

## **Job Management Partner 1/Client Security Control**

### **Description, User's Guide and Operator's Guide**

3020-3-S71-30(E)

## ■ Relevant program products

P-2642-1S97 Job Management Partner 1/Client Security Control - Manager 09-50 (for Windows Server 2003 and Windows Server 2008)

P-2642-1T97 Job Management Partner 1/Client Security Control - Agent 09-00 (for Windows Server 2003 and Windows Server 2008)

## ■ Trademarks

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

AntiVir is a registered trademark of Avira GmbH in the United States.

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

HP-UX is a product name of Hewlett-Packard Company.

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

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

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

Microsoft Internet Information Services is a product name of Microsoft Corporation

NetShield and VirusScan are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries.

OfficeScan and PC-Cillin are trademark of Trend Micro Incorporated.

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

ServerProtect is a trademark of Trend Micro Incorporated, registered in the U.S. and is a trademark in other countries.

Symantec is a U.S. registered trademark of Symantec Corporation.

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.

Windows Vista 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.

## ■ Microsoft product screen shots

Microsoft product screen shots reprinted with permission from Microsoft Corporation.

## ■ Restrictions

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

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

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

Printed in Japan.

## ■ Issued

December 2011: 3020-3-S71-30(E)

## ■ Copyright

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

Copyright, patent, trademark, and other intellectual property rights related to the "TMEng.dll" file are owned exclusively by Trend Micro Incorporated

## Summary of amendments

The following table lists changes in this manual (3020-3-S71-30(E)) and product changes related to this manual.

Changes	Location
The update information for an anti-virus product linked with automatic judgment policy updating for anti-virus products can now be acquired from a specified client.	1.2.7, 2.1, 2.3(1)(b), 3.1, 3.1(2), 3.1(3), 3.1(4), 3.2, 3.2(2), 4.1.1(2), 4.1.2(3), 4.3.1, 4.4.3, 4.6, 4.7.2(2), 5.1, 5.4.3, 5.5.2, 5.5.3, 5.5.3(2), 5.5.4, 6.4.6(1), 6.4.6(2), 12.2.1, 12.3.1(1), 12.4.1, 16.10.3(1), Appendix H
The following options have been added to the judgment policy update command ( <code>cscpolimport</code> ): <ul style="list-style-type: none"><li>The <code>-j</code> option, which specifies the name of a judgment policy to be imported</li><li>The <code>-f</code> option, which specifies the name of a policy import file containing information that is to be imported</li></ul> With these changes, the title <i>cscpolimport (updates settings for judgment policies relating to anti-virus products)</i> has been changed to <i>cscpolimport (updates settings for judgment policies)</i> in Chapter 15.	2.3(1), 6.1, 15. ( <i>cscpolimport</i> )
It is now possible to specify a MAC address in the PC Search window.	2.6(1), 8.2, 10.2.1
The following OSs have been added as OSs applicable to JP1/CSC: <ul style="list-style-type: none"><li>Windows Server 2008 R2</li><li>Windows 7</li></ul>	3.3(1), 3.3(2), 7.4(2), 12.3.2, 13.2.6(2)
F-Secure, McAfee, Symantec, and Trend Micro products have been added as anti-virus products for which judgment policies can be updated automatically.	4.6
Judgment items related to drive encryption by BitLocker have been added as judgment items related to PC security settings.	4.7.1(1), 4.7.2(5), 6.2.2, 6.7, 6.7.10, 8.3.5
A judgment condition for PC security settings has been changed so that whether the screensaver is password-protected is judged irrespective of the screensaver settings.	4.7.2(5)
A function that customizes the judgment results for an anti-virus product has been added.	5.4.3(1)

Changes	Location
The default value for initial environment setup for <b>Customize judgment results (security updates)</b> , which can be set in the Client Security Control - Manager Setup dialog box, has been changed to <b>Security level set for the judgment policy</b> .	5.4.3(1)
<b>Notification method</b> has been added as an item for setting the message notification method to be used for security level judgment in the Client Security Control - Manager Setup dialog box.	5.4.3(1)
It is now possible to change the email sender address to be used for the JP1/CSC email notification function.	5.4.3(1), 6.11.2(1), 9.4
A note applying when the OS is Windows Vista or Windows 7 has been added in the procedures for installing JP1/CSC - Manager Remote Option.	5.5.1(1), 5.5.1(2)
Windows 7 and Microsoft Internet Explorer 8.0 have been added as programs for which the automatic updating patch information is supported.	6.3.3(1)
A method for excluding a specific user account from password judgment has been added.	6.7.2
The <code>cscnwmaintenance</code> command can now delete a MAC address that is not registered in the AIM network information from the list of permitted devices for JP1/NM - Manager.	15. (List of commands), 15. (cscnwmaintenance)
The <code>cscpolexport</code> command, which outputs the specified judgment policy settings to a text file, has been added.	15. (List of commands), 15. (cscpolexport)
A function for deleting patch information that can be replaced with the latest cumulative patch information has been added to the <code>cscpatchupdate</code> command, which automatically updates patch information in judgment policies relating to security updates.	15. (cscpatchupdate)
The following definition files have been added: <ul style="list-style-type: none"> <li>Judgment policy information file</li> <li>Excluded user definition file</li> <li>Definition file of MAC addresses not subject to deletion</li> </ul>	16.1, 16.18, 16.19, 16.20
The following OSs have been added as OSs subject to judgment and action policies: <ul style="list-style-type: none"> <li>Windows Server 2008 R2</li> <li>Windows 7</li> </ul>	16.2.2(1), 16.11(2)



<b>Changes</b>	<b>Location</b>
The information output to the judgment result file (anti-virus products), which is a PC list information file, and the output conditions when multiple anti-virus products are installed on the client have been changed.	<i>16.10.3(1)</i>
The default values (the values used when no values have been set) of the following items to be set in the patch update condition file have been changed: <ul style="list-style-type: none"> <li>• Class</li> <li>• Security rating</li> <li>• Security level setting (critical)</li> <li>• Security level setting (important)</li> <li>• Security level setting (moderate)</li> </ul>	<i>16.11(2)</i>
The following messages have been added as JP1/CSC - Manager messages: KDSL0511-I, KDSL1130-I to KDSL1145-E, KDSL1500-I to KDSL1507-E, KDSL1600-I to KDSL1612-E, KDSL3032-I to KDSL3034-E	<i>17.2.1, 17.3.1(1), 17.3.1(2), 17.3.1(4)</i>
The following JP1/CSC - Manager message has been changed: KDSL1119-W	<i>17.3.1(2)</i>
Audit log information has been added to the files that must be backed up.	<i>18.4</i>
A sample file of an excluded user definition file has been added.	<i>Appendix A.4(10)</i>

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



---

# Preface

---

This manual explains how to set up and operate a system that manages client security. Such a system is referred to in this manual as a *client security control system*.

A client security control system consists of the following program products:

- Job Management Partner 1/Client Security Control (for client security management)
- Job Management Partner 1/Software Distribution (for software distribution and inventory management)
- Job Management Partner 1/Asset Information Manager (for integrated asset management) (optional product)

This manual primarily explains the functionality for Job Management Partner 1/Client Security Control. It also gives an overview of a client security control system, and explains linkages to other JP1 products and network control products. Read this manual before setting up a client security control system. In this manual, *Job Management Partner 1* is abbreviated to *JP1*. Hereafter in this manual, *Job Management Partner 1/Asset Information Manager* is referred to as *Asset Information Manager* or *AIM*.

## Intended readers

This manual is intended for administrators installing JP1/Client Security Control, and setting up and operating a client security control system.

Administrators are assumed to be familiar with the following:

- JP1/Software Distribution
- Asset Information Manager (optional product)
- Windows (Windows Server 2003 and Windows Server 2008)
- Linked network control products

## Organization of this manual

This manual consists of the following parts:

### *PART 1. Overview*

This part describes the features of a client security control system and typical ways in which it may be used.

## *PART 2. Functionality*

This part describes the functionality and system configuration of a client security control system.

## *PART 3. System Design and Setup*

This part describes factors to consider and the tasks involved from installation to operation of a client security control system. It also describes how to install and set up each program product, and how to edit security policies.

## *PART 4. System Operation*

This part describes how to operate a client security control system. It explains how to manage inventory information, monitor clients, handle security risks, conduct security audits, and link with JP1/Integrated Manager.

## *PART 5. Quarantine Systems*

This part describes the quarantine systems that can be implemented by linking JP1/Client Security Control with various program products.

## *PART 6. Reference*

This part describes the commands, definition files, and output messages of JP1/Client Security Control, and how to deal with any problems that may arise during the operation of your client security control system.

## **Related publications**

The following manuals are related to this manual. Read them as necessary.

For more information about how to set up and operate integrated asset management:

- *Job Management Partner 1/Asset Information Manager Description* (3020-3-S76(E))
- *Job Management Partner 1/Asset Information Manager Planning and Setup Guide* (3020-3-S77(E))
- *Job Management Partner 1/Asset Information Manager Administrator's Guide* (3020-3-S78(E))

For more information about how to set up and operate software distribution and inventory management:

- *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
- *Job Management Partner 1/Software Distribution SubManager* (3020-3-S85(E)), for UNIX Systems

For more information about JP1/IM linkage:

- *Job Management Partner 1/Integrated Management - Manager System Configuration and User's Guide* (3020-3-K01(E))
- *Job Management Partner 1/Integrated Management - Manager Reference* (3020-3-K02(E))
- *Job Management Partner 1/Base User's Guide* (3020-3-R71(E))

For more information about quarantine systems linked with JP1/Network Monitor:

- *Job Management Partner 1/Network Monitor Description, User's Guide and Operator's Guide* (3020-3-S73(E))
- *Job Management Partner 1/Network Monitor - Manager Description, User's Guide and Operator's Guide* (3020-3-S74(E))

## Conventions: Abbreviations for product names

This manual uses the following abbreviations for product names:

Abbreviation		Full name or meaning
Active Directory		Active Directory(R)
AIM	Asset Information Manager	Job Management Partner 1/Asset Information Manager
	Asset Information Manager Subset Component of JP1/Software Distribution Manager	Asset Information Manager Subset Component of Job Management Partner 1/Software Distribution Manager
AMT		Intel Active Management Technology
IE or Microsoft Internet Explorer		Microsoft(R) Internet Explorer(R)
		Windows(R) Internet Explorer(R)
JP1/CSC	JP1/CSC - Agent	Job Management Partner 1/Client Security Control - Agent
	JP1/CSC - Manager	Job Management Partner 1/Client Security Control - Manager

Abbreviation		Full name or meaning
	JP1/CSC - Manager Remote Option	Job Management Partner 1/Client Security Control - Manager Remote Option
JP1/IM	JP1/IM - Manager	Job Management Partner 1/Integrated Management - Manager
	JP1/IM - View	Job Management Partner 1/Integrated Management - View
JP1/NM	JP1/NM	Job Management Partner 1/Network Monitor
	JP1/NM - Manager	Job Management Partner 1/Network Monitor - Manager
JP1/Software Distribution	JP1/Software Distribution Client	Job Management Partner 1/Software Distribution Client
	JP1/Software Distribution Client (relay system)	Job Management Partner 1/Software Distribution Client(relay system)
	JP1/Software Distribution Manager	Job Management Partner 1/Software Distribution Manager
	JP1/Software Distribution SubManager	Job Management Partner 1/Software Distribution SubManager
MBSA		Microsoft(R) Baseline Security Analyzer
Microsoft IAS		Microsoft(R) Internet Authentication Service
Microsoft Internet Information Services		Microsoft(R) Internet Information Services
Microsoft Software Update Services		Microsoft(R) Software Update Services
MSCS or Microsoft Cluster Server		Microsoft(R) Cluster Server
NetMonitor	NetMonitor	Job Management Partner 1/CSC - Network Monitor
	NetMonitor/Manager	Job Management Partner 1/CSC - Network Monitor Manager
UNIX		UNIX(R)
Windows 2000 <sup>#</sup>	Windows 2000 Advanced Server	Microsoft(R) Windows(R) 2000 Advanced Server Operating System
	Windows 2000 Server	Microsoft(R) Windows(R) 2000 Server Operating System
Windows 7 <sup>#</sup>		Microsoft(R) Windows(R) 7 Enterprise
		Microsoft(R) Windows(R) 7 Professional

Abbreviation			Full name or meaning
			Microsoft(R) Windows(R) 7 Ultimate
Windows 95 <sup>#</sup>			Microsoft(R) Windows(R) 95 Operating System
Windows 98 <sup>#</sup>			Microsoft(R) Windows(R) 98 Operating System
Windows Me <sup>#</sup>			Microsoft(R) Windows(R) Millennium Edition Operating System
Windows NT <sup>#</sup>		Windows NT Server	Microsoft(R) Windows NT(R) Server Network Operating System Version 4.0
		Windows NT Workstation	Microsoft(R) Windows NT(R) Workstation Operating System Version 4.0
Windows Server 2003 <sup>#</sup>	Windows Server 2003	Windows Server 2003, Enterprise Edition	Microsoft(R) Windows Server(R) 2003, Enterprise Edition
		Windows Server 2003, Standard Edition	Microsoft(R) Windows Server(R) 2003, Standard Edition
	Windows Server 2003(x64)	Windows Server 2003, Enterprise x64 Edition	Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition
		Windows Server 2003, Standard x64 Edition	Microsoft(R) Windows Server(R) 2003, Standard x64 Edition
Windows Server 2008 <sup>#</sup>		Windows Server 2008 Datacenter	Microsoft(R) Windows Server(R) 2008 Datacenter
			Microsoft(R) Windows Server(R) 2008 R2 Datacenter
		Windows Server 2008 Enterprise	Microsoft(R) Windows Server(R) 2008 Enterprise
			Microsoft(R) Windows Server(R) 2008 R2 Enterprise
		Windows Server 2008 Standard	Microsoft(R) Windows Server(R) 2008 Standard
			Microsoft(R) Windows Server(R) 2008 R2 Standard
Windows Vista <sup>#</sup>		Windows Vista Business	Microsoft(R) Windows Vista(R) Business
		Windows Vista Enterprise	Microsoft(R) Windows Vista(R) Enterprise
		Windows Vista Ultimate	Microsoft(R) Windows Vista(R) Ultimate

Abbreviation		Full name or meaning
Windows XP <sup>#</sup>	Windows XP Home Edition	Microsoft(R) Windows(R) XP Home Edition Operating System
	Windows XP Professional	Microsoft(R) Windows(R) XP Professional Operating System
WUA		Windows(R) Update Agent

#

Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP, Windows 2000, Windows NT, Windows Me, Windows 98, and Windows 95 are referred to collectively as *Windows* when there are no functional differences between the operating systems.

