

**Job Management Partner 1/Asset  
Information Manager**

**Description**

3020-3-S76-90(E)

## ■ Relevant program products

P-2642-1N97 Job Management Partner 1/Asset Information Manager version 09-50 (for Windows Server 2008, Windows Server 2003, Windows XP Professional, Windows 2000)

## ■ Trademarks

Active Directory is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries. AMD, AMD Opteron, and combinations thereof, are trademarks of Advanced Micro Devices, Inc.

Internet Explorer is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. ITIL(R) is a Registered Trade Mark, and a Registered Community Trade Mark of the Office of Government Commerce, and is Registered in the U.S. Patent and Trademark Office.

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

OpenView is a trademark of Hewlett-Packard Company.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

Outlook is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Pentium is a trademark of Intel Corporation in the United States and other countries.

PowerPoint is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Windows is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Windows NT is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Windows Server is either a registered trademark or a trademark of Microsoft Corporation in the United States and/or other countries.

Other product and company names mentioned in this document may be the trademarks of their respective owners. Throughout this document Hitachi has attempted to distinguish trademarks from descriptive terms by writing the name with the capitalization used by the manufacturer, or by writing the name with initial capital letters. Hitachi cannot attest to the accuracy of this information. Use of a trademark in this document should not be regarded as affecting the validity of the trademark.

## ■ 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

Dec. 2011: 3020-3-S76-90(E)

## ■ Copyright

All Rights Reserved. Copyright (C) 2009, 2011, Hitachi, Ltd.

## Summary of amendments

The following table lists changes in the manuals 33020-3-S76-90(E), 3020-3-S77-90(E), and 3020-3-S78-90(E) for JP1/Asset Information Manager 09-50 and product changes related to these manuals.

Changes	Location
Related asset information can now be managed.	Description: <i>1.2.2</i> Planning and Setup Guide: <i>2.1.1(2)</i>
By assigning divisions to users, a single user can now manage information about multiple groups.	Description: <i>1.2.2, 1.2.3</i> Planning and Setup Guide: <i>3.1.3</i> Admin. Guide: <i>1.2, 1.3, 1.4, 1.4(1), 1.6</i>
Login authentication can now be performed by linking to Active Directory. In addition, Active Directory user information can now be acquired.	Description: <i>1.2.10, 2.10, 2.11</i> Planning and Setup Guide: <i>1.2.3, 3.5, 3.5.1, 3.5.2, 4.1, 4.1.1(9), 5.3, 5.3.6, 5.3.6(1), 5.3.6(3), 5.3.6(4), 5.3.6(5), 5.3.6(6), 5.3.6(7), 5.3.6(8), 5.3.6(9), Appendix D</i> Admin. Guide: <i>1.1.1</i>
The following operation logs can now be referenced and summarized: <ul style="list-style-type: none"> <li>• USB connection allowed</li> <li>• USB connection suppressed</li> <li>• Connection allowed for external media other than USB</li> <li>• Connection suppressed for external media other than USB</li> </ul>	Description: <i>2.9(1)</i> Planning and Setup Guide: <i>4.1.1(7)</i> Admin. Guide: <i>2.7.1, 2.7.1(1)(a), 2.7.1(2)(a)</i>
Microsoft SQL Server 2008 R2 is now supported as a database management system.	Description: Entire manual Planning and Setup Guide: Entire manual Admin. Guide: Entire manual
Under <b>Link with JP1/SD</b> in the Server Setup dialog box, the setting <b>Host ID</b> has been changed to <b>Targets for inventory</b> . <b>Targets for inventory</b> allows the user to acquire inventory information from all devices, or only from devices with host identifiers, or only from devices with system information.	Planning and Setup Guide: <i>1.3, 5.3.7(5)</i>
The setting <b>Inventory acquisition method</b> has been added under <b>Link with JP1/SD</b> in the Server Setup dialog box, which allows the user to select <b>Multithreading method</b> as the method for acquiring inventory information.	Planning and Setup Guide: <i>1.3, 5.3.7(20)</i>

Changes	Location
The setting <b>Multiplex level for inventory</b> has been added under <b>Link with JP1/SD</b> in the Server Setup dialog box, which allows the user to specify the multiplex level when inventory information is collected using the multithread method.	Planning and Setup Guide: <i>1.3, 5.3.7(21)</i>
By defining an assignment-exception MAC list, users can now register multiple devices as separate assets when JP1/Software Distribution inventory information is acquired, even if the devices have the same MAC address.	Planning and Setup Guide: <i>3.2.3, 3.2.3(17)</i>
<b>Machine serial number</b> can be selected as the assigned key when JP1/Software Distribution inventory information is acquired.	Planning and Setup Guide: <i>3.2.3(1), 3.2.3(11), 3.2.3(12), 3.2.3(13), 3.2.3(14), 5.3.7(8), 5.3.7(9), 5.3.7(10), 9.6.1, Appendix D</i>
The following items have been added under <b>Link with Directory Server</b> in the Server Setup dialog box: <ul style="list-style-type: none"> <li>• <b>Directory server usage</b></li> <li>• <b>Server name</b></li> <li>• <b>Port number</b></li> <li>• <b>Access user</b></li> <li>• <b>Response monitoring time</b></li> <li>• <b>User information DN</b></li> <li>• <b>User ID attribute name</b></li> <li>• <b>User name attribute name</b></li> </ul>	Planning and Setup Guide: <i>3.5.1, 5.3, 5.3.1, 5.3.6, 5.3.6(1), 5.3.6(3), 5.3.6(4), 5.3.6(5), 5.3.6(6), 5.3.6(7), 5.3.6(8), 5.3.6(9), Appendix D</i>
Microsoft Internet Explorer 9 is now supported as a Web browser.	Planning and Setup Guide: <i>4.1.1(2), 4.2.1, 5.2.1(2), 11.8(1)</i>
The setting <b>Status to display in device search windows</b> under <b>Basic Information</b> in the Server Setup dialog box has been added to the Add Related Device window.	Planning and Setup Guide: <i>5.3.4(21), 8.2</i>
The setting <b>Device log management</b> has been added under <b>Basic Information</b> in the Server Setup dialog box, which allows the user to select whether to manage the initial change history of a device to be managed when a <b>Delete change log</b> task is performed.	Planning and Setup Guide: <i>5.3.4(22)</i>
Items in the outbox can now be copied to create new Items.	Planning and Setup Guide: <i>5.3.4(20), Appendix D</i> Admin. Guide: <i>3.3.1, 3.3.6, 3.3.6(1)</i>
Asset Information Manager operations can now be output to an audit log.	Planning and Setup Guide: <i>5.3.4(23), 5.3.4(24), Appendix D, Appendix G, G.1, G.2, G.3, G.3(1), G.3(2), G.3(3), G.3(3)(a), G.3(3)(b), G.3(4), G.4, G.5</i>
When an Item is attached, users who have been assigned as agents for that Item can now be notified by email.	Planning and Setup Guide: <i>5.3.5, 5.3.5(2), Appendix D</i> Admin. Guide: <i>3.1.1, 3.2.2</i>

Changes	Location
The setting <b>Number of JP1/CSC notifications</b> has been added under <b>Link with JP1/SD</b> in the Server Setup dialog box, which allows the user to set the timing for reporting the acquisition of JP1/Software Distribution inventory information to JP1/Client Security Control.	Planning and Setup Guide: 5.3.7(19)
The following operations have been added for data maintenance tasks: <ul style="list-style-type: none"> <li>• <i>Delete related asset information that does not have target asset information</i></li> <li>• <i>Delete division information set for groups that no longer exist</i></li> </ul>	Planning and Setup Guide: 5.9.3(1), 5.9.3(3)
Settings for Windows Server 2008 have been added to the following cluster administrator resources: <ul style="list-style-type: none"> <li>• Microsoft Internet Information Services resource</li> <li>• Embedded RDB service resource</li> </ul>	Planning and Setup Guide: 5.13.3
The following asset types have been added for importing and exporting: <ul style="list-style-type: none"> <li>• Division information</li> <li>• Assign division</li> </ul>	Planning and Setup Guide: 7.1.2(2), 7.1.2(3), 7.1.3(3), 7.1.4(16), 7.2.3(3), 14.1.1, 14.1.2, 14.2.9, 14.3.5, 14.3.6, 14.4, 14.4.20, 14.4.21 Admin. Guide: 4.10.1(3)(q), 4.10.1(3)(r), 4.10.2(1), 4.10.2(2)
<b>Related asset information</b> has been added as an asset type that can be specified when importing asset information with the <b>Import</b> job menu or with <code>jamCsvImport.bat</code> , and when exporting asset information with the <b>Export</b> job menu or with <code>jamCsvExport.bat</code> .	Planning and Setup Guide: 7.1.2(2), 7.1.3(3), 7.1.4(15), 7.2.3(3), 14.1.1, 14.1.2, 14.1.3, 14.2.26, 14.3.11, 14.4, 14.4.19 Admin. Guide: 4.10.1(3)(p), 4.10.2(1), 4.10.2(2)
The official authority <i>Item auditor</i> has been added. Users who have this official authority can view the latest Item content and attachments in the Execution Item Management window.	Planning and Setup Guide: 10.1.1, 10.2, 10.2.3 Admin. Guide: 3.4
A table object has been added to allow multiple entries for a single Item object. In addition, the component Table Designer has been added for defining table objects.	Planning and Setup Guide: 10.4.3, 10.4.3(1), 10.4.3(1)(e), 10.4.3(3), 10.4.5, 10.4.5(1), 10.4.5(2), 10.4.5(3), 10.4.5(4), 10.5.2, 10.5.4(1), 10.5.4(2)
A date can now be set to the subject data type of an Item.	Planning and Setup Guide: 10.4.3(3)(b)
A note about the work required to rebuild Microsoft Internet Information Services has been added.	Planning and Setup Guide: 11.5.6
Greater detail is now provided in the table that shows the correspondence between information created for Asset Information classes and the inventory information assigned in JP1/Software Distribution.	Planning and Setup Guide: 13.1

Changes	Location
The modification date of system configuration information and the modification date of registry information can now be managed as asset information.	Planning and Setup Guide: <i>13.1.1, 14.2.2, 14.4.1</i>
DivisionInfo has been added as an object class.	Planning and Setup Guide: <i>14.1.1, 14.1.3, 14.2.9, 14.4, 14.4.20, 14.4.21</i>
The following association classes have been added: <ul style="list-style-type: none"> <li>• DivisionLink</li> <li>• DivisionUserLink</li> </ul>	Planning and Setup Guide: <i>14.1.2, 14.1.3, 14.3.5, 14.3.6, 14.4</i>
In the table listing the size of each information item in the section on the disk space required by the asset management database, the size of the hardware information item has been changed from 51.7 KB to 52.1 KB.	Planning and Setup Guide: <i>C.2(1)</i>
The number of assigned license keys can now be displayed in the Owned License List window.	Admin. Guide: <i>2.4.1</i>
The <b>Related devices</b> tab has been added to the Device Details dialog box, which allows the user to manage linkages between devices.	Admin. Guide: <i>2.8, 2.8.6</i>
A <b>Divisions</b> tab has been added to the Group Details dialog box of the <b>Group and User</b> job menu, in which options such as modifying division information and outputting a list of divisions to a CSV file have been added. An option for assigning divisions to users has also been added to the <b>Divisions</b> tab.	Admin. Guide: <i>4.1, 4.1.3, 4.1.5, 4.1.5(1), 4.1.5(2), 4.1.6, 4.1.6(1), 4.1.6(2), 4.1.6(3), 4.1.6(4), 4.1.6(5)</i>
A note has been added about the format of CSV files that are imported using the <b>Import</b> job menu.	Admin. Guide: <i>4.10.1(1)</i>

Legend:

Description: *Job Management Partner 1/Asset Information Manager Description*

Planning and Setup Guide: *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*

Admin. Guide: *Job Management Partner 1/Asset Information Manager Administrator's Guide*

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

---

# Preface

---

This manual describes the functions of the following program product:

- Job Management Partner 1/Asset Information Manager

In this manual:

- *Job Management Partner 1* is usually abbreviated to *JPI*.
- *Job Management Partner 1/Asset Information Manager* is abbreviated to *Asset Information Manager*.

This manual provides a brief overview of Asset Information Manager features and some typical ways in which Asset Information Manager is used. The manuals for Asset Information Manager (including this manual) are listed below. The descriptions of each manual will help you decide the order in which you should read them.

### *JPI Version 9 Job Management Partner 1/Asset Information Manager Description*

Read this manual first.

This manual provides a brief overview of Asset Information Manager features and some typical ways in which Asset Information Manager is used.

### *JPI Version 9 Job Management Partner 1/Asset Information Manager Planning and Setup Guide*

This manual explains the points you need to consider before you set up Asset Information Manager, and provides detailed procedures that explain how to install and set up Asset Information Manager. The manual also explains how to optimize Asset Information Manager to best suit your asset management operations.

### *JPI Version 9 Job Management Partner 1/Asset Information Manager Administrator's Guide*

This manual explains the functional details and procedures you need to understand in order to operate Asset Information Manager.

## **Intended readers**

The explanations in this manual assume that the readers are the following:

- First-time users of Asset Information Manager
- System administrators planning to set up an asset management system that uses Asset Information Manager
- Asset managers who will manage asset information

- Persons who will reference asset information and use it in applications

This manual also assumes readers have an understanding of the following:

- How to use Windows Server 2008, Windows Server 2003, Windows XP Professional, or Windows 2000
- A basic knowledge of relational databases
- Knowledge of Microsoft SQL Server or Oracle (if Microsoft SQL Server or Oracle is being used)
- How to use linkage products (if Asset Information Manager is being linked to JP1/Software Distribution, Network Node Manager version 8 or earlier, or JP1/Integrated Management)
- A basic knowledge of software licensing

## Organization of this manual

This manual consists of the following chapters and appendices:

### 1. Overview

Chapter 1 describes the purpose and features of Asset Information Manager. This chapter also provides an overview of the information and applications that can be managed and executed by Asset Information Manager.

### 2. Typical Usage

Chapter 2 describes typical usage of Asset Information Manager, such as how to use Asset Information Manager in asset management jobs, and the preparations needed to use Asset Information Manager once it has been installed.

#### A. Version Changes

Appendix A describes the changes that have been made in each version.

#### B. Glossary

Appendix B defines terms used in this manual.

## 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/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))*

For details about collecting inventory information, collecting operation log data,



and distributing software:

- *Job Management Partner 1/Software Distribution Description and Planning Guide* (3020-3-S79(E)), for Windows systems
- *Job Management Partner 1/Software Distribution Setup Guide* (3020-3-S80(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

For functions needed to handle problems in asset management systems on the basis of JP1 event information:

- *Job Management Partner 1/Integrated Management - Manager Overview and System Design Guide* (3020-3-R76(E))
- *Job Management Partner 1/Integrated Management - Manager GUI Reference* (3020-3-R79(E))
- *Job Management Partner 1/Base User's Guide* (3020-3-R71(E))

For functions needed to manage client security on the basis of asset management system information:

- *Job Management Partner 1/Client Security Control Description, User's Guide and Operator's Guide* (3020-3-S71(E))

For understanding messages output from an Embedded RDB database:

- *HiRDB Version 8 Messages* (3020-6-358(E))

## About online Help

Asset Information Manager provides the following manuals as online (HTML) Help. The text in parentheses following each manual title denotes the name of the corresponding online Help file.

### **Job Management Partner 1/Asset Information Manager (*assetim.chm*)**

The following manuals constitute an integrated set:

- *Job Management Partner 1/Asset Information Manager Description* (*aimintro.chm*)
- *Job Management Partner 1/Asset Information Manager Planning and Setup Guide* (*aimconst.chm*)
- *Job Management Partner 1/Asset Information Manager Administrator's Guide* (*aimuse.chm*)

## Job Management Partner 1/Asset Information Manager - Creating an Access Definition File (*assetscr.chm*)

To access online Help, you must use a computer on which Microsoft Internet Explorer 6 SP1 or later is installed.

The online Help files are stored in the following folder:

*Asset-Information-Manager-installation-folder\help*

### Conventions: Abbreviations for product names

This manual uses the following abbreviations for product names:

Abbreviation		Full name or meaning
Asset Information Manager, AIM		Job Management Partner 1/Asset Information Manager
Asset Information Manager Embedded RDB Edition		Job Management Partner 1/Asset Information Manager Embedded RDB Edition
JP1/Base		Job Management Partner 1/Base
JP1/Client Security Control, JP1/CSC		Job Management Partner 1/Client Security Control - Agent
		Job Management Partner 1/Client Security Control - Manager
JP1/IM		Job Management Partner 1/Integrated Management - Manager
		Job Management Partner 1/Integrated Management - Rule Operation
		Job Management Partner 1/Integrated Management - View
		Job Management Partner 1/Integrated Manager - Central Console
		Job Management Partner 1/Integrated Manager - Central Scope
JP1/IM - Manager		Job Management Partner 1/Integrated Manager - Manager
		Job Management Partner 1/Integrated Manager - Central Console
JP1/Software Distribution, JP1/SD	JP1/Software Distribution Client	Job Management Partner 1/Software Distribution Client
	JP1/Software Distribution Manager	Job Management Partner 1/Software Distribution Manager
MBSA		Microsoft(R) Baseline Security Analyzer
Microsoft Internet Explorer		Microsoft(R) Internet Explorer(R) 6 SP1 or later

Abbreviation		Full name or meaning	
		Windows(R) Internet Explorer(R) 7	
		Windows(R) Internet Explorer(R) 8	
		Windows(R) Internet Explorer(R) 9	
Microsoft Office		Microsoft(R) Office 2000	
		Microsoft(R) Office 2003	
		Microsoft(R) Office 2007	
		Microsoft(R) Office 2010	
		Microsoft(R) Office XP	
Microsoft SQL Server	Microsoft SQL Server 2000	Microsoft(R) SQL Server 2000 Enterprise Edition	
		Microsoft(R) SQL Server 2000 Standard Edition	
	Microsoft SQL Server 2005	Microsoft(R) SQL Server 2005 Enterprise Edition	
		Microsoft(R) SQL Server 2005 Standard Edition	
		Microsoft(R) SQL Server 2005 Enterprise x64 Edition	
		Microsoft(R) SQL Server 2005 Standard x64 Edition	
	Microsoft SQL Server 2008	Microsoft(R) SQL Server 2008 Enterprise	
		Microsoft(R) SQL Server 2008 Standard	
		Microsoft(R) SQL Server 2008 R2 Enterprise	
		Microsoft(R) SQL Server 2008 R2 Standard	
	Microsoft SQL Server 7.0	Microsoft(R) SQL Server 7.0	
		Microsoft(R) SQL Server 7.0 Enterprise Edition	
	HP NNM, HP NNM Version 7.5 or earlier		HP OpenView network node manager 6.4
			HP OpenView Network Node Manager Starter Edition 7.5
HP OpenView NNM SE 7.51			
ORACLE, Oracle		Oracle8i and Oracle9i	
Pentium		Pentium(R)	

Abbreviation		Full name or meaning
Windows	Windows 2000	Microsoft(R) Windows(R) 2000 Advanced Server Operating System
		Microsoft(R) Windows(R) 2000 Professional Operating System
		Microsoft(R) Windows(R) 2000 Server Operating System
	Windows 95	Microsoft(R) Windows(R) 95 Operating System
	Windows 98	Microsoft(R) Windows(R) 98 Operating System
	Windows CE	Microsoft(R) Windows(R) CE, Handheld PC Professional Edition
	Windows Me	Microsoft(R) Windows(R) Millennium Edition Operating System
	Windows NT 4.0	Microsoft(R) Windows NT(R) Server Enterprise Edition Version 4.0
		Microsoft(R) Windows NT(R) Server Network Operating System Version 4.0
	Windows Server 2003	Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition
		Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition
		Microsoft(R) Windows Server(R) 2003 R2, Standard Edition
		Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition
		Microsoft(R) Windows Server(R) 2003, Enterprise Edition
		Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
		Microsoft(R) Windows Server(R) 2003, Standard Edition
		Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
	Windows Server 2003 (x64)	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, Standard x64 Edition
		Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
Windows Server 2008 <sup>#</sup>	Microsoft(R) Windows Server(R) 2008 Enterprise	
	Microsoft(R) Windows Server(R) 2008 Standard	
	Microsoft(R) Windows Server(R) 2008 R2 Datacenter	

Abbreviation		Full name or meaning
		Microsoft(R) Windows Server(R) 2008 R2 Enterprise
		Microsoft(R) Windows Server(R) 2008 R2 Standard
	Windows XP	Microsoft(R) Windows(R) XP Home Edition Operating System
		Microsoft(R) Windows(R) XP Professional Operating System
Windows XP Professional		Microsoft(R) Windows(R) XP Professional Operating System
WSUS		Microsoft(R) Windows Server(R) Update Services

#: Does not include installations that include the Server Core option.

## Conventions: Acronyms

This manual also uses the following acronyms:

Acronym	Full name or meaning
AMD	Advanced Micro Devices
CD	Compact Disc
CN	Common Name
CPU	Central Processing Unit
CSV	Comma Separated Value
DBMS	Data Base Management System
DC	Domain Component
DN	Distinguished Name
GUI	Graphical User Interface
ID	Identification
IT	Information Technology
ITIL	IT Infrastructure Library
ITU	International Telecommunication Union
LDAP	Lightweight Directory Access Protocol
MIB	Management Information Base
MO	Magneto-Optical disk

<b>Acronym</b>	<b>Full name or meaning</b>
OS	Operating System
OU	Organization Unit
PC	Personal Computer
RDB	Relational Database
SNMP	Simple Network Management Protocol
SP	Service Pack
URL	Uniform Resource Locator
USB	Universal Serial Bus
WS	Work Station

## Conventions: Diagrams

This manual uses the following conventions in diagrams:

• Computer



• Database, file, or disk



• Input/output operation



• User



• Server



• Location information



• Notebook PC



• Program



• CD-ROM or software



• Network



• Email



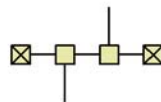
• Contract information



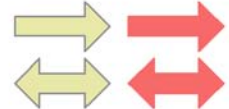
• Error



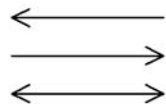
• Bus-type LAN



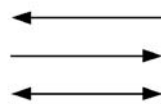
• Communication line • Flow of data



• Flow of control



• Other flow



## Conventions: Fonts and symbols

The following table explains the fonts used in this manual:

Font	Convention
<b>Bold</b>	<p><b>Bold</b> 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:</p> <ul style="list-style-type: none"> <li>• From the <b>File</b> menu, choose <b>Open</b>.</li> <li>• Click the <b>Cancel</b> button.</li> <li>• In the <b>Enter name</b> entry box, type your name.</li> </ul>
<i>Italics</i>	<p><i>Italics</i> are used to indicate a placeholder for some actual text to be provided by the user or system. For example:</p> <ul style="list-style-type: none"> <li>• Write the command as follows: <code>copy source-file target-file</code></li> <li>• The following message appears: A file was not found. (file = <i>file-name</i>)</li> </ul> <p><i>Italics</i> are also used for emphasis. For example:</p> <ul style="list-style-type: none"> <li>• Do <i>not</i> delete the configuration file.</li> </ul>
Code font	<p>A code font indicates text that the user enters without change, or text (such as messages) output by the system. For example:</p> <ul style="list-style-type: none"> <li>• At the prompt, enter <code>dir</code>.</li> <li>• Use the <code>send</code> command to send mail.</li> <li>• The following message is displayed: <code>The password is incorrect.</code></li> </ul>

The following table explains the symbols used in this manual:

Symbol	Convention
	<p>In syntax explanations, a vertical bar separates multiple items, and has the meaning of OR. For example: <code>A B C</code> means A, or B, or C.</p>
{ }	<p>In syntax explanations, curly brackets indicate that only one of the enclosed items is to be selected. For example: <code>{A B C}</code> means only one of A, or B, or C.</p>
[ ]	<p>In syntax explanations, square brackets indicate that the enclosed item or items are optional. For example: <code>[A]</code> means that you can specify A or nothing. <code>[B C]</code> means that you can specify B, or C, or nothing.</p>
...	<p>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: <code>A, B, B, ...</code> means that, after you specify A, B, you can specify B as many times as necessary.</p>



## Conventions for permitted characters

In most cases, only the following characters are permitted as syntax elements (if other characters are permitted, the manual will state this explicitly):

Type	Definition
Alphabetic characters	A to Z, a to z
Upper-case alphabetic characters	A to Z
Lower-case alphabetic characters	a to z
Numeric characters	0 to 9
Alphanumeric characters	A to Z, a to z, 0 to 9
Symbols	! " # \$ % & ' ( ) + , - . / : ; < = > @ [ ] ^ _ { } ~ ? space

## 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<sup>2</sup> bytes.
- 1 GB (gigabyte) is 1,024<sup>3</sup> bytes.
- 1 TB (terabyte) is 1,024<sup>4</sup> bytes.

## Conventions: References to other manuals

Within the group of manuals *Description, Planning and Setup Guide*, and *Administrator's Guide*, references in one manual to another manual are 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 might 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/Asset Information Manager*, 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

---

<b>Preface</b>	<b>i</b>
Intended readers .....	i
Organization of this manual .....	ii
Related publications .....	ii
About online Help .....	iii
Conventions: Abbreviations for product names .....	iv
Conventions: Acronyms .....	vii
Conventions: Diagrams .....	ix
Conventions: Fonts and symbols .....	ix
Conventions: KB, MB, GB, and TB .....	xi
Conventions: References to other manuals .....	xi
Conventions: Version numbers .....	xii
<b>1. Overview</b>	<b>1</b>
1.1 Purpose of Asset Information Manager .....	2
1.2 Features of Asset Information Manager .....	4
1.2.1 Integrated asset management achieved by linking to JP1 products .....	4
1.2.2 Integrated management of corporate asset information .....	7
1.2.3 Practical totaling functions and search functions designed for each type of work task .....	11
1.2.4 Automating database maintenance and status monitoring .....	12
1.2.5 Creating operation windows for routine jobs .....	14
1.2.6 Restricting and extending tasks according to user roles .....	15
1.2.7 License management of various license types .....	16
1.2.8 Using a flow to apply for requests and approve tasks .....	23
1.2.9 Managing patch application statuses .....	25
1.2.10 Login authentication using Active Directory services .....	27
<b>2. Typical Usage</b>	<b>29</b>
2.1 Importing and exporting device information .....	30
2.2 Managing the usage statuses of IP addresses .....	38
2.3 Stocktaking .....	41
2.4 Determining whether licenses are handled legally .....	44
2.5 Applying updates by linking to a WSUS server .....	55
2.6 Adding asset information statuses, managed items, and windows .....	59
2.7 Limiting available functions by user roles .....	63
2.8 Solving problems using Items .....	69
2.9 Checking user operations by means of operation logs .....	75

2.10 Login authentication via linkage with Active Directory .....	85
2.11 Including Active Directory information in the asset management database .....	87
<b>Appendixes</b> .....	89
<hr/>	
A. Version Changes.....	90
B. Glossary.....	101
<b>Index</b> .....	117
<hr/>	

## Chapter

---

# 1. Overview

---

Asset Information Manager is a product developed to help solve problems that can occur while managing IT assets. Asset Information Manager provides efficient ways to manage IT assets through the centralized management of information. This chapter describes the purpose and features of Asset Information Manager. It also provides an overview of the information and tasks that can be managed and executed by Asset Information Manager.

- 1.1 Purpose of Asset Information Manager
- 1.2 Features of Asset Information Manager

---

## 1.1 Purpose of Asset Information Manager

---

This section explains the purpose of Asset Information Manager, which can be used for the centralized management of IT asset information.

### **(1) Resolving issues through the management of IT assets**

The number of PCs and workstations owned by corporations increases every year, and the overhead of managing IT asset information, including hardware and software assets, has become significant.

Many corporations manage IT asset information by department according to purpose, such as device information managed by the system management department, network information managed by the network management department, and maintenance contract information managed by the resources department. Also, individual tools and databases are used for gathering and managing information, and formats vary between different management departments. Having the various departments manage IT asset information individually while maintaining a record of everything in a variety of different formats requires a large amount of overhead and costs.

Furthermore, if the improper use of licenses were to become public knowledge, adverse impacts on business are unavoidable, due to the damage to the corporation's reputation. To prevent this, it is essential that software licenses be properly managed not only to reduce costs but also to protect against copyright violations.

To address these issues concerning corporate IT asset management, there is a need for an *asset management system* that can handle IT assets efficiently. By using *Asset Information Manager* to construct your asset management system, you can handle your corporate IT assets efficiently and solve any existing issues concerning asset management.

### **(2) Improving the efficiency of asset management tasks and reducing management costs**

An asset management system using Asset Information Manager allows you to centrally manage collected corporate IT asset information, as well as view that information from various perspectives. More specifically, all IT asset information, including information on both hardware and software assets, as well as information on network devices and maintenance contract information, can be stored in a database and centrally managed. This improves the efficiency of asset management tasks and reduces management costs associated with stocktaking and with introducing and transferring devices.

### **(3) Providing support for security measures**

To protect IT devices against the threat of computer viruses, security measures must be systematically and exhaustively established and maintained on every device

throughout the entire system. Asset Information Manager allows you to detect devices to which the latest patches or virus definition files have not been applied. Such devices can be detected by using a variety of management information associated with the devices.

To further strengthen security measures, you must regularly check for actions that might lead to the unauthorized information leaks, in order to protect against unexpected situations, such as the undesired disclosure of internal company information. By using logs to centrally manage each device from Asset Information Manager operation windows, Asset Information Manager can be a valuable tool in tracing and investigating causes that lead to the occurrence of such problems.

#### **(4) *Providing support for IT governance***

Asset Information Manager allows you to detect and investigate PC operations or operations that might lead to the disclosure of information that is in conflict with the risk management policies outlined by the company. Asset Information Manager allows you to follow up leads based on changes in the number of particular incidents detected for each group, and it allows you to quantitatively evaluate statuses in order to establish the most appropriate IT asset management practices while improving the effectiveness of constraints being imposed for adhering to company standards.

#### **(5) *Broad sharing of Web-based IT asset information***

Asset Information Manager uses a Web browser to manage IT asset information. Because no special program is required, you can manage your IT assets by logging into Asset Information Manager from anywhere.

Users other than the administrator can also use the information in the database to check their PC information and the status of licenses for installed software programs.

