is now displayed.
- The method for acquiring the CPU clock speed has been changed.
- Microsoft Office products have been added as software information that can be acquired.
- *OS language* can now be counted in Inventory Viewer.
- The following commands can now be executed from JP1/Software Distribution SubManager:
  `dcmcoll.exe`, `dcminst.exe`, `dcmjbrm.exe`, `dcmjexe.exe`, `dcmpkrm.exe`, `dcmrmgen.exe`, `dcmrtry.exe`, `dcmstat.exe`, `dcmstsw.exe`
- The causes and actions to take for event log messages of maintenance codes `300097140000` and `30009F070000` have been changed.
- A section has been added that describes the functional differences between JP1/Software Distribution Manager and JP1/Software Distribution SubManager.
- An AIT file for distributing Windows Installer modules has been provided.

(7) Changes in version 07-00

- Windows 95 is no longer supported by JP1/Software Distribution Client. However, because JP1/Software Distribution Client versions earlier than 07-00 can connect to a higher system of version 07-00, explanations for Windows 95 were added to the manual.
- For a *Get software information from client* job, **Search for Microsoft Office products** and **Search for anti-virus products** were added to the **Software to be searched** option. Also, the number of hosts can now be counted for each product name, virus-definition file version, and residency setting of anti-virus products.
- AIT files, which are script files used to send responses to a software installer automatically, are supported. If an AIT file is packaged and remote-installed together with software, the software can be installed automatically.
- Extraction and packaging of differing-components is no longer supported by JP1/Software Distribution versions 07-00 or later (differing-components packages created with JP1/Software Distribution versions earlier than 07-00 can still be used).
- Client information can now be checked using Local System Viewer.
- Client systems can be monitored and alerts can be sent to the local PC or higher system in the event of errors.
- Alerts reported from clients can be checked at the higher system using alert information files, Event Viewer, and JP1/IM.
- The default values for client setup were changed.
- The **Remote Installation Client** and **Remote Installation Logon Manager** icons are no longer created in the Windows **Startup** group.
- The user can now choose to create the Software Distribution Client Setup folder.
- When the connection destination is undetermined, JP1/Software Distribution Client can be run by specifying `?`.
- The following features were added regarding job suspension and restart:
  - A relay manager can be specified as the destination of *Suspend file transfer* and *Resume file transfer* jobs.

  - Remote Installation Manager of JP1/Software Distribution Manager can suspend and restart file transfer between the local system and its lower systems.
  - Jobs can be suspended and restarted between lower systems in UNIX versions.
  - The `dcmsusp` command was added to suspend and restart file transfer.
- On the **Job Distribution Attributes** page, the user can specify whether or not to distribute jobs even if file transfer is currently suspended.
- Even if the client is not resident, a client user who logs on with non-Administrator user permissions can now install packages that could not be installed previously.
- A procedure was added for upgrading a relational database at the same time that JP1/Software Distribution was upgraded to Version 7i.
- When a version is not set in the software search list and acquisition of version information from the version resource for a specified file fails, `0000` is set as the version.
- During a search using a software search list, a file whose size is 0 bytes can now be searched.
- The detailed information about a destination can be displayed by starting Event Viewer from the Job Status window.
- When the Count Clients facility is executed from the System Configuration or Destination window, the selection status of hosts and host groups is also applied to the host selection window of Inventory Viewer. Additionally, the Count Clients facility can now be executed by specifying a template from the System Configuration or Destination window.
- The user can now specify a desired font in the Software Distribution Manager Unarchiver window (or Software Distribution SubManager Unarchiver window), JP1/Software Distribution Packager window, and Package Setup Manager window.
- The *Suspend file transfer* and *Resume file transfer* job types were added to enable file transfer to be suspended and restarted between a relay system and its lower systems.
- Remote startup and shutdown by the Client Control facility were implemented without having to place one or more relay managers or relay systems per router.
- JP1/Software Distribution can now establish connection even when another application has already established dial-up connection with the same destination.
- The maneuverability of the installer was improved.
- System configuration information can be used to manage the history of host deletions. Because of this change, the formula for determining the database size was also changed.
- The **Error Handling** page was added to the Server Setup dialog box to specify the number of generations of log files to be saved, the maximum number of entries, and the type of Event Viewer messages.
- The cause of the *Client not started* job execution status can be broken down.
- In the relay manager setup, the **Relay System Customization** page was changed to the **Report To Higher System** page.
- In the relay system setup, the **Report To Higher System** page was added, and the description of the **Send the result file to the server** option was moved from the **Relay System Customization** page to the **Report To Higher System** page.
- The client computer can be restarted automatically after package installation. Also, the client setup includes an option to specify whether or not to allow restart of the client computer.
- Display of a processing message during package installation can be specified for a package.
- A file was added to output a basic log related to client actions (`USER_CLT.LOG`).
- A facility was added to enable software to be deleted from the software inventory and to use the deleted software management table to manage deleted software. Because of this change, the formula for determining the database size was also changed.
- Partial match search is supported when host names are searched from the System Configuration window.
- In the Find dialog box, the search item **The hosts that have not had inventory updated within a certain period** was added to the **Find by Dates** page.
- Even when a package with installation date/time specified is distributed in a UNIX client, an external program can now be started immediately after installation.