## Conventions: Acronyms

This manual also uses the following acronyms:

Acronym	Full name or meaning
API	Application Program Interface
BCC	Blind Carbon Copy
CSV	Comma Separated Value
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
FD	Floppy Disc
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control
OS	Operating System
PC	Personal Computer
PDCA	Plan Do Check Action



Acronym	Full name or meaning
RADIUS	Remote Authentication Dial In User Service
SMTP	Simple Mail Transfer Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WWW	World Wide Web

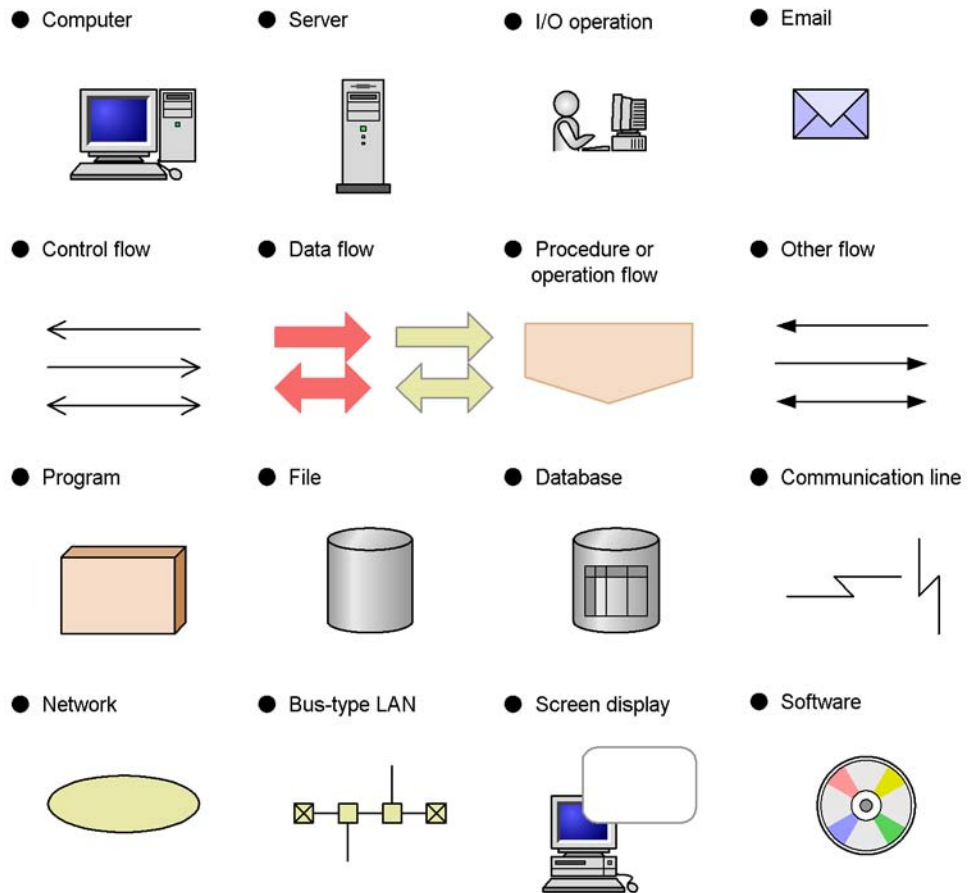
## Conventions: Date and time notation used in this manual

The following table gives definitions of the date and time format used in this manual.

Notation	Definition
<i>YYYY/MM/DD</i> or <i>YYYYMMDD</i>	Date expressed as year, month, and day ( <i>YYYY</i> : year; <i>MM</i> : month; <i>DD</i> : day)
<i>hh:mm:ss</i>	Time expressed as hour, minute, and second ( <i>hh</i> : hour; <i>mm</i> : minute; <i>ss</i> : second)
<i>YYYYMMDDhhmmssnnn</i> or <i>YYYYMMDDhhmmss.nnn</i>	Date and time expressed as year, month, day, hour, minute, second, and millisecond ( <i>YYYY</i> : year; <i>MM</i> : month; <i>DD</i> : day; <i>hh</i> : hour; <i>mm</i> : minute; <i>ss</i> : second; <i>nnn</i> : millisecond)

## Conventions: Diagrams

This manual uses the following conventions in diagrams:



## 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>

Font	Convention
<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: A B C 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: {A B C} 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: [A] means that you can specify A or nothing. [B C] 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.</p> <p>In syntax explanations, an ellipsis indicates that the immediately preceding item can be repeated as many times as necessary. For example: A, B, B, ... means that, after you specify A, B, you can specify B as many times as necessary.</p>

## 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: Structural elements used in this manual

The following table gives definitions of the types of structural elements (ranges for user-specified values) used in this manual.

Type	Definition
Numeric character	0 to 9
Alphanumeric character	A to Z, a to z, and 0 to 9
Symbol	! " # \$ % & ' ( ) + , - . / : ; < = > @ [ ] ^ _ { } ? Space character

Note: In Japanese systems, specify all characters as Hankaku characters.

## 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*.

## Default installation folders

This manual represents the default installation folders as follows.

Product name	Installation folder notation	Default installation folder <sup>#</sup>
JP1/CSC - Manager	<i>JP1/CSC - Manager-installation-folder</i>	<ul style="list-style-type: none"> <li>• For a 64-bit edition of Windows: C:\Program Files(x86)\HITACHI\jplnetmcscm</li> <li>• For other OSs C:\Program Files\HITACHI\jplnetmcscm</li> </ul>

Product name	Installation folder notation	Default installation folder <sup>#</sup>
JP1/CSC - Manager Remote Option	<i>JP1/CSC - Manager-Remote-Option-installation-folder</i>	<ul style="list-style-type: none"> <li>For a 64-bit edition of Windows: C:\Program Files(x86)\HITACHI\jplnetmcscm\remote</li> <li>For other OSs C:\Program Files\HITACHI\jplnetmcscm\remote</li> </ul>
JP1/CSC - Agent	<i>JP1/CSC - Agent-installation-folder</i>	<ul style="list-style-type: none"> <li>For a 64-bit edition of Windows: C:\Program Files(x86)\HITACHI\jplnetmcscsca</li> <li>For other OSs C:\Program Files\HITACHI\jplnetmcscsca</li> </ul>

#

Indicates the installation folder when the product is installed in the default location (when the drive on which the OS is installed is C:).



---

# Contents

---

<b>Preface</b>	<b>i</b>
Intended readers .....	i
Organization of this manual .....	i
Related publications .....	ii
Conventions: Abbreviations for product names .....	iii
Conventions: Acronyms .....	vi
Conventions: Date and time notation used in this manual .....	vii
Conventions: Diagrams .....	vii
Conventions: Fonts and symbols.....	viii
Conventions: KB, MB, GB, and TB .....	ix
Conventions: Structural elements used in this manual.....	x
Conventions: Version numbers.....	x
Default installation folders .....	x

## **PART 1: Overview**

<b>1. Overview</b>	<b>1</b>
1.1 Client security control system overview .....	2
1.2 Client security control system features.....	4
1.2.1 Integrated management of information about IT assets .....	4
1.2.2 Judgment of client security levels .....	6
1.2.3 Implementation of actions appropriate to security level .....	7
1.2.4 Security audit of clients.....	8
1.2.5 Viewing trends in security measures .....	10
1.2.6 Automatic update of security policies relating to security updates.....	11
1.2.7 Automatic update of security policies relating to anti-virus products .....	12
1.2.8 Building and running a quarantine system by linking with a network control product .....	13
1.2.9 Linkage with JP1/IM.....	14
1.3 Typical uses of a client security control system .....	16
1.3.1 Send warning messages to clients with inadequate security .....	16
1.3.2 Denying network connections to clients with inadequate security .....	18
1.3.3 Distributing the latest security update programs and definition files to clients with inadequate security .....	20
1.3.4 Creating a list of clients with inadequate security.....	22
1.3.5 Viewing a history of judgments and actions for a specific client.....	23
1.3.6 Outputting PC list information to a file .....	25

1.3.7 Implementing actions after all security level judgments have been made ...	27
1.3.8 Gauge trends in security countermeasure statuses .....	29
1.3.9 Gauge trends in countermeasure usage for user-defined judgment items ....	32
1.4 Work flow from installation to starting operation.....	36

## **PART 2: Functionality**

<b>2. Client Security Control System Functionality</b>	<b>37</b>
2.1 Overview of functionality .....	38
2.2 Managing inventory information .....	41
2.3 Managing security policies .....	43
2.4 Judging security levels .....	51
2.5 Implementing actions .....	54
2.5.1 Implementing an action as a result of security level judgment .....	54
2.5.2 Implementing an action as a result of administrator instructions .....	55
2.6 Managing client security levels .....	58
<b>3. Client Security Control System Configuration</b>	<b>63</b>
3.1 System configuration .....	64
3.2 Product configuration .....	77
3.3 Prerequisite programs .....	80

## **PART 3: System Design and Setup**

<b>4. Considerations for Installing and Operating a Client Security Control System</b>	<b>83</b>
4.1 Design considerations and system configuration.....	84
4.1.1 Items to consider for system installation .....	84
4.1.2 Designing a system configuration .....	86
4.1.3 Operating on a cluster system.....	90
4.2 Setting up a management server .....	92
4.2.1 Procedures for program setup.....	92
4.2.2 Setting up a database .....	92
4.2.3 Setting up a management terminal .....	92
4.3 Setting up a remote management server .....	94
4.3.1 Anti-virus products .....	94
4.4 Setting up a client .....	95
4.4.1 Functionality limitations by the version of JP1/Software Distribution Client .....	95
4.4.2 MBSA or WUA .....	96
4.4.3 Anti-virus products .....	97
4.5 Setting up a quarantine system .....	98



4.6	Installing anti-virus products that link with automatic judgment policy updating...	99
4.7	Considerations for security policies .....	104
4.7.1	Guides for security level judgment standards .....	104
4.7.2	Considerations for judgment policies.....	107
4.7.3	Considerations for action policies .....	111
4.7.4	Considerations for assigning security policies to clients .....	119
4.8	Lifecycle of a client security control system .....	122
<b>5.</b>	<b>Installation and Setup</b>	<b>125</b>
5.1	Procedures for installation and setup.....	126
5.2	Installing and setting up JP1/Software Distribution Manager.....	129
5.2.1	Installing JP1/Software Distribution Manager.....	129
5.2.2	Setting up JP1/Software Distribution Manager.....	129
5.3	Installing and setting up Asset Information Manager (optional).....	133
5.3.1	Installing Asset Information Manager.....	133
5.3.2	Setting up Asset Information Manager .....	133
5.4	Installing and setting up JP1/CSC - Manager.....	135
5.4.1	Installing JP1/CSC - Manager.....	135
5.4.2	Uninstalling JP1/CSC - Manager .....	138
5.4.3	Setting up JP1/CSC - Manager.....	139
5.4.4	Setting up JP1/CSC - Manager and the remote service to start automatically .....	156
5.5	Installing and setting up JP1/CSC - Manager Remote Option .....	158
5.5.1	Installing JP1/CSC - Manager Remote Option .....	158
5.5.2	Uninstalling JP1/CSC - Manager Remote Option.....	162
5.5.3	Setting up JP1/CSC - Manager Remote Option .....	162
5.5.4	Setting up the virus definition information monitoring service to start automatically .....	168
5.6	Installing and setting up JP1/Software Distribution Client .....	170
5.7	Installing and setting up JP1/CSC - Agent .....	171
5.7.1	Installing JP1/CSC - Agent .....	171
5.7.2	Uninstalling JP1/CSC - Agent.....	173
5.7.3	Setting up JP1/CSC - Agent.....	173
5.7.4	Setting up JP1/CSC - Agent to start automatically .....	173
5.8	Creating CSC administrators and CSC users .....	174
5.8.1	Setting up CSC administrators during installation.....	176
5.8.2	Creating a CSC user .....	179
5.8.3	Preventing update processing for detailed device information .....	189
5.9	Procedures for setting a task in Scheduled Tasks .....	192
<b>6.</b>	<b>Managing Security Policies</b>	<b>197</b>
6.1	Procedures and window transitions for policy settings .....	198
6.2	Managing judgment policies .....	205
6.2.1	Creating a judgment policy .....	207