---

## 1.2 Features of Asset Information Manager

---

This section explains the Asset Information Manager features developed to support solutions to a wide variety of issues that can occur in managing IT assets.

### 1.2.1 Integrated asset management achieved by linking to JP1 products

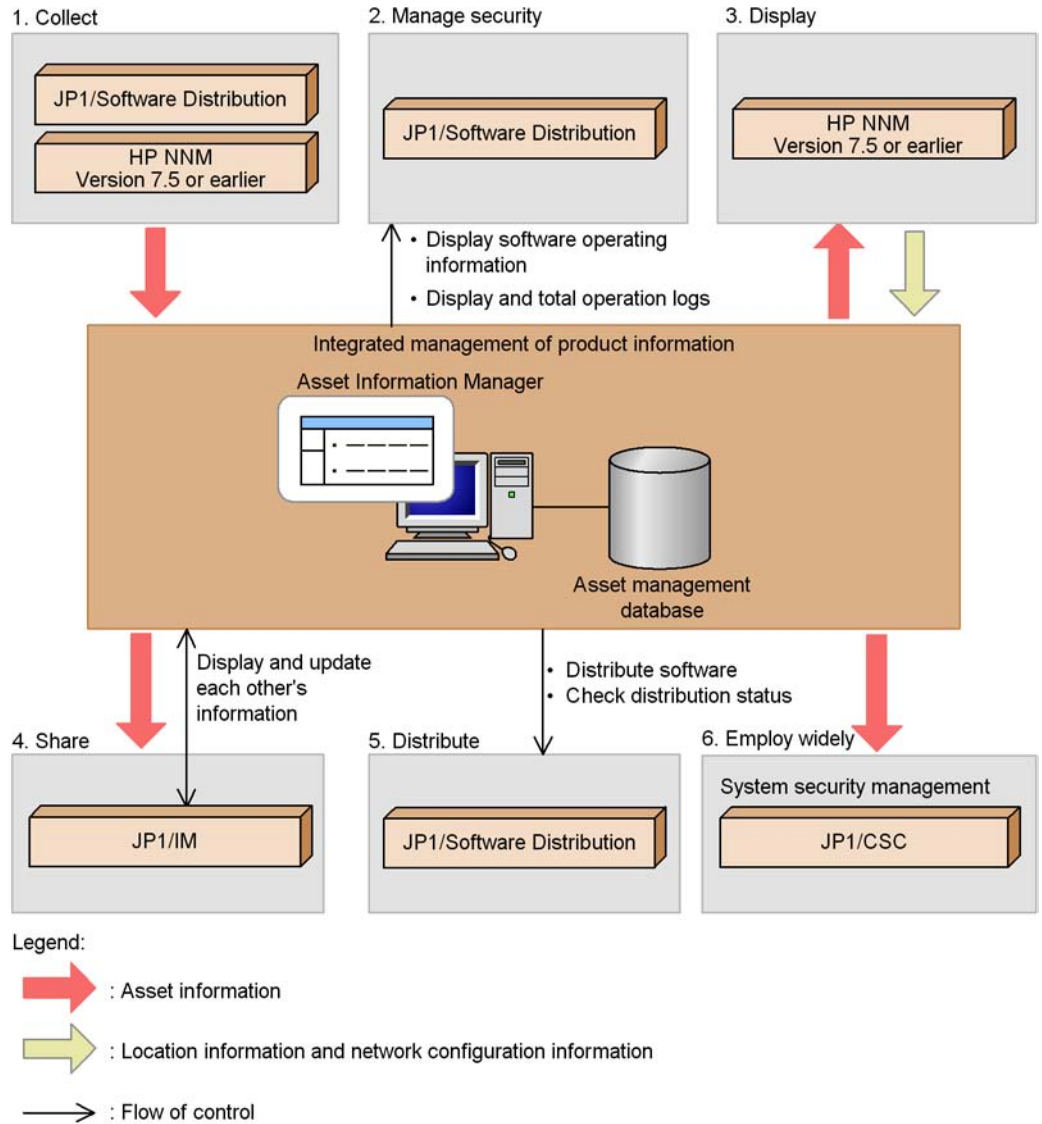
You can assemble an integrated asset management system by linking Asset Information Manager to such JP1 products as JP1/Software Distribution, HP NNM Version 7.5 or earlier, JP1/IM, and JP1/CSC.

For example, you can efficiently execute asset management jobs by loading database information from a linked product into Asset Information Manager's asset management database or by referencing information about a linked product from Asset Information Manager operation windows.

The figure below shows the concept of the integrated operation of an asset management system linked to JP1 products.



Figure 1-1: Concept of integrated asset management by linking to JP1 products



1. Register JP1 product information into the asset management database.

Asset Information Manager allows you to link your system to JP1/Software Distribution, and use batch operations to register (into the asset management database) *inventory information* collected by JP1/Software Distribution, such as CPU information, OS types, and installed software programs.

You can also link AIM to HP NNM Version 7.5 or earlier and batch register network device node information into the asset management database.

Registering various types of information and always keeping it up to date requires a large time investment and overhead. An asset management system using Asset Information Manager handles these tasks easily, even in a large system, because in addition to enabling you to collect inventory information from JP1/Software Distribution in real time, it also allows you to execute registration and update operations periodically by using tasks registered in Windows Task Scheduler.

2. Manage information collected by JP1 products.

Asset Information Manager allows you to perform security management tasks by using the operation logs collected by JP1/Software Distribution. You can also check the operating status of software installed on various devices by viewing the operation times of software managed via JP1/Software Distribution.

3. Display JP1 product windows by using Asset Information Manager window operations.

By activating HP NNM Version 7.5 or earlier from Asset Information Manager, you can display *Network Presenter* for target devices.

Using the Network Presenter, the devices in a network can be displayed as a diagram, enabling you to view the connections of all the configuration elements and to pinpoint network problems.

4. Share information with JP1 products.

If you are using JP1/IM to achieve the integrated management of resources, such as networks, servers, and applications, and to centrally monitor events that occur in the system, you can share information about events in the system and check on problems and their status from Asset Information Manager windows. For a problem for which action has been taken, you can register the details of the action and report the completion of the action to JP1/IM - Manager.

You can also view asset information related to JP1 events by displaying Asset Information Manager operation windows from the JP1/IM Event Console window.

5. Distribute software programs from the Asset Information Manager operation window.

You can use Asset Information Manager operation windows to access the functionality of JP1/Software Distribution and distribute (transfer and install) software programs to each device. You can also check the status of software distribution.

By using the software information managed by Asset Information Manager, you can perform searches for devices to which particular software needs to be

distributed, thereby ensuring accurate distribution of software programs even in a large system.

6. Use Asset Information Manager to access centrally managed asset information for a wide variety of purposes.

In JP1/CSC, you can use asset information managed by Asset Information Manager to perform security measures for a system by using the windows under the Client Security Management job category. A security management system with JP1/CSC installed uses the policies set by the administrator as the basis for automatically determining the danger levels of devices and taking the appropriate action (countermeasures).

### 1.2.2 Integrated management of corporate asset information

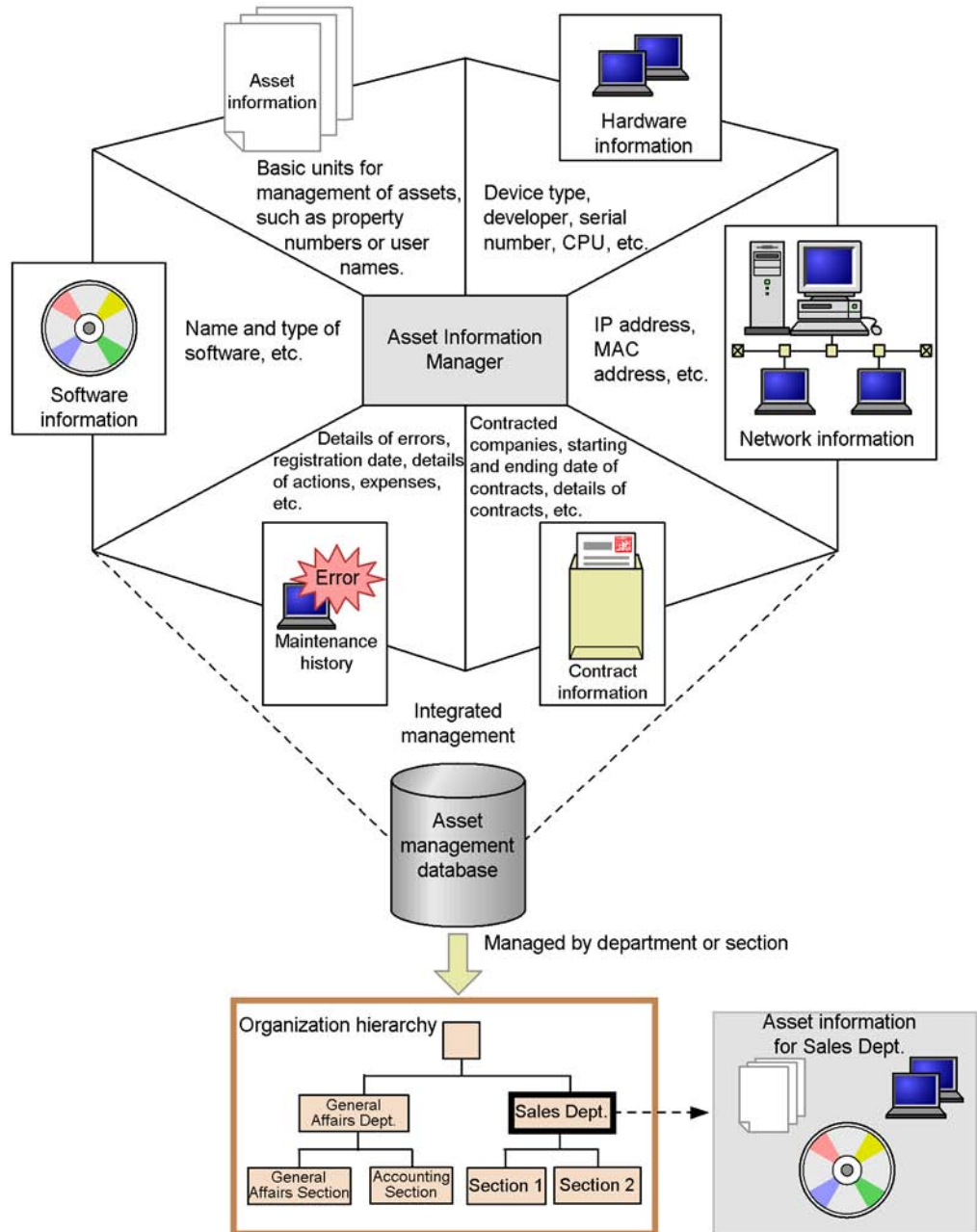
Managing corporate assets requires various types of information, such as information about devices, software programs, networks, and about maintenance and lease contracts. Defining inter-relationships among these information types allows you to effectively use this information. For example, you can perform operations such as comparing licenses installed on devices to the number of licenses owned by each group.

An asset management system based on Asset Information Manager can achieve integrated management of the *asset information* needed for asset management. For any specific device or software program, asset information can be added based on a variety of approaches. Corporate assets, such as equipment and networks, can be managed comprehensively by storing asset information in an asset management database.

Additionally, you can easily handle changes to the organization because the information managed for each group can be extracted from the centrally managed asset information. A user to whom a division is assigned can also manage the asset information of other groups.

The figure below shows the concept of the integrated management of asset information using Asset Information Manager.

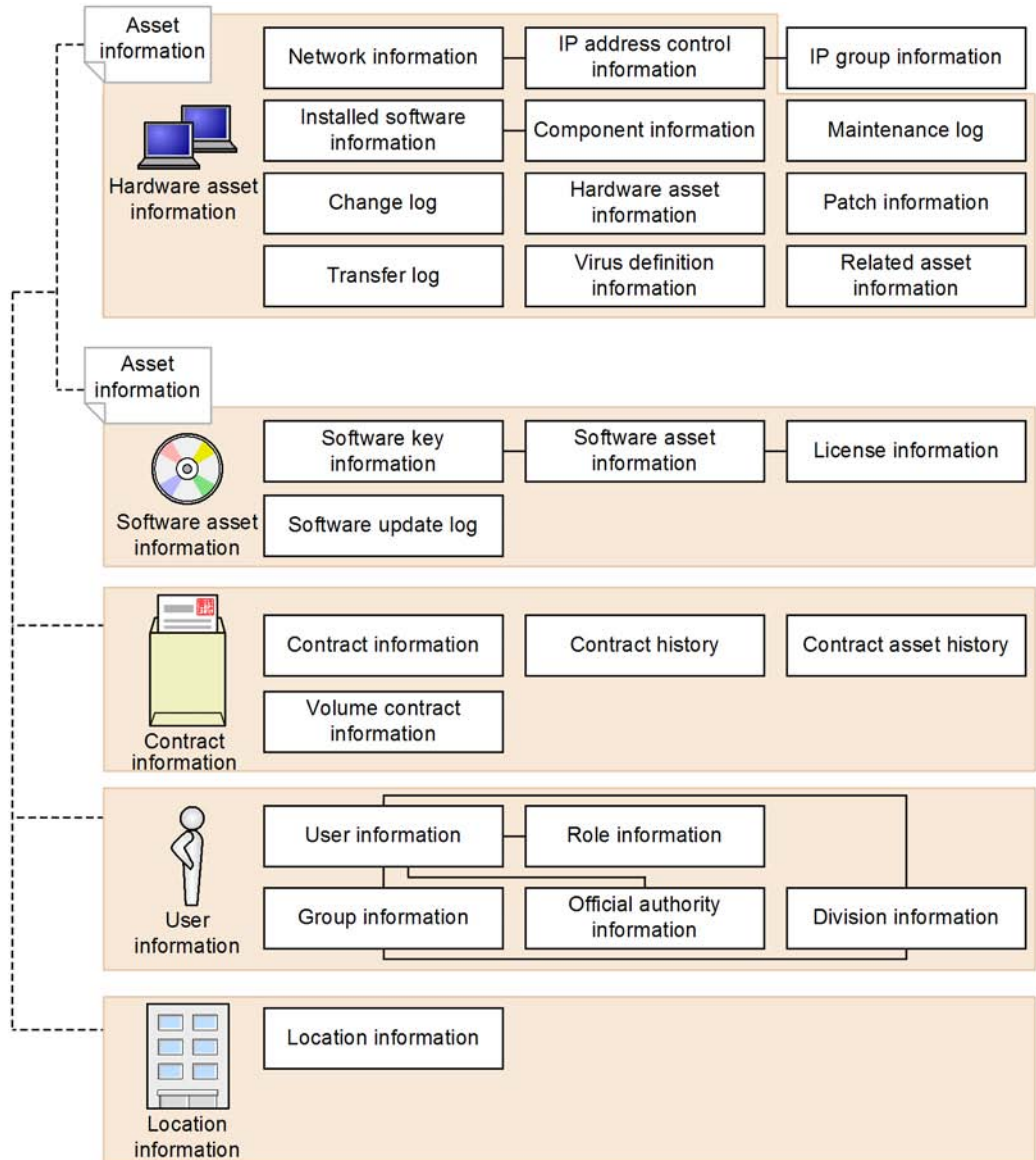
Figure 1-2: Concept of the integrated management of asset information



Asset Information Manager can manage many types of information, in addition to

those shown in Figure 1-2. Figure 1-3 shows the connection between the various types of information managed by Asset Information Manager and asset management databases.

Figure 1-3: Connection between asset information



Legend:

— : Link to information type

- - - - : Link to asset class

Information that can be managed by Asset Information Manager can be classified broadly into hardware asset information, software asset information, contract

information, user information, and location information.

Asset information is management information created for each and every unit of hardware and unit of software. The information is designed to connect the various types of attribute information of each asset. Asset information is also used as a generic term to refer to information that can be managed by Asset Information Manager.

The various types of interconnected information, such as network information, IP address control information, and IP group information, can also be associated and managed in the asset management database. For details about how to manage information using the asset management database, see *8.1 Asset management database* in the *Planning and Setup Guide*.

### **1.2.3 Practical totaling functions and search functions designed for each type of work task**

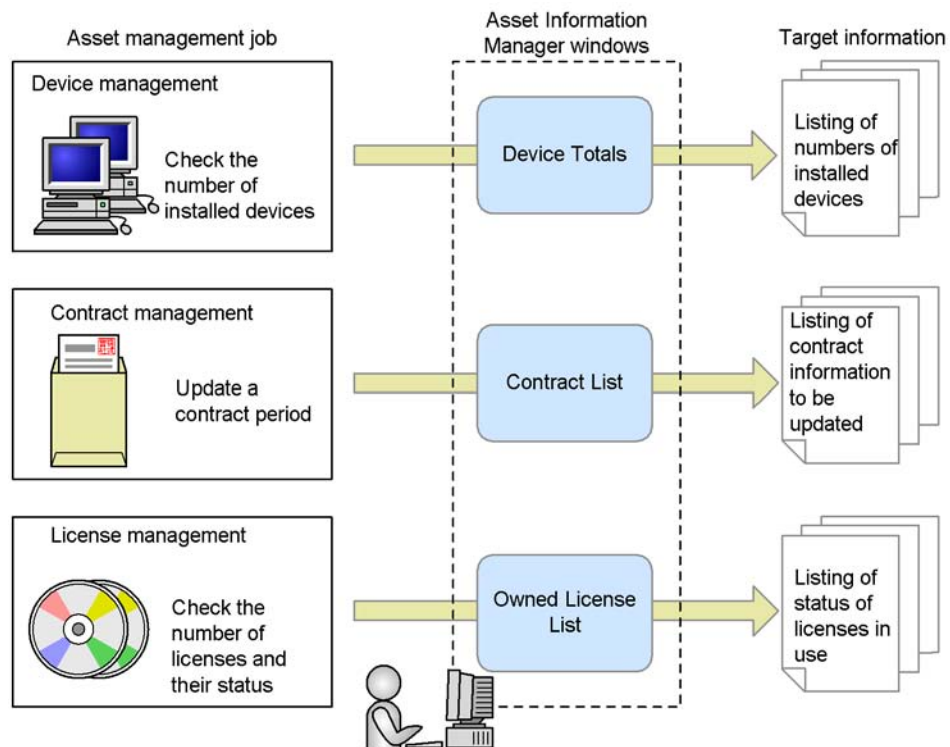
Taking advantage of centrally managed asset information for actual work requires the ability to perform certain tasks, such as totaling information, and selecting lists of required information.

Asset Information Manager allows you to use the main totaling functions used in asset management tasks and the search functions for listing appropriate asset information in each operation window. These totaling and search functions (which are performed from operation windows) can also be classified by group or location. A user to whom a division is assigned can also search the asset information of other groups.

You can use the results of such operations to determine the status of current assets, and take appropriate action.

The figure below shows the concept of performing a search for appropriate information from an operation window.

Figure 1-4: Concept of asset management tasks that use operation windows



For details about the configuration of the windows and common search and registration procedures, see *1. Basic Operating Procedure* in the *Administrator's Guide*. For details about the operating procedures in each operation window, see *2. Executing Asset Management Jobs* in the *Administrator's Guide*.

#### 1.2.4 Automating database maintenance and status monitoring

Among the issues in managing a large number of assets are the issues of how to efficiently maintain the asset management database containing the information and how to monitor the status of the assets.

Asset Information Manager allows you to use Windows Task Scheduler to maintain the asset management database containing the asset information as well as monitor asset statuses. Specified processing is executed automatically by tasks at specified dates and times. This reduces the workload on asset managers to maintain the database and monitor managed information.

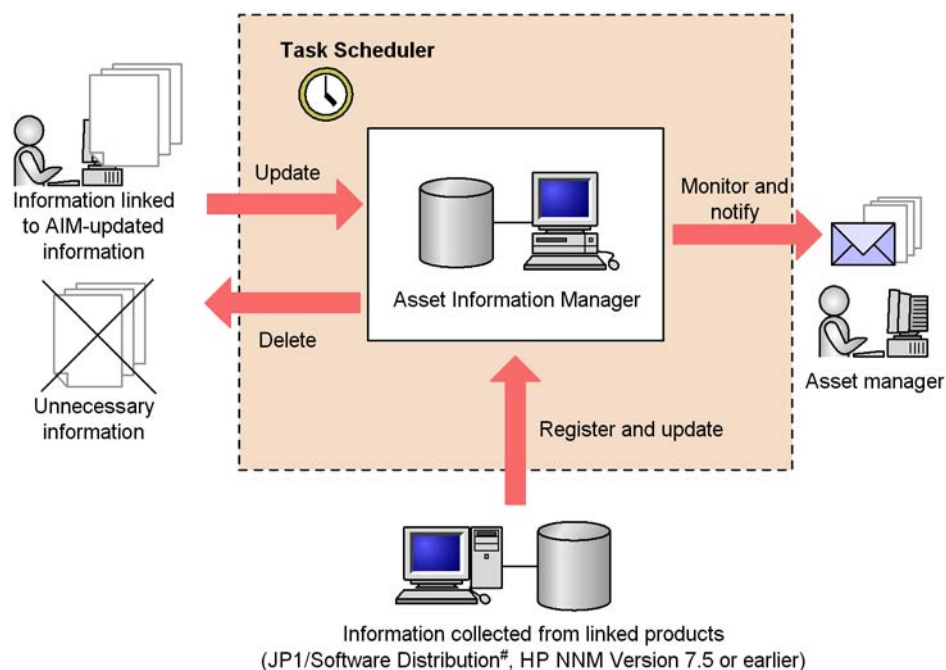
Furthermore, by using the *Asset Information Synchronous Service* provided by Asset Information Manager to monitor the inventory information collected by JP1/Software Distribution, JP1/Software Distribution updates can be applied in real time to the asset




management database.

The figure below shows the concept of maintaining the asset management database and monitoring operating statuses.

*Figure 1-5: Concept of using tasks to update and monitor data in the asset management database*



Legend:

 : Processing that is performed by tasks

#: You can also use a service to perform monitoring and updating in realtime, without using a task.

## Database maintenance

Asset Information Manager allows you to effectively use database capacity while maintaining the integrity of data in the asset management database by also updating information related to the information being updated by Asset Information Manager and removing unnecessary information.

You can also register and periodically update information from linked products in the asset management databases based on node information collected by HP NNM Version 7.5 or earlier.

For inventory information collected by JP1/Software Distribution, you can choose between using a service to perform monitoring and updating in real time,

or using a task to perform periodic updates.

#### Monitoring of operating statuses

You can periodically check for contracts whose expiration dates are getting close, and notify an asset manager by email. This informs the asset manager about contracts that are about to expire, so that they can be renewed in a timely manner.

You can also periodically total the usage statuses of software licenses, and provide an email notification if an installation exceeds the number of owned licenses or an installation using an unauthorized license is detected.

For details about setting up tasks with Task Scheduler, see *5.9 Setting the tasks that are registered in Task Scheduler* in the *Planning and Setup Guide*.

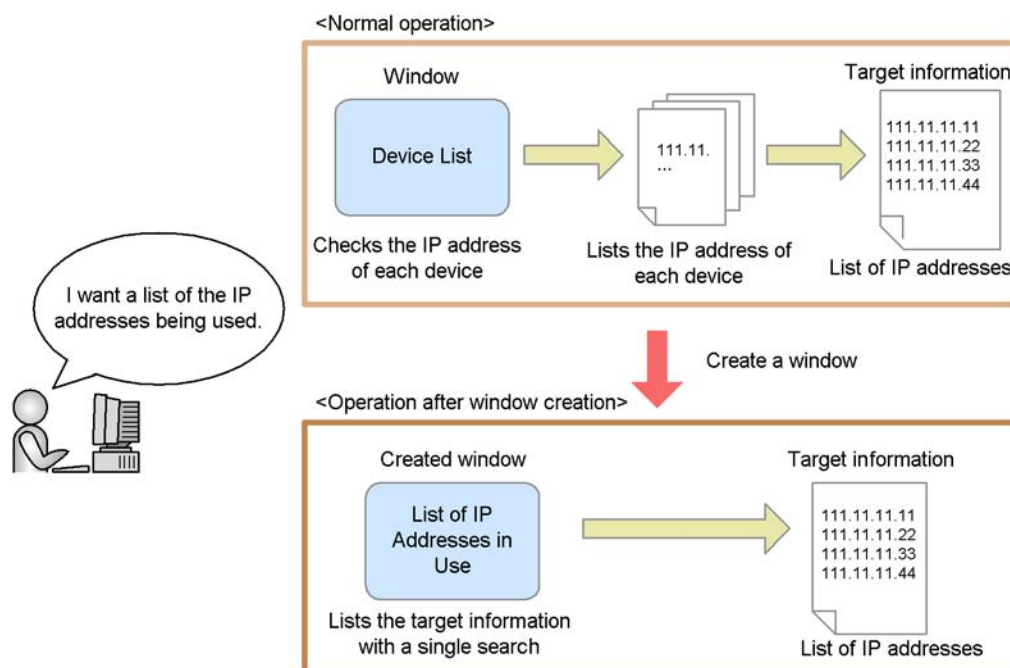
### **1.2.5 Creating operation windows for routine jobs**

You can improve operational efficiency by creating operation windows suitable for routine jobs that search for a specific type of information. For example, by creating an operation window, you can search by group for information that normally can be searched for only by device, or search for only the IP addresses that are currently in use.

You can use the provided GUI to easily create windows appropriate for routine jobs. Note that you can create a window that searches the asset information managed by the asset management database and displays the results as a list, but you cannot create a window that totals or registers asset information.

The figure below shows the concept of managing assets by using a window created for a routine job.

Figure 1-6: Concept of managing assets by using a window created for a routine job



For details about creating windows, see *9.5 Adding windows for routine jobs (Create User Report)* in the *Planning and Setup Guide*.

## 1.2.6 Restricting and extending tasks according to user roles

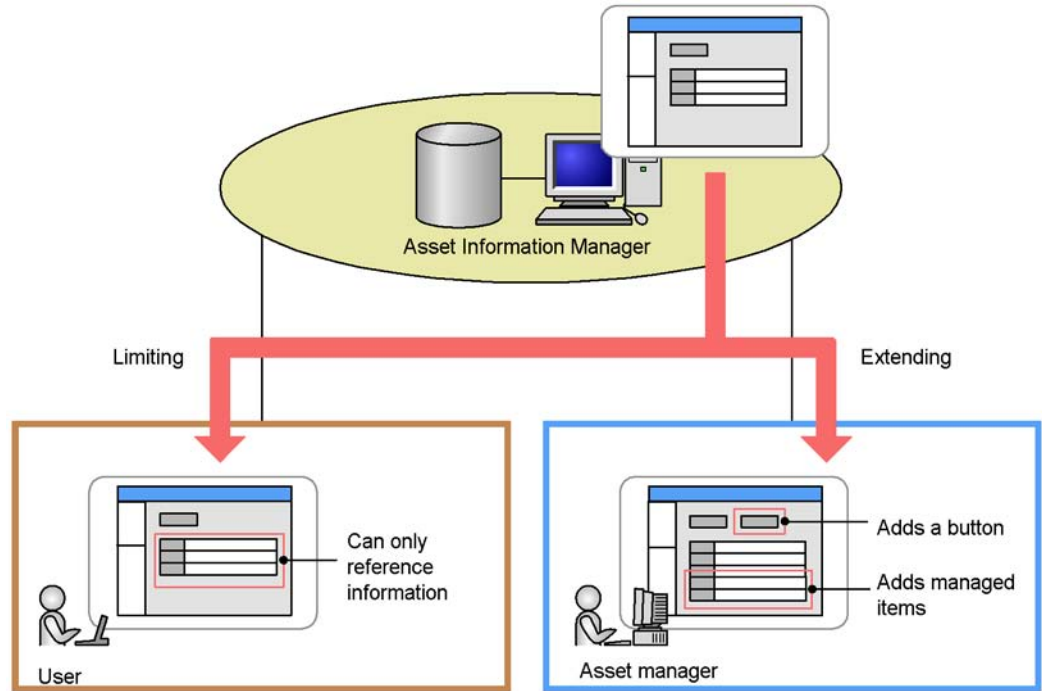
User permissions can be used to restrict or extend the scope of jobs that can be performed by the user. Being able to change the functionality that is available for each set of user permissions allows you to better use the centrally managed asset information for your desired purposes.

For example, for users who will use the windows only for checking their own PC information and the statuses of the licenses for installed software programs, you can restrict the window functionality associated with updating asset information, and permit those users to only being able to perform view operations.

For the asset manager, you can extend the window functionality available so that the asset manager can register multiple contracts with a contract company or delete contract information from the Contract List window.

The figure below shows the concept of restricting and extending work tasks by using user permissions.

*Figure 1-7: Concept of restricting and extending work tasks by using user permissions*



For details about restricting and extending functions of window operations, see 2.7 *Limiting available functions by user roles*. For details about how to perform such operations, see 9.3 *Changing a window for a user role (Customize Job windows)* in the *Planning and Setup Guide*.

### 1.2.7 License management of various license types

Asset Information Manager allows you to manage various types of software licenses.

This section describes the typical license types and the license management methods, and the license management method used by Asset Information Manager.

#### (1) License types

There are many types of licenses, but the main ones are as follows.

- Installation license  
This license permits installation on a single device.
- User license  
This license permits use by a single user. It permits installation on multiple

devices that are owned by the same user.

- Pre-installed

This license covers installation on a purchased device.

- Server license

This is a license for server products. Server products normally have additional licenses, such as for the permitted number of times the server can be accessed (client access license), the permitted number of CPUs (CPU license), or the permitted number of manageable nodes (managed node license).

- Second license

This license permits installation on a specific second device, such as a portable device. It is typically together with an installation license that permits installation on only a single device.

- Concurrent execution license

This license might be necessary, depending on the number of software programs that are to be concurrently executed or reside on a device.

- Volume license

This license allows you to freely purchase any number of licenses within the predefined range. The purchaser can choose the desired combination and number of licenses, but both the minimum and maximum number of points that can be used during the contract period are predetermined.

In addition to the above types of licenses, there are various options, such as whether software is upgradeable or downgradable.

## **(2) License management methods**

The two main license management methods are *total count management* and *per-license management*. You can select the method that is best for your asset management system (or is appropriate for your software programs).