- An option was added to support customization of default values in the Software Distribution Packaging dialog box and the Create Job dialog box dialog box.
- Packager and Remote Installation Manager can be used to check the detailed attributes of stored packages.
- For the following items among the system information that can be obtained, a supplementary explanation was provided:

  Name of OS family, drive capacity, free space, partition size, file system, logon user name, full name of user, user description
- **IE Patch and BIOS version** (SMBIOS) were added to the system information that can be acquired. Because of this change, the items that can be output to a CSV file were supplemented.
- A description was added regarding the handling when multiple Remote Installation Managers attempt to edit registry collection items and user inventory items at the same time.
- **Hold** was added as a software inventory management status. Also, detailed condition settings were supported to display only specific software in the Filter Software Inventory dialog box.
- For counting by Inventory Viewer, ranges that support combined conditions were increased.
- Hosts can be counted for each IE patch, BIOS manufacturer, and BIOS version (SMBIOS).
- **Restart specification** and **Display processing message** were added to the items that can be output to CSV files using the Package attributes template.
- **Restart specification** and **Display processing message** were added in the Package window to the items that can be printed.
- Previously, the client was unable to install some packages when the user was logged on to Windows NT with the non-Administrator user permissions, but the client can now install the packages if the client is in the running status.
- The `dcmstsw.exe` command was added to monitor job execution status.
- The `dcmdice.exe` command was added to save software inventory information to a CSV file. The `dcmdici.exe` command was also added to import software information from CSV file to the software inventory.
- `reboot` and `processing_dialog` of the `OPTION` tag were added as parameters that can be specified in the parameter file for the `dcmpack.exe` command. Because of this change, specifiable arguments were added.
- `JOB_SCHEDULE` and `JOB_DESTINATION_ID` were added as tabs that can be specified in the parameter file for the `dcmcoll.exe` command. Because of this change, specifiable arguments were added.
- Event log messages related to import and export of user inventory items and commands were added.

H. Glossary

agent

A host in which the Remote Control Agent operates.

AIT file

A file that contains a procedure for installing software interactively using a tool such as a dedicated installer. Automatic Installation Tool is used to create an AIT file.

alert report

An alert is a single message that is displayed by a program. If user operation may result in a serious error, an alert is displayed to attract the user's attention or to provide a warning.

With JP1/Software Distribution, when an error such as a hardware error is detected while monitoring a client system, the error event is reported to the user by means of a method such as a pop-up message. This is called an *alert report*.

all lower clients

A destination type specified when the central manager executes a job for all hosts under a relay manager.

application gateway method

A method of building a firewall that prohibits packet relay and controls access using an application gateway. Users cannot gain direct access to the system from the outside; they must first log in to a gateway and enter a password.

archive

A collection of files.

asset information

Information used by Asset Information Manager Subset to manage hardware and software.