6.2.2	Editing a judgment policy.....	209
6.2.3	Deleting a judgment policy.....	213
6.2.4	Renaming a judgment policy .....	213
6.2.5	Copying a judgment policy.....	214
6.3	Editing a security update judgment policy .....	216
6.3.1	Performing judgment by the latest security updates.....	220
6.3.2	Performing judgment by a specified security update .....	226
6.3.3	Automatically updating judgment policies for security updates .....	243
6.4	Editing an anti-virus product judgment policy .....	247
6.4.1	Adding anti-virus product information.....	250
6.4.2	Changing anti-virus product information .....	252
6.4.3	Deleting anti-virus product information .....	253
6.4.4	Importing anti-virus product information.....	254
6.4.5	Exporting anti-virus product information.....	255
6.4.6	Updating judgment policies for anti-virus products automatically or manually .....	256
6.5	Editing a prohibited software judgment policy.....	262
6.5.1	Adding prohibited software information .....	264
6.5.2	Changing prohibited software information.....	265
6.5.3	Deleting prohibited software information .....	266
6.5.4	Importing prohibited software information .....	267
6.5.5	Exporting prohibited software information .....	268
6.6	Editing a mandatory software judgment policy .....	270
6.6.1	Adding mandatory software information .....	274
6.6.2	Changing mandatory software information.....	278
6.6.3	Deleting mandatory software information.....	280
6.6.4	Importing mandatory software information .....	281
6.6.5	Exporting mandatory software information .....	282
6.7	Editing a PC security setting judgment policy.....	284
6.7.1	Defining account settings .....	286
6.7.2	Defining password settings.....	288
6.7.3	Defining logon settings.....	292
6.7.4	Defining share settings .....	294
6.7.5	Defining anonymous connection settings.....	296
6.7.6	Defining service settings .....	298
6.7.7	Defining firewall settings .....	300
6.7.8	Defining automatic update settings .....	302
6.7.9	Defining screensaver settings .....	304
6.7.10	Defining drive encryption.....	307
6.8	Editing a user-defined judgment policy .....	309
6.8.1	Adding a judgment item to a user definition .....	311
6.8.2	Changing a judgment item in a user definition.....	327
6.8.3	Deleting a judgment item in a user definition .....	329
6.8.4	Importing user-defined judgment items.....	330

6.8.5	Exporting user-defined judgment items .....	330
6.9	Managing action policies.....	332
6.9.1	Creating an action policy.....	334
6.9.2	Editing an action policy.....	336
6.9.3	Deleting an action policy.....	339
6.9.4	Renaming an action policy .....	339
6.9.5	Copying an action policy.....	340
6.10	Setting an action for each security level.....	342
6.10.1	Setting an action for a security level in the Edit Action Policy window ..	342
6.10.2	Command execution for user-defined actions .....	351
6.11	Editing an administrator notification email .....	353
6.11.1	Editing email in the Edit Action Policy (Customize Email) window .....	353
6.11.2	Email sender address and transmission unit.....	359
6.12	Editing a client user notification message .....	362
6.12.1	Editing messages in the Edit Action Policy (Customize Message) window.....	362
6.12.2	Checking the execution results of message notification jobs.....	373
6.13	Assigning security policies to clients .....	374
6.14	Displaying clients that meet specified conditions .....	379

## **PART 4: System Operation**

<b>7. Managing Inventory Information</b>	<b>385</b>
7.1 Managing inventory information.....	386
7.1.1 Inventory information used on a client security control system .....	388
7.1.2 Detecting non-Software Distribution clients.....	389
7.1.3 Automatically collecting inventory information .....	389
7.1.4 Detecting unapplied security updates.....	389
7.2 Detecting non-Software Distribution clients .....	390
7.2.1 Using the JP1/Software Distribution host search to detect non-Software Distribution clients.....	390
7.2.2 Excluding non-Windows machines from detection .....	390
7.3 Automatically obtaining client inventory information .....	392
7.3.1 Setup methods .....	392
7.3.2 Notification timing for inventory information .....	393
7.3.3 Precautions .....	394
7.4 Detecting security updates not applied to a client .....	396
<b>8. Monitoring Clients</b>	<b>399</b>
8.1 Transitions of windows used for client monitoring .....	400
8.2 Searching for clients .....	402
8.3 Checking detailed information for a client .....	412
8.3.1 Checking detailed information for a security update .....	413

8.3.2	Checking detailed information for an anti-virus product .....	416
8.3.3	Checking detailed information for prohibited software .....	418
8.3.4	Checking detailed information for mandatory software.....	420
8.3.5	Checking detailed information for PC security settings.....	422
8.3.6	Checking detailed information for a user definition.....	424
8.3.7	Checking device details for a client.....	426
8.3.8	Checking history of judgments and actions for a client .....	426
8.4	Judging a client security level.....	431
8.5	Enabling and disabling security management for a client .....	432
8.5.1	Disabling security management.....	432
8.5.2	Enabling security management.....	433
8.6	Outputting history of judgments and actions as a CSV file.....	434
<b>9.</b>	<b>Dealing with Security Risks</b> .....	<b>437</b>
9.1	Action implementation methods and action types .....	438
9.1.1	Action implementation methods.....	438
9.1.2	Action types.....	439
9.2	Sending messages to client users .....	440
9.2.1	Message notification by action policy .....	440
9.2.2	Message notification by administrator .....	440
9.2.3	Example of a notification message to a client user .....	442
9.3	Controlling client network connections .....	445
9.3.1	Network connection control by action policy.....	445
9.3.2	Network connection control by administrator .....	445
9.4	Sending email to administrators .....	448
9.5	Executing user-defined actions .....	449
<b>10.</b>	<b>Auditing Security</b> .....	<b>451</b>
10.1	Transitions of windows used for auditing security .....	452
10.2	Outputting search results of clients to a file .....	453
10.2.1	Outputting search results as a CSV .....	453
10.3	Evaluating the status of security measures on clients.....	457
10.3.1	Searching for the evaluation results of the status of security measures ...	458
10.3.2	Outputting results of estimation to a CSV file .....	465
10.4	Gauging trends in security measure evaluation .....	469
10.4.1	Storing statistics.....	470
10.4.2	Searching statistics .....	471
10.4.3	Outputting statistics to a CSV file .....	480
10.4.4	Displaying statistics as a graph.....	485
<b>11.</b>	<b>Linking to JP1/IM</b> .....	<b>493</b>
11.1	Linking to JP1/IM .....	494
11.1.1	Example system configuration .....	494
11.1.2	Setting up JP1/IM linkage .....	494

11.1.3 Displaying JP1/IM integrated console windows .....	495
---	-----

## **PART 5: Quarantine Systems**

### **12. Overview of Quarantine Systems** 497

12.1 About quarantine systems.....	498
12.1.1 Network control products that can link to JP1/CSC .....	500
12.1.2 Quarantine system overview by linked product.....	501
12.2 Quarantine system linked to JP1/NM.....	509
12.2.1 Basic configuration of quarantine system linked to JP1/NM.....	509
12.2.2 Required products and prerequisite OSs .....	512
12.3 Quarantine system linked to an authentication server.....	515
12.3.1 Configuration of a quarantine system linked to an authentication server.....	515
12.3.2 Required products and prerequisite OSs .....	522
12.4 Quarantine system linked to JP1/Software Distribution (AMT Linkage facility).....	524
12.4.1 Basic configuration of quarantine system linked to JP1/Software Distribution (AMT Linkage facility) .....	524
12.4.2 Required products and prerequisite OS.....	526

### **13. Setting Up a Quarantine System** 529

13.1 Setting up a quarantine system linked to JP1/NM.....	530
13.1.1 Flow of system setup.....	530
13.1.2 Setting up a network control server.....	532
13.1.3 Setting up a treatment or monitoring server.....	540
13.1.4 Setting up a client.....	541
13.1.5 Setting up the environment for operation.....	541
13.2 Setting up a quarantine system linked to an authentication server.....	545
13.2.1 Flow of system setup.....	545
13.2.2 Setting up an authentication server .....	547
13.2.3 Setting up the network control device (dynamic VLAN environment) ....	557
13.2.4 Setting up the network control device (static VLAN environment) .....	560
13.2.5 Setting up a treatment server .....	563
13.2.6 Setting up a client.....	563
13.2.7 Setting up the environment before operation can be started .....	567
13.3 Setting up a quarantine system linked to JP1/Software Distribution (AMT Linkage facility) .....	572
13.3.1 Flow of system setup.....	572
13.3.2 Setting up a management and network control server .....	572
13.3.3 Setting up a treatment server .....	576
13.3.4 Setting up the environment for operation.....	576

### **14. Operating a Quarantine System** 579

14.1 Operating a quarantine system linked to JP1/NM.....	580
--	-----

14.1.1	Example of quarantine system operation using the JP1/NM quarantine support facility.....	580
14.1.2	Operation without the JP1/NM quarantine support facility.....	587
14.1.3	Tasks during operation of a quarantine system linked to JP1/NM .....	592
14.1.4	Implementing client security measures .....	593
14.1.5	Adding new clients to the network.....	595
14.1.6	Registering permitted PCs.....	596
14.1.7	Removing a client after operation has started .....	600
14.2	Operating a quarantine system linked to an authentication server .....	603
14.2.1	Example of operating a quarantine system linked to an authentication server in a dynamic VLAN environment (IEEE 802.1X authentication) .....	603
14.2.2	Example of operating a quarantine system linked to an authentication server in a static VLAN environment (MAC authentication).....	618
14.2.3	Tasks during operation of a quarantine system linked to an authentication server .....	632
14.2.4	Managing the connection control list .....	634
14.2.5	Implementing security measures on a client.....	638
14.2.6	Adding a new client to the network.....	639
14.2.7	Removing clients after operation has started.....	643
14.2.8	Managing network connection histories for clients.....	645
14.3	Operating a quarantine system linked to JP1/Software Distribution (AMT Linkage facility).....	648
14.3.1	Example of quarantine system operation linked to JP1/Software Distribution (AMT Linkage facility).....	648
14.3.2	Tasks during operation of a quarantine system linked to JP1/Software Distribution (AMT Linkage facility).....	654
14.3.3	Implementing client security measures .....	655
14.3.4	Adding new clients to the network.....	655
14.3.5	Removing a client after operation has started .....	655

## PART 6: Reference

<b>15. Commands</b>	<b>659</b>
List of commands.....	660
Command details .....	662
cscaction (implements actions for a specified client) .....	664
cscassign (assigns security policies to clients) .....	667
cscexportcount (outputs statistics on the status of security measures) .....	669
cscexportplist (outputs PC list information) .....	674
cscjudge (judges security levels) .....	678
cscnetctrl (controls network connections) .....	681
cscnwmaintenance (maintains a list of permitted devices).....	684

cscpatchupdate (updates patch information for judgment policies relating to security updates).....	686
cscpolexport (exports judgment policies).....	690
cscpolimport (updates judgment policy settings).....	692
cscrdelete (deletes information about a specified client from the connection control list).....	695
cscrexport (exports a connection control list).....	697
cscrimport (imports a connection control list).....	699
cscsetup (sets up JP1/CSC - Manager).....	700
cscstorecount (stores statistics about the status of security measures).....	701
Command used in a user-defined action.....	703

## **16. Definition Files** 705

---

16.1 List of definition files .....	706
16.2 Judgment policy definition files .....	709
16.2.1 Import destination of judgment policy definition files.....	709
16.2.2 List of setting values .....	710
16.2.3 Definition file of excluded security updates .....	715
16.2.4 Definition file for mandatory security updates .....	716
16.2.5 Definition file for mandatory service packs.....	718
16.2.6 Anti-virus products definition file .....	720
16.2.7 Prohibited software definition file.....	722
16.2.8 Mandatory software definition file.....	723
16.2.9 User definition file .....	724
16.3 Mail address definition file.....	728
16.4 Product name definition file .....	729
16.5 Asset number file.....	731
16.6 Search condition file.....	732
16.7 Policy assignment definition file .....	734
16.8 Asset information file .....	737
16.9 Judgment result file for security level .....	739
16.9.1 Judgment result (summary) file.....	740
16.9.2 Judgment result (security updates) file.....	742
16.9.3 Judgment result (anti-virus product) file.....	744
16.9.4 Judgment result (prohibited software) file .....	746
16.9.5 Judgment result (mandatory software) file.....	747
16.9.6 Judgment result (user definition) file .....	748
16.9.7 Judgment result (PC security settings) file.....	749
16.10 PC list information file .....	751
16.10.1 Asset information list file.....	752
16.10.2 Judgment result file (security updates).....	755
16.10.3 Judgment result file (anti-virus products) .....	756
16.10.4 Judgment result file (prohibited software) .....	758
16.10.5 Judgment result file (mandatory software).....	759