### Total count management

This method manages licenses by comparing the total number of software licenses owned by the company or a group to the number of licenses in use. It eliminates the need for allocating individual licenses, thereby making management tasks comparatively easy.

However, if licenses are not used properly, it is difficult to identify a specific device or user where a license violation is occurring. Even with the same license, if permitted options depend on purchase contract terms, it is difficult to determine whether the license is being used properly by each device or user.

You cannot clearly determine which devices downgrade software licenses are

being used for.

#### Per-license management

This method manages licenses by associating each owned license with a specific device or user. This method allows you to accurately determine the usage status according to each license's terms of purchase. It is also easy to identify devices or users that are illegally using licenses.

However, this method requires that each license be associated with a device or a user.

### **(3) License management via Asset Information Manager**

Asset Information Manager provides you with the flexibility to create license information appropriate to the types of licenses you have and the management method you are already using, thereby making it possible to manage licenses on a very detailed level.

For example, you can efficiently manage licenses by using the appropriate management method for each license, such as employing *total count management* for licenses that are used throughout the entire company and *per-license management* for licenses that are individually purchased.

In addition to the volume license management method, this section describes *total count management* and *per-license management*, which are license management methods supported by Asset Information Manager.

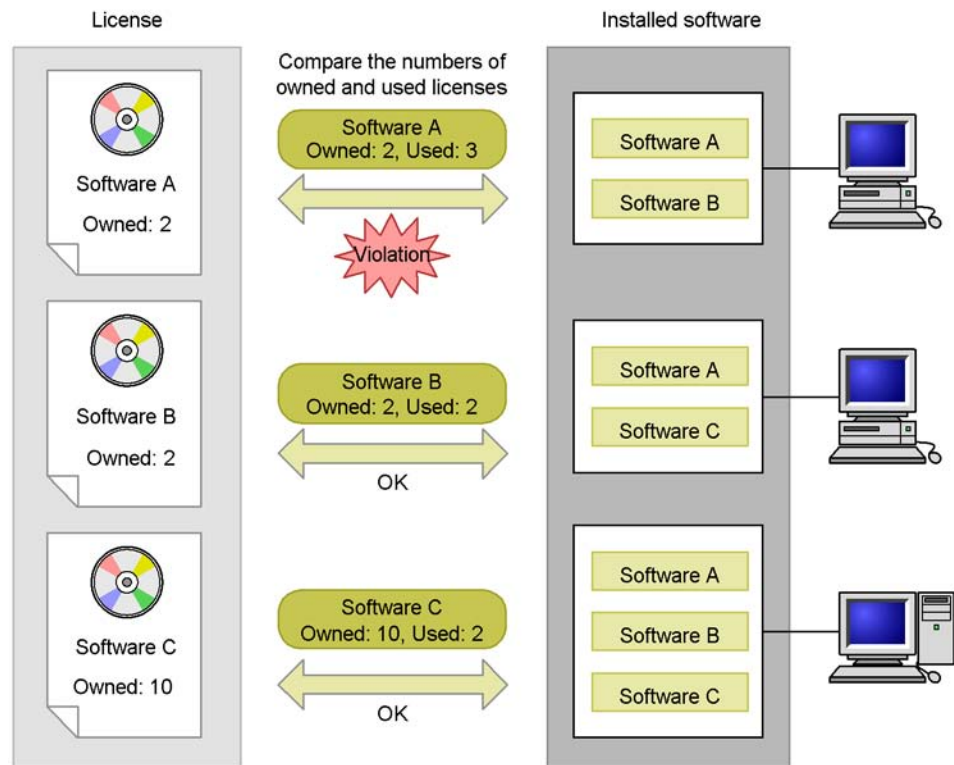
#### **(a) Managing licenses based on the number of owned licenses and the number of used licenses**

This is the *total count management* method.

This method registers the number of licenses you own (referred to as the *number of owned licenses*) when a license is purchased, obtains the number of licenses being used from the licenses installed on devices, and then compares these numbers.

The figure below shows the concept of managing licenses on the basis of the number of owned licenses and the number of used licenses.

Figure 1-8: Concept of managing on the basis of the number of owned licenses and the number of used licenses



For an example of total count management, see 2.4(1) *Checking the operation status by comparing the number of owned licenses to the number of used licenses.*

### (b) Managing licenses by assigning them to devices or users

This is the *per-license management* method.

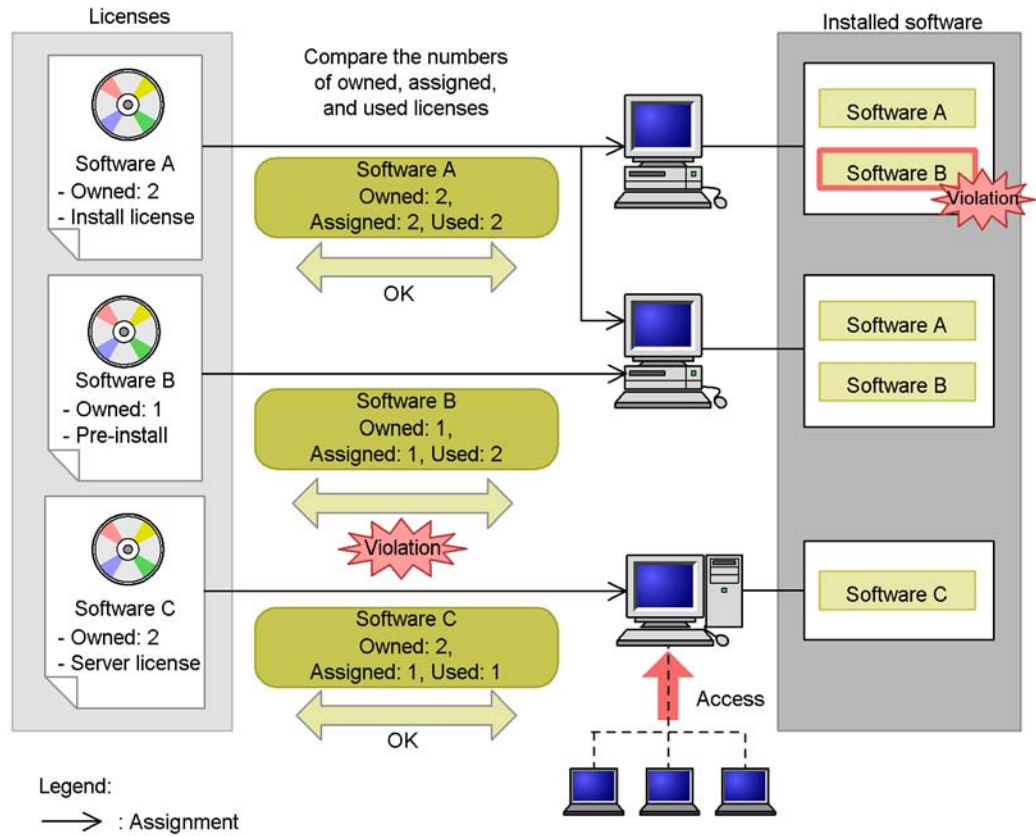
Managing licenses by assigning them to devices

This method manages licenses that are required for each device, such as installation licenses and second licenses, by assigning them to devices.

A license's acquisition method, such as part of a package or pre-installed, can be managed as an attribute within the license information.

The figure below shows the concept of managing licenses by assigning them to devices.

Figure 1-9: Concept of managing licenses by assigning them to devices



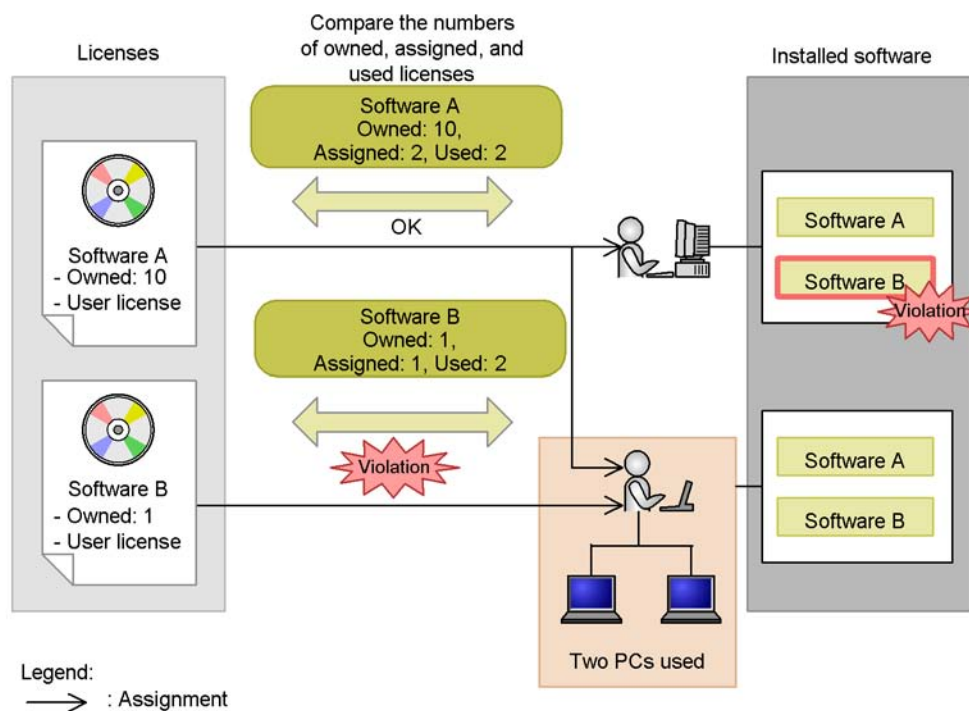
### Managing licenses by assigning them to users

This method manages licenses as user licenses by assigning them to users who are managed by Asset Information Manager.

The figure below shows the concept of managing licenses by assigning them to users.



Figure 1-10: Concept of managing licenses by assigning them to users



Second and concurrent execution licenses are managed as follows:

- Managing second licenses

You can manage second licenses by adding and assigning them to devices, or by managing them as user licenses without adding the licenses.

- Managing concurrent execution licenses

You can manage concurrent execution licenses by registering the number of licenses that can be executed concurrently as the number of owned licenses, or you can manage the number of copies that can be executed concurrently as a license attribute.

For an example of *per-license management*, see 2.4(2) *Accurately managing targets according to the assigned licenses*.

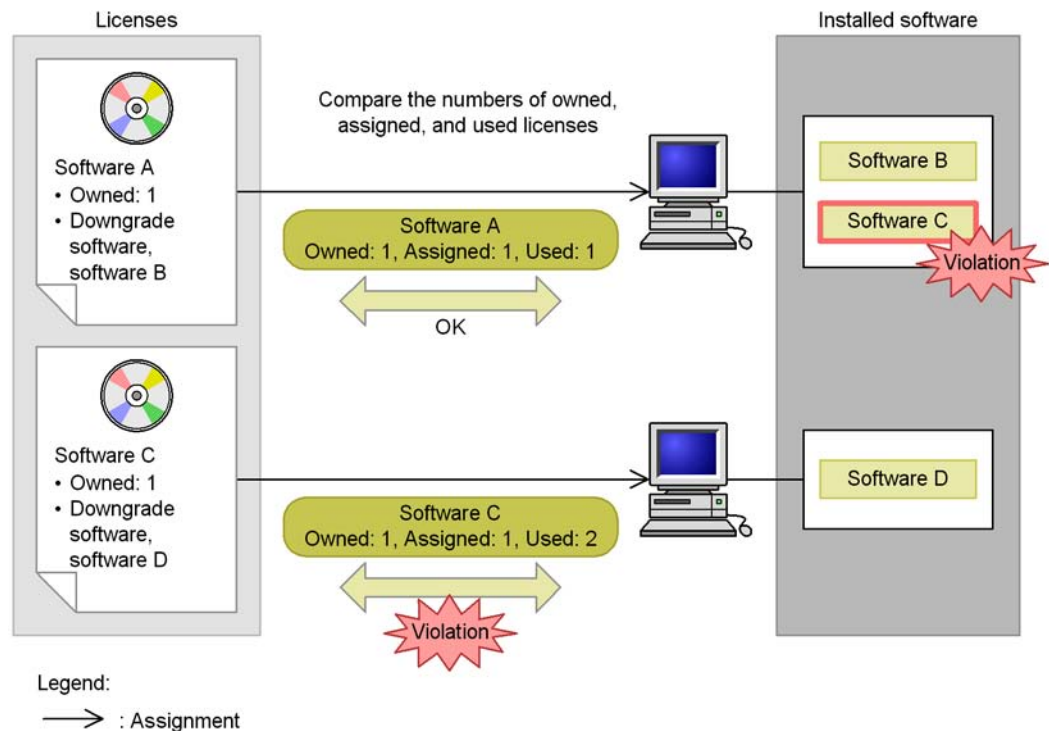
### (c) Managing downgrade software

When you use a purchased license for an older version of some software (for example, if you purchased a license for Windows XP Professional, but you are actually using it for Windows 2000 Professional), the older version of the software is called *downgrade software*. To manage downgrade software, you must perform per-license management

as described in subsection (b) above.

The figure below shows the concept of managing downgrade software by assigning licenses for each device and managing them as installation licenses.

Figure 1-11: Concept of managing downgrade software



Managing downgrade software requires specifying a number of settings in addition to performing per-license management. For details, see 4.6.9 *Adding downgrade software assets* in the *Administrator's Guide*.

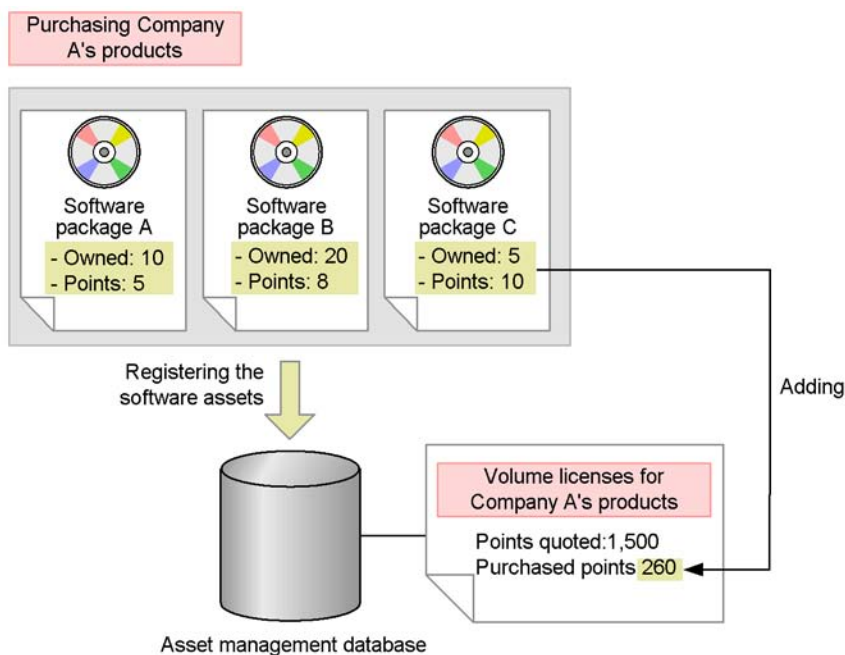
**(d) Managing volume license points**

You can manage the status of the number of accrued points by registering the volume license information and associating it with the applicable licenses.

Options for volume licenses (such as whether software is upgradeable) are managed as part of the license information for software.

The figure below shows the concept of managing volume license points.

Figure 1-12: Concept of managing volume license points



### 1.2.8 Using a flow to apply for requests and approve tasks

Asset management tasks include those that require applying for and getting approval for something, as well as tasks that must be passed through an acceptance and handling process. For example, the installation of a new device requires a process for obtaining approval from a manager. Also, the details of actually arranging for and distributing the device must be dealt with by persons within the organization responsible for the overall management of the system.

With Asset Information Manager, these types of jobs are performed by creating an *Item*. An Item is a job that travels along a defined route. An Item can also be thought of as the electronic form used when performing the job.

A task, such as the installation of a device or software program, proceeds through a system as it is sent and received by various parties. This process is referred to as a *flow*. Flows make it easier to achieve ITIL processing.

Asset management tasks that use flows have the following benefits:

- By creating a single Item, you can process an application without needing to know who will handle the details, thereby making it easier to distribute required information.
- Information to be used by the procedure is registered onto the server, enabling the

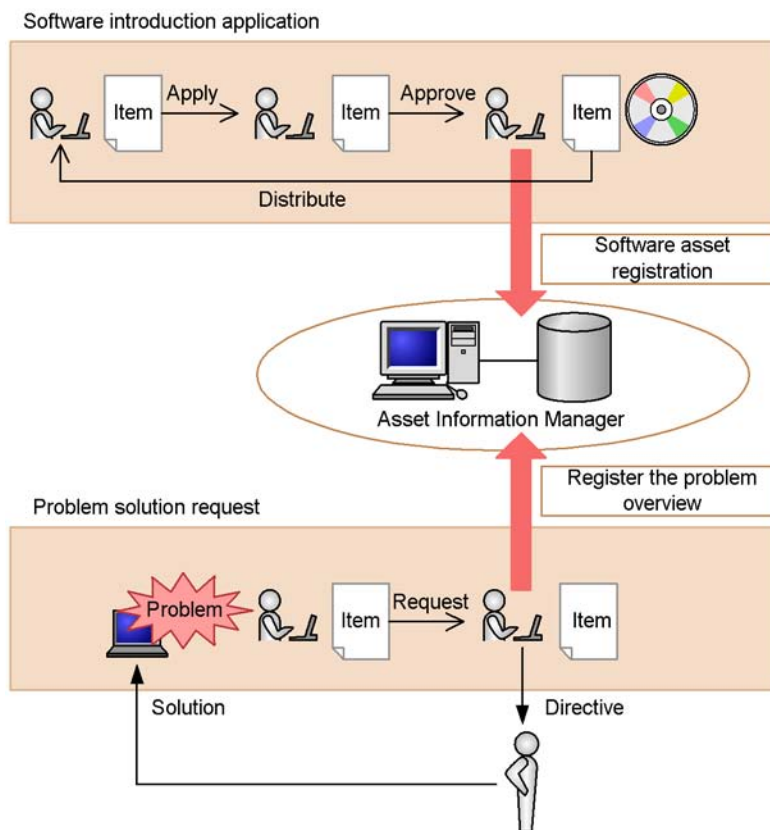
information to be managed reliably.

- Items can be managed centrally, making it easier to understand how far work related to the task has progressed.
- The use of Items for applying for and approving things also allows Items to be used as draft planning instruments, since all approvals are obtained through a formal processing route.

Furthermore, Asset Information Manager enables more efficient asset management with features, such as linking Items to JP1/Software Distribution to distribute software to the PC that submitted the application, and automatically registering information for problem resolutions as requested by an Item when a problem is resolved.

The figure below shows the concept of performing application and approval tasks by using a flow.

Figure 1-13: Concept of performing application and approval tasks by using a flow



### 1.2.9 Managing patch application statuses

By linking Asset Information Manager to WSUS or JP1/Software Distribution, you can easily apply patches and other updates to devices. Asset Information Manager supports taking security measures by allowing you to monitor the centrally managed asset information while patches are being applied.

- Efficient application of patches via linkage to a WSUS server

Asset Information Manager uses a batch operation to apply patches to devices that have been determined (detected) by the WSUS server to require a patch. If deemed necessary, you can use Asset Information Manager to view the asset information of the detected device when a patch is applied. Because you can quickly check the user, administrator, and other information associated with any

device on which an error occurs, this is also helpful to ensure that the patches have been fully applied.

You can also set the timing of the WSUS server to be synchronized with Microsoft Update. When new updates are released to the WSUS server, an email notification can be sent to the asset manager. This saves you the trouble of having to synchronize the WSUS server and check for new updates, thus enabling you to manage updates more effectively.

- **Reliable application of patches via linkage to JP1/Software Distribution**

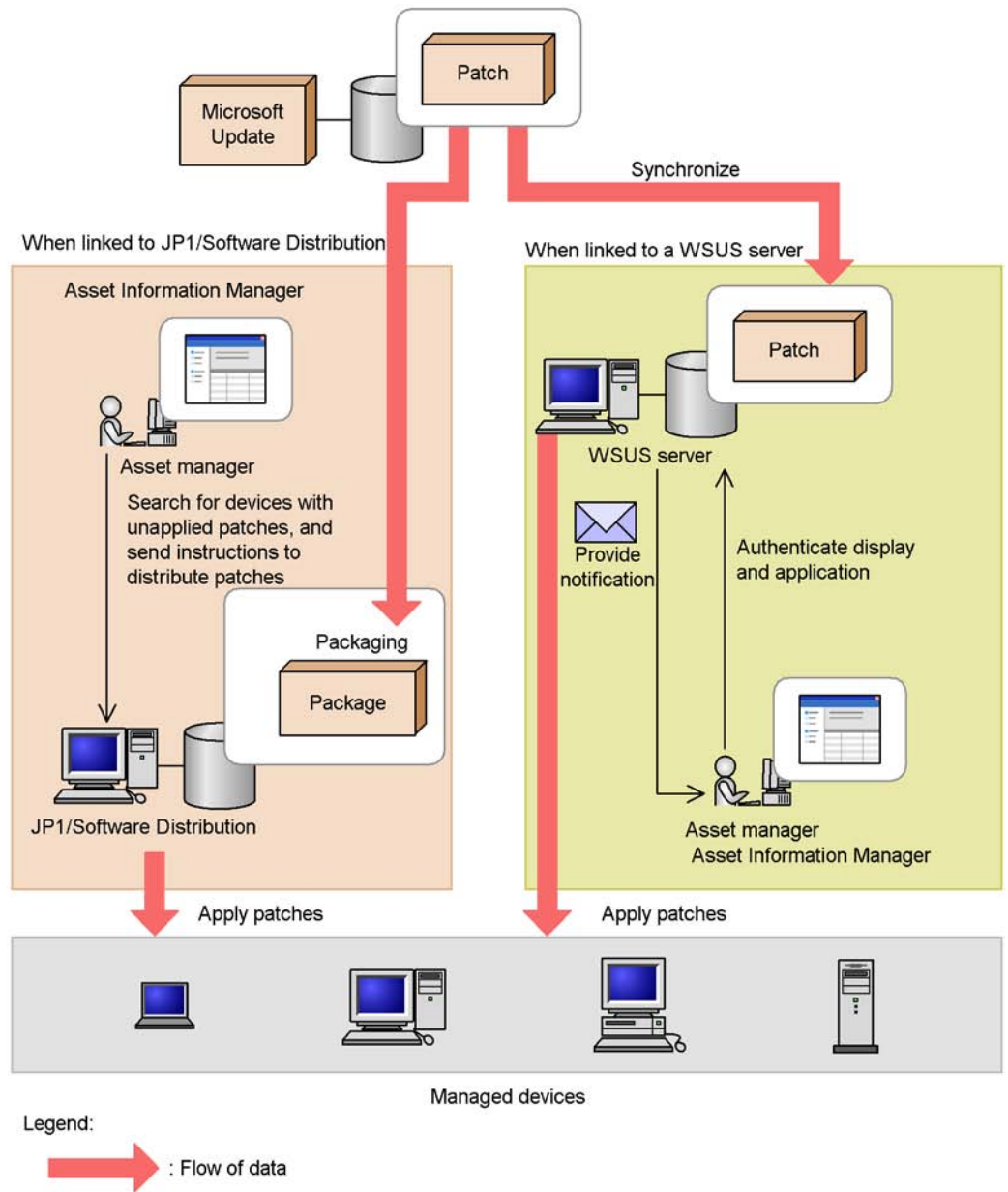
JP1/Software Distribution packages and distributes patches to devices that have been found by Asset Information Manager to require application of a patch. The fact that you can obtain the current status of patch applications by collecting inventory information gives you the assurance that the patch was applied.

If the system supports JP1/Software Distribution, you can distribute patches even in systems that do not support a WSUS server.

You can use the same procedure to distribute virus definition files and other updates.

The following figure shows the concept of linking to JP1/Software Distribution or to a WSUS server, and applying a Microsoft Update patch to managed devices.

Figure 1-14: Concept of applying a patch from Microsoft Update to devices



### 1.2.10 Login authentication using Active Directory services

Active Directory services can be used for authentication when logging in to Asset

## 1. Overview

**Information Manager.** This allows login passwords to be consolidated in Active Directory, and means that you do not have to use Asset Information Manager to manage passwords.



## Chapter

---

# 2. Typical Usage

---

This chapter describes the typical usage of Asset Information Manager, such as how to use Asset Information Manager in asset management tasks and the preparations needed to use Asset Information Manager after it has been installed.

- 2.1 Importing and exporting device information
- 2.2 Managing the usage statuses of IP addresses
- 2.3 Stocktaking
- 2.4 Determining whether licenses are handled legally
- 2.5 Applying updates by linking to a WSUS server
- 2.6 Adding asset information statuses, managed items, and windows
- 2.7 Limiting available functions by user roles
- 2.8 Solving problems using Items
- 2.9 Checking user operations by means of operation logs
- 2.10 Login authentication via linkage with Active Directory
- 2.11 Including Active Directory information in the asset management database

---

## 2.1 Importing and exporting device information

---

With Asset Information Manager, you can import CSV data into asset management databases, and export asset management database information in CSV format.

The following lists examples of tasks that you can perform:

- Importing data from another system into the asset management database.
- Select output items, and perform regular backups.

This section uses the example of device information to explain importing and exporting operations.

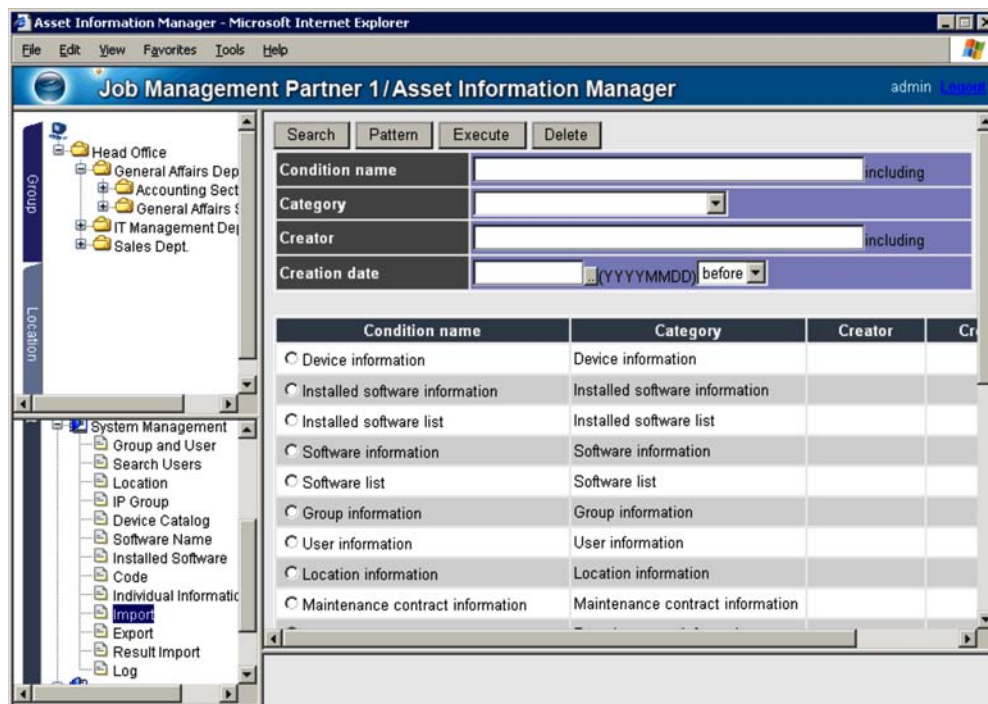
### ***(1) Importing data from another system into the asset management database***

By importing data into the asset management system, you are effectively using a batch operation to register from another system. Provided you are working in a system environment that allows you to log in to Asset Information Manager, you can import data from any location.

You can use the Import window to import data from a CSV file.

The figure below shows the Import window.

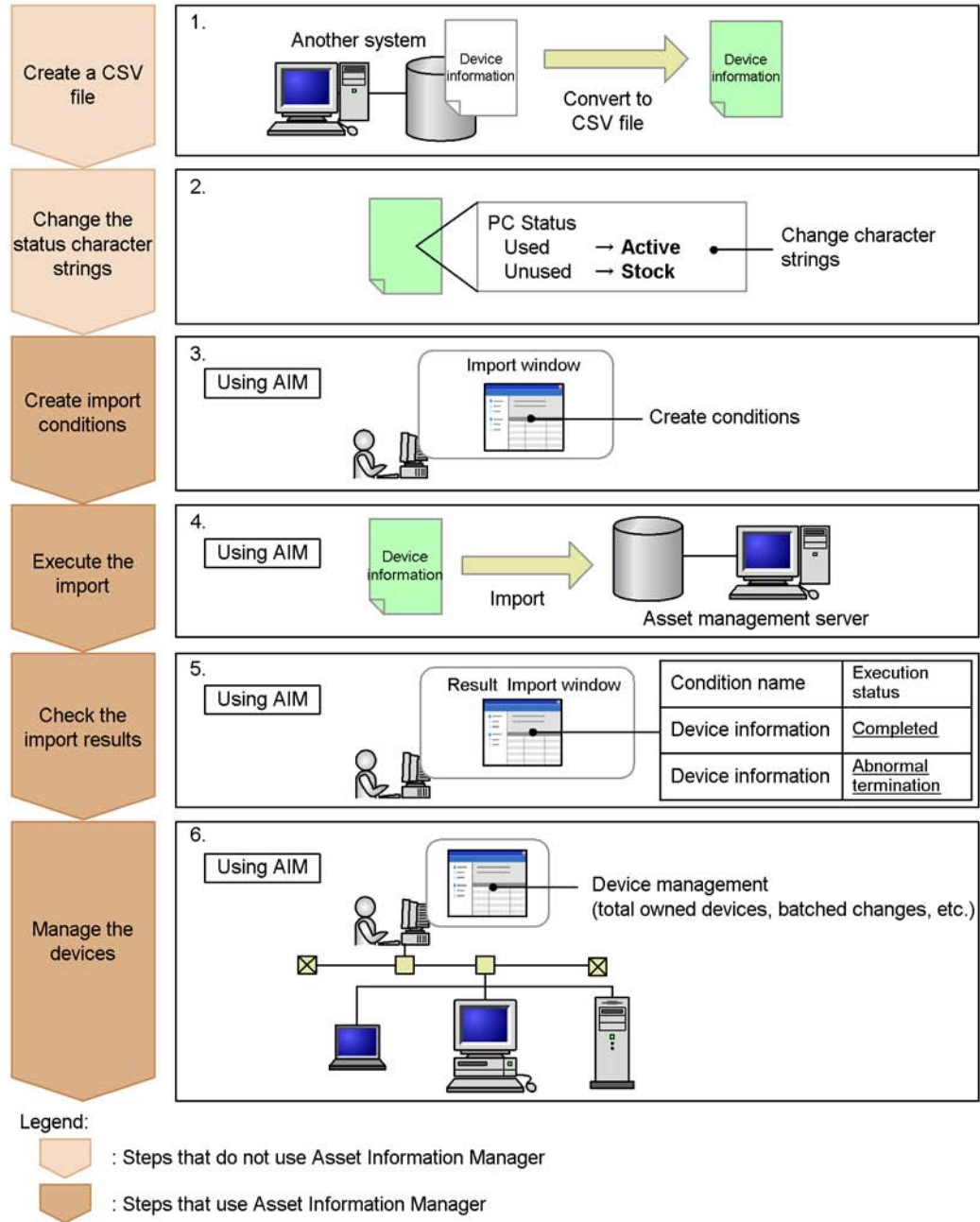
Figure 2-1: Import window



To import data, you must first create conditions, and then import the data according to the conditions. A sample is provided for the import conditions for each information type. For details about these sample asset types, see *4.10.2(1) Selecting the asset type* in the *Administrator's Guide*.