Asset Information Manager Subset

A component that provides a GUI for totaling and searching the inventory information and operation logs collected by JP1/Software Distribution, according to the desired purpose.

By installing Asset Information Manager Subset, you can also open a window for managing software operation information from Remote Installation Manager.

It also provides GUI for client security management when JP1/Client Security Control is linked.

audit log

A log that is output in common by JP1 products. It provides a record of who performed each operation, when it was performed, and the type of operation that was performed.

authentication server

A server that uses JP1/Base to manage access permissions for JP1 users. One authentication server must be installed for each user authentication block. With this server, all JP1 users can be managed in a single batch. To manage JP1/Software Distribution users in linkage with JP1/Base, the JP1 users must be registered in this server.

automatic maintenance policy file

A text-format file that contains a policy for automatic maintenance of host groups and ID groups.

business filter

A function used by Asset Information Manager Subset to restrict the processes that can be executed from operation windows according to user permissions.

The constituent elements (buttons, search conditions, edit items, etc.) of each operation window are changed according to the user's permissions.

cabinet

An area in a managing server for storing packages.

central manager

JP1/Software Distribution Manager that is positioned at the top of the system in the case where managing servers are configured hierarchically.

change history

Information used by Asset Information Manager Subset to manage changes in the memory size and disk capacity of devices. You can use the change history to determine whether the CPU, memory, or disk has been physically modified without authorization.

The change history includes the change date, disk capacity, memory size, CPU, and so forth.

client

A computer on which the JP1/Software Distribution Client (client) software or the client facility of JP1/Software Distribution Manager or JP1/Software Distribution Client (relay system) is installed. A client receives software programs directly or through a relay manager/ system from the managing server and notifies the managing server of the results of installing the software.

client control facility

Facility for starting and shutting down remote PCs connected via a network from the local PC. Using this facility, JP1/Software Distribution can install software on a remote PC when its power is off, such as at night and on weekends/holidays. Note that in order to use this facility, the remote PCs (the motherboard, BIOS, power supply, LAN card, etc.) must support Wake on LAN and automatic shutdown.

collected file

A file collected from clients by remote collection.

collection script

A script that specifies the procedure for remote collection executed by a client. A collection script is created automatically when remote collection is executed from a Windows higher system. When remote collection is executed from a UNIX higher system, the client users can create user-specific collection scripts to achieve desired processing.

controller

A host in which the Remote Control Manager operates.

count clients

A facility that counts the number of hosts by types of information managed by JP1/Software Distribution Manager. This facility is used in a relational database system.

Database Manager

A JP1 software component used to create and maintain relational databases. Database Manager is provided in two component types, one for JP1/Software Distribution Manager and the other for the Asset Information Manager Subset component.

The Database Manager for JP1/Software Distribution Manager is a component of JP1/Software Distribution Manager that is used to create and maintain relational databases used by JP1/Software Distribution.

The Database Manager for Asset Information Manager Subset component is a subcomponent of Asset Information Manager Subset that is used to create and maintain relational databases for Asset Information Manager Subset.

deleted software management table

An internal table in which software deleted from the software inventory is registered. If a *Get software information from client* job with **Search for a file** specified is executed and software information reported from a host is registered in the deleted software management table, the obtained software information is not added to the software inventory nor to the software inventory of the host.

device operation

A target to which operation monitoring is applied. Reading from or writing to media via a USB storage device, internal CD/DVD drive, internal floppy disk drive, IEEE 1394-connected device, internal SD card slot, Bluetooth device, or imaging device can be suppressed as a *device operation*. This can only be used with clients running version 09-50 or later.

Connection and disconnection (removal) information for these devices is also collected in device operation logs.

directory information

User information and computer information acquired from Active Directory. The acquired directory information can be used as a job destination or for viewing the client information from Inventory Viewer.

division

In Asset Information Manager Subset, this is information that allows a user to manage other groups as a group job. Multiple divisions can be set for each group. By assigning a division to a user, that user can also manage the information of the groups (division groups) set to that division.

division information

In Asset Information Manager Subset, this is information about the groups set to a division.

domain

A unit for managing hosts and users in a network.