16.10.6	Judgment result file (user definition).....	760
16.10.7	Judgment result file (PC security settings).....	761
16.11	Patch update condition file.....	763
16.12	Statistics output file.....	769
16.12.1	Evaluation point file .....	770
16.12.2	Countermeasure usage file.....	771
16.12.3	Countermeasure usage details file .....	772
16.12.4	Countermeasure usage file for user-defined judgment items .....	775
16.13	Anti-virus product policy import file .....	777
16.14	Policy import execution file (manual) .....	779
16.15	Network connection control list file .....	780
16.16	Import file .....	782
16.17	MAC address list file .....	784
16.18	Judgment policy information file.....	786
16.19	Excluded user definition file .....	801
16.20	Definition file of MAC addresses not subject to deletion .....	803
<b>17.</b>	<b>Messages</b>	<b>805</b>
17.1	Format of messages .....	806
17.1.1	Format of output messages .....	806
17.1.2	Format of message explanations.....	806
17.2	List of output destinations of messages .....	808
17.2.1	Output destinations of JP1/CSC - Manager messages.....	808
17.2.2	Output destinations of JP1/CSC - Manager Remote Option messages ....	822
17.2.3	Output destinations of JP1/CSC - Agent messages .....	824
17.3	List of JP1/CSC messages .....	829
17.3.1	List of JP1/CSC - Manager messages.....	829
17.3.2	List of JP1/CSC - Manager Remote Option messages .....	921
17.3.3	List of JP1/CSC - Agent messages .....	932
17.4	List of messages in the Client Security Management window .....	952
17.4.1	Action messages in the PC List window .....	952
17.4.2	Error messages in the PC Security Level Details window .....	956
17.4.3	Messages in the Register Permitted PCs window .....	962
17.4.4	Error message in the Evaluation Result List window.....	963
17.4.5	Error message in the Statistics List window.....	963
17.4.6	Error message in the Statistics Graph Display window.....	963
17.4.7	Error message in the Statistics Details window.....	964
17.4.8	Error message in the Statistics Details Graph Display window .....	964
<b>18.</b>	<b>Troubleshooting</b>	<b>965</b>
18.1	Troubleshooting procedure .....	966
18.2	Data that must be collected if a problem occurs .....	967
18.2.1	Data for resolving problems in JP1/CSC - Manager .....	967
18.2.2	Data for resolving problems in JP1/CSC - Manager Remote Option.....	967



18.2.3 Data for resolving problems in JP1/CSC - Agent .....	968
18.2.4 Data for resolving problems in JP1/Software Distribution and AIM.....	968
18.3 Common problems and their solutions .....	970
18.4 Backup and restoration .....	972

<b>Appendixes</b>	<b>975</b>
-------------------	------------

---

A. List of Files .....	976
A.1 List of files for JP1/CSC - Manager .....	976
A.2 List of files for JP1/CSC - Manager Remote Option .....	976
A.3 List of files for JP1/CSC - Agent .....	976
A.4 List of sample definition files.....	977
B. List of Port Numbers.....	987
B.1 Port numbers.....	987
B.2 Direction in which data passes through the firewall.....	987
C. List of Processes .....	988
D. Operation on a Cluster System .....	989
D.1 Cluster system overview .....	989
D.2 Prerequisites and supported operations .....	991
D.3 Installing and setting up JP1/CSC - Manager .....	993
D.4 Performing an overwrite installation of JP1/CSC - Manager.....	997
D.5 Uninstalling JP1/CSC - Manager .....	999
D.6 Installing and setting up JP1/CSC - Agent .....	1001
D.7 Performing an overwrite installation of JP1/CSC - Agent .....	1005
D.8 Uninstalling JP1/CSC - Agent.....	1006
D.9 Operation during failover .....	1008
E. Estimating Required Disk Capacity .....	1011
E.1 Disk capacity used by JP1/CSC - Manager .....	1011
E.2 Disk capacity used by JP1/CSC - Manager Remote Option.....	1014
E.3 Disk capacity used by JP1/CSC - Agent.....	1015
F. Audit Log Output.....	1017
F.1 Event types output to the audit log.....	1017
F.2 Audit log save format.....	1018
F.3 Audit log output format.....	1019
F.4 Configuration for outputting audit logs.....	1024
G. Version Changes.....	1026
H. Glossary .....	1035

<b>Index</b>	<b>1045</b>
--------------	-------------

---



## **Chapter**

---

# **1. Overview**

---

This chapter describes the features of a client security control system and typical ways in which it may be used.

- 1.1 Client security control system overview
- 1.2 Client security control system features
- 1.3 Typical uses of a client security control system
- 1.4 Work flow from installation to starting operation

---

## 1.1 Client security control system overview

---

With the recent advances in IT and trends toward open networks, problems in information security management such as sensitive information leaks and computer virus infections are having a profound impact on corporate management. More than ever, efforts to bolster information security are an important issue in the corporate community.

While acting to secure information security is critical to maintaining business activities, corporations are encountering the following problems in developing information security measures:

- Integrated management of the company's information of IT assets (network information, hardware information, and software information) is difficult to perform.
- Network-wide safety cannot be obtained, because client users have little knowledge about security.
- It is difficult to accurately assess the status of security measures on clients.
- Leaks due to smuggled information and missing computers are unavoidable.
- Responses to continuing information security problems are often not in time.

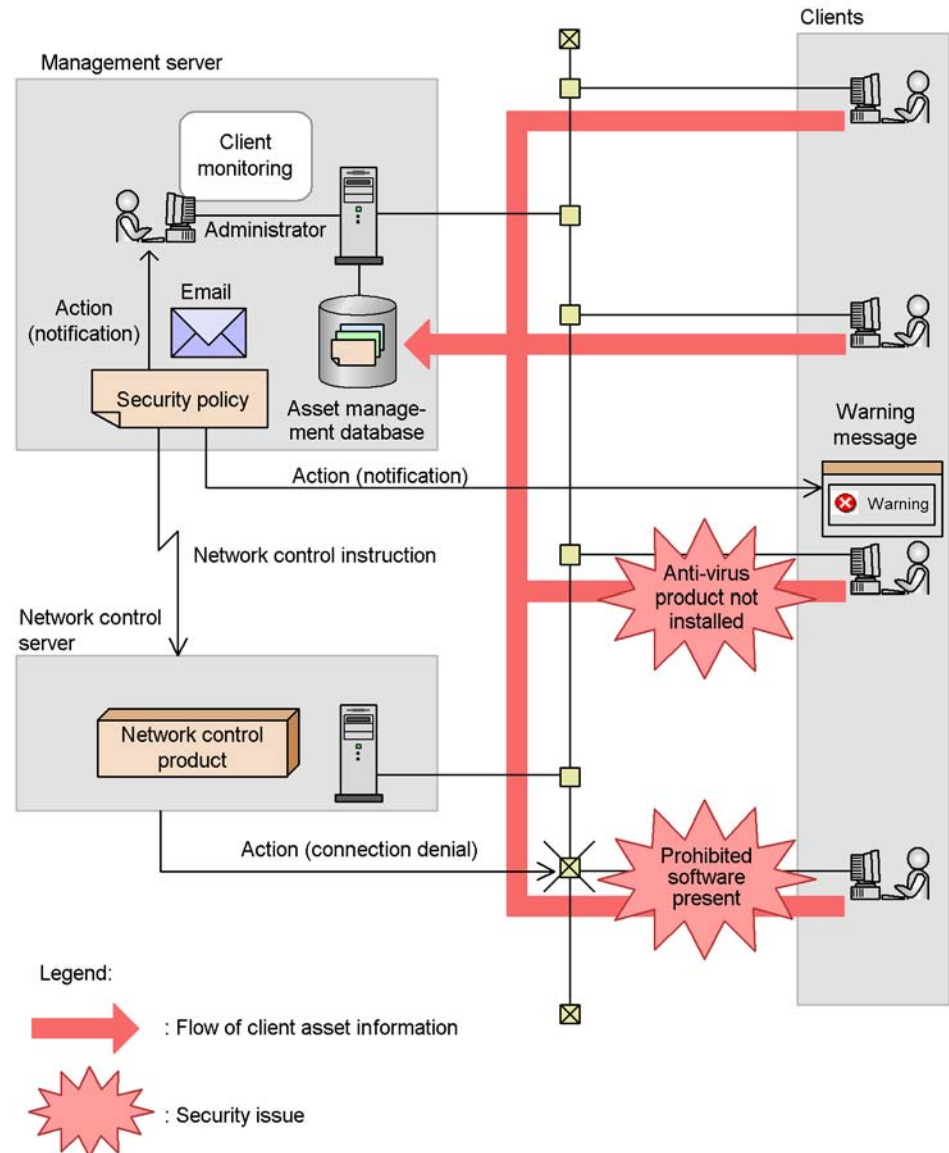
To solve these problems, it is important to first completely assess the company's information of IT assets, automatically eliminate any vulnerabilities of clients connected to the network, and implement a variety of risk prevention measures for information security. Also, it is important to constantly evaluate and improve corporate information security measures, to respond to the daily changes in security risks.

A *client security control system* provides overall security management based on the information security measure, from management of client asset information and client monitoring through to dealing with security risks.

By using a client security control system, an administrator can use centrally managed client asset information to monitor the status of client security measures in real-time. The administrator can also judge the security level, implementing actions such as warning message notification and denying network connections to clients with inadequate security measures.

The following figure shows an overview of a client security control system.

Figure 1-1: Overview of a client security control system



---

## 1.2 Client security control system features

---

The features of a client security control system are as follows:

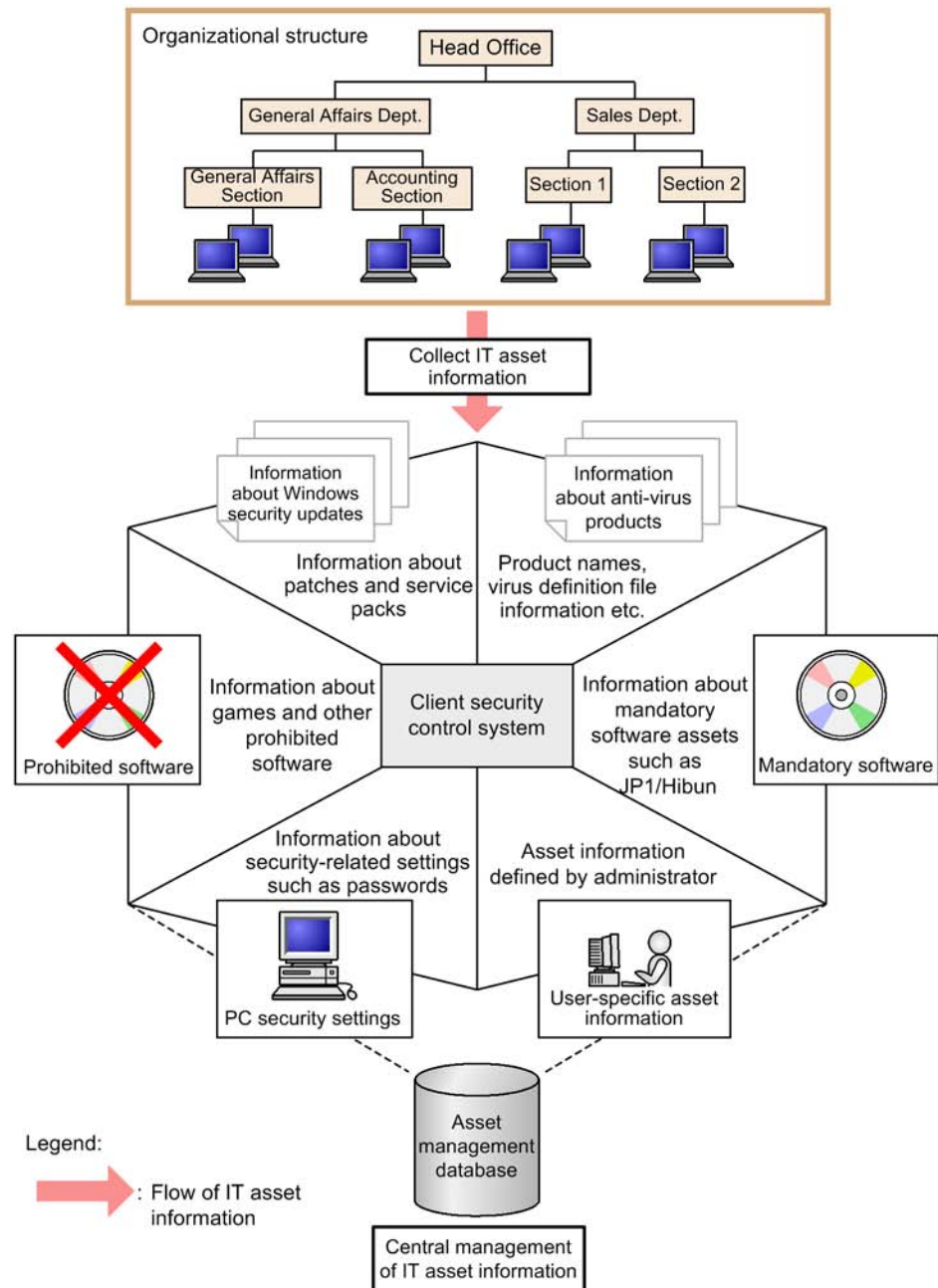
### 1.2.1 Integrated management of information about IT assets

The ability to accurately assess the information about IT assets distributed within a company is a fundamental part of implementing security measures. With a client security control system, information about software and anti-virus products installed on clients can be collected to a management server, and managed centrally. An administrator can use this information to assess the status of security measures on a client, and respond quickly to any security issues.

A client security control system that centrally manages asset information uses the following strategies to solve security problems:

- By collecting information about the Windows security updates such as patches and service packs applied to clients, unauthorized access that exploits vulnerabilities in Windows components can be prevented.
- By collecting information about the anti-virus products installed on the client and whether the latest virus definitions and version of the virus detection engine have been applied, virus infection can be prevented.
- By collecting information about whether games and other prohibited software are installed on clients, security issues that arise from the use of such prohibited software can be prevented.
- The client security control system can manage information about whether mandatory software designated by the administrator is installed on the client. For example, by specifying software designed to prevent information leakage as mandatory software, the administrator can prevent data from being compromised.
- By collecting PC security information such as account and password settings, the client security control system can prevent the security level from being compromised by users leaving guest accounts or choosing weak passwords.
- By collecting information about specific assets defined by the administrator, the client security control system can prevent security issues that are associated with those assets.