The procedure below describes the workflow for importing information managed by another system into the asset management database. This example assumes that Machine No. (a unique value assigned to each asset), Name, PC Status (Used/Unused), and MAC Address are being managed.

Figure 2-2: Workflow for importing information regarding devices managed by another system



To import information managed by another system:

1. Create a CSV file.

Only CSV data can be imported into the asset management database. As such, you must first create a CSV file containing the data you want to import. You can use any character string for the item names in the CSV file. For details about the CSV file format, see *4.10.1(1) CSV file format* in the *Administrator's Guide*.

The following figure shows an example of a created CSV file.

*Figure 2-3: Example of a created CSV file*

Machine No.	Name	PC Status	MAC Address
11111,	Smith,	Used,	00:11:22:AA:BB:CC
22222,	,	Unused,	33:44:55:DD:EE:FF
		:	
		:	

2. Change the *Used* and *Unused* character strings under *PC Status*.

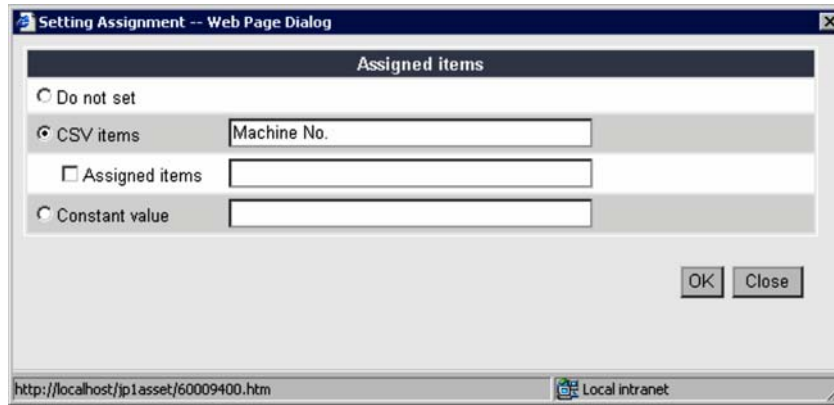
To match legacy operation of Asset Information Manager, you must change instances of *Used* and *Unused* under *PC Status* in the CSV file to *Active* and *Stock*.

To inherit the pre-transfer names, use the Code window to change the status character strings. For details about how to use the Code window, see *4.8.2 Changing a code's display value* in the *Administrator's Guide*.

3. Create import conditions.

To register data into the asset management database, create import conditions and assign item names in the CSV file to the managed items. To create import conditions, first click the **Pattern** button in the Import window to display the Select Category dialog box. After that, select **Device information** in the **Category** column. Next, click the **Browse** button for the managed items to display the Setting Assignment dialog box. Set the assigned items from this dialog box. The following figure shows the Setting Assignment dialog box.

Figure 2-4: Setting Assignment dialog box



The following table shows the settings for the assigned items when the conditions are created:

Table 2-1: Settings for assigned items when the conditions are created

Managed items	Setting for assigned items
Asset information.Asset No.	Specify Machine No. for CSV items.
Asset information.User name	Specify Name for CSV items.
Asset information.Usage management	Specify Used for Constant value.
Asset information.Status	<ul style="list-style-type: none"> <li>Specify PC Status for CSV items</li> <li>Select the <b>Assigned items</b> check box, and choose Active.</li> </ul>
Asset information.Reg. date	Specify 2006/01/01 for Constant value.
Hardware information.MAC address	Specify MAC Address for CSV items.

The following lists important points to keep in mind when you are creating conditions:

- Always specify item names that have a star (★).
- By assigning a unique value to each asset as its asset number, you can manage values managed by other systems as asset numbers. If you do not register any values, asset numbers are provided automatically.
- When you import MAC addresses, the inventory information collected from JP1/Software Distribution is assigned as the information of the imported devices.

For details about how to create import conditions, see *4.10.2 Creating import*

*conditions* in the *Administrator's Guide*.

After you save the conditions, click the **Back** button to return to the previous window.

4. Import the data.

In the Import window, specify the created conditions, and import the data. For details about how to import data, see *4.10.3 Executing imports* in the *Administrator's Guide*.

5. Check the import results.

In the Result Import window, check the results of the import operation. For details about how to check the import results, see *4.12 Checking the import results (Result Import)* in the *Administrator's Guide*.

6. Manage the devices.

By using the Device Totals window, you can total the number of owned devices, change device information from the Batch Update window, and perform other device management activities.

Repeat steps 1 to 4 of the import procedure until you have imported all of the information.

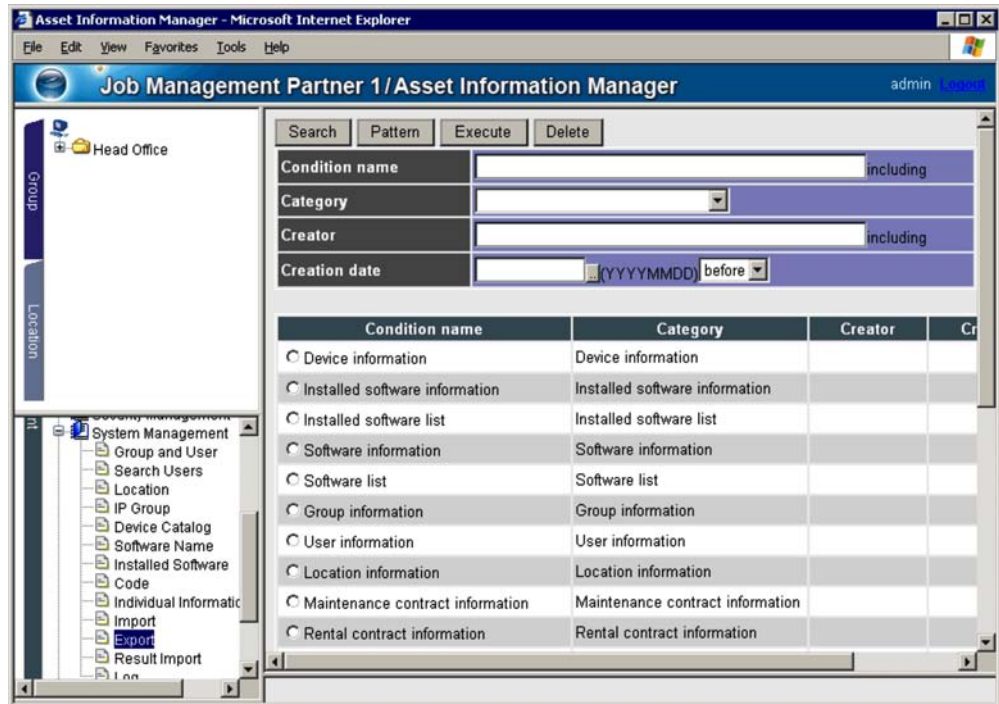
## **(2) Limiting items being exported for regular backups**

By creating conditions in advance for filtering items to be exported, you can export only the information that you want to export. By specifying conditions that you have created, you can also easily limit the items to export when you back up the asset management database.

The Export window is used to export data to be backed up.

The figure below shows the Export window.

Figure 2-5: Export window



To export data, first create conditions, and then export the data according to those conditions. Samples of export conditions are provided for each type of information. You can use these samples to export all items. For details about these sample categories, also known as asset types, see 4.10.2(1) *Selecting the asset type* in the *Administrator's Guide*.

The procedure below describes the workflow for exporting device information in CSV format.

To export device information to a CSV file:

1. Create export conditions.

Begin by creating export conditions for making backups. To create export conditions, first click the **Pattern** button in the Export window to display the Select Category dialog box. After that, select **Device information** in the **Category** column. Next, set the items to be exported to the CSV file.

The following lists the export items to set when creating conditions:

- **Asset No. (Asset information)**
- **User name (Asset information)**



- **Status (Asset information)**
- **MAC address (Hardware information)**

For details about how to create export conditions, see *4.11.1 Creating export conditions* in the *Administrator's Guide*.

Save the conditions, and then click the **Back** button to return to the previous window.

2. Export the data.

In the Export window, specify the conditions created in step 1 and export the data. If you want to export only information from managed groups or otherwise filter the data being exported, click the **Filter** link to display the Set Condition dialog box, where you can filter the number of items. For details about how to export data, see *4.11.2 Executing an export operation* in the *Administrator's Guide*.

3. Specify a file name, and then save the data.

We recommend that you specify a file name that makes it easy to determine the date the file was exported and the contents of the file; for example, `060701_device-info.csv`.

4. Check the exported data.

Check the data to make sure the export executed normally.

To make use of the export functionality when you make regular data backups, repeat steps 2 to 4 using the export conditions created in step 1.

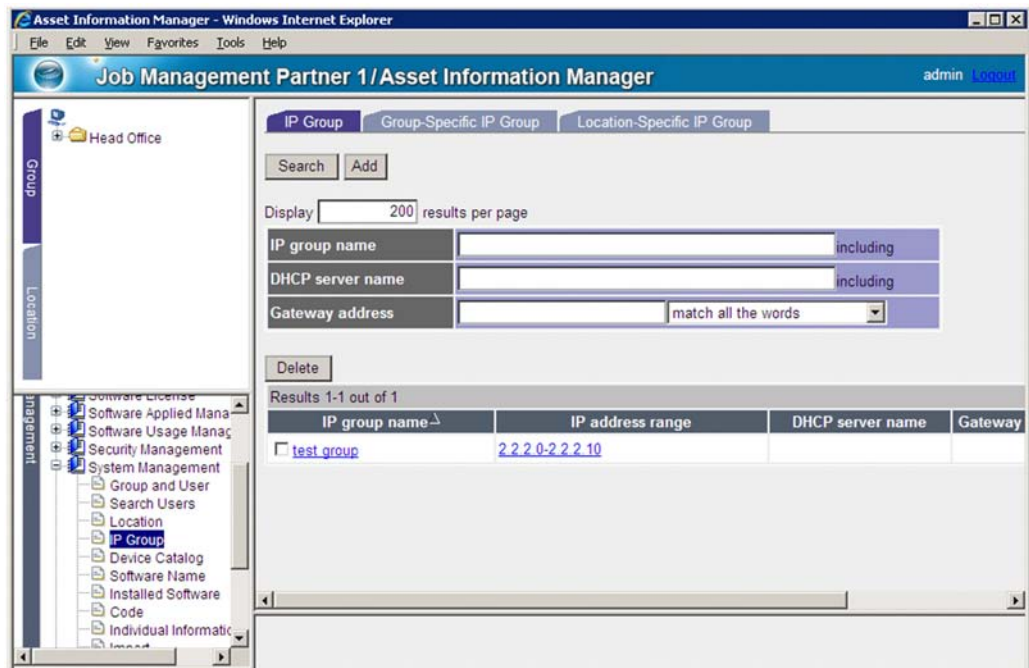
## 2.2 Managing the usage statuses of IP addresses

The usage statuses of IP addresses are managed by associating them with groups. By separating the IP addresses into IP address ranges and managing them in group-specific IP groups, the group associated with the IP address of any particular device can be set automatically, even if JP1/Software Distribution does not collect the group information as user inventory information. This allows you to manage the usage statuses of IP addresses by group.

The usage statuses of IP addresses are managed in the IP Group window.

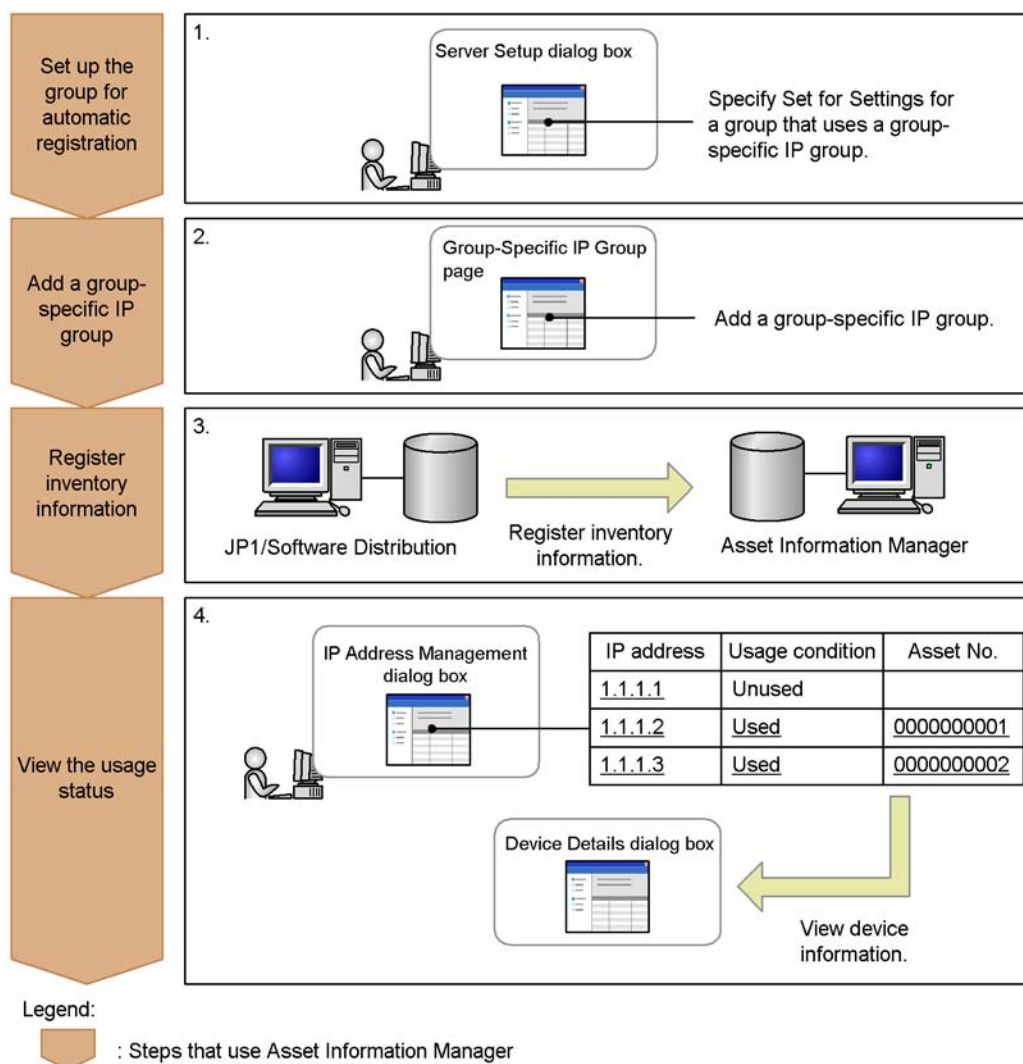
The figure below shows the IP Group window.

Figure 2-6: IP Group window



The following figure illustrates the workflow for managing the usage statuses of IP addresses by group, by registering the group associated with the IP addresses that are assigned to devices owned by the group. This example assumes that JP1/Software Distribution does not collect group information as user inventory information.

Figure 2-7: Workflow for associating a group with IP addresses, and managing the IP group



To associate and manage IP addresses by group:

1. Set up automatic registration for the group to be associated with the IP addresses.

To configure the system so that, when the IP address of a device changes, the group that includes the changed IP address is set automatically, specify **Set for Settings for a group that uses a group-specific IP group** in the Server Setup dialog box. For details about how to set values in the Server Setup dialog box, see

### 5.3.4 Setting Basic Information in the *Planning and Setup Guide*.

*Reference note:*

You can also have the group corresponding to the IP address be recorded automatically during a task scheduler data maintenance task. Even when group information is being collected from the JP1/Software Distribution user inventory, by executing this task, you can update the group to match the values set with the **IP Group** job menu.

2. Add an IP group.

Add the IP group you want to manage using the **Group-Specific IP Group** tab in the IP Group window. For details about how to add an IP group, see *4.4.1 Adding an IP group* in the *Administrator's Guide*.

3. Register inventory information to the asset management database.

You can register the desired device information using the inventory information collected by JP1/Software Distribution. For details about how to register inventory information, see *5.1.1 Workflow necessary for linking to JP1/Software Distribution* in the *Planning and Setup Guide*.

You can also use node information collected by HP NNM Version 7.5 or earlier to register device information. For details about how to register node information, see *6.1 Settings for linking to HP NNM Version 7.5 or earlier* in the *Planning and Setup Guide*.

4. View the IP address usage status.

In the IP Address Management dialog box, you can view information about devices to which IP addresses are assigned and check for unused IP addresses. You can also display the Device Details dialog box by clicking the **Asset No.** link. For details about how to view IP address usage status, see *4.4.2 Viewing IP address usage* in the *Administrator's Guide*.

When a new device is installed, you can check the IP group of the distribution destination group, and instruct the person responsible to assign an available IP address to the device. If more than one device is assigned to a single IP address, you can release the IP address of the invalidly assigned device, and assign a different IP address to that device. For details about how to release an IP address assigned to a device, see *4.4.4 Releasing the IP addresses assigned to devices* in the *Administrator's Guide*. For details about how to assign an IP address to a device, see *4.4.3 Assigning IP addresses to devices* in the *Administrator's Guide*.

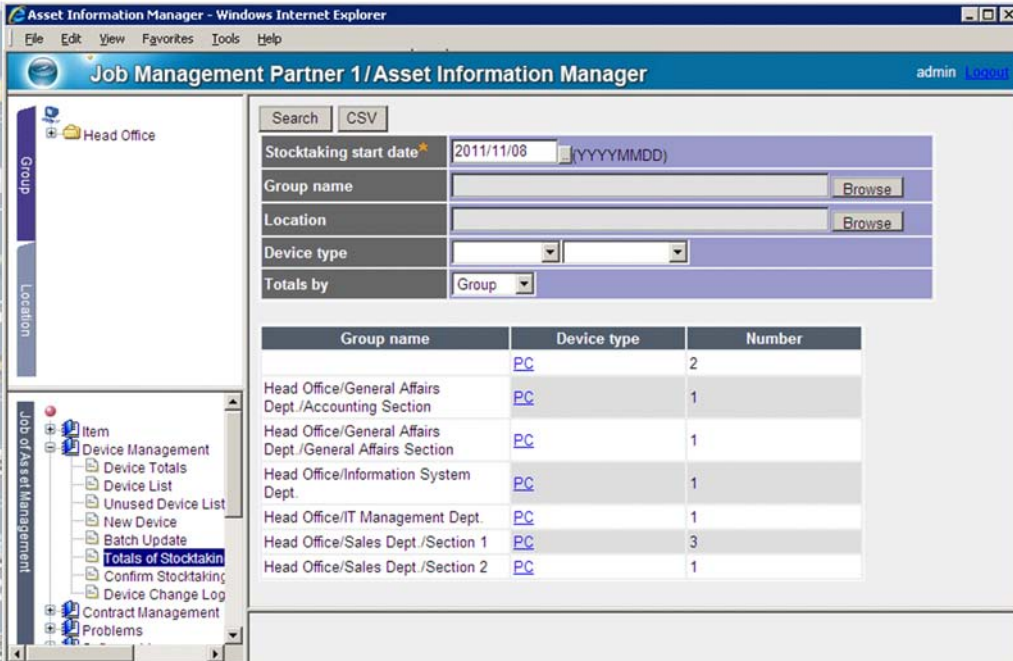
## 2.3 Stocktaking

You can search for devices for which stocktaking has not been completed by registering information about the devices for which stocktaking has been completed and the stocktaking date. This reduces the complexity of stocktaking jobs because you can check job progress and prevent items from being overlooked. If it exists, you can also use actual stocktaking data obtained using a device such as a bar-code reader to register such devices.

To search for devices for which stocktaking has not been completed, use the Totals of Stocktaking-Unexecuted Devices window. The number of devices for which stocktaking has not yet been completed from the stocktaking start date can be confirmed in the Totals of Stocktaking-Unexecuted Devices window.

The figure below shows the Totals of Stocktaking-Unexecuted Devices window.

Figure 2-8: Totals of Stocktaking-Unexecuted Devices window



The screenshot shows the 'Asset Information Manager' web application interface. The main content area is titled 'Job Management Partner 1/Asset Information Manager'. It features a search section with the following fields:

- Search: CSV
- Stocktaking start date\*: 2011/11/08 (YYYYMMDD)
- Group name: [Text input] Browse
- Location: [Text input] Browse
- Device type: [Dropdown menu]
- Totals by: Group

Below the search section is a table showing the results of the search:

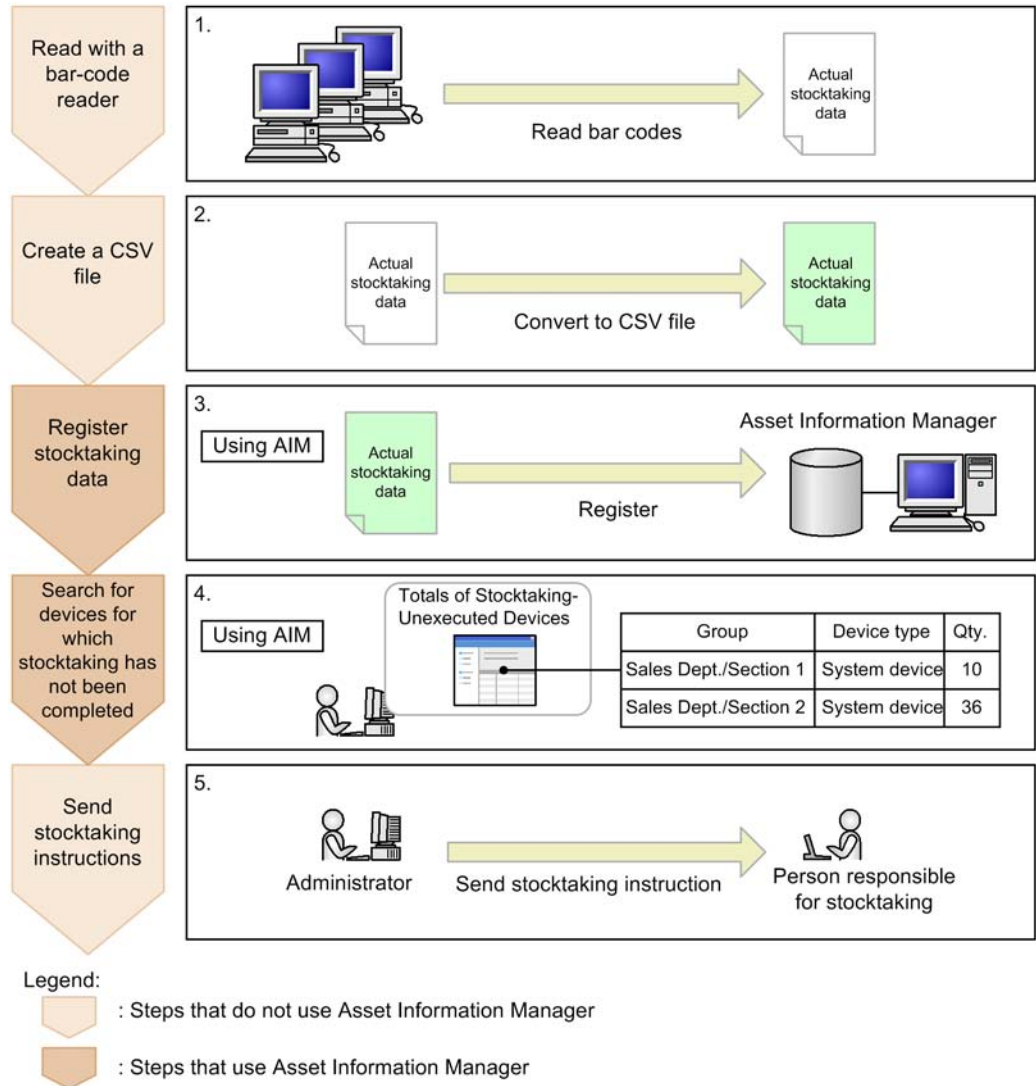
Group name	Device type	Number
	PC	2
Head Office/General Affairs Dept./Accounting Section	PC	1
Head Office/General Affairs Dept./General Affairs Section	PC	1
Head Office/Information System Dept.	PC	1
Head Office/IT Management Dept.	PC	1
Head Office/Sales Dept./Section 1	PC	3
Head Office/Sales Dept./Section 2	PC	1

The left sidebar shows a navigation menu with 'Totals of Stocktaking' highlighted. The top right corner shows the user 'admin' and a 'Logout' link.

You can easily register the actual stocktaking data into the asset management database by reading it with a bar-code reader or saving existing data in a ledger in CSV format.

The figure below shows by way of example the procedure for a stocktaking job when a bar-code reader is used.

Figure 2-9: Procedure for stocktaking job



To perform stocktaking:

1. Use a bar-code reader to read the asset number of each device.
2. Create a CSV file from the obtained data.

To manage the allocation of asset numbers for each device, specify the asset number and the stocktaking date in the CSV file that contains the actual stocktaking data. You can omit the stocktaking date, but make sure that the asset

number is specified.

For details about the format of the CSV file for actual stocktaking data, see *2.1.7 Registering actual stocktaking data (Confirm Stocktaking Device)* in the *Administrator's Guide*.

3. Register the CSV file containing the actual stocktaking data into the asset management database.

You can register the actual stocktaking data by specifying its file from a window. For details about registering the actual stocktaking data, see *2.1.7 Registering actual stocktaking data (Confirm Stocktaking Device)* in the *Administrator's Guide*.

4. In the Totals of Stocktaking-Unexecuted Devices window, search for devices for which stocktaking has not been performed.

Specify **Stocktaking start date** and **Totals by** to search for the devices for which stocktaking has not been performed. For **Totals by**, you can select **Group name** or **Location**.

For details about using the Totals of Stocktaking-Unexecuted Devices window, see *2.1.6 Checking the number of devices that require stocktaking (Totals of Stocktaking-Unexecuted Devices)* in the *Administrator's Guide*.

5. Instruct the user in charge of stocktaking to inventory the devices that were not counted.

The search results for missing devices is useful for issuing instructions because it is provided for each group or location, making it easy to identify groups or locations that have not been included in stocktaking.

You can also use the search results to view details about each device's users and group. You can also output the search results to a CSV file.

Repeat steps 1 to 5 of the stocktaking job until stocktaking is completed for all devices.

---

## 2.4 Determining whether licenses are handled legally

---

You can determine whether licenses are being handled legally by totaling usage in terms of whether the numbers of licenses being used have exceeded permitted values and whether licenses are being used by the correct users.

There are two ways to manage licenses. One is called *total count management*, and it is based on comparing the number of licenses held (called owned licenses) with the number of licenses actually in use. The other is called *per-license management*, and it assigns each license individually.

This section describes the job for managing licenses with each method.

### **(1) Checking the operation status by comparing the number of owned licenses to the number of used licenses**

You can perform basic license management, such as determining use of an excess number of licenses and use of unauthorized licenses, by managing the license totals based on information about the installed licenses on all devices.

To manage licenses, start from the job menus under **Software License**.

In the Owned License List window (opened by clicking the **Owned License List** job menu), you can obtain the license usage status at a glance, because this window displays a table comparing the number of owned licenses, the number of licenses being used, and the number of available licenses.

The figure below shows the Owned License List window.



Figure 2-10: Owned License List window

The screenshot shows the 'Owned License List' window in the Asset Information Manager. The window includes a search bar with a 'CSV' button, a 'Date of summary' dropdown set to '2009/07/06 17:53:01', and input fields for 'Software name', 'Software type', and 'Group name'. Below the search fields is a table listing software licenses.

Software name	Software type	License category	Owned	Used	Available
<a href="#">Adobe Acrobat Reader 7.0</a>	Commercial	-	40	1	39
<a href="#">Asset Information Manager</a>	Commercial	-	0	5	-5
<a href="#">Client Security Control - Manager</a>	Commercial	-	0	1	-1
<a href="#">HIRDB/ODBC Driver Version 7</a>	Commercial	-	0	2	-2
<a href="#">HIRDB/ODBC Driver Version 8</a>	Commercial	-	0	2	-2
<a href="#">InstallShield Professional Edition 12</a>	Commercial	-	10	2	8
<a href="#">Internet Explorer</a>	Commercial	-	0	3	-3
<a href="#">Internet Information Server</a>	Commercial	-	0	3	-3
<a href="#">Job Management Partner 1/Asset Information Manager</a>	Commercial	-	0	2	-2
<a href="#">Job Management Partner 1/Software Distribution Ass</a>	Commercial	-	0	1	-1
<a href="#">JP1/Software Distribution Client 07-50</a>	Commercial	-	-	0	-
<a href="#">JP1/Software Distribution Client 08-00</a>	Commercial	-	0	5	-5
<a href="#">JP1/Software Distribution Client 08-00</a>	Commercial	Install license	10	3	7
<a href="#">Microsoft .NET Framework 2.0 Service Pack 1</a>	Commercial	-	0	1	-1
<a href="#">Microsoft .NET Framework 3.0</a>	Commercial	-	0	1	-1

You can use this comparison table to purchase licenses when no more are available or to search for groups with too many licenses for transfer to groups with too few licenses.