Embedded RDB

An embedded relational database provided by JP1/Software Distribution Manager. The user can select whether or not to install Embedded RDB when JP1/Software Distribution Manager is installed.

external media operations

See *operations to or from external media*.

firewall

A component installed at the boundary between the Internet and an internal system, which prevents unauthorized access to the internal system from the outside.

group information

Information used by Asset Information Manager Subset to manage organizations, such as departments that use the asset management system. Group information includes items such as group name, group code, cost group code, and so forth.

higher system addresses, file for

A settings file that contains the mappings of host names and IP addresses. It is used by a client to recognize the IP address of a higher system when a host name-keyed client cannot resolve the name of the higher system.

host

A networked personal computer or workstation that is a target for JP1/Software Distribution operations.

host group

A method of grouping multiple clients for remote installation of software at those clients. This method allows you to group hosts from a managing system in a way that matches the job, organization, or other distribution purpose.

host ID

A key that uniquely identifies a host in a system. Because host IDs are not affected by the network configuration, the system administrator can use host IDs to reduce the work of managing hosts. The system must use a relational database to use host IDs.

host on which JP1/Software Distribution is not installed

A host on which JP1/Software Distribution Manager has not been installed.

host search

Function for searching hosts in a specified range of the network; used to detect hosts on which JP1/Software Distribution is not installed.

HP NNM

A generic term for integrated network management programs that manage the configuration, performance, and problems in a network. If the OpenView Linkage facility is used, JP1/Software Distribution inventory information and job execution status can be managed from the monitoring windows of HP NNM version 7.5 or earlier.

ID group

A method of grouping multiple clients for remote installation of software at those clients. Clients are registered into an ID group at the clients or managing server.

ID group job

A job that specifies an ID group as the destination.

installation mode

The mode for installing a package in a client. The two options are **GUI installation mode**, which uses an installer, and **Background installation mode**, which does not use an installer and in which the files are simply copied.

installation script

A script executed by clients that specifies the procedure for an installation. An installation script is created automatically when a package is created. Users can create their own installation scripts to execute user-specific processes.

installation timing

The timing for installing a package in a client. You can select either **Install when system starts**, which installs the package when the client is started, or **Normal installation**, which installs the package when the package is transferred to the client.

installed software information

Information used by Asset Information Manager Subset to manage the software installed in various devices.

Installed software information, that is, the inventory information managed by the managing server, is imported into and used by the database of Asset Information Manager Subset.

Therefore, the software name and version being managed by the information-importing program, such as JP1/Software Distribution, are used.

installed software list

Information used by Asset Information Manager Subset to manage the names of software installed in various devices. This list is also used for managing the various settings of the installed software.

InstallShield environment deletion tool

A tool that re-initializes the installation environment. It is used before JP1/Software Distribution Client is re-installed after an installation has been stopped due to an installation error.

inventory

Information required for managing clients, such as hardware usage conditions and types of software installed in the client. A client's inventory is retrieved from the client by executing a job from the managing server.

Inventory Viewer

A window for displaying and counting inventory information retrieved from clients. This window provides a wide range of reporting functions. It can be used by JP1/Software Distribution Manager.

job

The execution unit of a JP1/Software Distribution facility. There are 21 job types:

- *Install package*
- *Transfer package to relay system*
- *Batch delete packages on relay system*
- *Collect files from client*
- *Collect files from client to relay system*
- *Acquire collected files from relay system*
- *Delete collected files from relay system*
- *Send package, allow client to choose*
- *Get system configuration information*
- *Get system information from client*
- *Get software information from client*
- *Transfer user inventory schema to client*
- *Get user inventory information*
- *Transfer registry collection definition*
- *Hold report*
- *Hold-report release*
- *Suspend file transfer*
- *Resume file transfer*
- *Report message*
- *Set the software monitoring policy*
- *Get software monitoring information from the client*

JP1 event

Information that is reported to JP1/Base about an event that has occurred in a system.