Figure 1-2: Integrated management of information about IT assets



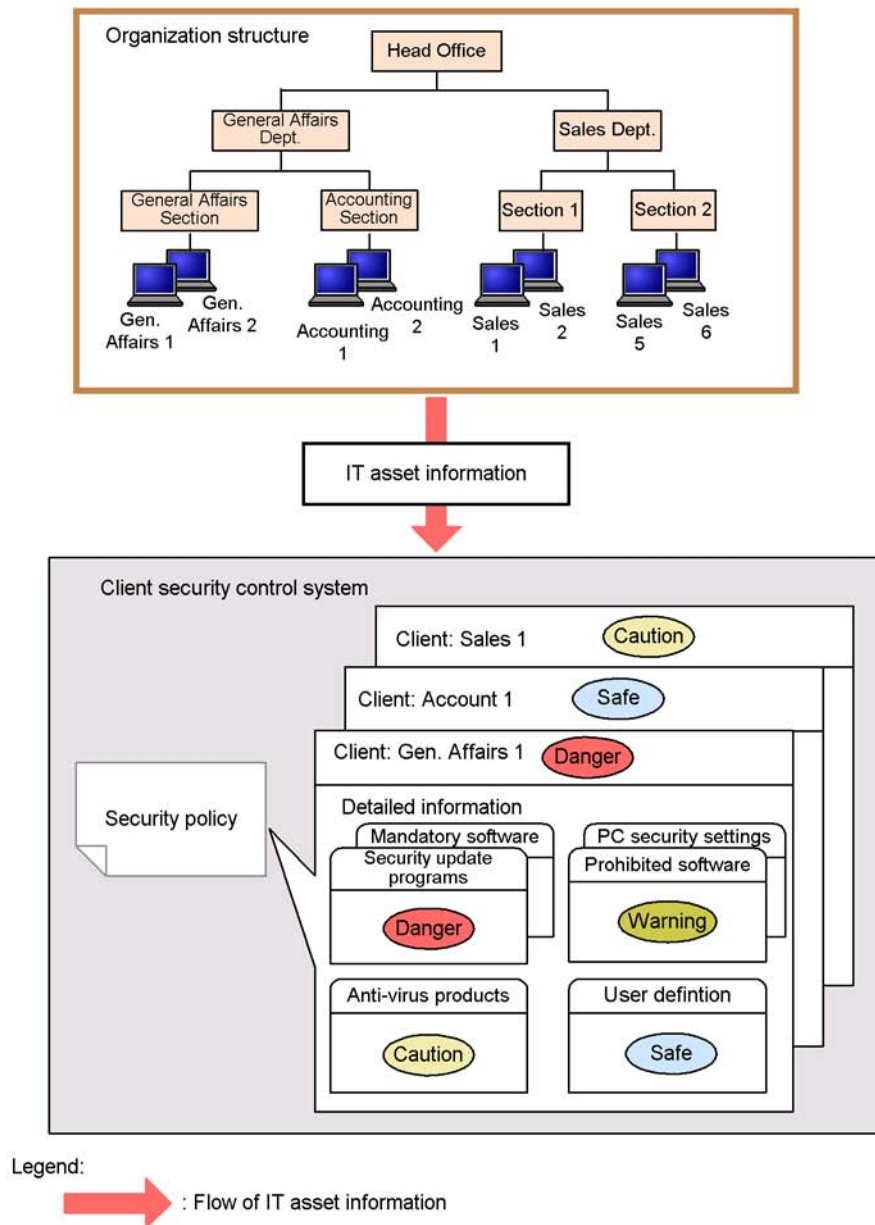
## 1.2.2 Judgment of client security levels

The status of security measures on a client can be judged by the client's security level. An administrator sets a security policy to judge the security level of a client, based on each item already used for judging client security levels. When information about software and anti-virus products is updated on a client, the security policy is used to automatically judge the client's security level. In addition to being displayed in a window, the judgment result can be output to a CSV file. Furthermore, the asset information and judgment result for a client can be output to a CSV file as PC list information based on the date and time that the security level was judged.

There are four kinds of security level: Danger, Warning, Caution, and Safe.



Figure 1-3: Judgment of client security levels



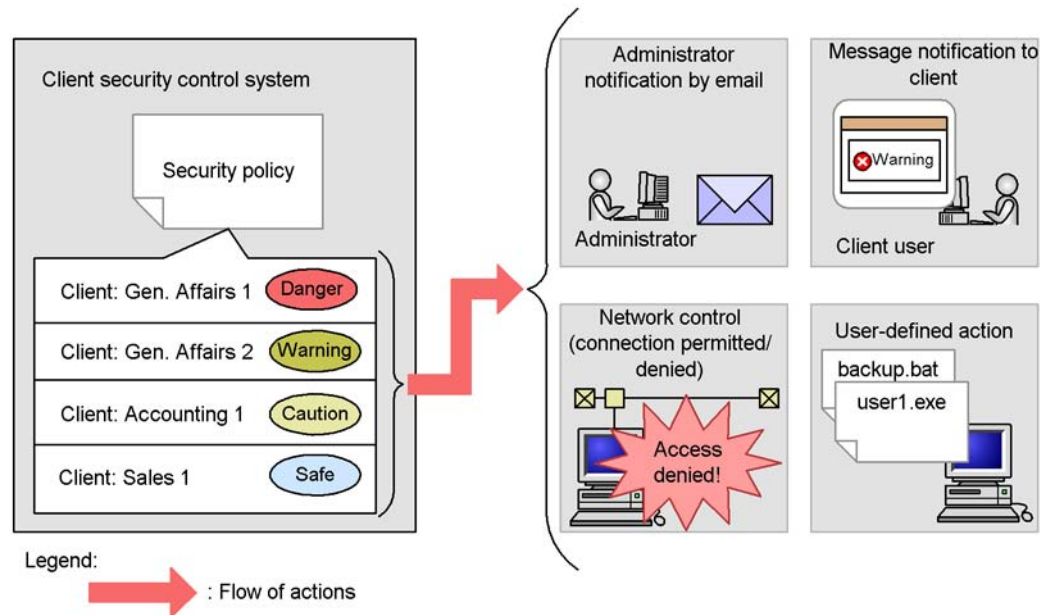
### 1.2.3 Implementation of actions appropriate to security level

A security policy can be used to set what kind of action is to be implemented for a client with a given security level. When a client with inadequate security measures is

detected, an action appropriate to the security level is automatically implemented based on the security policy. Actions that can be implemented include sending a warning message to the user of the client, or linking with the network control product to deny a network connection.

An action can be implemented as soon as a security level has been judged. It is also possible to implement actions independently based on the result of the latest security level judgment.

Figure 1-4: Implementation of actions appropriate to the security level



#### 1.2.4 Security audit of clients

The status of security measures on each client can be checked, and the status of security measures on each user or group can be evaluated on the basis of points awarded for security measures taken. Information for each client and the evaluation results of security measures on each user or group can be output to a CSV file, as well as displayed in a window. An administrator can easily find and audit a client for whom security measures have not been taken.

Figure 1-5: Security audit of clients

Results of security measure evaluations

CSV file

```
"Asset No.", "Host name", "PC security level"
"1000000004", "Gen. Affairs 1", "Danger"
"1000000005", "Gen. Affairs 2", "Caution"
"1000000006", "Accounting 1", "Safe"
"1000000007", "Sales 5", "Warning"
```

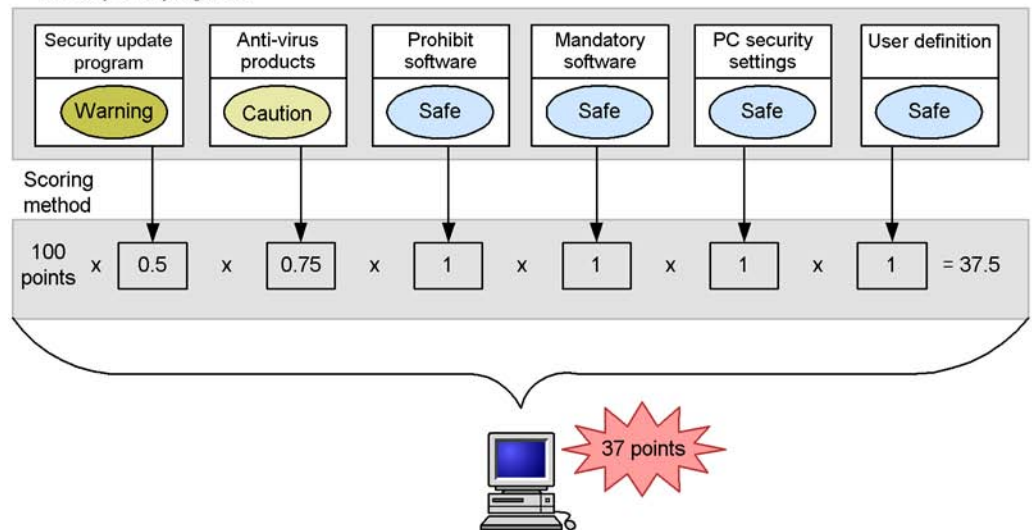
PDF file

Client security level management information

Asset No.	Host name	PC security level
1000000004	Gen. Affairs 1	Danger
1000000005	Gen. Affairs 2	Caution
1000000006	Accounting 1	Safe
1000000007	Sales 5	Warning



Security level judgment



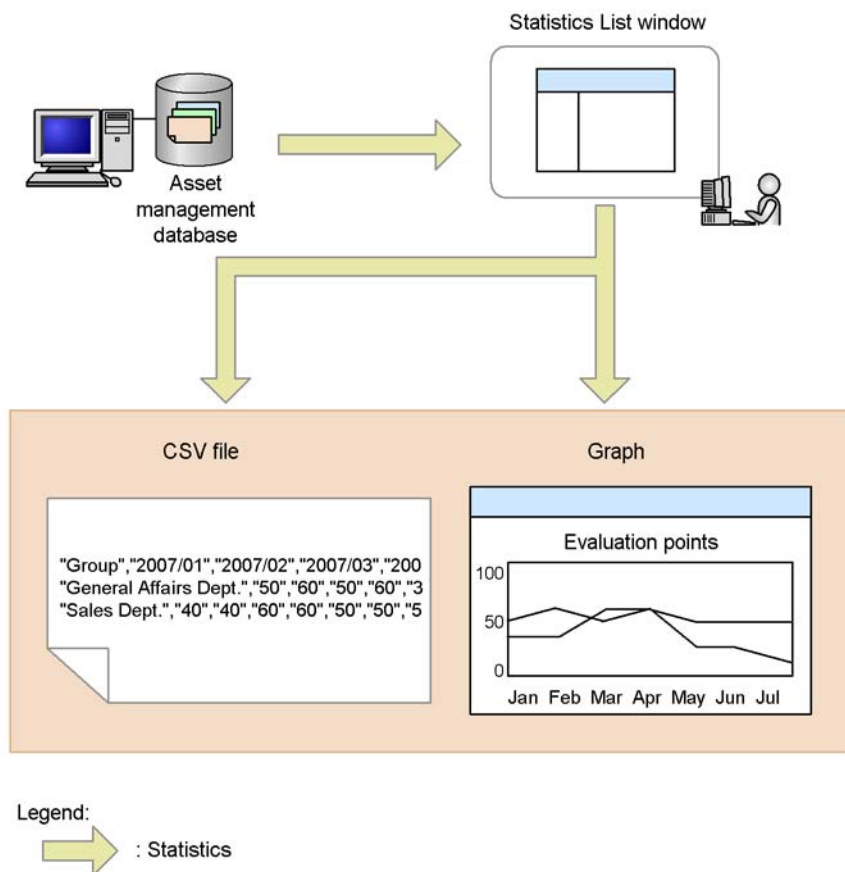
### 1.2.5 Viewing trends in security measures

*Statistics* describing the status of security measures can be checked on a group-by-group basis. For example, the administrator can view a graph showing how the proportion of clients with a satisfactory evaluation point rating and security level (called *countermeasure usage*) has changed over time. This information can also be output to a CSV file.

Trends in countermeasure usage for user-defined judgment items can also be checked on a group-by-group basis. For example, the administrator can view the trend over time in the proportion of clients running power-saving CPUs as part of an effort to reduce power consumption.

Statistics can be used to judge whether a problem with security measures is a short-term or long-term problem. Also, by checking the countermeasure usage for specific judgment items, the administrator can gauge which judgment items are associated with inadequate countermeasure usage, and take effective measures to resolve the situation for problem groups.