You can use the following job menus to identify inappropriate license usage:

- **Excess License List**

Allows you to check if any licenses are being used that exceed the number that has been set for owned licenses.

- **Unauthorized Usage List**

Allows you to check if any expired licenses are being used, or whether licenses that have not been obtained are being used.

- **Unknown Usage List**

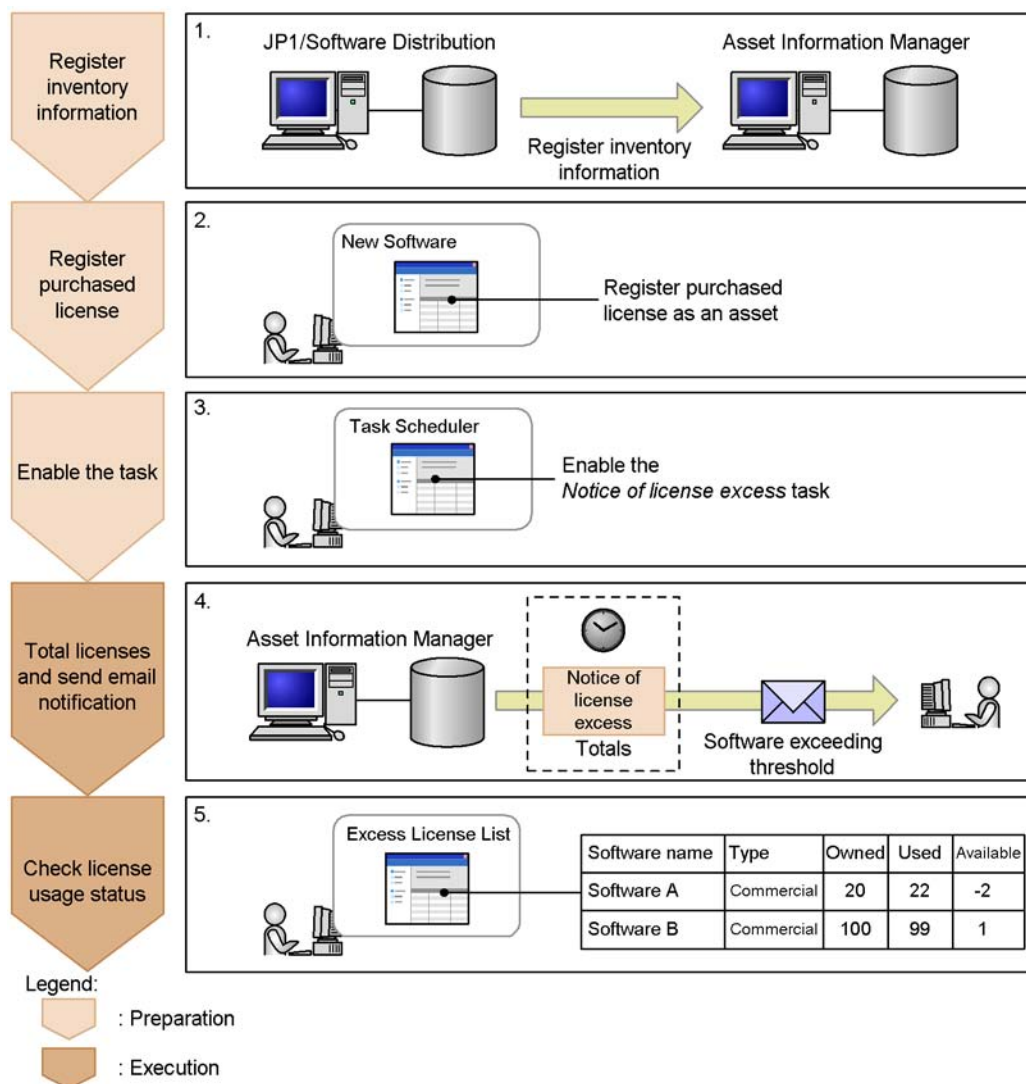
Allows you to check if software programs with unregistered software names are being used.

*Hint:*

You can set up the system to notify the asset manager by email if an excess license is detected. This means you can prevent excess licenses from being overlooked, thereby reducing the asset manager's workload. Events that trigger asset manager email notification can be monitored by registering a task to the Windows Task Scheduler to check for excess licenses. For details about how to set tasks, see *5.9 Setting the tasks that are registered in Task Scheduler* in the *Planning and Setup Guide*.

The figure below shows the procedure for checking license status.

Figure 2-11: Procedure for checking license status



To check the license status:

1. Register inventory information into the asset management database.

To check license usage status, you need two types of information:

- Information about devices
- Information about the software programs installed on the devices

You can use the inventory information acquired by JP1/Software Distribution to register information about devices and about software programs installed on the devices. For details about registering inventory information, see *5.1.1 Workflow necessary for linking to JP1/Software Distribution* in the *Planning and Setup Guide*.

To efficiently manage licenses, we recommend that you configure the system to automatically assign the installed software name to a software name when you collect inventory information. For details about how to automatically assign the installed software name to a software name, see *3.2.4 Setting the software name assignment method* in the *Planning and Setup Guide*. If the assignments are not performed automatically, you must use the **Software Name** job menu to assign names one at a time.

2. Register purchased license information.

In this step, register the purchased license. For details about how to register licenses, see *2.4.6 Adding a license (New Software)* in the *Administrator's Guide*.

3. In Task Scheduler enable the **Notice of license excess** task.
4. The task totals the license usage statuses and reports excess licenses.

The task registered in Task Scheduler is executed at the specified date and time and totals the licenses. If any software exceeds a usage threshold (the default threshold is 100%), the task sends an email to the asset manager reporting that excess licenses are in use.

You can also total the licenses from the window that is displayed by selecting **Totals List & Execution** from the job menu. For details about how to total licenses using window operations, see *2.4.11 Totaling licenses (Totals List & Execution)* in the *Administrator's Guide*.

5. Check license usage status.

In the window that is displayed by selecting **Excess License List** from the job menu, check for licenses that have been installed in excess of the number owned.

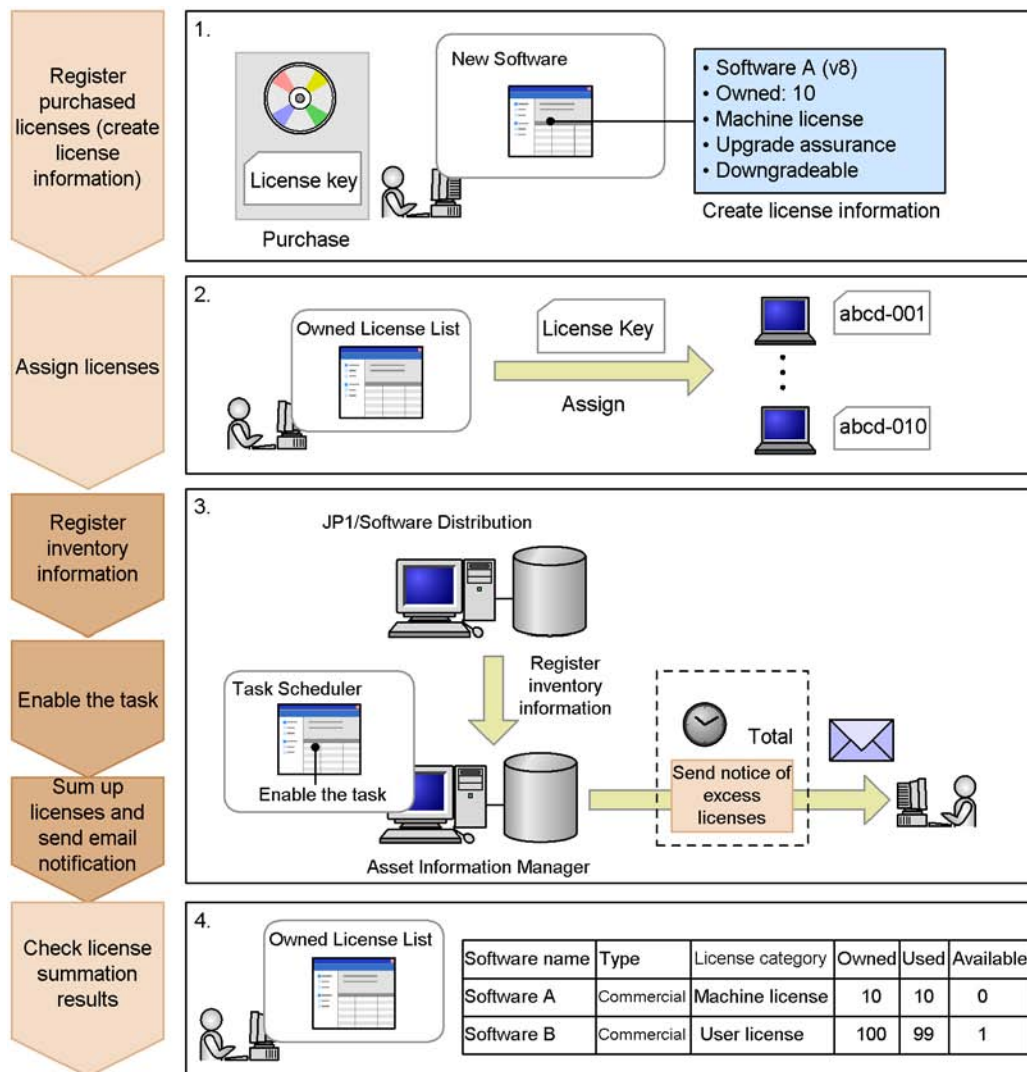
You can also download the totals using a CSV file. For details about checking the excess licenses, see *2.4.2 Checking for exceeded licenses (Excess License List)* in the *Administrator's Guide*.

## **(2) Accurately managing targets according to the assigned licenses**


You can accurately manage license usage status by creating license information according to license types and options and assigning licenses to specific targets.


The figure below shows the procedure for managing licenses by assigning them, which is an alternative to the procedure for total count management described in (1) above.

Figure 2-12: Procedure for managing licenses by assignment



Legend:

 : Steps required for management by assignment

 : Steps that duplicate management by total tasks

To manage licenses by assigning them:

1. Create and register license information when you purchase licenses.  
Create the license information according to the license type and option settings.

For example, for an Install license, register information such as upgrade assurance and compatibility with downgrade software.

For details about how to register license information, see 2.4.6 *Adding a license (New Software)* in the *Administrator's Guide*.

2. Assign the licenses to the targets.

Assign the licenses to devices or users according to the license category.

To assign a license, establish correspondence between the key information such as product ID and the targets. For details about assigning licenses, see 2.4.7(2) *Assigning licenses* in the *Administrator's Guide*.

3. Execute the same steps as for total count management.

Install the software program on the devices to which licenses have been assigned and then execute the steps common to total count management (register inventory information, establish correspondence between software names, set up the task, and total the licenses).

4. Check to see if the licenses are handled correctly.

Under **Software License**, you can use the following job menus to check the registered license information:

- **Owned License List**

This menu lets you check the total for each license category.

- **Excess License List**

This menu lets you check for any licenses being used that exceed the threshold set by the license category for owned licenses. If illegal use of a license is detected, you can identify the user or device immediately.

To accurately manage licenses, it is important to create license information according to the license type and options and select an assignment method that is appropriate for your operating procedures. Also, all types of information that can be managed as license information must have been prepared, and the total number owned is executed on the basis of the *license category*.

The following presents examples of license management that are suggested for license management using Asset Information Manager:

**(a) Example of managing Install licenses**

You can manage licenses assigned to devices as follows:

- Create license information as Install license.

To assign a license to a device, specify **Install license** for **License category**. Also specify other settings appropriate to the license, such as downgrade and upgrade

assurance.

- Register the key information, such as the product ID of the purchased licenses, and assign one license to each device.

This allows you to check whether use of the license is permitted for any particular device.

### (b) Example of managing User licenses

You can manage licenses assigned to users as follows:

- Create license information as User license.

To assign a license to a user, specify **User license** for **License category**. Also specify other settings appropriate to the license, such as downgrade and upgrade assurance.

- Register the key information, such as the product ID of the purchased license, and assign one license to each user.

This allows you to total licenses correctly, even when the same user uses a license on multiple devices.

To manage a license by assigning it to a user, the user must be registered in the applicable device. Additionally, this user must also be registered as an Asset Information Manager user.

### (c) Example of managing pre-installed licenses

You can manage pre-installed software licenses as follows:

- Create license information as Install license.

Specify **Install license** for **License category**. Use **Licensing method** to specify that this is a pre-installed license.

- Disable the Downgrade property because normal pre-installed software programs are not downgradable.

This enables you to determine whether the correct version has been installed.

- For the number of owned licenses, specify unlimited licenses.

You can register a license by owning a single license per device; however, by specifying unlimited licenses, you can manage software programs more efficiently because any additional pre-installed licenses for the same software program can be assigned later, simply by adding its key information.

- Assign a license to a single device by registering the key information such as product ID.

As a result, you can determine whether the pre-installed software program is being used on the assigned device.

### (d) Example of managing server licenses

You can manage the license of a server product as follows:

- Create license information as Install license.

To assign a license to a device, specify **Install license** for **License category**. Also specify other settings appropriate to the license, such as downgrade and upgrade assurance.

A server license is accompanied by other licenses, such as Client access, Managed node, and CPU licenses. The following describes a management example for each license:

#### Client access license

This license is given according to the number of licenses (users) that access the server. Select one of the following management methods:

##### Managing accessible clients as the number of owned licenses

Register a single license separately from the server license and create client access license information. For example, register a client license with 100 accesses permitted as a software asset with 100 licenses owned. For **License type**, specify **Client access license**.

This allows you to total the number of accesses permitted as the number of owned licenses.

Note that information such as the number of used licenses is not totaled because there is no device-related information.

##### Managing as the additional information for the server license

As a simple method, register the number of accesses as remarks without registering the client access license as a license. You need to calculate the number of owned licenses manually.

#### Managed node license

This license is given according to the number of clients managed by the server. Select one of the following management methods:

##### Managing the number of clients managed by the server as the number of owned licenses

Register a single license separately from the server license and create managed node license information. For example, register a managed node license that permits 100 managed nodes as 100 owned licenses. For **License type**, specify **Managed node license**.

This allows you to total the number of managed nodes permitted as the number of owned licenses.



Note that information such as the number of used licenses is not totaled because there is no device-related information.

#### Managing as the additional information for the server license

As a simple method, register the number of managed nodes as additional information associated with the server license, without registering the managed node license as a license. In this case you need to calculate the number of owned licenses manually.

#### CPU license

This license is given according to the number of CPUs. Create license information as CPU license, not as server license.

### (e) Example of managing second licenses

This section presents an example of managing licenses when installation on a second device is permitted. Select one of the following management methods:

#### Managing as User license

Create license information as User license (specify **User license** for **License category**).

The license is managed assuming that installation on a second device that is used by the same user is permitted. However, the system cannot detect exceeded licenses even if the applicable software program is installed on more than two devices.

#### Managing the license by adding second license information

Register a license separately from the server license and create second license information. In this case, remarks about its correspondence with the original license would be useful.

### (f) Example of concurrent execution license

This section presents an example of managing concurrent execution licenses. Select one of the following managing methods:

#### Managing the number of concurrently executable licenses as the number of owned licenses

Register a single license separately from the server license, and create concurrent execution license information.

For example, register a concurrent execution license that permits 100 concurrent executions as 100 owned licenses. For **License type**, specify **Concurrent execution license**.

This allows you to total the number of concurrent executions permitted by the license as the number of owned licenses.

Note that information such as the number of used licenses is not totaled because there is no device-related information.

#### Managing as the additional information for the server license

As a simple method, register the number of executions as additional information associated with the server license without registering the concurrent execution license as a license. In this case, you need to calculate the number of owned licenses manually.

#### Managing by assigning to devices

- Register the license using the permitted number of concurrent executions as the number of owned licenses.
- Create the license information as concurrent execution license, not as server license.
- Register the key information, such as the product ID of the purchased licenses, and assign one license to each device.

You can limit the number of concurrent executions by permitting as many installations as there are permitted concurrent executions.

## 2.5 Applying updates by linking to a WSUS server

You can apply patches and other updates to the entire system by linking to a WSUS server.

With Asset Information Manager, you can configure your system so that email notification is sent when a new update is released to the WSUS server, thereby saving you the trouble of having to check for new updates. You can also specify any time or interval, allowing you to synchronize the WSUS server with Microsoft Update.

We recommend that you first examine the update on test PCs for a set period of time to make sure no system or device problems occur. Create the test PCs with the WSUS server as a computer group, and use the WSUS Automatic Approval function to automatically apply updates to the test PC computer group.

The WSUS Updates Management window can be used to link to the WSUS server and apply updates.

The figure below shows the WSUS Updates Management window.

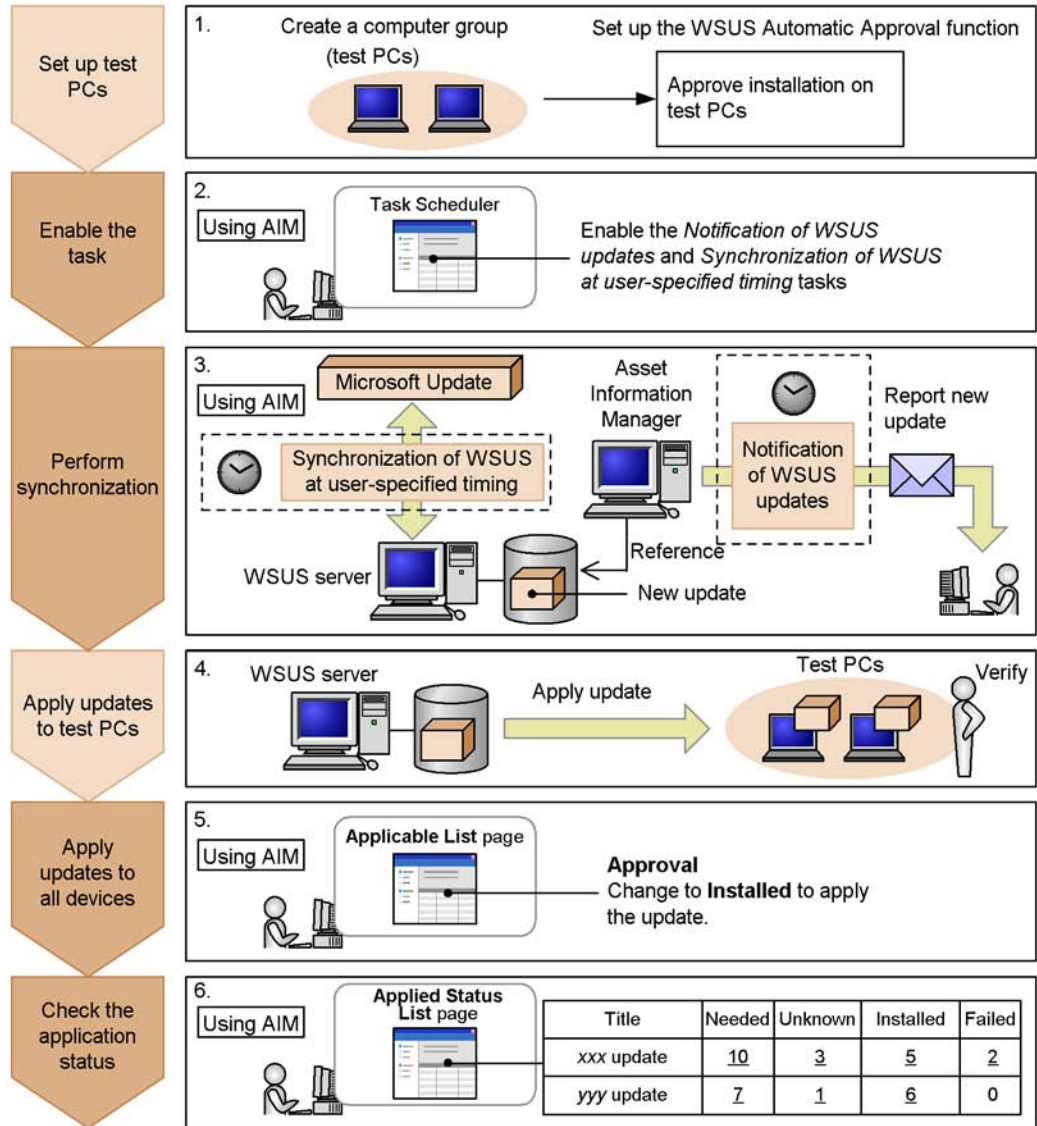
Figure 2-13: WSUS Updates Management window

The screenshot displays the WSUS Updates Management window within the Asset Information Manager interface. The window is titled 'Job Management Partner 1 / Asset Information Manager' and shows a list of updates. The 'Approval' column is highlighted, indicating the current status of each update.

Released	Title	Products	Classification	Approval
2006/08/08	<a href="#">Cumulative Security Update for Internet Explorer 6 Service Pack 1 (KB918899)</a>	Windows 2000, Windows XP	Security Updates	Not approved
2006/08/22	<a href="#">Cumulative Security Update for Internet Explorer 6 Service Pack 1 (KB918899)</a>	Windows 2000, Windows XP	Security Updates	Detect only
2006/08/22	<a href="#">Korean Fair Trade Commission Promotional Links</a>	Windows XP	Critical Updates	Detect only
2006/09/12	<a href="#">Security Update for Windows 2000 (KB917537)</a>	Windows 2000	Security Updates	Detect only
2006/09/12	<a href="#">Update for Windows Server 2003 (KB922582)</a>	Windows Server 2003, Datacenter Edition, Windows Server 2003	Critical Updates	Detect only
2006/09/12	<a href="#">Update for Windows Server 2003 for Itanium-based Systems (KB922582)</a>	Windows Server 2003, Datacenter Edition, Windows Server 2003	Critical Updates	Detect only
2006/09/12	<a href="#">Update for Windows Server 2003 x64 Edition (KB922582)</a>	Windows Server 2003, Datacenter Edition, Windows Server 2003	Critical Updates	Detect only
2006/09/12	<a href="#">Update for Windows XP (KB922582)</a>	Windows XP	Critical Updates	Detect only
2006/09/12	<a href="#">Update for Windows XP x64 Edition (KB922582)</a>	Windows XP x64 Edition	Critical Updates	Detect only
2006/09/12	<a href="#">Update for Windows XP (KB916595)</a>	Windows XP	Critical Updates	Not approved
2006/09/12	<a href="#">Security Update for Windows Server 2003 (KB921883)</a>	Windows Server 2003, Datacenter Edition, Windows Server 2003	Security Updates	Detect only
2006/09/12	<a href="#">Security Update for Windows Server 2003 for</a>	Windows Server 2003, Datacenter	Security Updates	Detect only

The following figure illustrates the workflow required to verify and apply new updates.

Figure 2-14: Workflow for verifying and applying new updates



Legend:

- : Steps that do not use Asset Information Manager
- : Steps that use Asset Information Manager

To verify and apply new updates:

1. Using functions provided by WSUS, create a computer group, and configure the Automatic Approval function.

Perform the two operations described below before you try to use Asset Information Manager to view the approval status of the updates.

- Create a computer group

Create in advance a computer group consisting of test PCs for verifying updates. For details about creating a computer group, see the Microsoft WSUS documentation.

- Configure the WSUS Automatic Approval function

Use the WSUS Automatic Approval function to configure installation approval for the test PCs' computer group. By performing this setup, when updates arrive on the WSUS server, the server automatically changes the approval status of the updates to **Installed**, and applies the updates to the test PCs.

For details about the Automatic Approval function, see the Microsoft WSUS documentation.

2. In the Task Scheduler, enable the *Notification of WSUS updates* and *Synchronization of WSUS at user-specified timing* tasks.

When you use a *Synchronization of WSUS at user-specified timing* task, manually set the WSUS server synchronization. Also configure **Products and Classifications** and **Proxy Server** settings to suit your intended use.

3. Execute the *Synchronization of WSUS at user-specified timing* task to synchronize the WSUS server with Microsoft Update.

The *Synchronization of WSUS at user-specified timing* task, registered in Task Scheduler, automatically executes and performs synchronization at the specified date and time. If, as a result of this synchronization, new updates were downloaded to the WSUS server, an email is automatically sent by the *Notification of WSUS updates* task, notifying the asset manager that updates have been downloaded. To ensure that email notification of downloaded updates is provided, set the date and time so that the *Notification of WSUS updates* task is executed after that of the *Synchronization of WSUS at user-specified timing* task.

4. Apply the new updates to the test PCs.

The updates are automatically applied to the test PCs according to the settings configured for the WSUS Automatic Approval function. Verify the updates on the test PCs for a set period of time to help ensure that no problems occur when the updates are applied to the entire system.

5. Apply the updates to all devices in the system.

In the WSUS Updates Management window, use the **Applicable List** tab or the **Not Applied List** tab to check the devices on which the updates will be applied. Then, change the approval status for the update to **Installed** to apply the update to all devices that require it. For details about how to use the **Applicable List** tab to check applicable devices, see 2.5.3(3) *Checking devices that require updates application (Applicable List tab)* in the *Administrator's Guide*. For details about how to use the **Not Applied List** tab to check for devices among those requiring the patch to which it has not been applied, see 2.5.3(4) *Checking devices on which updates have not been applied (Not Applied List tab)* in the *Administrator's Guide*.

6. Check the application status of the updates.

If the **Not Applied List** tab of the WSUS Updates Management window does not list any devices to which the updates have not been applied, the updates were applied successfully. If there is a device to which the updates were not applied, you can use the **Applied Status List** tab to check the number of devices for which the updates failed and other application status details. For details about how to use the **Not Applied List** tab to check the device application status, see 2.5.3(4) *Checking devices on which updates have not been applied (Not Applied List tab)* in the *Administrator's Guide*. To use the **Applied Status List** tab to check update application status details, see 2.5.3(5) *Checking the application status of updates (Applied Status List tab)* in the *Administrator's Guide*.

If needed, repeat steps 5 and 6 until you have applied the updates to all devices that need them.

---

## 2.6 Adding asset information statuses, managed items, and windows

---

As an addition to the window operations provided by Asset Information Manager, you might want to modify the system environment to better suit specific jobs, such as to perform more in-depth management of device and contract status or to add management items. In this case, you can easily use window operations to add statuses and managed items.

You can also create a window for searching your assets on the basis of the added statuses or managed items as key values and then add asset management jobs that can be executed from Asset Information Manager.

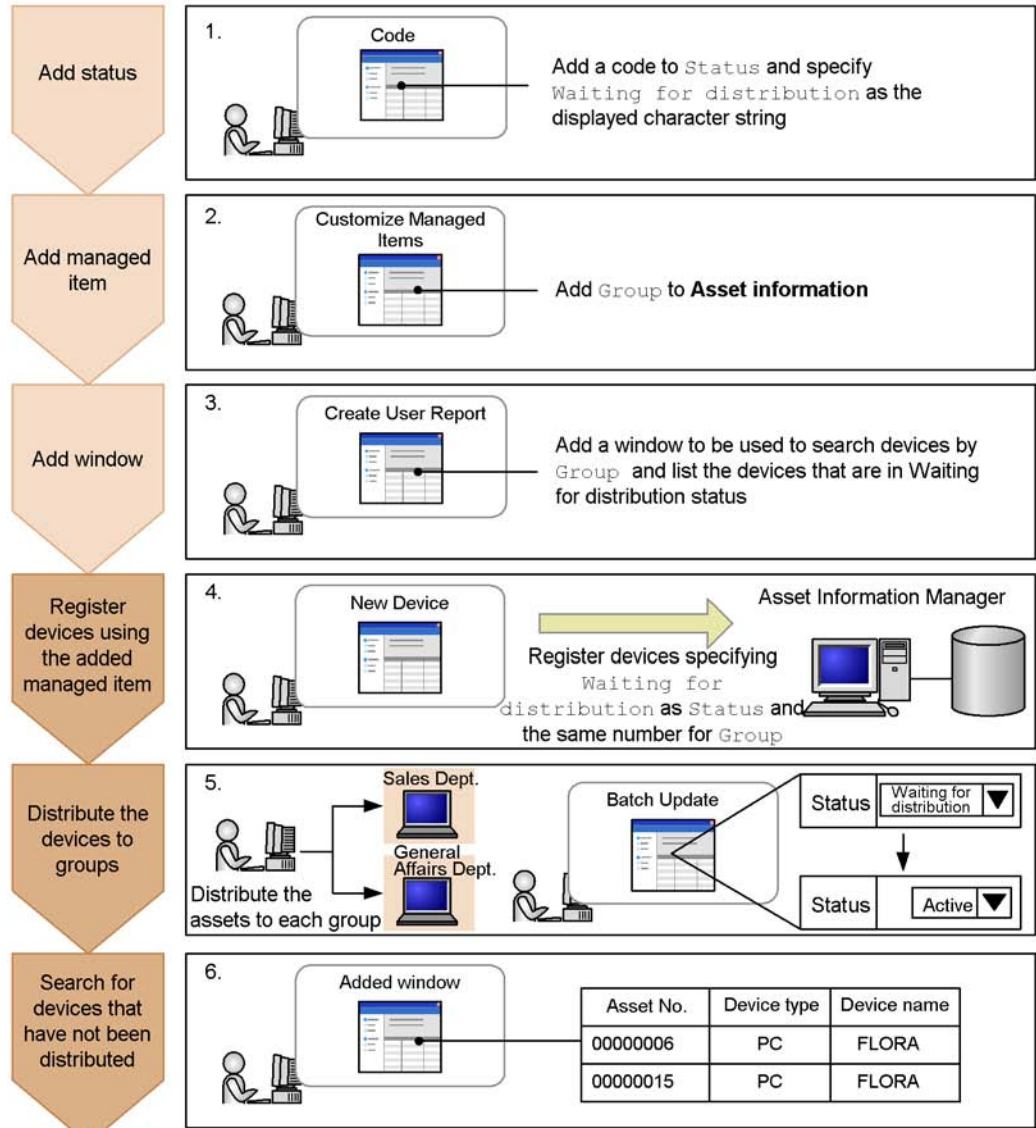
For example, you can add a job that groups devices by installation period and then manages the distribution status of the devices in groups. To do this, the following preparations are needed:

- Adding the status *Waiting for distribution* indicating that distribution has not been made to the device.
- Adding the managed item *Group* to manage the devices installed in the same period as a group.
- Adding a window for searching for devices by group to which distribution has not been made since installation

You can easily do all this from the windows that are displayed by selecting the job menus under the **System Management** and **System Definition** job categories.