JP1 user

An account used by JP1/Software Distribution for user authentication when user management is performed in linkage with JP1/Base. Such an account is set up in the authentication server installed with JP1/Base. JP1/IM and JP1/AJS can also be used to perform user authentication of JP1 users.

JP1/AJS

A program for running jobs automatically. JP1/AJS enables you to routinely execute processes in a given order and to start a process when a specified event occurs.

JP1/Asset Information Manager

A program that supports streamlining of IT asset management applications and reduction of management cost required in tasks, such as installation of assets, software license management, and device maintenance, by using a database to achieve central management of information, such as hardware including network devices, software, and contracts.

JP1/Base

A program that provides the core functionality for JP1/IM.

JP1/Base sends and receives JP1 events, manages users, and controls client startup. It also functions as the JP1/IM system agent.

JP1/Base is a prerequisite program for JP1/IM - Manager.

JP1/IM

A program that centrally monitors a distributed system. Information about events such as job processing and failures in the distributed system is sent to JP1/IM as JP1 events. JP1/IM registers and manages JP1 events, and displays them on the system administrator's screen.

JP1/Software Distribution not installed, host on which

See *host on which JP1/Software Distribution is not installed*.

JP1/Software Distribution system

The entire network consisting of the hosts on which JP1/Software Distribution is installed.

Local System Viewer

A window that displays information about the hardware and software of clients, including the system monitoring status, alerts history, system information, and installed software. The client user can use this window for local system management purposes, because the information is available even when the client is not connected to a higher system.

managing server

A program that stores software to be remotely installed and gives the instructions for remote installation. This program can check the software installed in each host and the status and results of remote installation.

Microsoft SQL Server

Microsoft Corporation's relational database management system running on Windows NT. Microsoft SQL Server can be used as the relational database management system for JP1/Software Distribution information.

multicast address

The IP address of a multicast group. The address is specified when the sender and receivers for multicast distribution are set up.

multicast distribution

A method of job distribution that uses the IP multicast protocol to send packets to many specific clients from a higher system. Traffic is reduced because the higher system only needs to send the job packet to one multicast group location, regardless of the number of clients.

multicast group

A conceptual group to which jobs are distributed by multicast distribution. A multicast group has a specific IP address, known as the *multicast address*. When a higher system sends job packets to a multicast group, the packets are then distributed to each client within that group.

multiple LAN connections

A facility of JP1 for handling systems that consist of multiple local area networks (LANs).

Using this function, you can preset the LAN to be used for JP1 transmission on hosts that are connected to multiple LANs. Because JP1 communications can be set up independently of the system and other applications, this function supports a wide range of networks and modes of operation.

Hosts connected to multiple LANs may also be called multi-homed hosts or multiple Network Interface Card (NIC) hosts.

JP1/Software Distribution supports the following multi-LAN environments:

- Environments separated into multiple networks
- Environments with duplex networks

network configuration information file

A CSV file that contains information, such as the IP and MAC addresses, and subnet mask, of the hosts that are connected to the network.

network information

Information used by Asset Information Manager Subset to manage the location of each device on a network. Network information includes items such as IP address, MAC address, node name, computer name, and so forth.

offline folder

A folder for managing inventory information and operation information that is obtained from an offline machine. The offline folder is indicated as {OFFLINE} in the System Configuration and Destination windows.

offline installation

Facility for installing software using an installation medium instead of via a network.

offline machine

A Windows client that has not been registered in JP1/Software Distribution's system configuration information, such as the following PCs:

- PC on which a stand-alone JP1/Software Distribution Client (client) has been installed
- PC in a network on which JP1/Software Distribution Client (client) has been installed but not registered in JP1/Software Distribution's system configuration information

Inventory information and operation information can be obtained from offline machines. Software can be installed on offline machines.

offline machine Information

Inventory information and operation information that is obtained from offline machines.