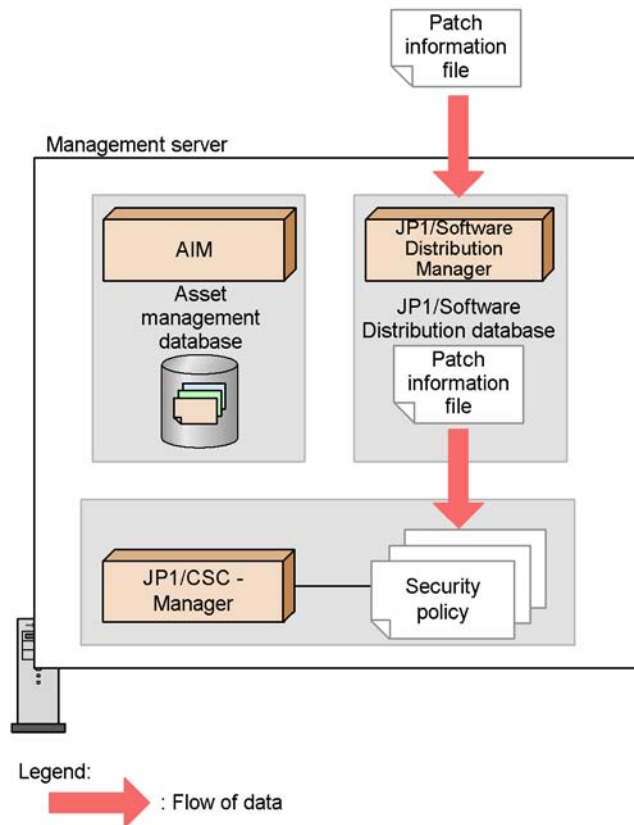
Figure 1-6: Graph and CSV output of statistics



### 1.2.6 Automatic update of security policies relating to security updates

Patch information for security policies relating to security updates can be updated automatically by using the patch information files collected by Job Management Partner 1/Software Distribution. This feature applies to patch information for Windows and Internet Explorer. This relieves the administrator from having to verify and update security policy information, as well as preventing wrong settings and other errors. For details about patch information files, see the manual *Job Management Partner 1/Software Distribution Description and Planning Guide*, for Windows systems.

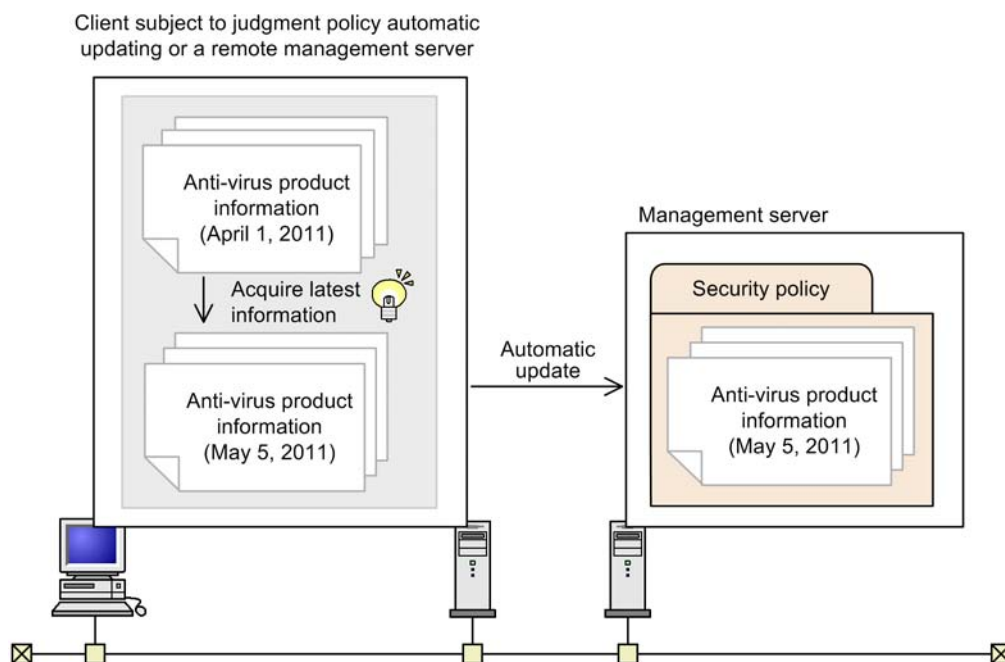
Figure 1-7: Automatic update of security policy for security updates



### 1.2.7 Automatic update of security policies relating to anti-virus products

Security policies relating to anti-virus products can be updated automatically by linking with the anti-virus product and collecting the latest virus definition files, the version of the virus detection engine, and other information. This relieves the administrator from having to verify and update security policy information, as well as preventing wrong settings and other errors.

Figure 1-8: Automatic update of security policy for anti-virus products



### 1.2.8 Building and running a quarantine system by linking with a network control product

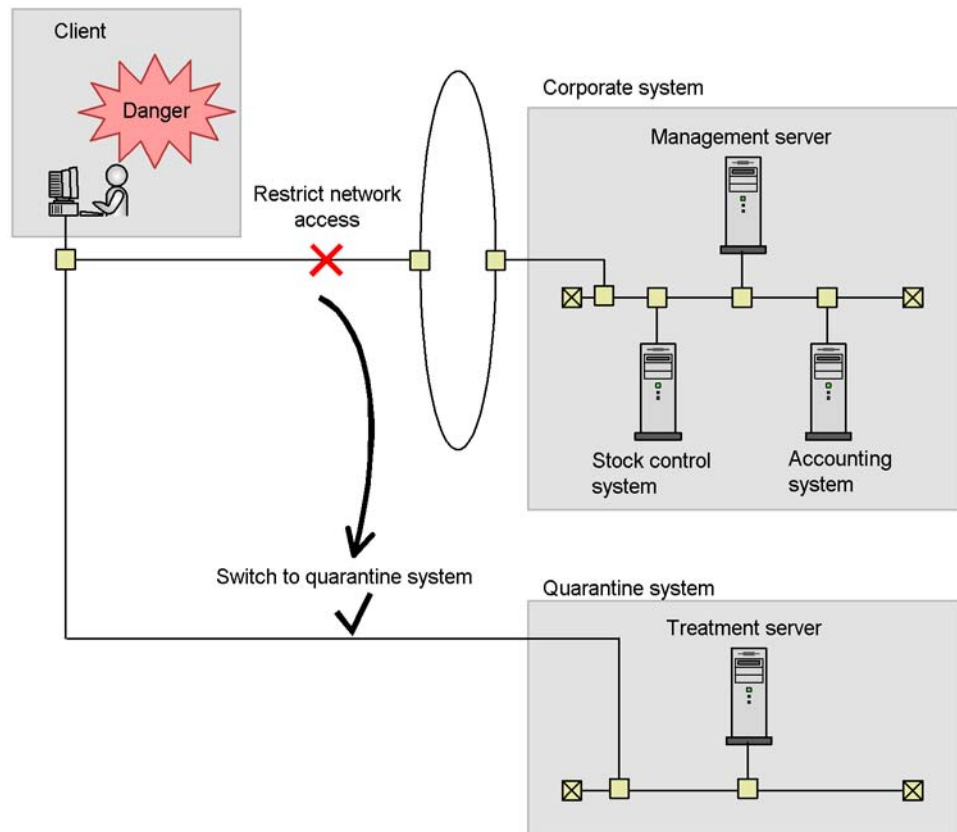
Users can build and run a quarantine system by linking the client security control system with a network control product capable of denying or permitting client connection to a network.

The quarantine system provides overall process management, including disconnection of clients that pose a high security risk, implementation of security measures, and reconnection to the network.

The quarantine system can be linked to the following network control products:

- JP1/Network Monitor
- An authentication server using either IEEE 802.1X authentication or MAC authentication
- JP1/Software Distribution (AMT linkage facility)

Figure 1-9: Building and running a quarantine system

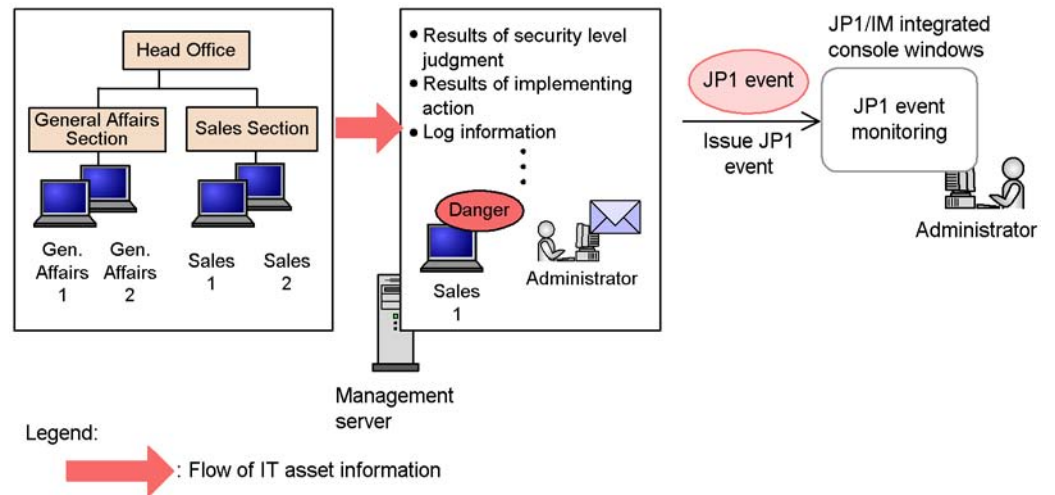


### 1.2.9 Linkage with JP1/IM

By linking to JP1/IM, JP1/CSC messages can be sent to JP1/IM as JP1 events. The judgment results of a client security level and implementation results of an action can be checked from the JP1/IM integrated console.



Figure 1-10: Linkage with JP1/IM



## 1.3 Typical uses of a client security control system

The following presents some typical ways in which a client security control system can be used.

*Table 1-1:* Examples of typical uses of a client security control system

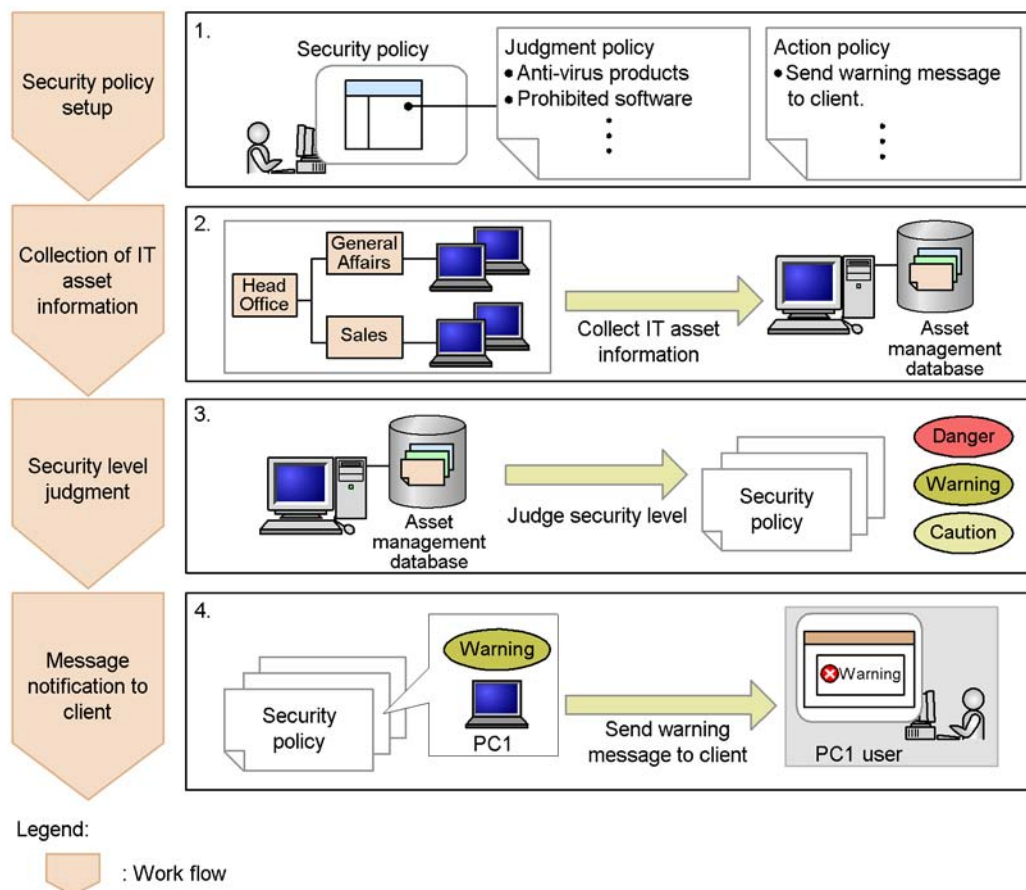
Example	Section in manual
Send warning messages to clients with inadequate security.	1.3.1
Deny network connections to clients with inadequate security.	1.3.2
Distribute the latest security update programs and definition files to clients with inadequate security.	1.3.3
Create a list of clients with inadequate security.	1.3.4
View a history of judgments and actions for a specific client.	1.3.5
Output PC list information to a file.	1.3.6
Implement actions after all security level judgments have been made.	1.3.7
Discover trends in the status of security countermeasures.	1.3.8
Discover trends in countermeasure usage for user-defined judgment items.	1.3.9

### 1.3.1 Send warning messages to clients with inadequate security

#### ■ Overview

An action based on the corporate security policy can be sent automatically to a client with inadequate security. The example below shows how a warning message can be sent to the client via a client security control system in a basic configuration.

Figure 1-11: Warning message notification to a client with inadequate security



## ■ Work flow

### 1. Security policy setup

Based on the corporate security policy, the administrator sets the judgment policy (judgment items) and the action policy (actions triggered according to the judgment result).

- Consider the security policy. ➔ 4.7 *Considerations for security policies*
- Set the security policy. ➔ 6. *Managing Security Policies*

### 2. Collection of IT asset information

The client's IT asset information is collected and centrally managed in the asset management database.