The figure below shows the procedure for preparing and executing the job for checking the distribution status.

Figure 2-15: Procedure for checking the distribution status of devices by group



Legend:  
 : Preparation needed to manage devices by group  
 : Task for running devices by group

To prepare and execute the job for checking the distribution status:



1. In the Code window, add the status.

Add the status `Waiting for distribution` indicating that the device has not been distributed to a group after installation.

The status is associated with the code and managed by the asset management database. Therefore, to add the status `Waiting for distribution` to devices, add the corresponding code to **Status**.

For details about the operation in the Code window, see *4.8 Adding and changing types and statuses (Code)* in the *Administrator's Guide*.
2. In the Customize Managed Items window, add a managed item.

To manage the devices installed in the same period as a group, add `Group` to the managed items of **Asset information**.

The added managed item takes effect in the entire asset management system.

For details about the operation in the Customize Managed Items window, see *9.2 Changing managed items (Customize Managed Items)* in the *Planning and Setup Guide*.
3. In the Create User Report window, add a window.

Add a window for checking for any device that was installed in the same period, but has not been distributed. In the window, search for devices using **Group** as the condition and list only those devices whose status is `Waiting for distribution` as the result.

You can display the added window from the menu that is added to the job menu. You can also change the window's view setting (view or hide) from the Customize Job Menu window.

For details about the operation in the Create User Report window, see *9.5 Adding windows for routine jobs (Create User Report)* in the *Planning and Setup Guide*; for details about the operation in the Customize Job Menu window, see *9.4 Changing the executable jobs (Customize Job Menu)* in the *Planning and Setup Guide*.
4. In the New Device window, register new devices.

Register newly installed devices. When registering the devices, specify `Waiting for distribution` as **Status**. To manage the devices installed in the same period as one group, register the same number in **Group**. If the device installation date is included in the number, device management by group is facilitated.

For details about the operation in the New Device window, see *2.1.4 Registering device information (New Device)* in the *Administrator's Guide*.
5. Distribute the newly installed devices to groups.

## 2. Typical Usage

After distributing the devices, the system administrator must use the Batch Update window to change the status of the distributed devices from `Waiting for distribution` to `Active`.

For details about the operation in the Batch Update window, see *2.1.5 Changing device information (Batch Update)* in the *Administrator's Guide*.

6. Use the added window to search for any devices that have not been distributed.

By executing a search with **Group** specified as the search condition, you can display a list of devices in the specified group that have not been distributed. You can then distribute those devices on the basis of this list.

---

## 2.7 Limiting available functions by user roles

---

Asset Information Manager's asset management system enables corporate assets information to be widely shared among users, from general users to the staff in charge of the asset management jobs. However, the asset management system might contain some information that should not be shared or manipulated by general users.

If the usage of Asset Information Manager depends on the nature of user jobs, available information and functions can be limited by means of user roles.

For example, you can set the following limitations for general users:

- Prohibit updating of information about software programs installed on devices.
- Prohibit execution of **Transfer License** jobs.

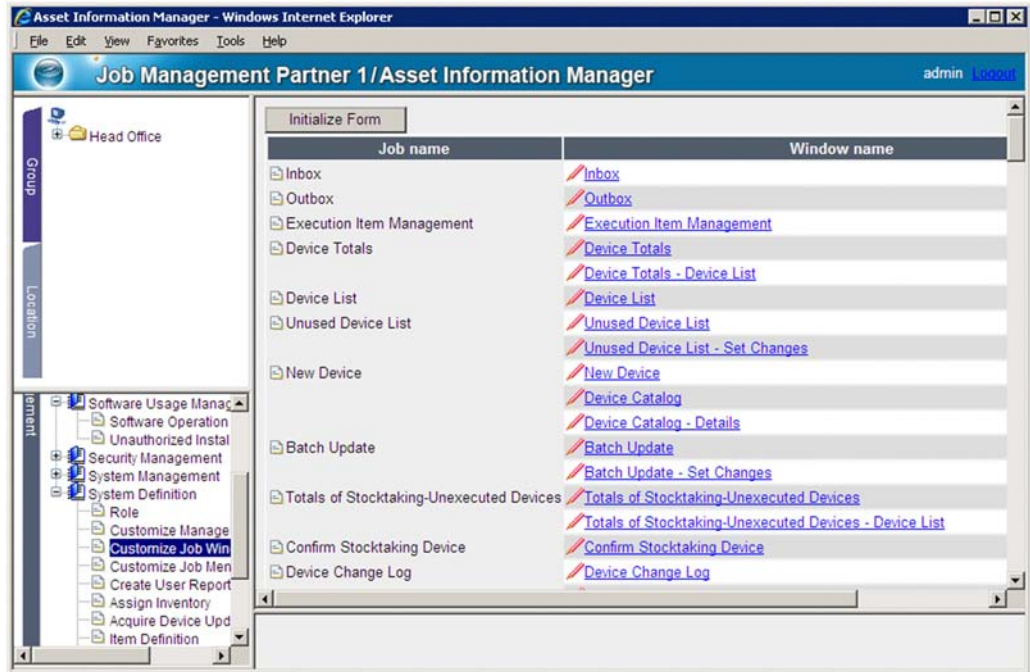
This section describes the procedures executed by the asset manager to set limitations on the operations available to general users.

### ***(1) Prohibiting updating of information about software programs installed on devices***

To strictly control the installation of unauthorized software, set up the system in such a manner that no user other than an administrator can update information about installed software. To limit the functions of a specific window, use the Customize Job Windows window.

The figure below shows the Customize Job Windows window.

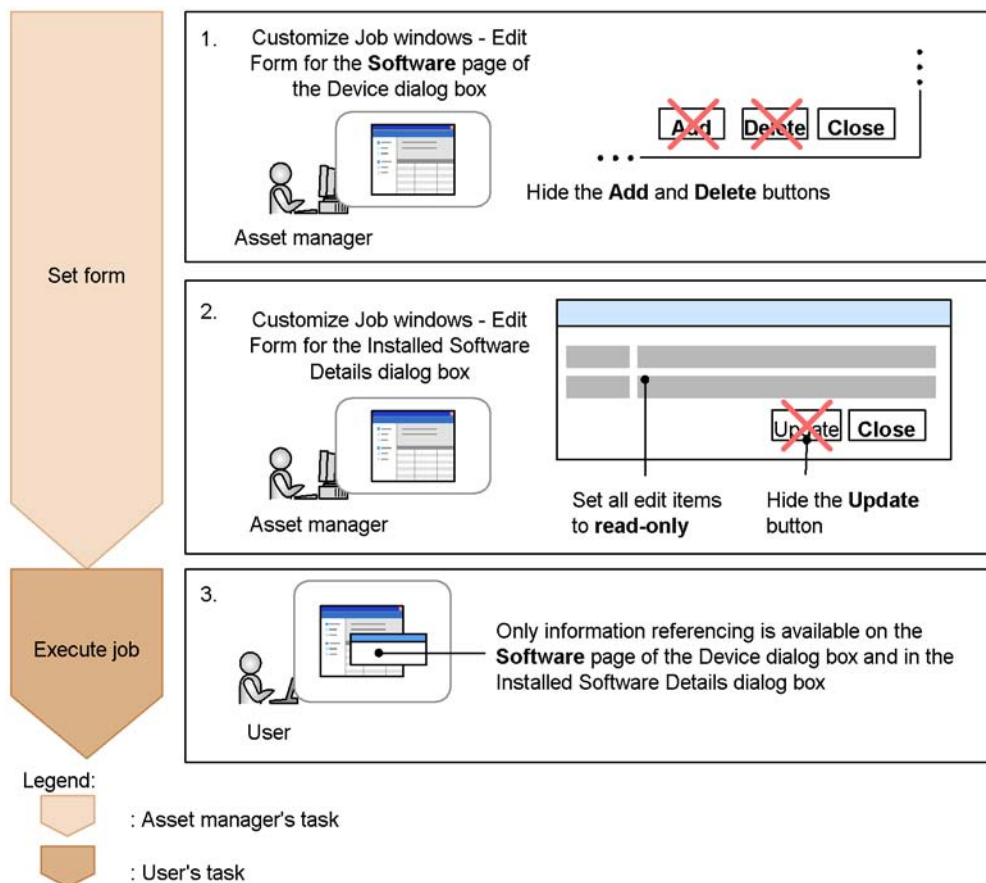
Figure 2-16: Customize Job Windows window



This window lists all Asset Information Manager windows by job. Clicking the link for a desired window displays the window for changing the settings for that window (Customize Job Windows - Edit Form). The window settings are called a *form*.

The following figure shows the procedure for limiting the functions of a specific window.

Figure 2-17: Procedure for limiting the functions of a window for a user role



To limit the functions of a specific window:

1. In the Customize Job Windows - Edit Form in the **Software** tab of the Device Details dialog box, set the form.

In the Customize Job Windows window, select **Device - Software** from the list of window names, and then in the displayed Customize Job Windows - Edit Form, specify the following settings:

- **Object role:** Apply to **User**.
- **Button:** Hide **Add** and **Delete**.

For details about the operation in the Customize Job Windows window, see 9.3 *Changing a window for a user role (Customize Job Windows)* in the *Planning and Setup Guide*.

## 2. Typical Usage

2. In the Customize Job Windows - Edit Form for the Installed Software Details dialog box, set the form.

In the Customize Job Windows window, select **Device - Software - Installed Software Details** from the list of window names. Click the link to display the Customize Job Windows - Edit Form and then specify the following settings:

- **Object role:** Apply User.
  - **Button:** Hide Update.
  - **Editable items:** Set all items to **read-only**.
3. Log in to Asset Information Manager and execute a job.  
For a general user, the displayed **Software** tab of the Device Details dialog box and the Installed Software Details dialog box allow only information referencing.

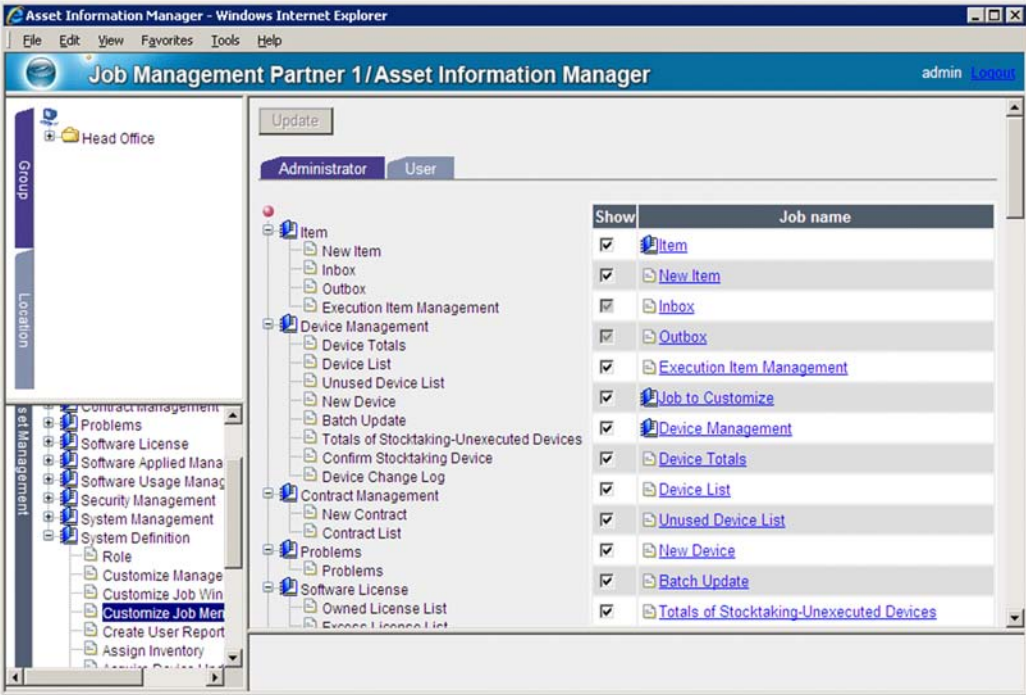
Note that steps 1 and 2 can be reversed.

### ***(2) Prohibiting execution of a Transfer License job***

If the asset manager is to use a batch operation to transfer licenses, you must hide the job menu itself from general users. To hide a specific job menu, use the Customize Job Menu window.

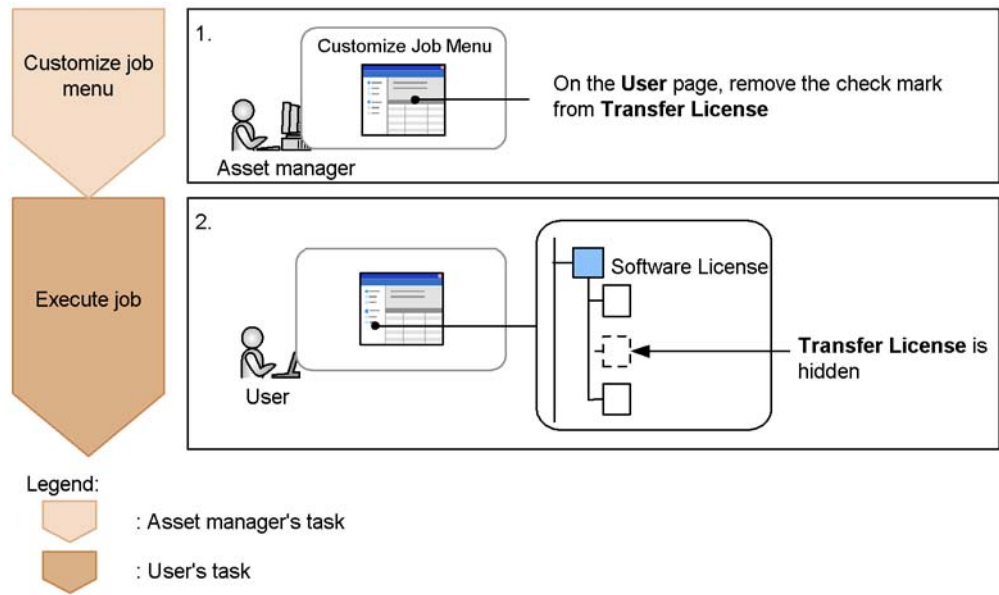
The figure below shows the Customize Job Menu window.

Figure 2-18: Customize Job Menu window



In the tab for each user role, specify the view setting (view/hide) for a job menu. The figure below shows the procedure for hiding a specific job menu.

Figure 2-19: Procedure for hiding a job menu according to the user role



1. In the Customize Job Menu window, change the job assignment.  
Choose the **Customize Job Menu** job menu and then in the displayed window, remove **Transfer License** from the jobs that are available to general users.  
For details about the operation in the Customize Job Menu window, see 9.4 *Changing the executable jobs (Customize Job Menu)* in the *Planning and Setup Guide*.
2. Log in to Asset Information Manager and execute a job.  
For a general user, the **Transfer License** job menu is no longer displayed.



## 2.8 Solving problems using Items

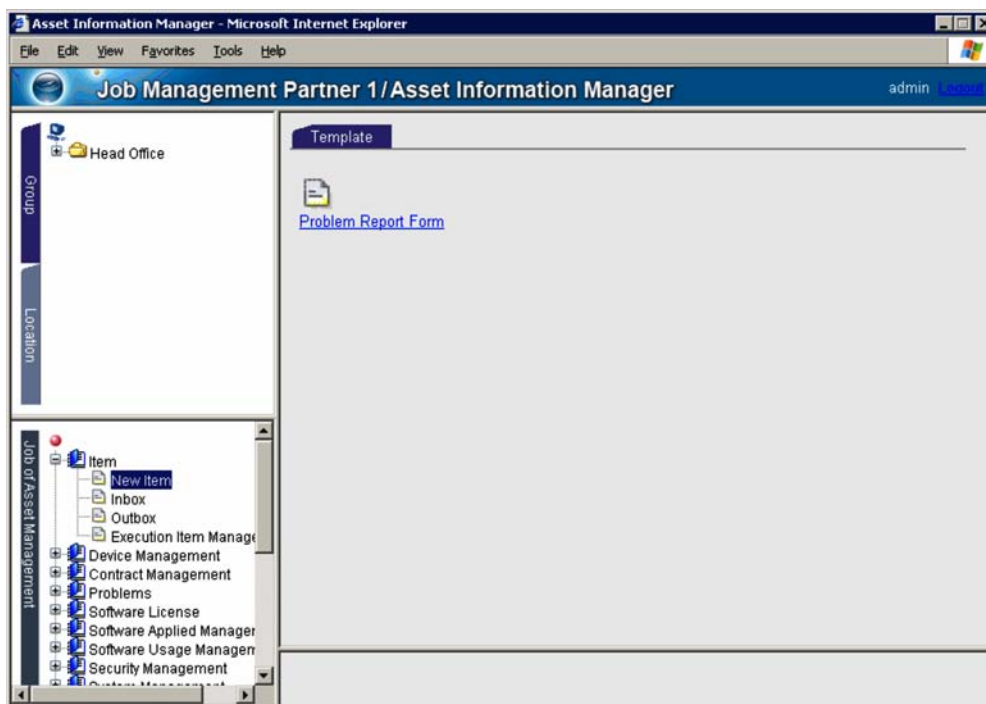
If any type of problem occurs in a device used by the system, it is necessary in order to solve the problem to distribute information about the problem to pre-designated individuals within the organization who are responsible for receiving and solving problems.

Normally, problem information is conveyed in a document or by email, but this makes it difficult to keep track of the processing progress. By using Items, an overview of the problem can be easily determined and the processing status can be tracked.

Items are selected and created from the New Item window. In the New Item window, the Items that can be used are displayed by tab according to category.

The figure below shows the New Item window.

Figure 2-20: New Item window

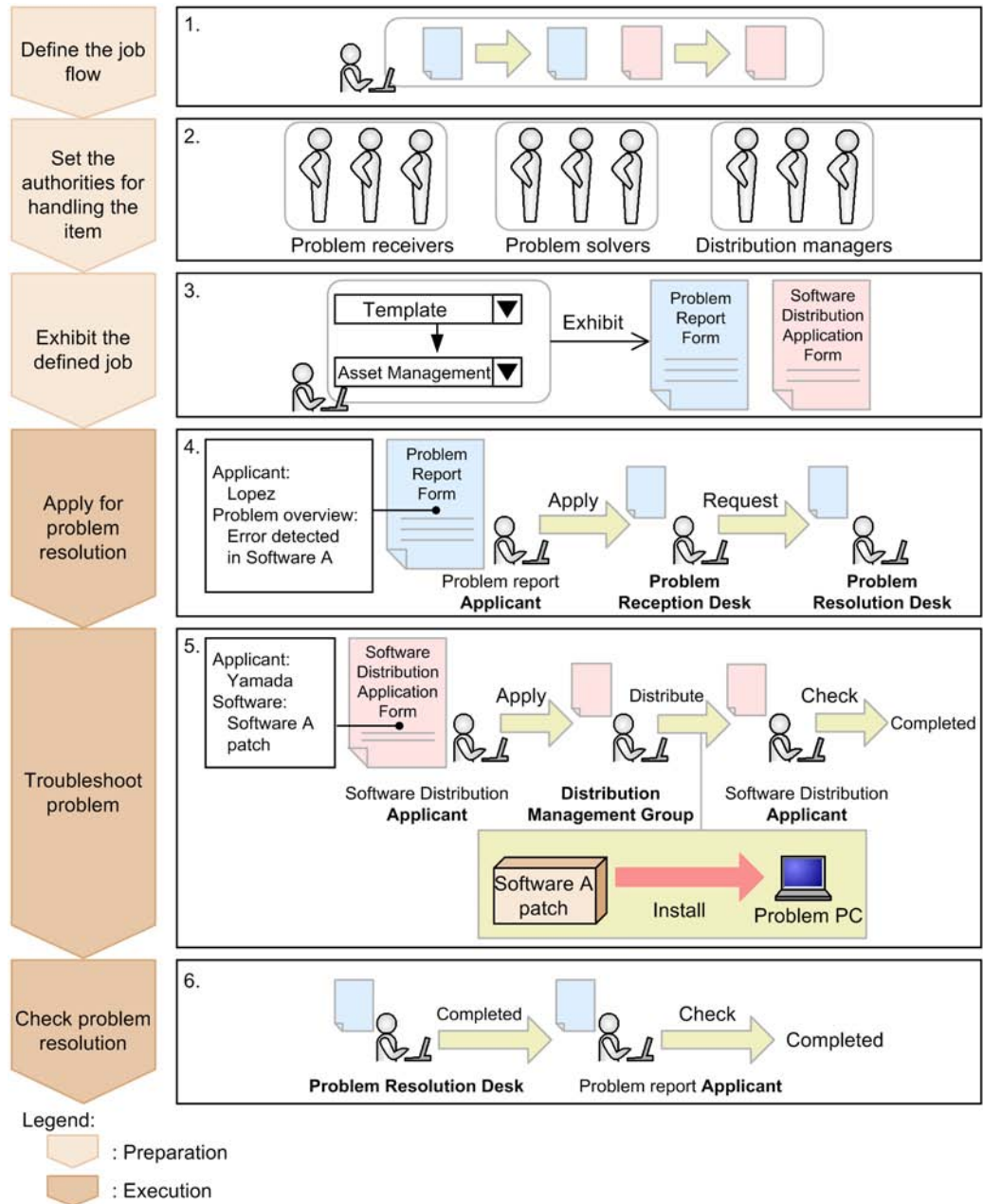


Asset Information Manager provides a *Problem Report Form* as a sample Item. The problem report form assumes a problem with software; it is set up so that during the flow of the Item a software upgrade distribution Item can be generated.

The figure below shows the flow when the problem report form Item is used, from

notification of the party responsible for problems with the particular asset to the request for a solution and its processing.

Figure 2-21: Flow of a problem resolution job using Items



To resolve a problem using an item:

1. Define the job flow

When a problem occurs, define the types of information, the path over which that information will be routed, and whether to perform troubleshooting. If you use the sample Item provided without any change, you can skip this step.

Use the Item Definition window to define a workflow that uses an Item. For details about how to define an Item, see *10.1 Overview of Item definition* in the *Planning and Setup Guide*.

2. Use the Official Authority window to assign authorities to the users who will handle the Item.

For **Problem Report Form** and **Software Distribution Application Form** Items, define problem receivers, problem solvers, and distribution managers with the authority required to process the Item.

The authorities needed for the Item provided in the sample are already defined, so simply assign the authorities to users who have sufficient permissions to perform the processing involved. For details on how to define users with authorities, see *10.2 Defining authority for processing the Item (Official Authority)* in the *Planning and Setup Guide*.

3. Exhibit the Item in the **Problem Report Form** and the **Software Distribution Application Form**.

Because the status of the sample Item is registered as **Creating**, the status must be changed to **Exhibit**. For details on how to exhibit Items, see *10.7.2 Setting an Item to Exhibit or Not exhibit* in the *Planning and Setup Guide*.

*Reference note:*

In the New Item window, Items are displayed in tabs on the basis of the *Item category*. Initially, the **Template** tab is provided. Depending on the type or the contents of the work, change the name of this tab or add new tabs. For details on how to add or change Item categories, see *4.8.1 Adding codes* in the *Administrator's Guide*.

To display the Item in the Item category that was added, change the Item category before you exhibit the Item. For details about how to change Item categories, see *10.3.2 Placing workers and processing* in the *Planning and Setup Guide*.

4. Create a problem report form and request a problem resolution.

From the New Item window, create a problem report form Item and submit an application. The sent Item is placed in the next worker's inbox.

The person responsible for receiving the problem opens the problem report form in the inbox, checks the overview of the application, and requests a solution from the person responsible for solving the problem.

For details on how to create Items and how to process received Items, see 3. *Executing Asset Management Jobs That Use Items* in the *Administrator's Guide*.

5. Distribute the software used to solve the problem.

- Application for software distribution

If the person responsible for solving the problem determines that software must be installed to solve the problem, that person creates a **Software Distribution Application Form** Item to apply for installation of the required software. With the **Software Distribution Application Form** Item, that person can link to JP1/Software Distribution and have the software distributed (installed). Furthermore, this **Software Distribution Application Form** Item can be displayed and created from the **Problem Report Form** Item window.

- Software distribution

The person responsible for distribution management specifies the package in the **Software Distribution Application Form** Item, and the requested software is installed on the device where the problem occurred.

- Confirming the distribution

In response to the software distribution application, the person responsible for solving the problem confirms that the requested version of the software was installed on the relevant device, and then closes out the Item. The result of execution can be confirmed from the **Distribution Status** job menu.

6. Confirm the overview of the problem resolution.

The person responsible for solving the problem, who confirmed the result of software distribution, records in the problem report form the fact that the requested version of the software has been installed, and then sends the report form to the applicant. The applicant who filled out the problem report form confirms that the requested version of the software installed on the device has corrected the problem, and then completes the Item.

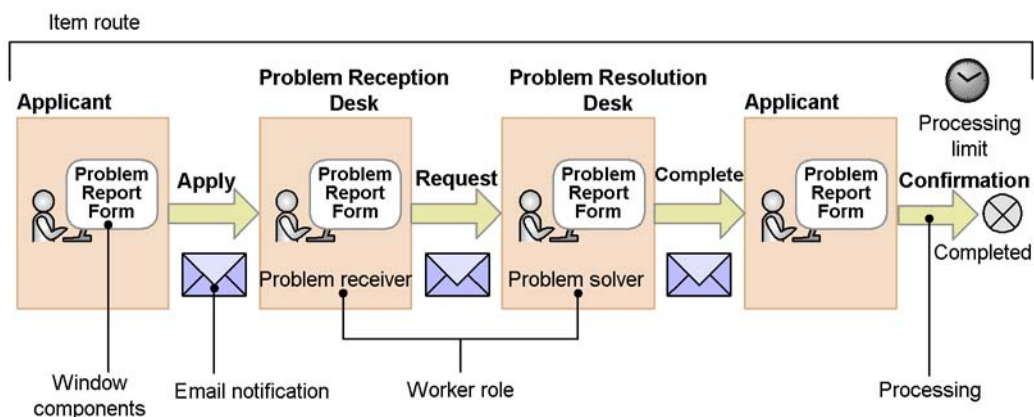
Changing the contents of an Item definition

The sample Item provided by Asset Information Manager is a model case of an asset management job. The settings should be changed, based on this sample, depending on the details of the actual asset management job.

For details about how to confirm and change the contents of an Item definition, see *10.1 Overview of Item definition* in the *Planning and Setup Guide*.

The following figure shows the Item definition elements required when considering jobs that use Items.

Figure 2-22: Item definition elements



- Item route

This defines the workers who are responsible, from the applicant and the problem reception desk until the Item is completed. The department and the personnel who execute the series of work, and the contents of that work, until completion of an Item are known as the *node*.

For details on how to define the route, see *10.3 Defining the route (Flow Designer)* in the *Planning and Setup Guide*.

- Worker role

The management node problem reception desk and problem resolution desk are defined so that Items are sent to workers with authority to execute the processing. The authority required to process Items is called *official authority*. For details on how to define official authority, see *10.2 Defining authority for processing the Item (Official Authority)* in the *Planning and Setup Guide*.

- Window components processed by each worker

Each worker defines the items to be specified and the buttons for execution in the windows. Such worker-processed windows are called *Item window*.

For details on how to define the Item window, see *10.4 Defining the Item window (Form Designer)* in the *Planning and Setup Guide*.

- Processing that accompanies Item execution

This defines the processing to be executed once the solution has been

implemented, when the overview of the problem and the overview of the solution are registered and the Item is sent to the next worker. Such processing that accompanies execution is called an *activity*.

For details on how to define this processing, see *10.5 Defining each node's task (Activity Designer)* in the *Planning and Setup Guide*.

- Setting whether to send email and processing time limits

You can set options for an Item, such as whether the worker is to be notified by email when the Item arrives at the next worker, or to specify a processing time limit. These send-time options for Items are called *Item options*.

For details on how to define Item options, see *10.6 Setting the Item options (Flow Designer)* in the *Planning and Setup Guide*.

---

## 2.9 Checking user operations by means of operation logs

---

With Asset Information Manager, you can search for and check user operations by means of operation logs. With operation logs, you can check operations such as when and where files were copied or file names were changed, and trace these operations chronologically. By totaling operation log entries, you can also gain an understanding from the totals of the state of each group.

For example, you can perform the following operations based on operation logs:

- Check whether a file containing confidential information was copied.
- Determine the operation log state for each group based on the totals.
- Trace and investigate user operations.

Using as an example the copying of the `EmployeeList.xls` file, which contains confidential information, we will explain in the following subsections how to perform each of the above operations by checking the operation log entries for this file.

Before you check operation logs, you must use JP1/Software Distribution to collect operation logs from the managed devices.

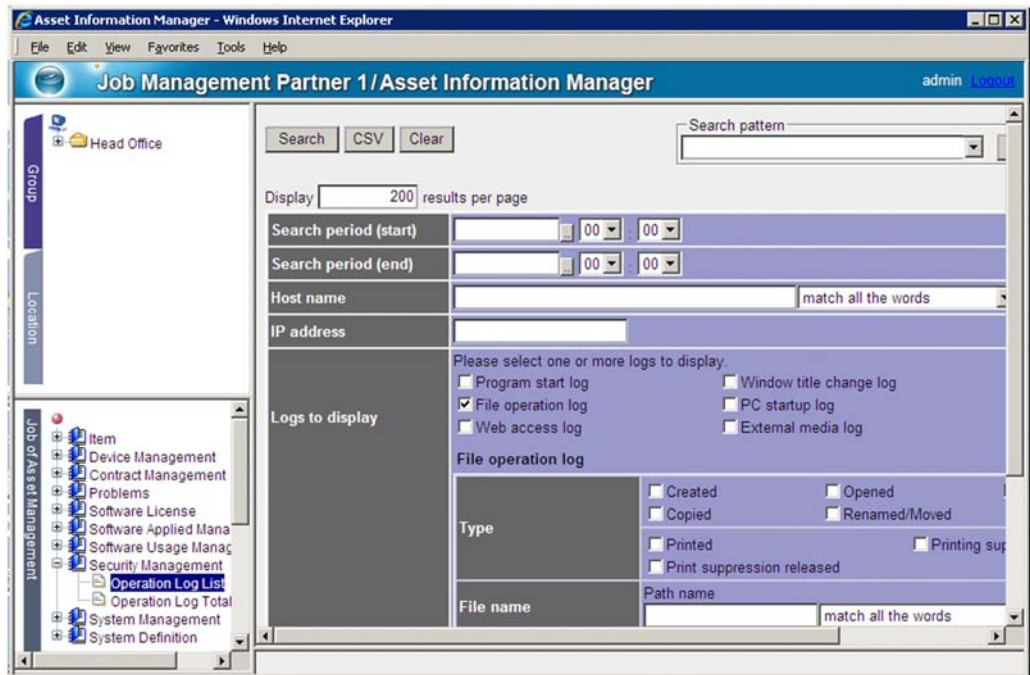
### **(1) *Checking whether a file containing confidential information was copied***

This subsection explains how to search the operation logs to determine if `EmployeeList.xls`, which contains confidential information, was copied.