operation history

Information on the software and files manipulated at a client. The following types of operation logs can be collected:

- Start process
- Stop process
- Change caption
- Change active window
- Start/stop of machine
- Logons/logoffs
- File options
- Web access
- Print operations
- Operations to or from external media
- Device operations

Operation Log List window

When client operation information is collected by the managing server, this window is used to extract the software startup history, the print operations suppression history, and the software and file operation history under various conditions, and to view the extracted history.

operation logs

When the user operation logs stored in the database for the suppression history and operation history acquired by JP1/Software Distribution are checked in the Operation Log List window, the displayed information is referred to in general as *operation logs*.

operation monitoring policy

Conditions specified in order to monitor the software operation status. A policy sets software whose startup is to be suppressed and operations whose history is to be acquired.

operations to or from external media

A target to which operation monitoring is applied. Reading from or writing to media via a USB-connected storage device, internal CD/DVD drive, internal floppy disk drive, IEEE 1394-connection, or an internal SD card slot can be suppressed as an *operation to or from external media*. This can only be used with clients running versions between 08-50 and 09-10.

Connection and disconnection (removal) information for these external media is also collected in external media operation logs. Note that logs are not collected on operations to or from internal floppy disk drives.

package

The unit in which software programs are remotely installed. Packages are stored in the cabinet of a managing server.

Package Setup Manager

A facility that enables clients to select and install desired software programs received from the managing server or relay systems. It can reject installation or change the installation directory.

package type

There are three package types, user programs and data, Hitachi program products, and other companies' software.

Packager

A program that registers into the managing server software that is to be remote-installed. It corresponds to the Packager of Windows JP1/ Software Distribution system. This is a JP1/Software Distribution term for UNIX.

packaging

The process of using Packager to create packages of software programs.

packet filtering method

A method of building a firewall that limits the packets that can pass through the firewall. This method allows access from within the system to the outside but prohibits access into the system from the outside. This method can limit the number of terminals that are permitted to access the Internet.

patch information file

File that contains information for obtaining patches from a Microsoft server. This file is needed by JP1/Software Distribution in order to obtain patches. JP1/Software Distribution obtains the path information file by connecting to a Hitachi Web server. It is updated based on the provisioning status of patches supplied by Microsoft.

patch information, unapplied

Information about patches that have not been applied to the client. Of the scanning results of the `mbsacli.exe` MBSA command, JP1/ Software Distribution treats the information for which the most recent patch was not found (information indicated as `NOT Found` in the scanning results) as unapplied patch information.

policy

Conditions for automatic assignment to a host group or ID group of a new host being added to the system configuration by a facility for automatic registration into the system configuration.

RD area

A logical area used by Embedded RDB for storing tables and indexes.

recorder file

A file that defines the procedure for installing software interactively using a dedicated installer. JP1/Software Distribution provides recorder files for some software programs distributed by other companies. The user can also create recorder files.

relational database

Database used for managing JP1/Software Distribution Manager's information. The supported relational databases are Embedded RDB, Microsoft SQL Server, and Oracle.

relay manager

JP1/Software Distribution Manager positioned under the highest managing server (central manager) in a system where managing servers are configured hierarchically. A relay manager relays jobs such as remote installation and collection of inventory information between the managing server and clients.

relay manager/system

Collective name for programs that relay jobs such as remote installation and collection of inventory information between the managing server and clients.

relay managing the ID

A relay manager or relay system that manages ID group jobs and clients that belong to an ID group. When an ID group job is executed, the relay managing the ID saves the job in the local system and executes it for clients that are registered in the ID group.

relay system

JP1/Software Distribution Client that relays jobs such as remote installation and collection of inventory information between the managing server and clients.

remote collection

A facility for collecting files from clients to the managing server. Instructions are issued from the managing server.

remote control

A facility that executes client operations remotely from a managing server.

Remote Control Agent

A program executed on a remote PC that is controlled by remote operations from the Remote Control Manager.

Remote Control Manager

A program that issues remote control operations to the Remote Control Agent.