## 1. Overview

### 3. Security level judgment

To determine the client's security level, the IT asset information collected at step 2 is compared against the judgment policy set at step 1.

A security level judgment can be triggered in any of three ways: Automatic judgment when inventory information is updated, periodic judgment via Scheduled Tasks in Windows, or judgment by an administrator.

- Judge the security level. ➔ *2.4 Judging security levels*

### 4. Message notification to client

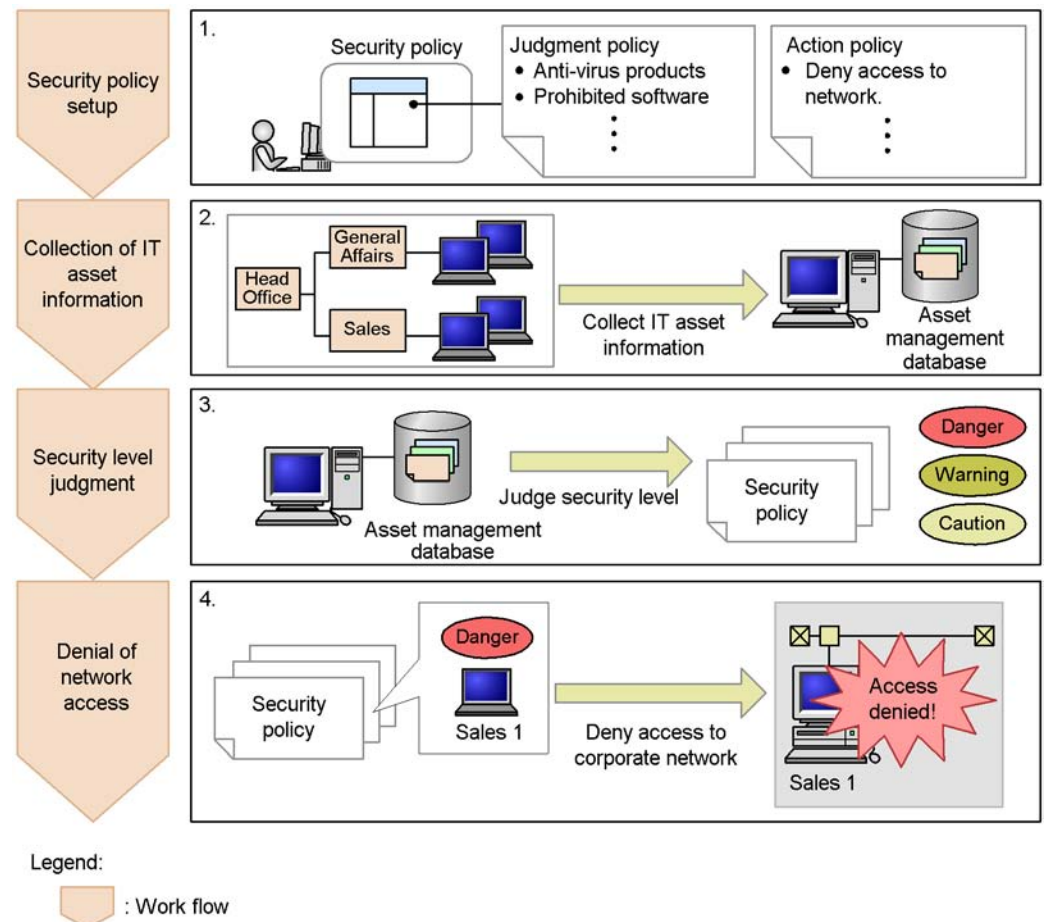
A warning message is sent to the client based on the action policy set at step 1.

## 1.3.2 Denying network connections to clients with inadequate security

### ■ Overview

The example below shows how a client security control system configured as a quarantine system can be used to prevent a client with inadequate security from accessing the network.

Figure 1-12: Denying network connection to a client with inadequate security



## ■ Work flow

### 1. Security policy setup

Based on the corporate security policy, the administrator sets the judgment policy (judgment items) and the action policy (actions triggered according to the judgment result).

- Consider the security policy. ➔ 4.7 *Considerations for security policies*
- Set the security policy. ➔ 6. *Managing Security Policies*

### 2. Collection of IT asset information

The client's IT asset information is collected and centrally managed in the asset

management database.

3. Security level judgment

To determine the client's security level, the IT asset information collected at step 2 is compared against the judgment policy set at step 1.

A security level judgment can be triggered in any of three ways: Automatic judgment when inventory information is updated, periodic judgment via Scheduled Tasks in Windows, or judgment by an administrator.

- Judge the security level. ➔ *2.4 Judging security levels*

4. Denial of network access

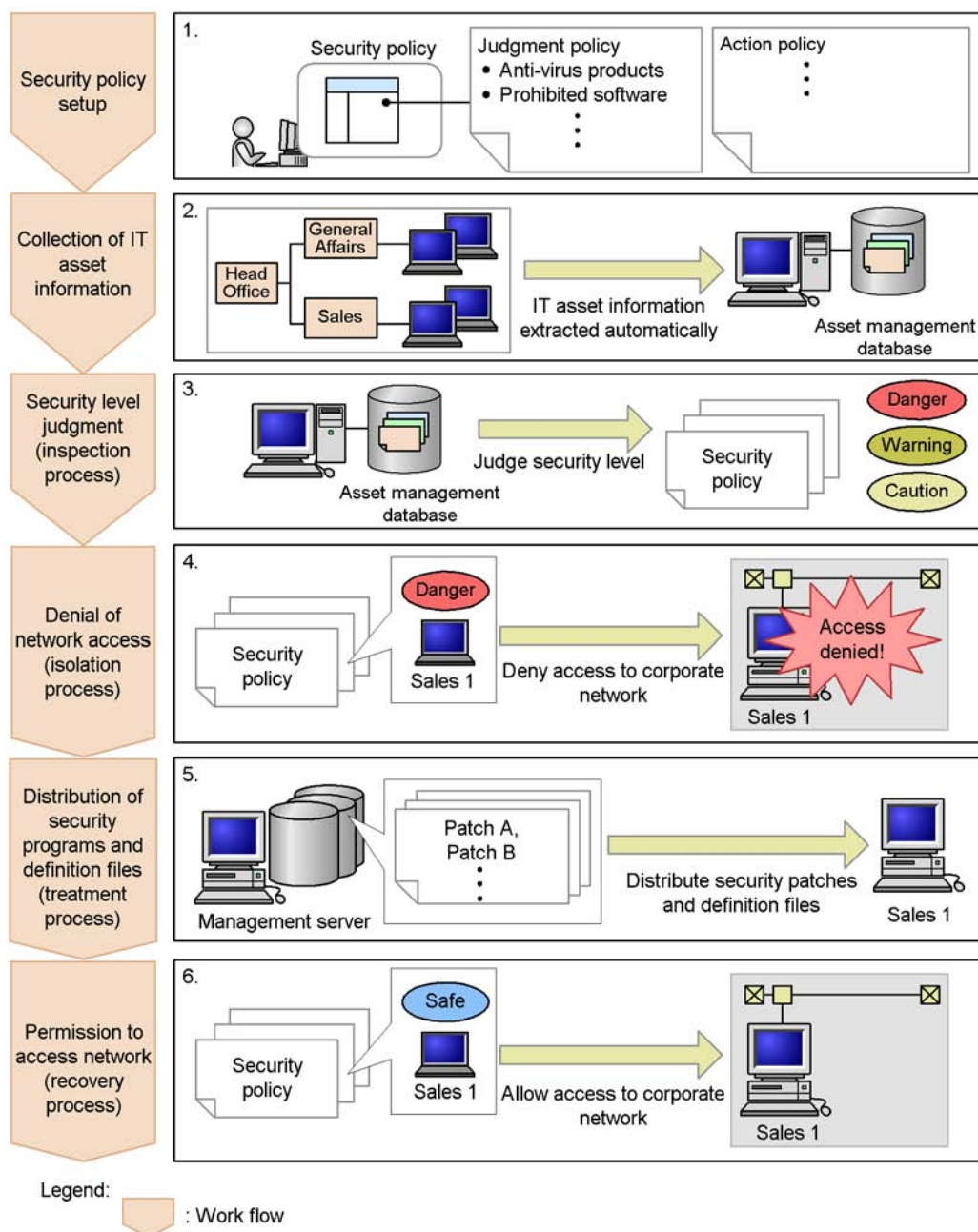
Based on the action policy set at step 1, the client is denied access to the corporate network.

### 1.3.3 Distributing the latest security update programs and definition files to clients with inadequate security

#### ■ Overview

The example below shows how the latest security update programs and definition files can be distributed to a client with inadequate security via a client security control system configured as a quarantine system.

Figure 1-13: Distributing the latest security update programs and definition files to clients with inadequate security



## ■ Work flow

### 1. Security policy setup

Based on the corporate security policy, the administrator sets the judgment policy (judgment items) and the action policy (actions triggered according to the judgment result).

- Consider the security policy. ➔ *4.7 Considerations for security policies*
- Set the security policy. ➔ *6. Managing Security Policies*

### 2. Collection of IT asset information

The client's IT asset information is collected and centrally managed in the asset management database.

### 3. Security level judgment (inspection process)

To determine the client's security level, the IT asset information collected at step 2 is compared against the judgment policy set at step 1.

A security level judgment can be triggered in any of three ways: Automatic judgment when inventory information is updated, periodic judgment via Scheduled Tasks in Windows, or judgment by an administrator.

- Judge the security level. ➔ *2.4 Judging security levels*

### 4. Denial of network access (isolation process)

Based on the action policy set at step 1, the client is denied access to the corporate network.

### 5. Distribution of the latest security update programs and definition files (treatment process)

Based on the judgment policy set at step 1, the administrator distributes the latest security update programs and definition files to the client either from JPI/ Software Distribution Manager on the management server or by using installation media.

### 6. Permission to access network (recovery process)

The client's security level is re-evaluated and the client is granted permission to access the corporate network.

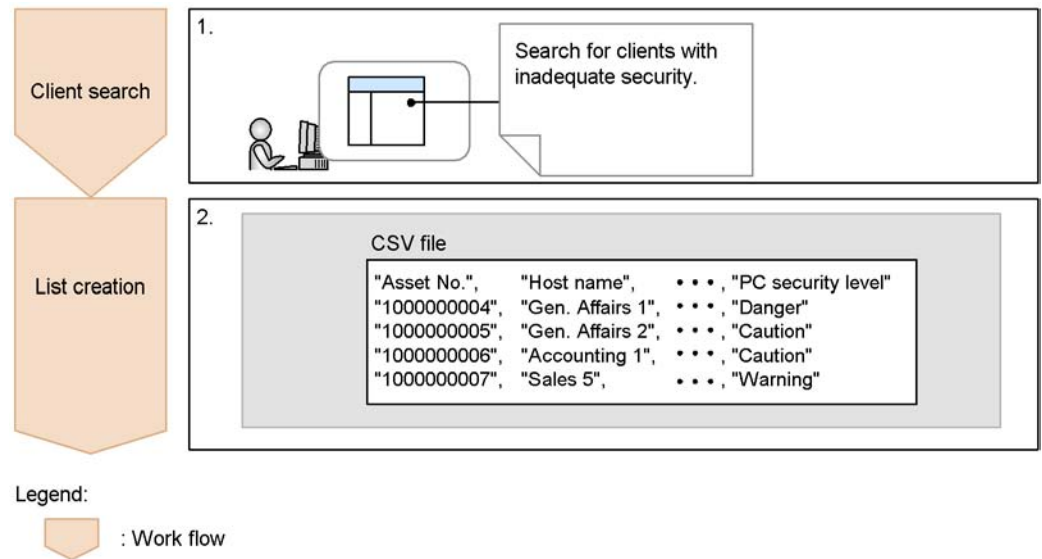
## 1.3.4 Creating a list of clients with inadequate security

### ■ Overview

The example below shows how the administrator can create a list of clients with inadequate security for management purposes.



Figure 1-14: Creating a list of clients with inadequate security



### ■ Work flow

#### 1. Client search

Use the PC Search window to find the clients with inadequate security.

- Specify the search conditions. ➔ *8.2 Searching for clients*

#### 2. List creation

From the search results, create a client list as a CSV file.