The Operation Log List window can be used to search for operation log entries.

The following figure shows the Operation Log List window.

Figure 2-23: Operation Log List window

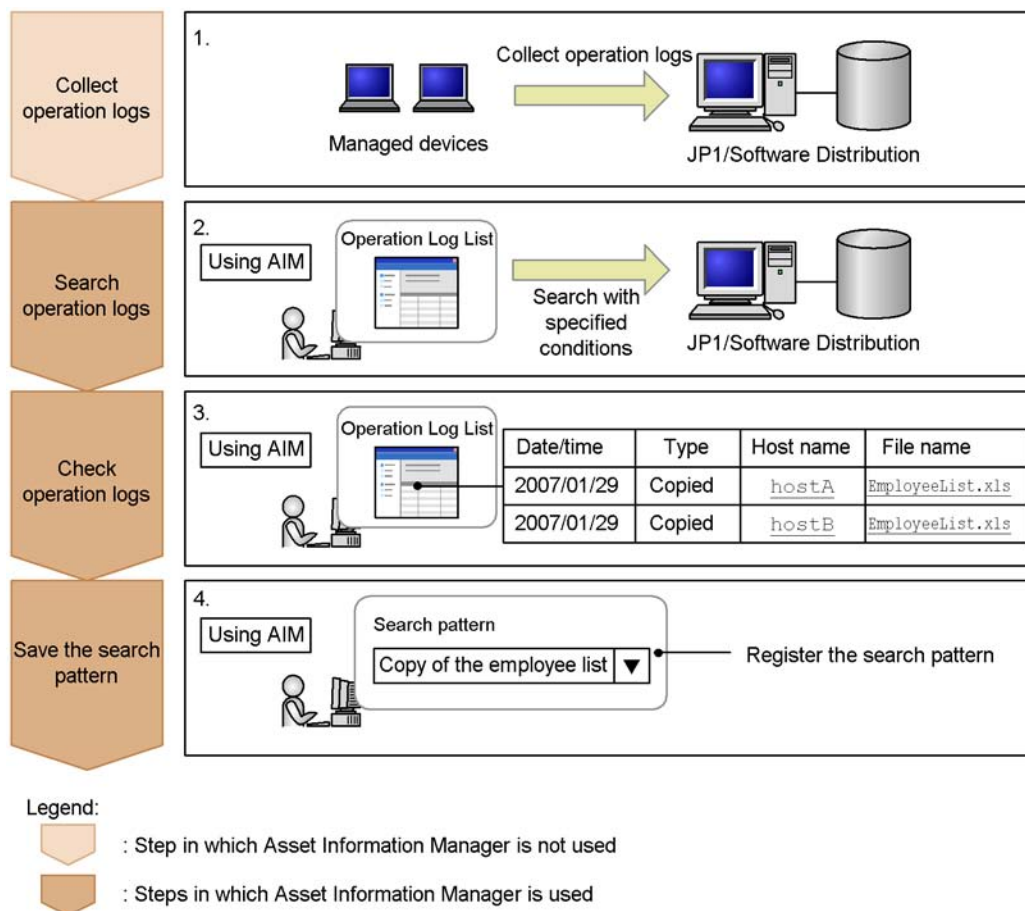


From the operation log entries that are displayed in the search results, you can check the date and time, type, and other information about each operation.

The following figure shows the operation flow for specifying search conditions and for searching operation logs to determine if `EmployeeList.xls` was copied.



Figure 2-24: Operation flow for specifying search conditions and searching operation logs



To search operation logs:

1. Collect operation logs.

Before you can search for file copying operations in operation logs, you must use JP1/Software Distribution to collect operation logs on file operations.

2. Specify search conditions and search the operation logs.

In the Operation Log List window, specify the conditions listed below, and click the **Search** button. To minimize the search time, we recommend that you narrow down the scope of the search by specifying as many conditions as possible.

- **Search period (start) and Search period (end):** Specify these options to limit the search period.

The search operation might take a while if you either do not specify a search period or if you specify a long search period.

- **Logs to display:** Select the **File operation log** check box.
- **Type:** Select the **Copied** check box.
- **File name:** Enter `EmployeeList.xls` in the **File name** text box.
- **Drive type:** Select all of the check boxes.

For details and notes about how to specify search conditions, see 2.7.1(1) *Searching for operation logs* in the *Administrator's Guide*.

3. Check the operation log entries.

From the operation log entries displayed in the search results, check the account, host name, and other information about the user who copied the file.

4. Register the specified search conditions as a search pattern.

If you plan to use the same search conditions to search operation logs again, register the specified search conditions as a search pattern. The search period is not registered as part of the search pattern, so you can reuse the search conditions without having to reuse the search period. We recommend that you register a search pattern name that makes it easy to determine the name and type of the search file, such as `Copy of the Employee List`. For details about how to register search patterns, see 2.7.1(2)(b) *Registering or updating a search pattern* in the *Administrator's Guide*.

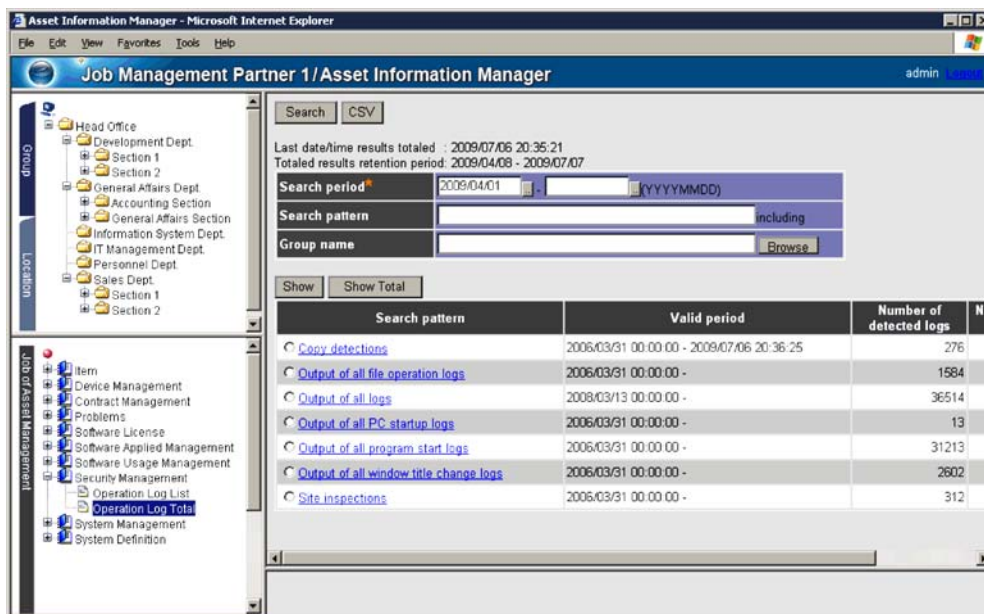
## **(2) Determining the operation log state for each group based on the totals**

You can use the totals from the operation log entries to determine how many users in a group have copied `EmployeeList.xls`. You can also check how the number of incidents detected in the operation logs has changed over time for each group.

You can use the Operation Log Total window to check the operation log entry totals.

The following figure shows the Operation Log Total window.

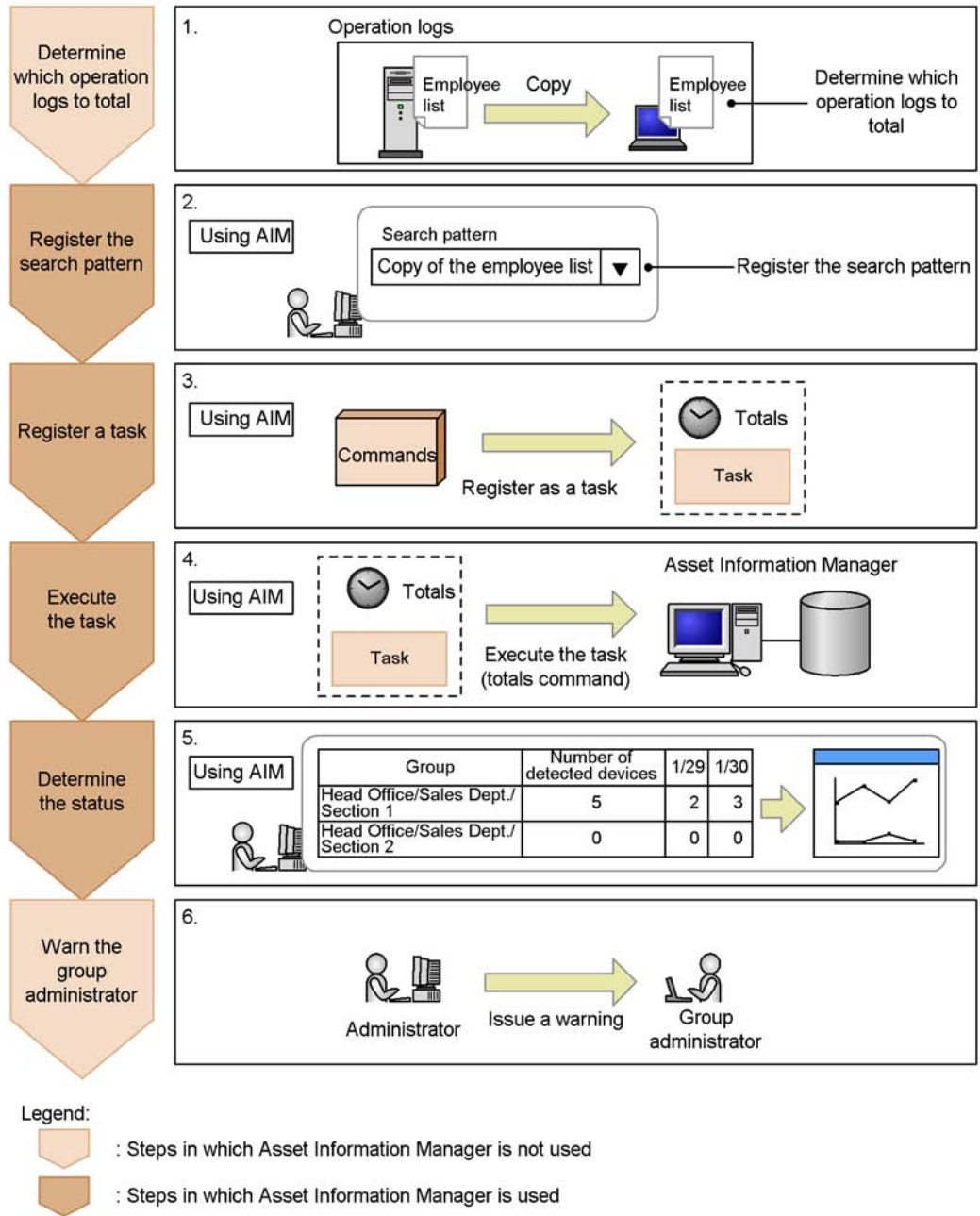
Figure 2-25: Operation Log Total window



The totals display how many operation log entries were detected for each search pattern.

The following figure shows the operation flow for scheduling that operation log entries indicating the copying of EmployeeList.xls are to be totaled once per week, and for determining the state thereof by group.

Figure 2-26: Operation flow for totaling copy operation log entries and determining their state



1. Determine which type of operation log entries to total.

Determine which type of operation logs that you want to check for each group, such as operation logs on unauthorized operations. In this example, we plan to total the operation log entries regarding the copying of `EmployeeList.xls`.

2. Register the search pattern in the Operation Log List window.

Register the search pattern to use when performing totaling. The search conditions are the same as those specified in step 2 of the procedure described in subsection (1) above. For details about how to register search patterns, see 2.7.1(2)(b) *Registering or updating a search pattern* in the *Administrator's Guide*.

3. Register the operation log entry totaling command as a task.

In order to periodically check totals, register the operation log entry totaling command as a task in Windows Task Scheduler. When you register the task, specify that the command be executed once a week. Also, specify the following value as the file to run:

- File to run

```
Asset-Information-Manager-installation-folder\exe\jamOperationLogAddUp.exe -p "Copy of EmployeeList"
```

In this example, the task executes once a week, so you do not need to specify any options other than the `-p` option. For details about how to register tasks, see 5.9.10 *Notification of device information change* in the *Planning and Setup Guide*.

4. Execute the registered task.

Execute the task to total the operation log entries.

5. In the Operation Log Total window, use the totals to determine the status of each group.

From the totals, for each group determine the number of operation log entries that indicate copying of `EmployeeList.xls`. You can also display a graph of the change through time in the number of operation log entries, which you can use to determine if the number of copy operations is declining. For details about how to display the totals, see 2.7.2(1) *Specifying conditions and displaying totals* in the *Administrator's Guide*. For details about how to display a graph, see 2.7.2(4) *Displaying the operation log totals in graph format* in the *Administrator's Guide*.

6. Warn the group administrator.

If necessary, you can warn the administrator of a group where a problem might exist, such as a group in which a large number of suspicious operation log entries are detected, or if the percentage of suspicious devices detected does not decrease.

Note

If you execute an Asset Information Manager task on a 64-bit OS, you must execute it from the 32-bit command prompt. For details about how to execute commands, see *F(2) Notes on executing commands and tasks in a 64-bit OS* in the *Planning and Setup Guide*.

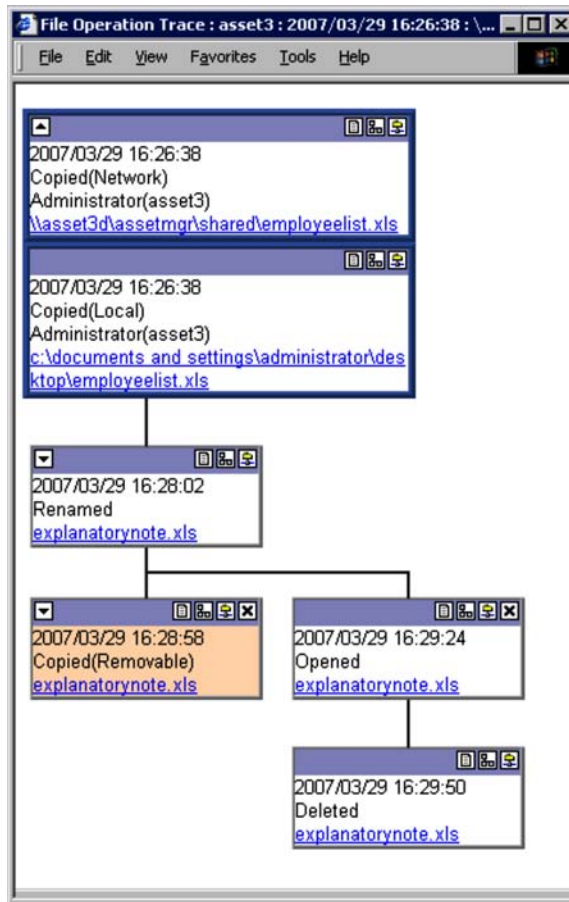
**(3) Tracing and investigating user operations**

You can check the operations performed on the `EmployeeList.xls` file after it was copied. Based on the operation logs from the target device, you can also trace operations performed across the network from other devices.

You can use the File Operation Trace dialog box to trace user operations.

The following window shows the File Operation Trace dialog box.

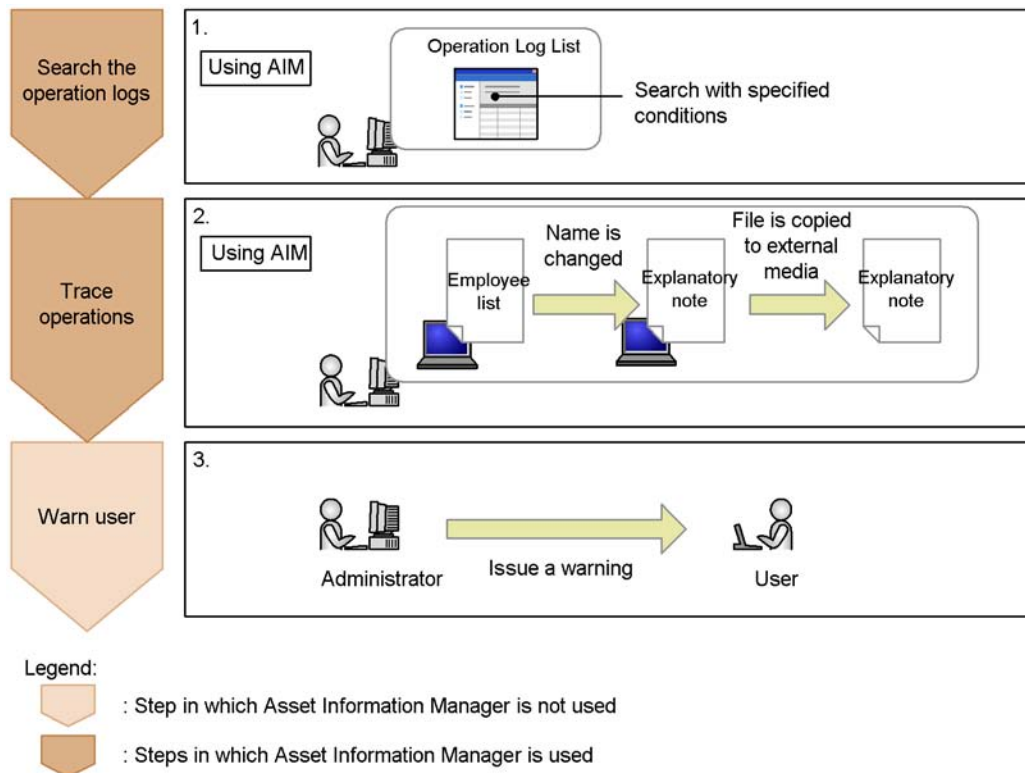
Figure 2-27: File Operation Trace dialog box



You can use a similar dialog box to trace operations performed across the network from another device.

The following figure shows the operation flow for tracing user operations related to copying `EmployeeList.xls`.

*Figure 2-28: Operation flow for tracing user operations related to copying the EmployeeList.xls file*



1. In the Operation Log List window, specify the search conditions and search the operation logs.

Search for operation log entries that indicate copying of `EmployeeList.xls`. Specify the same conditions as specified in step 2 of the procedure described in subsection (1) above.

2. Trace the file operations based on the search results.

Use the File Operation Trace dialog box to trace the operations, and to check if the name of the copied `EmployeeList.xls` file was changed or if the file was copied to external media. For details about how to trace operations, see 2.7.3 *Tracing user operations in the Administrator's Guide*.

2. Typical Usage

3. Warn the user.  
If necessary, warn the user.



## 2.10 Login authentication via linkage with Active Directory

Active Directory services can be used for authentication when logging in to Asset Information Manager. This allows login passwords to be consolidated in Active Directory, and means that you do not have to manage passwords separately for each system you are using.

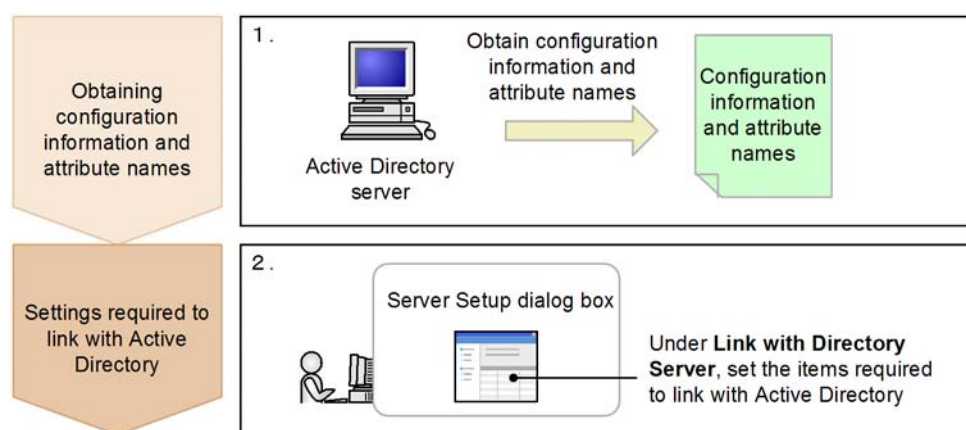
### Note

Only passwords can be consolidated when Active Directory is used for login authentication.

Asset Information Manager user information must be used to manage user group information.

The following figure shows the workflow for user authentication via linkage with Active Directory.

*Figure 2-29:* Workflow for user authentication via linkage with Active Directory



### Legend:

- : Jobs that do not use Asset Information Manager
- : Jobs that use Asset Information Manager

1. Obtain configuration information and attribute names from the Active Directory server.

The information required to configure linkage with Active Directory must be obtained in advance. For details about how to obtain this information, see *3.5.1 Login authentication* in the *Planning and Setup Guide*.

## 2. Typical Usage

### 2. Configure the settings to link with Active Directory.

In order to link to Active Directory, you must configure the settings under **Link with Directory Server** in the **Server Setup** dialog box. For details about the settings required to link with Active Directory, see *5.3.6 Setting Link with Directory Server* in the *Planning and Setup Guide*.

---

## 2.11 Including Active Directory information in the asset management database

---

User information managed by Active Directory services can be registered into the asset management database.

You must create and periodically execute an Asset Information Manager script in order to update the asset management database (user management information) with the user information that is managed by Active Directory services. Asset Information Manager provides a sample script that can be used as a reference for creating your own script. The sample script updates the following items:

- Role names
- Email addresses
- Phone numbers

For details about how to update the asset management database via linkage with Active Directory, see *3.5.2 Acquiring user organization information* in the *Planning and Setup Guide*.



---

# Appendixes

---

- A. Version Changes
- B. Glossary

---

## A. Version Changes

---

### (1) Changes in version 09-00

- A description has been added about the concept of managing downgrade software.
- Microsoft SQL Server 2008 can now be used as a DBMS.
- The minimum value that can be specified for the **Communication-less monitoring time** setting under **Session Information** in the Server Setup dialog box has been changed to 5 minutes.
- The **Display substitute items by default** setting has been added under **Basic Information** in the Server Setup dialog box, allowing the user to choose whether to display substitute Items by default in the Inbox window.
- The **Status to display in device search windows** setting has been added under **Basic Information** in the Server Setup dialog box, allowing the user to choose the device statuses to display in the **Status** search condition pull-down menu displayed in the Device Totals and Device List windows.
- The MIME settings used by Asset Information Manager can now be re-registered by setting up a virtual directory from the Setup dialog box.
- A file attachment can now be specified in the New Device job menu and in the Device Details dialog box.
- `Text_Title` (text for dialog box titles) has been added to the items in the `VariousInfo` management class, allowing the user to change the title of operation windows.
- `OPTIONS` has been added as a condition statement definition item for search conditions in user reports, allowing pull-down menus to be displayed in user reports.
- The following user properties have been added to hardware asset information and device catalog information to allow even more user-specific information to be managed:
  - user property code-7 to user property code-12
  - user property field 32-7 and user property field 32-8
  - user property field 64-5 to user property field 64-8
  - user property field 128-3 to user property field 128-8
  - user property field 255-3 to user property field 255-8
  - user property area-3 and user property area-4

- When defining an Item's route in Flow Designer, for each activity you can now set whether to send an email informing the next worker that the Item has been sent.
- Problems that could occur when a user logs in to Asset Information Manager, and the main causes and recommended handling for such problems, are now described in more detail.
- The method of modifying the `pdsys` file when the Embedded RDB host is renamed has been revised.
- When an asset information database is created using Embedded RDB, the size of the database can now be set to increase automatically. With this change, the procedure for configuring a cluster system environment has also been changed.
- In dialog boxes that are displayed when an anchor or button in an operation window is clicked, when the **Browse** button is clicked with a value specified in the specification area for a group, user name, or location, a tree can be displayed that expands only the specified group, user name, or location.
- The user name, host name, and IP address can now be specified as search conditions in the Batch Update window.
- 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 entries in an operation log.
- A CSV-format backup of asset management databases can now be obtained by executing `jamdbexport.bat`.

## (2) Changes in version 08-51

- The following new operation logs that are acquired by JP1/Software Distribution 08-51 can now be viewed and totaled:
  - Web access log
  - External media log
  - File operation log (print operation)
- Windows Server 2008 is now supported.
- JP1/Software Distribution directory information can now be imported to the asset management database by the *Acquiring directory information* task.
- A URL to be included in emails can now be specified when the *Notification of WSUS updates* task is used to send email notification to the administrator.
- A description of setting **Database Character Set** to `WE8MSWIN1252` has been added for the Oracle asset management database and the Oracle JP1/Software Distribution database.

- A description of the WSUS server-linked system configuration has been added.
- Whether a search is case-sensitive can now be specified when Embedded RDB is used to search for a partial match, including a leading or a trailing match.
- The sender's address can now be set when the execution result of a task registered in the Task Scheduler is reported by email.
- A procedure for renaming the Embedded RDB host has been added.
- A procedure for changing the database size has been added for the Embedded RDB asset management database.
- The minimum database size has been changed to 100 megabytes for the Embedded RDB asset management database.
- Procedures for starting and stopping Embedded RDB have been added.
- There are revised descriptions of the major causes of errors that result in execution failure, and of the actions to take during asset management database creation.
- Commands can now be used to back up and reorganize the asset management database.
- Items to be imported have been added for the following asset types:
  - Device information
  - Installed software information
  - Installed software list
  - Software information
  - Assigned license information
  - Patches
  - Virus definition
- All items that can be set to be displayed by the **Customize Managed Items** job menu are now indicated.
- The required minimum memory size has been changed from 512 megabytes to 1 gigabyte.
- The size and breakdown of the information used in the asset management database have been changed.
- When Asset Information Manager is upgraded from version 08-00 or later, the format set by the **Customize Job Windows** job menu can now be migrated.
- A procedure for upgrading the asset management database in a cluster environment has been added.



- The software information can now be changed on the **License** tab of the Device Details dialog box.
- A description and notes have been added on how to create a CSV file to be imported from the **Import** job menu.

### **(3) Changes in version 08-10**

- The operation log entries can now be summed and the totaled results can be checked from the **Operation Log Total** job menu.
- Device operation can now be traced from the operation log.
- The following tasks required for setting up Asset Information Manager can now be executed from the Setup dialog box:
  - Setting the asset management server
  - Creating an asset management database
  - Creating a data source or a net service
  - Setting a virtual directory
- The sample data for design (linkage with JP1/SD) can now be used to manipulate the main windows of Asset Information Manager.
- JP1/Software Distribution can now be linked to manage the software operating status.
- JP1/Software Distribution can now be linked to check unused licenses.
- The device change log can now be sent by email.
- The Oracle8i version that can be used as an asset management database has been changed.
- The fields that can be included in the device change log can now be selected. Additionally, the following fields have been added to the available device change log information:
  - Host name
  - IP address
  - MAC address
  - User properties of hardware information
- The search functions supported for created user reports can now be executed from the command line.
- **Screen display information** has been added to the Create User Report window to allow the sort order and display width to be set for the output items.

- The same property can now be specified more than once in the user report search condition.
- A subject can now be defined in the Items window.
- Backup, restoration, and reorganization of Embedded RDB can now be executed from the Database Manager dialog box.
- When patch information is to be acquired from the JP1/Software Distribution installation package, and the package ID begins with WUA-SUP, **Apply** is set as the applied status.
- The codes corresponding to the following CPUs have been added to the **CPU type** in the hardware information:
  - Intel Core2
  - Intel Core
  - AMD Athlon 64 X2
  - AMD Turion 64
- The size of definition data has been changed from 20 to 30 megabytes.
- The asset management database can now be upgraded or migrated from the Database Manager dialog box.