Remote Desktop

In this manual, the following functions are referred to as *Remote Desktop*:

- Remote Desktop for Administration or Remote Desktop in Windows Server 2012, Windows Server 2008, Windows Server 2003, Windows 8, Windows 7, Windows Vista, and Windows XP
- Terminal Services in Windows 2000 Server

remote installation

A facility that transfers packaged software from a managing server to a client system and installs it in the client.

Remote Installation Manager

A program that provides the interactive (GUI) capability at a managing server.

search pattern

The search conditions used to search for operation logs in the Operation Log List window are saved as search patterns. The search patterns used for the main searching purposes are registered as defaults. You can also edit the default search patterns or register new search patterns.

security PC

A PC that has only the minimally necessary functions, and that is not equipped with any external storage devices, such as a hard disk and floppy disk. A security PC can connect to an agent and remotely control application software and files. You can use JP1/Software Distribution to remotely install the update data for a security PC.

software information

Information about software installed on hosts comprising a JP1/Software Distribution system. It is acquired by executing jobs from a managing server.

software inventory dictionary

A dictionary for specifying the software to be managed by JP1/Software Distribution. From the software obtained through a file search, you can select the software to be managed. You can also specify the license information needed for managing software licenses using Inventory Viewer.

software search list

A list that is used to acquire software information. There are two types of software search lists, the *standard retrieve list*, which is provided by JP1/Software Distribution, and the *optional software list*, which can be edited by the user.

split distribution

A method of reducing the load on the network by dividing a package into units of a user-specified size and transferring them at a user-specified interval (distribution interval). The user can specify the file split size at setup or job creation, or even at relay locations along the package transfer route. Split distribution is useful for distributing large packages.

SQL

Structured Query Language, a language for relational databases.

suppress history

Shows the history of software startup and printing suppression executed on a client

system information

Information about the hardware of hosts comprising a JP1/Software Distribution system. It is acquired by executing jobs from a managing server.

system monitoring

A facility used by the client to monitor the status of specific hardware according to predefined conditions. During system monitoring, the status of a program being monitored is displayed on the **System Conditions** page of Local System Viewer. If an error occurs in the program being monitored, this event is reported to the user by displaying an alert message or changing the appearance of an icon. While the client is connected to its higher system, alerts can also be reported to the higher system.

System Monitoring icon

An icon displayed in the task bar notification area. The status of the system monitoring facility and the presence of alert messages can be identified by the icon's status (appearance). Double-clicking on the **System Monitoring** icon starts Local System Viewer.

To display the **System Monitoring** icon, in the Client Setup dialog box, on the **System Monitoring** page, choose the **Display the System Monitoring icon in the task bar notification area** option.

terminal server

In this manual, the following servers are referred to as a *terminal server*:

- For Windows Server 2012 or Windows Server 2008 R2, servers on which Remote Desktop Session Host Role Service of Remote Desktop Services is installed
- For Windows Server 2008 or Windows Server 2003, servers on which Terminal Server Role Service of Terminal Services is installed
- For Windows 2000 Server, servers on which Terminal Services has been installed in Application Server Mode

unarchiver

A program that restores archived and compressed files to their original formats during remote collection.

unicast distribution

A method of job distribution in which packets are sent from a higher system to each client individually. Because the higher system has to send each job packet separately to each target client, the number of times a packet is sent increases proportionally to the number of clients in the system.

user inventory information

Information unique to a client (such as name and PC serial number). The managing server executes a job to obtain this information.

user inventory item

An entry item for user inventory information. The user inventory items created in the managing server are distributed to clients by executing jobs.

Visual Test

A program that supports debugging of programs that run in a Windows environment.

Wake on LAN

A standard for turning on a computer in a local area network (LAN) from another computer in the network.

Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, and Windows Vista version of JP1/Software Distribution Client

A program needed in order to manage a computer running a Windows 8, Windows Server 2012, Windows 7, Windows Server 2008, or Windows Vista operating system as a client in a JP1/Software Distribution system. It can also be used as a relay system.

Index