**(4) Changes in version 08-00**

- Microsoft SQL Server 2005 has been added as an available DBMS.
- Operation logs can now be managed by linking to JP1/Software Distribution.
- Microsoft Internet Explorer 6 (SP1 or later) is now required to use Asset Information Manager.
- Contract update history can now be managed.
- In addition to **Unapplied**, **Apply** information can now be collected for the **Applied status** of updated patch information when inventory information is collected.
- Categories and names of some of the settings in the Setup dialog box were changed as follows:

07-50 and earlier		08-00	
Category	Environment setting	Category	Environment setting
Basic Information	Open map name	Link with NNM	Open map name

07-50 and earlier		08-00	
Category	Environment setting	Category	Environment setting
	Name of connection destination server		Name of connection destination server
Mail Information	Notification by E-mail	Mail Notification Information	Notification by e-mail
	Address to E-mail		Address to e-mail
Directory Information	Code set	Link with Directory Server	Code set
Inventory Information	Login ID for taking inventory	Link with JP1/SD	JP1/SD database login ID
	Service name for taking inventory		Connection service for JP1/SD database
	Take machines without SD installed		Acquire devices on which JP1/SD is not installed
	JP1/Software Distribution working key		Working key
	Assign key for asset information		Assign key for asset information
	Conditions for assigning Asset Information 1		Conditions for assigning asset information 1
	Conditions for assigning Asset Information 2		Conditions for assigning asset information 2
	Perform new registration of unassigned assets		Perform new registration of unassigned assets
	MAC address for dial up connection		MAC address for dial up connection
	Type of information to acquire		Type of information to acquire
	Watch interval for update inventory		Watch interval for update inventory
	Status of machines deleted with JP1/SD		Status of machines deleted with JP1/SD
	Code specified for deleted assets		Code specified for deleted assets

07-50 and earlier		08-00	
Category	Environment setting	Category	Environment setting
Software Distribution Information	Job storage folder name used in JP1/SD	Link with JP1/SD	Job storage folder name used in JP1/SD

- Management and application of updates can now be performed by linking to a WSUS server.
- A **Trash** that provides a temporary backup for locations that have been deleted with the **Location** job menu has been added.
- From the **IP Group** job menu, group-specific and location-specific IP groups can now be created, enabling IP addresses to be managed by group and location. When collecting JP1/Software Distribution inventory information and HP NNM node information, and when executing a data maintenance task, the group and location of each device can now be set according to its IP group.
- The following operations have been added to those that can be performed with data maintenance tasks.
  - Operations that break the relationship between the user and the software key information, or that break the relationship between hardware information and the software key information, to match the license category
  - Operations that integrate, respectively, the number of software asset licenses and license keys that have been transferred
  - Operations that delete installed software information about software whose managed level is set to **Unmanaged object**
  - Operations that delete the group-specific or location-specific IP group of associated groups or locations that have been deleted
  - Operations that register **Group name** in asset information based on the value of **IP address** in hardware information
  - Operations that register **Location** in asset information based on the value of **IP address** in hardware information
  - Operations that delete an attached file for which corresponding information does not exist
- Operations that are executed with a data maintenance task can now be selected by purpose.
- The following JP1 events have been added to those issued by Asset Information Manager:

- Item transition event
  - Item status change event
  - Item deletion event
  - Problem status change event
  - Problem deletion event
- If expiration of the time specified for setup causes an automatic logoff, the logon window is now displayed following a message indicating that the system has been logged off automatically.
  - Registered settings can now be deleted in the Set Changes dialog box, which is displayed from the Unused Device List and Batch Update windows.
  - Devices not assigned licenses now appear as icons in the device list displayed in the window that appears for the software discovered from the Excess License List window.
  - License assignment and cancellation can now be performed in the Excess License List - by Used window on devices and users found to be excess license users.
  - When a new software asset is registered, the installed software name can now be assigned to a software name.
  - The progress of an Item can now be checked from the Outbox and Execution Item Management windows.
  - Relationships to the software name of the installed software name can now be created and modified from the Installed Software window.
  - Formats can now be deleted and initialized in a batch operation.
  - Whether to overwrite the values set to assigned items when JP1/Software Distribution inventory information is being collected can now be configured.
  - A **JP1 event notification** task that issues a JP1 event at an Item transition has been added.
  - A **Computer ID** field that can be managed as hardware information has been added.
  - User-selectable management items can now be assigned and used in the user extension area of the problem status change event.
  - Code supporting the following CPU types in hardware information has been added:
    - Intel Pentium D
    - Intel Celeron D

## A. Version Changes

- AMD Duron MP
  - Mobile AMD Athlon XP-M
  - AMD Sempron
  - Mobile AMD Sempron
  - AMD Athlon 64
  - AMD Athlon 64 FX
  - Mobile AMD Athlon 64
  - AMD64 compatible CPU
  - AMD Opteron
- Windows Server 2003(x64) has been added as a supported OS.
  - Package IDs can now be collected when JP1/Software Distribution inventory information is being collected.
  - When JP1/Software Distribution inventory information is being collected, the package ID and package name can now be used to automatically assign an installed software name to a software name, based on assignment of the existing installed software information. If an installed software name not assigned to a software name is assigned by this process, the new software name is registered and assigned.
  - Security management can now be performed by linking to JP1/CSC.

### **(5) Changes in version 07-50**

- The usage status of user software and the operational status of window displays can now be monitored by collecting operation history from JP1/Software Distribution.
- Changes made by JP1/Software Distribution can now be obtained in real time when JP1/Software Distribution inventory information is collected.
- By linking with HP NNM, node information can now be obtained and displayed as network maps. Asset information maintained by Asset Information Manager can also be viewed from HP NNM.
- You can now view information related to JP1 events by linking with JP1/IM and displaying the Asset Information Manager operation window from the JP1/IM Event Console window.
- Patch information and virus definition information can now be managed.
- Asset management jobs that use Items can now be executed.
- The job category name *Software Distribution Management* has been changed to

*Software Applied Management.*

- Searching for and checking the applied status of installed software, patch information, and virus definition information can now be performed from separate tabs in the **Software Applied Status** job menu and, if needed, can also be distributed. Distribution to a destination group in a JP1/Software Distribution host group can also be specified.
- Devices that are deleted from JP1/Software Distribution inventory can now be maintained temporarily by Asset Information Manager in a status called *pre-scrap*.
- Asset Information Manager Embedded RDB Edition has been added; it provides an embedded database.
- Information collected from machines on which JP1/Software Distribution Client is not installed (machines on which JP1/Software Distribution is not installed) can now be imported into the asset management database.
- Asset Information Manager can now be operated on a cluster system.
- The **Number of concurrent connections** setting under **Basic Information** in the Setup dialog box has been removed.
- The number of search results to be displayed per tab can now be specified.
- Settings for assigning JP1/Software Distribution inventory information and Asset Information Manager asset information have been changed.
- A task dedicated to summarizing licenses has been added.
- A delete option has been added for deleting generations of totals results other than a specified number of most recent generations.
- Email notification of contract information about contracts that are about to expire can now be scheduled.
- Software update history can now be managed.
- The collection status of inventory information can now be checked from the **Log** job menu.
- Importing and exporting can now be performed from job menus.
- Batch files can also be used to perform importing and exporting, in a process similar to that used with the **Import** and **Export** job menus.
- When registering asset information, files you want to manage can now be specified as attached files.
- **Device List by Devices Needing Patches** has been removed from the job menu.
- User searches can now be performed from the **Search Users** job menu.

- **Point of totals** has been added to the **Device Management** job menu, which enables devices to be counted by specifying them as a management item.
- Network information is no longer displayed in the **Device List** job menu.
- The **Batch Update** button in the **Unused Device List** job menu can now be used to change the status of all devices.
- **Usage management, Device type, Device name, Model, Developer, Serial No., Composition, Monitor type, Monitor resolution, Monitor size, and Specification** have been added to the **Batch Update** job menu.
- A time period can now be specified for searching device change logs.
- In addition to transfer logs, change logs of both software and hardware can now be viewed from the Device Details dialog box.
- Whether the device type is to be changed can now be selected in accordance with JP1/Software Distribution inventory information.
- Numerical value information has been added through use of a user property unit.
- In the Edit Form window, **Usable buttons** and **Usable items** have been changed to **Hide**.
- *SD installed status* and *Inventory last update date/time* have been added as asset information that can be managed.
- *IP address, MAC address, host name, MBSA version, OS information, OS version, SD operation update date, SD operation history start-date, SD operation history end-date, SD operation history entry No.* have been added to hardware information that can be managed.
- Program execution history and window title update history have been added to information that can be managed.
- User properties have been added for the following information:
  - Asset information
  - Hardware information
  - Device catalog information
  - IP group information
- CPU types have been added to hardware information.
- *Managed number* has been added as managed information.



---

## B. Glossary

---

### accessory (device type)

A type of hardware asset, including **Monitor**, **Hard disk**, **CD-R**, **DAT**, **MO**, or **Printer**. In the asset management system, hardware is classified into three device types: computing, accessories, and networking.

### access permission

Restrictions set for some of the asset information managed in an asset management system so that the users who can access it are limited. Examples of such information are information about tax returns or maintenance contract fees.

Access permissions that can be set in an asset management system include restrictions on the following:

- User authentication based on user ID and password
- Availability of the system by user role
- Role-based limitations on the functionality that can be executed from windows
- Role-based limitations on the menus

### Active Directory services

Windows main component that manages information on objects comprising a Windows network environment and the relationships between these objects. The following generic names also exist:

- Active Directory Rights Management Service (AD RMS)
- Active Directory Domain Service (AD DS)
- Active Directory Lightweight Directory Service (AD LDS)
- Active Directory Certificate Service (AD CS)
- Active Directory Federation Service (AD FS)

### activity

Processing that is a component of an Item definition and which is executed when the Item is sent to the next worker. Examples of such processing are **Apply** and **Approve**.

Flow Designer is used to define activities, and Activity Designer is used to set activity details.

### administrator

A network manager or device administrator in the group that handles company IT asset management tasks (an information systems management department). The

administrator can handle all asset information.

### **asset**

A unit of managing assets by user.

Assets include device-related, software-related, and user-specific assets. The device-related assets consist of one or more devices, and software-related assets consist of one or more software items. User-specific assets consist of user-specific information.

### **asset information**

Information used to manage the hardware and software assets in a company. The asset information is represented by data such as **Asset No.**, **Group name**, **User name**, **Location name**, and is not the hardware or software asset itself.

**Asset No.** is used to identify each asset and can be assigned by the user. In an asset management system, **Asset No.** is the most basic unit of asset management.

### **Asset Information Manager**

A product that can reduce management costs and can streamline IT asset management jobs required for tasks such as installing assets, managing software licenses, and performing device maintenance. The product helps achieve these goals by using a database to implement integrated management of asset information such as hardware information (including network devices), software information, and contract information. Additionally, integrated management of IT assets can be achieved by linking Asset Information Manager to JP1 products such as JP1/Software Distribution, HP NNM Version 7.5 or earlier, and JP1/IM.

### **asset management database**

A database that stores asset information. The asset management system supports Microsoft SQL Server, Embedded RDB, and Oracle as its database systems.

### **asset management database server**

A server containing the database that stores asset information.

### **asset management server**

A server that manages asset information and provides services related to asset information.

### **asset management system**

A system that manages asset information. An asset management system consists of the following programs:

- Asset management server
- Asset management database server

- Web browser

### **association class**

A class defining the relationship between object classes.

An association represents a relationship between multiple classes. Specifically, an association defines a multiplex level between two classes and how the two classes are processed when data is added or deleted.

### **cabinet**

An area for storing packages; the area is located in JP1/Software Distribution's managing server.

Asset Information Manager can distribute packages stored in JP1/Software Distribution cabinets.

### **class**

1. A set of management information classified by asset information category. An asset management system handles object classes and association classes.
2. WSUS updates categories, such as security updates and critical updates.

### **CN (Common Name)**

Entry name attribute in Active Directory. For example, the name of a person (user) is a CN.

### **code ID**

A unique ID assigned to an item managed by code in the asset management database. When codes are edited, codes are added or deleted based on this code ID.

### **computing (device type)**

A type of hardware asset, including **PC**, **PC server**, **UNIX**, and **UNIX server**. In the asset management system, hardware is classified into three device types: computing, accessories, and networking.

### **contract information**

Information used to manage device and software assets under maintenance, lease, or rental contracts.

By grouping multiple devices and software assets with the same contract and then assigning a contract number to the group, the user can manage the devices and software assets by contract.

### **Customize Job Windows**

A function for limiting the operations available from windows by user role.

This functionality allows the components of each window (such as buttons, search

conditions, and editable items) to be changed according to the user role.

### **data file**

A CSV file required for importing or exporting data. A data file consists of item title lines and data lines.

For an import operation, asset information (asset data) is specified for each association class.

For an export operation, the output destination of asset information is specified for each association class.

### **data files definition file**

A text file that is needed in order to import or export multiple data files in a batch operation.

A data files definition file defines the names of all data files to be imported or exported, and defines the display names of the association classes that correspond to the data files.

### **DC (Domain Component)**

The element that constitutes a domain name in Active Directory.

### **destination**

A client subject to execution when a job is executed from JP1/Software Distribution's managing server.

Asset Information Manager enables software assets to be distributed to devices that are found by searches in operation windows. The user can also distribute software by specifying a host group created by JP1/Software Distribution.

### **device catalog**

Registration information that is predetermined for a product, such as CPU and memory size.

When registering a new device, the user can select a product from the device catalog and thereby save the time needed to enter the items predetermined for the product.

### **device change log**

Information used to manage changes to devices, such as memory size and disk space. This information can be used to check for any illegitimate physical changes to a CPU, memory, or disk.

The device change log data is organized into fields such as **Update date**, **Hard disk sizes**, **Memory**, and **Processor**.

**division**

Information for managing other groups as group jobs. Multiple divisions can be set up for each group. Assigning a division to a user allows that user to manage the information about the group (division group) that is set up as a division group for the division.

**division group**

Information about the group that is set to a division.

**DN (Distinguished Name)**

Identifier for uniquely identifying each entry in the Active Directory's directory tree. A distinguished name consists of a character string made up by linking entry attributes using commas (,).

**Embedded RDB**

A database that is built into Asset Information Manager and JP1/Software Distribution Manager. By using Embedded RDB, you can install Asset Information Manager and JP1/Software Distribution without having to install a DBMS product.

**event manager**

A user assigned to check Asset Information Manager asset information from JP1/IM. If a password is set up for this user in advance, the user can automatically be logged into Asset Information Manager when the user checks asset information from the Event Console window.

**export**

Output of information from the asset management database to a CSV file, in a batch operation.

There are three export methods:

- Export by using the **Export** job menu
 

The user creates export conditions for selecting the asset information to be output and, in a batch operation, outputs the information to a CSV file. This method can be used at any location where the user can log in to Asset Information Manager.
- Export by using `jamCsvExport.bat`

By executing this from the command line on the asset management server, the user can perform the same export processing as can be performed from the Export window.
- Export by using the `jamexport` command
 

This method outputs data, in a batch operation, from the asset management database to CSV files as is. A CSV file is output for each class. This export

function is implemented by a command provided by Asset Information Manager.

### **file operation log**

An operation log that collects folder and file operation events, such as when a file or folder is created or copied. These logs are collected by JP1/Software Distribution.

### **form**

Settings of each window customized by the **Customize Job Windows** function. For example, the settings can specify whether to show or hide buttons and search conditions.

A form is set for each window, and multiple forms can be set for the same window.

### **group**

A unit for handling user information. If user information is handled according to the groups to which users belong, access to the information can be controlled for each group.

### **group information**

Information required for managing groups, such as the departments using the asset management system. Group information is represented by fields such as **Local name**, **Group code**, and **Cost group code**.

### **hardware information**

Information used to manage hardware assets. Hardware information includes information about all hardware assets handled in an asset management system that uses Asset Information Manager. Hardware information is about the devices themselves, and includes fields such as **Device type** and **Device name**.

### **HP NNM**

A product that provides functionality for managing multiple applications and multiple systems connected by a network, from a single network graphics window.

### **import**

The loading of information, in a batch operation, from a CSV file into the asset management database.

There are three import methods:

- Import by using the **Import** job menu

This user creates import conditions and updates asset information in the CSV file in a batch operation.

This method can be used at any location where the user can log in to Asset Information Manager. It enables the user to update asset management database information without having to know the CSV file format, classes, or the

relationships between classes.

- Import by using `jamCsvImport.bat`

By executing this from the command line at the asset management server, the user can perform the same import processing as can be performed from the **Import** job menu. This method is useful for automating operations because the user can update asset management database information without having to know the CSV file format, classes, or the relationships between classes. Compared to the `jamimport` command, however, the processing takes more time.

- Import by using the `jamimport` command

This method loads, in a batch operation, all data from a CSV file into the asset management database as is. The CSV file contains information about data in the asset management database that is to be added, changed, or deleted. This import function is implemented by a command provided by Asset Information Manager.

### **installed software information**

Information used to manage the software assets installed on each device.

Installed software information is used by importing information (such as JP1/Software Distribution's inventory information) into an asset management database.

Therefore, the names and versions of software assets depend on the source system (such as JP1/Software Distribution) from which the information is imported.

### **installed software list**

Information used to manage the names of software assets installed on each device. It is also used to manage various settings for installed software assets.

### **inventory information**

Information such as the status of hardware utilization and the types of software assets installed at a client. Clients are managed based on this information. Inventory information is acquired from JP1/Software Distribution's managing server by executing jobs.

The asset management system can register inventory information acquired from JP1/Software Distribution as asset information.

### **IP group information**

Information used to manage IP addresses in groups. IP addresses can be managed under easy-to-understand names assigned to the groups.

### **IT assets**

IT devices, such as PCs and printers, existing in a company, software assets, and the network environment for using them.

## **Item**

Work with a defined route: such as **Equipment Deployment Request Form** or **Software Distribution Application Form**.

(Note: To avoid confusing this term with the everyday meaning of *item*, this manual uses upper-case "I" (*Item*). Other manuals, messages, or windows might not use this convention.)

## **Item auditor**

The official authority for auditing execution Items.

A user who has this official authority can view the latest Item statuses and attached files in the Execution Item Management window.

## **Item category**

A category of Items classified by the nature of the work.

In the New Item window used to select a new Item, each Item category is displayed on a separate tab.

## **ITIL**

A framework that systematizes IT system setup and operations. Setting up an IT system based on this framework is expected to enable the user to optimize IT services and continually improve day-to-day processes.

## **job**

An execution unit of JP1/Software Distribution functionality.

Two types of jobs can be executed from Asset Information Manager windows:

- *Install package*
- *Install by client user*

## **JP1 event**

JP1-specific management information generated for detecting and reporting events (such as job execution results and service errors) that occur in a system managed by JP1.

Asset Information Manager can acquire these JP1 events via JP1/IM.

## **JP1/Base**

The product that provides the basic functionality of JP1/IM. This product includes functionality for sending and receiving JP1 events, managing users, and controlling startup. The product also functions as an agent of a JP1/IM system.

JP1/Base is a prerequisite for JP1/IM.



**JP1/CSC**

A product that uses asset information managed by Asset Information Manager to take security measures for a system. A security management system that has JP1/CSC installed uses policies set by the administrator as a base to automatically evaluate the danger level for devices, and then takes appropriate actions (countermeasures).

Administrators can use the windows under the Client Security Management job category to monitor clients and perform actions as necessary.

**JP1/IM**

A product that achieves integrated management of an entire corporate information system. By collaborating with JP1-series products that manage system operations in various ways, JP1/IM uses JP1 events to implement integrated management of the events that occur in the system. If an error occurs, JP1/IM promptly notifies the administrator and provides the infrastructure for operations needed to identify the location of the error and investigate its cause.

**JP1/Software Distribution**

The collective name for a system that achieves software distribution and client management by batch operation over a network.

**JP1/Software Distribution not installed, machine on which**

*See machine on which JP1/Software Distribution is not installed.*

**LDAP (Lightweight Directory Access Protocol)**

A subset of the Directory Access Protocol used for accessing directories that support the ITU-recommended X.500 model. Active Directory is compatible with LDAP.

**license category**

The license categories for a purchased license are **Install license** and **User license**. Licenses are totaled for each license category.

**license information**

Information used to manage the details of software licenses.

License information includes fields such as **License name**, **Upgrade assurance**, **Downgrade**, **License type**, **Licensing method**, and **License category**.

**license type**

The type of a purchased license. The license types are listed below:

- **Install license**
- **User license**
- **Server license**

- **Client access license**
- **Managed node license**
- **CPU license**
- **Second license**
- **Concurrent execution license**

**License type** is used to manage the details of licenses and has no effect on the results of license totaling.

### **location information**

Information used to manage asset locations. The location information includes fields such as **Local name**, **Address**, **Area size**, and **Attribute**.

### **machine on which JP1/Software Distribution is not installed**

A device in the network on which JP1/Software Distribution Client has not been installed.

### **maintenance log**

Information used to manage details about device errors and remedial actions. If JP1/IM is linked, JP1 events can be acquired as maintenance log information.

The maintenance log data is organized into fields such as **Reg. date**, **Overview of problem**, **Importance**, **Host where problem occurred**, **Completion date**, **Overview of solution**, **Expense**, and **Reference materials (URL)**.

### **managed items**

An individual piece of information managed by Asset Information Manager. It corresponds to a class property managed in the asset management database.

### **managed label**

A label set to limit accesses by group. If the same managed label (any character string) is set for both a group and a user role, the users with the corresponding role can handle only the information belonging to the group and subgroups for which that managed label is set.

### **managed level**

A level for managing licenses. A managed level is set for installed software assets. When a managed level is set for each software asset, JP1/Software Distribution's inventory information is registered according to this setting. The managed level is set in the Installed Software window.

There are three managed levels:

- **Managed object**

Includes software assets in the number of used licenses.

- **Managed object not in license count**

Does not include software assets in the number of used licenses. Information is registered as installed software assets.

- **Unmanaged object**

Does not manage licenses nor register information as installed software assets.

### **management name**

A name used to identify the value for a text field, text area, or drop-down list defined by Form Designer when an Item is defined. The user can specify any character string without having to know the class properties.

This name is used with Activity Designer to specify how to update the asset management database.

### **meta table**

A table required to establish correspondence between class and table in the asset management database. When Asset Information Manager is set up, importing the meta table to the asset management database defines the data structure of the database.

### **network information**

Information used to manage the location of each device in the network. Network information includes **IP address**, **MAC address**, **Node name**, and **Computer name**.

### **networking (device type)**

A type of hardware asset, including **HUB**, **Router**, and **Network printer**. In an asset management system, hardware is classified into three device types: computing, accessories, and networking.

### **network manager**

A user who references Asset Information Manager asset information obtained from HP NNM Version 7.5 or earlier. If a password is set up for this user in advance, this user can automatically be logged into Asset Information Manager when checking asset information from the Network Presenter or Submap window.

### **Network Presenter**

A map of network devices detected by HP NNM Version 7.5 or earlier. It enables the user to reference network device connections and network problems.

### **node**

A component of an Item definition that represents a worker (or group) on the route of the Item: for example, an **Applicant** or **Approval user** is a node.

Flow Designer is used to define the nodes.

**object**

A collective name for components placed on the Item window, such as text fields and buttons. Form Designer is used to set objects.

**object class**

A class is a unit for managing asset information. An *object class* is the information representing each item managed by the asset management system. The information is represented by tables that correspond to classes and properties, or represented in the format used to input data to or output data from the asset management database.

**official authority**

Authority to limit the workers that can execute processing, such as to approve an Item.

To execute work for which an official authority is defined, the user must have that official authority separately from the permissions needed to log in to Asset Information Manager.

**operation log**

User operation information acquired by JP1/Software Distribution. Asset Information Manager can directly access the JP1/Software Distribution database, and can search and check the operation log data stored in the databases.

Operation logs enable you to determine the time and location of executed operations, such as the copying and renaming of files, and enable the execution of time-series tracking. By totaling the operation log data, you can also understand the status of each group from the totaled results.

**OU (Organization Unit)**

The name attribute of organization entries in Active Directory. An organization unit corresponds to a group name.

**package**

Software that has been registered in JP1/Software Distribution's managing server and is ready to be distributed. It is stored in a cabinet in the managing server.

To distribute software from Asset Information Manager, a package must be created for it by using JP1/Software Distribution beforehand.

**packaging**

Creating a package by using JP1/Software Distribution.

**patch information**

Information used to manage each device's patch application status, such as **Installation date** and **Applied status**.

**patch name list**

Information, such as **Patch name** and **Patch version**, used to manage patch names.

**PC startup log**

An operation log in which information about PC startup, termination, logon, and logoff events is collected. These operation logs are collected by JP1/Software Distribution.

**program execution history**

The history of the start and termination of the programs used on a managed device. The program execution history can be accessed from the **Program Execution History** job menu. If the system is linked with JP1/Software Distribution 07-50 or later, this information can be acquired from the operation history obtained by JP1/Software Distribution.

Program execution history data is organized into fields such as **login user**, **program name**, **program version**, and **issue date/time**.

**program start log**

An operation log in which data about program startup, program termination, and events that prevented program startup is collected. These operation logs are collected by JP1/Software Distribution.

**property**

An attribute of a class.

**role information**

Information used to manage the user roles in the asset management system. *Administrator* and *User* are set as the default user roles.

**route**

The order of workers that handle an Item.

An Item is processed sequentially along the defined route. Flow Designer is used to define an Item's route.

**search pattern**

Stored search conditions that are used to search operation logs in the Operation Log List window. Frequently used search patterns are registered as default patterns. You can edit the default search patterns that have been registered as well as register new search patterns.

**SNMP trap**

A message sent from an SNMP agent to an SNMP manager, such as HP NNM version 7.5 or earlier, in response to a specific trigger.

Asset Information Manager can acquire SNMP traps from JP1/IM as JP1 events.

### **software information**

Information about the software assets registered in an asset management system, such as commercial software, shareware, and freeware.

### **software key information**

Key information used to assign licenses to target devices and users. Software key information includes **Product ID**, **License key**, and **Serial No.**

### **task**

The processing contents that are combined when defining an activity, which is the processing executed when an Item is sent to the next worker.

For example, an activity for registering information about a newly installed device is defined by combining the **Add new device** and **Add network information** tasks.

Activity Designer is used to set the tasks for each activity.

### **updates**

Programs provided by Microsoft Update to fix specific system problems. Asset Information Manager links with a WSUS server to manage updates.

### **user information**

Information used to manage the users of the asset management system. User information includes fields such as **User name**, **Phone**, **E-mail**, and **Official title**.

### **user inventory information**

Information that can be optionally set by the user, such as user name and asset number. User inventory information is acquired by executing a job from the JP1/Software Distribution managing server.

In an asset management system, the user inventory information acquired by JP1/Software Distribution can be registered as asset information.

### **user library**

A library for sharing images among Items by uploading the images to the asset management server. Images must be added to the user library before they can be inserted in an Item window by Form Designer.

### **user report**

Work (job) added by the user, and the window used to execute that work. Asset Information Manager not only provides predefined job menus, but also enables the user to add user-specific jobs (user reports).

**virus definition information**

Information about the anti-virus software product installed on a device and about the virus definition files. The information includes fields such as **Anti-virus product name**, **Anti-virus product version**, and **Virus definition version**.

**volume contract information**

Information used to manage details about software volume licenses.

The volume license information includes fields such as **Software assets**, **Number of Target points**, **Contract date**, **Contract start date**, **Contract end date**, **Contracted company**, **Overview of contract**, and **Status**.

**window title update history**

Management information that summarizes historical data collected about window title changes performed on managed devices. The window title update history can be accessed from the **Window Title Update History** job menu. When the system is linked with JP1/Software Distribution 07-50 or later, this information can be obtained from the operation history acquired by JP1/Software Distribution.

Window title update history data is organized into fields such as **login user**, **program name**, **program version**, **issue date/time**, and **window title**.

**window title update log**

An operation log in which window title changes of updated windows are collected. These operation logs are collected by JP1/Software Distribution.

**worker**

A user who executes an Item. An Item is sent to individual workers according to a defined route.

**WSUS server**

The server that manages updates from Microsoft Update.





---

# Index

---

## A

- abbreviations for products iv
- access permission 101
- accessory 101
- acronyms vii
- Active Directory information in asset management database, including 87
- Active Directory services 101
- activity 74, 101
- administrator 101
- asset 102
- asset information 7, 102
  - status, adding 59
- Asset Information Manager 1, 2, 102
  - features of 4
  - license management by 18
  - procedure for stocktaking job 42
  - purpose of 2
  - stocktaking 41
  - usage of 29
- asset management database 7, 102
- asset management database server 102
- asset management server 102
- asset management system 2, 102
- association class 103

## C

- cabinet 103
- classes 103
- CN (Common Name) 103
- code ID 103
- computing 103
- concurrent execution license, managing 21
- confidential information file, checking if copied 75
- contract information 103
- conventions
  - abbreviations for products iv
  - acronyms vii

- diagrams ix

- fonts and symbols ix
- KB, MB, GB, and TB xi
- permitted characters xi
- version numbers xii

- corporate asset information, integrated management of 7
- Customize Job Windows 103

## D

- data files 104
- data files definition file 104
- DC (Domain Component) 104
- destination 104
- device catalog 104
- device change log 104
- device information
  - exporting 30
  - importing 30
  - importing from devices managed by another system 32
- diagram conventions ix
- division 105
- division group 105
- DN (Distinguished Name) 105

## E

- Embedded RDB 105
- event manager 105
- export 105
- export items, limiting for backups 35

## F

- file operation log 106
- font conventions ix
- form 106

**G**

GB meaning xi  
glossary 101  
group 106  
group information 106

**H**

hardware information 106  
HP NNM 106

**I**

import 106  
installed software information 107  
installed software list 107  
inventory information 5, 107  
IP address  
    managing usage statuses of 38  
    workflow for associating and managing in  
    groups 39  
IP group information 107  
IT asset 107  
item 23, 108  
    definition elements 73  
    options 74  
    window 73  
Item auditor 108  
item category 71, 108  
ITIL 108

**J**

job 108  
JP1 event 108  
JP1/Base 108  
JP1/CSC 109  
JP1/IM 109  
JP1/Software Distribution 109  
    not installed, machine on which 109, 110

**K**

KB meaning xi

**L**

LDAP (Lightweight Directory Access Protocol) 109  
license  
    determining whether handled legally 44  
    managing by assigning to device 19  
    managing by assigning to user 20  
license category 109  
license information 109  
license management, examples of 50  
    concurrent execution licenses 53  
    install licenses 50  
    pre-installed licenses 51  
    second licenses 53  
    server licenses 52  
    user licenses 51  
license type 109  
location information 110  
login authentication via linkage with Active  
Directory 85

**M**

machine on which JP1/Software Distribution is not  
installed 109, 110  
maintenance log 110  
managed item 110  
    adding 59  
managed label 110  
managed level 110  
management  
    per-license 18  
    total count 17  
management name 111  
MB meaning xi  
meta table 111

**N**

network information 111  
network manager 111  
Network Presenter 6, 111  
networking 111  
node 73, 111

**O**

object 112  
 object class 112  
 official authority 73, 112  
 operation log 112  
     determining status based on totals 78  
 OU (Organization Unit) 112

**P**

package 112  
 packaging 112  
 patch information 112  
 patch name list 113  
 PC startup log 113  
 permitted characters conventions xi  
 program execution history 113  
 program start log 113  
 property 113

**R**

role information 113  
 route 113

**S**

search pattern 113  
 second license, managing 21  
 SNMP trap 113  
 software information 114  
 software key information 114  
 symbol conventions ix  
 system data, importing into asset management  
 database 30

**T**

tasks 114  
 TB meaning xi

**U**

update 114  
     applying 56  
     verifying 56  
 user information 114

user inventory information 114  
 user library 114  
 user operations  
     checking by means of operation log 75  
     investigating 82  
     tracing 82  
 user report 114

**V**

version number conventions xii  
 virus definition information 115  
 volume contract information 115  
 volume license points, managing 22

**W**

window title update history 115  
 window title update log 115  
 windows, adding 59  
 worker 115  
 WSUS server 115  
     applying updates by linking to 55