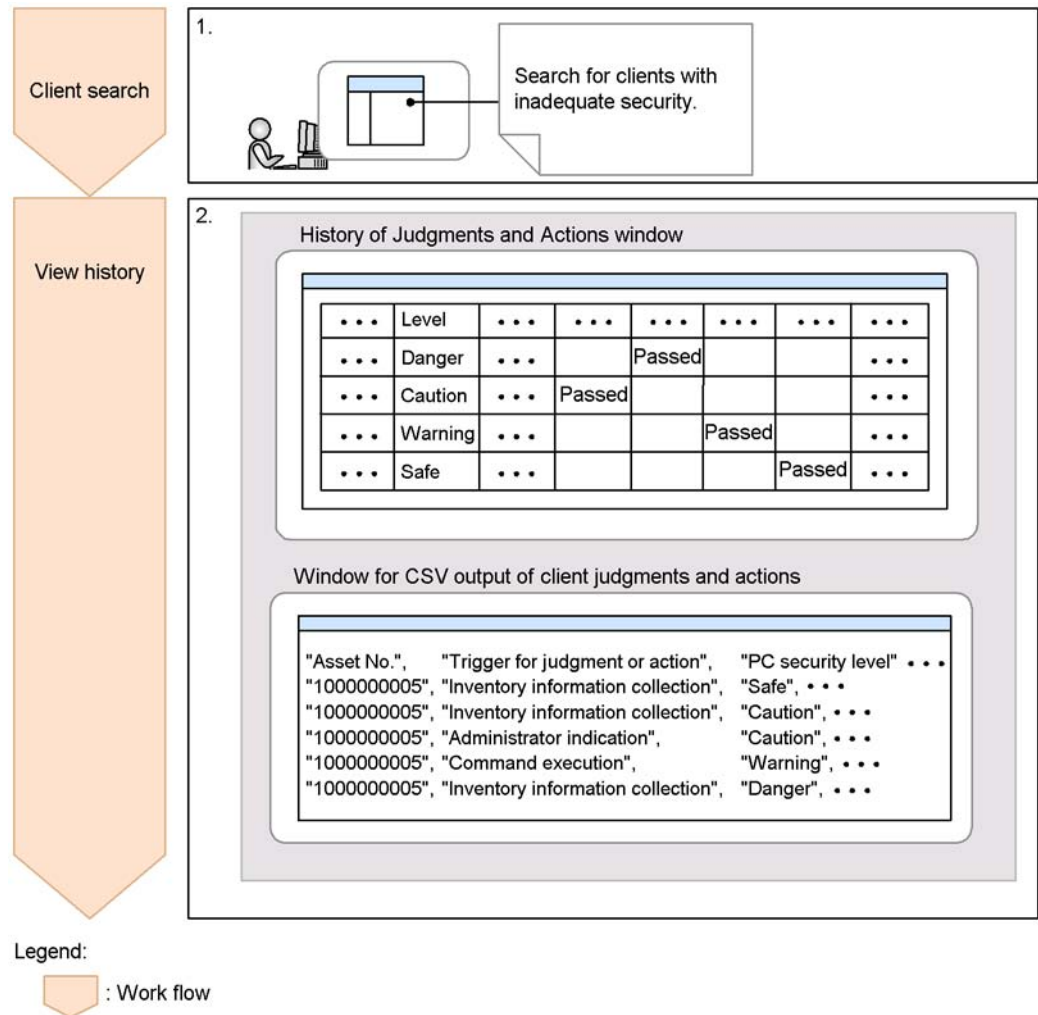
- Display the search results. ➔ *10.2 Outputting search results of clients to a file*

## 1.3.5 Viewing a history of judgments and actions for a specific client

### ■ Overview

The example below shows how the administrator can view a history of judgments and actions for a specific client for management purposes.

Figure 1-15: Viewing a history of judgments and actions



## ■ Work flow

### 1. Client search

Use the PC Search window to find the client whose judgments and actions you want to view.

- Specify the search conditions. ➔ *8.2 Searching for clients*

### 2. Data reference

View the client's judgments and actions history file in the History of Judgments

and Actions window or window for CSV output of client judgments and actions.

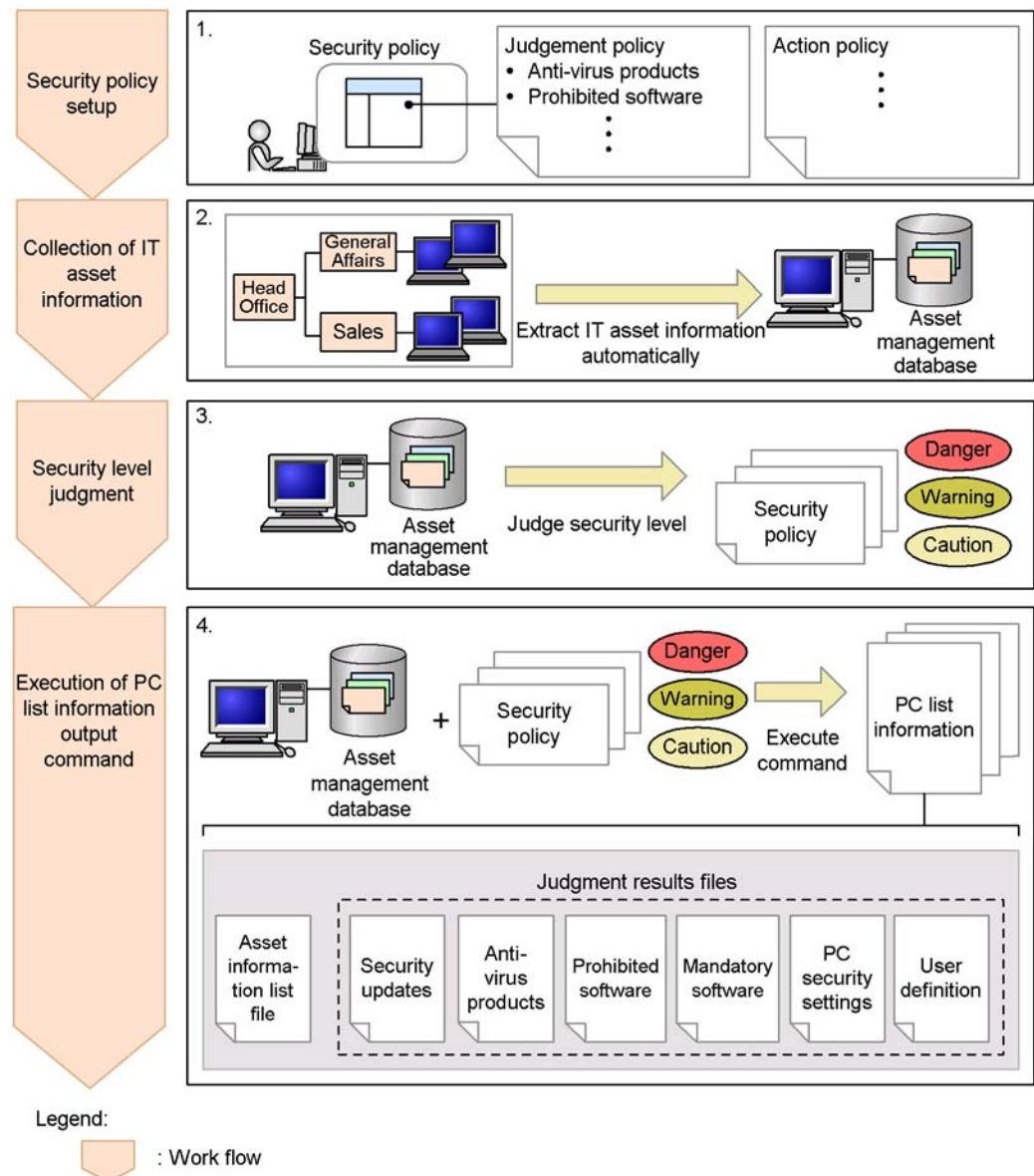
- View history. ➔ 8.3.8 *Checking history of judgments and actions for a client*

### 1.3.6 Outputting PC list information to a file

#### ■ Overview

The example below shows how the asset information and judgment result for a client whose security level was judged is output to a CSV file as PC list information. The administrator can use the PC list information file to manage PC security levels.

Figure 1-16: Outputting a PC list information file (CSV format)



## ■ Work flow

### 1. Security policy setup

Based on the corporate security policy, the administrator sets the judgment policy (judgment items) and the action policy (actions triggered according to the

judgment result).

- Consider what needs to be in the security policy. ➔ *4.7 Considerations for security policies*
- Set the security policy. ➔ *6. Managing Security Policies*

## 2. Collection of IT asset information

The IT asset information for a client is collected and centrally managed in the asset management database.

## 3. Security level judgment

To determine the client's security level, the IT asset information collected at step 2 is compared against the judgment policy set at step 1.

A security level judgment can be triggered in any of three ways: Automatic judgment when inventory information is updated, periodic judgment via Scheduled Tasks in Windows, or judgment by an administrator.

- Judge the security level. ➔ *2.4 Judging security levels*

## 4. Execution of PC list information output command

When the PC list information output command (`cscexportpclist`) is executed, the IT asset information collected at step 2 and the result of the security level judgment at step 3 are output as PC list information to a CSV file.

- PC list information output command ➔ *cscexportpclist (outputs PC list information) in 15. Commands*
- PC list information file ➔ *16.10 PC list information file.*

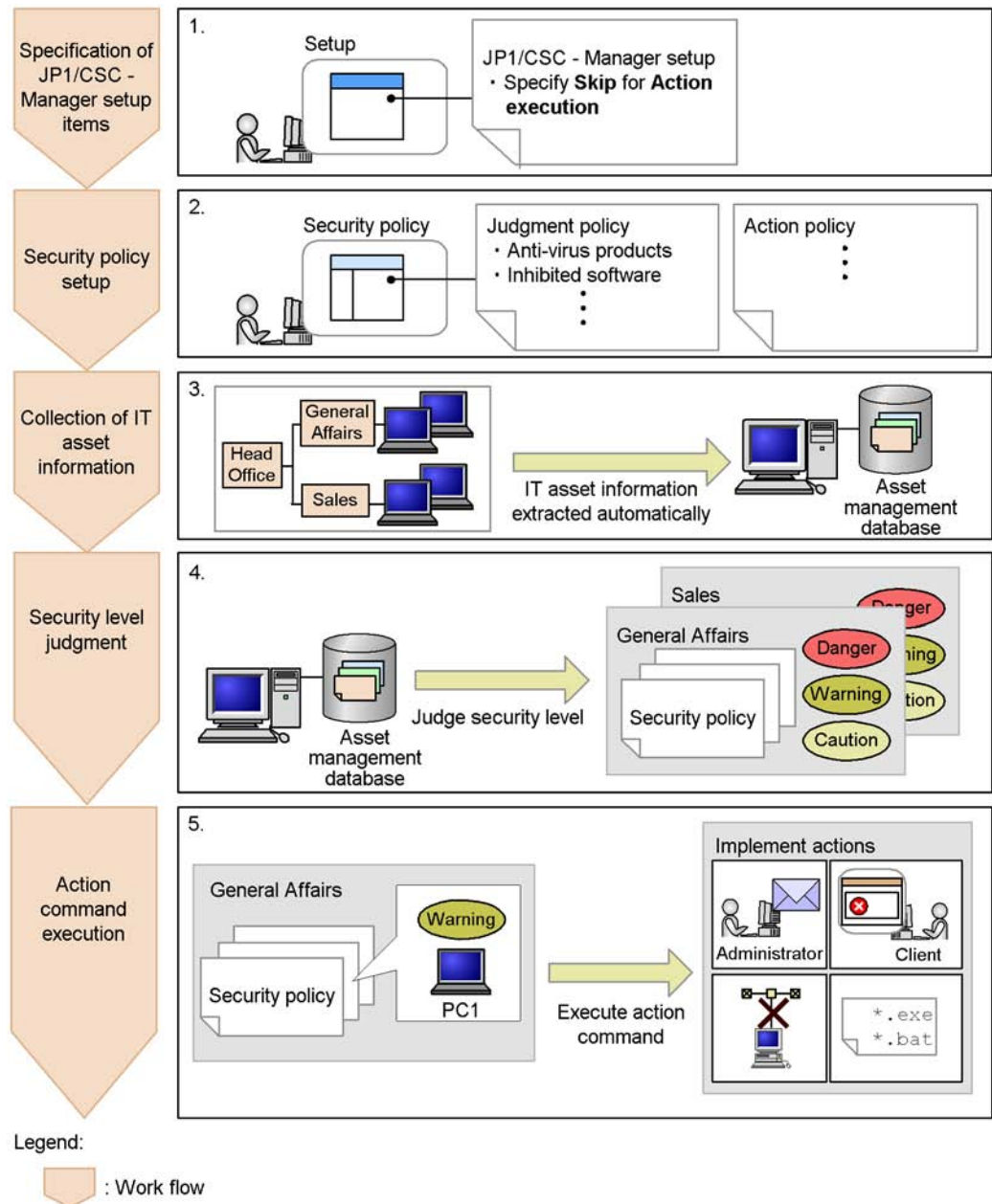
# 1.3.7 Implementing actions after all security level judgments have been made

## ■ Overview

The example below shows how the administrator can manually implement actions after all security level judgments of clients have been made.

This operation is recommended when the security levels of many clients are judged and time is needed to complete the judgments and actions, or when you want to create a report on the judgment results before implementing any actions.

Figure 1-17: Implementing actions after all security level judgments have been made



## ■ Work flow

### 1. Specification of JP1/CSC - Manager setup items

To prevent actions from being implemented as soon as a security level has been judged, in the JP1/CSC - Manager Setup dialog box, specify **Skip** for **Action execution**.

- Set up JP1/CSC - Manager. ➔ *5.4.3 Setting up JP1/CSC - Manager*

### 2. Security policy setup

The administrator sets the judgment policy (judgment items) and the action policy (the actions triggered according to the judgment results based on the corporate security policy).

- Consider what needs to be in the security policy. ➔ *4.7 Considerations for security policies*
- Set the security policy. ➔ *6. Managing Security Policies*

### 3. Collection of IT asset information

The IT asset information for the client is collected and centrally managed in the asset management database.

### 4. Security level judgment

To determine the client's security level, the IT asset information collected at step 3 is compared against the judgment policy set at step 2. The security levels of clients are judged one group at a time for the groups defined by the administrator.

A security level judgment can be triggered in any of three ways: Automatic judgment when inventory information is updated, periodic judgment via Scheduled Tasks in Windows, or judgment by an administrator.

- Judge the security level. ➔ *2.4 Judging security levels.*

### 5. Execution of action command

The action command (`cscaction`) executed for the specified client or clients implements actions according to the result of the latest security level judgment.

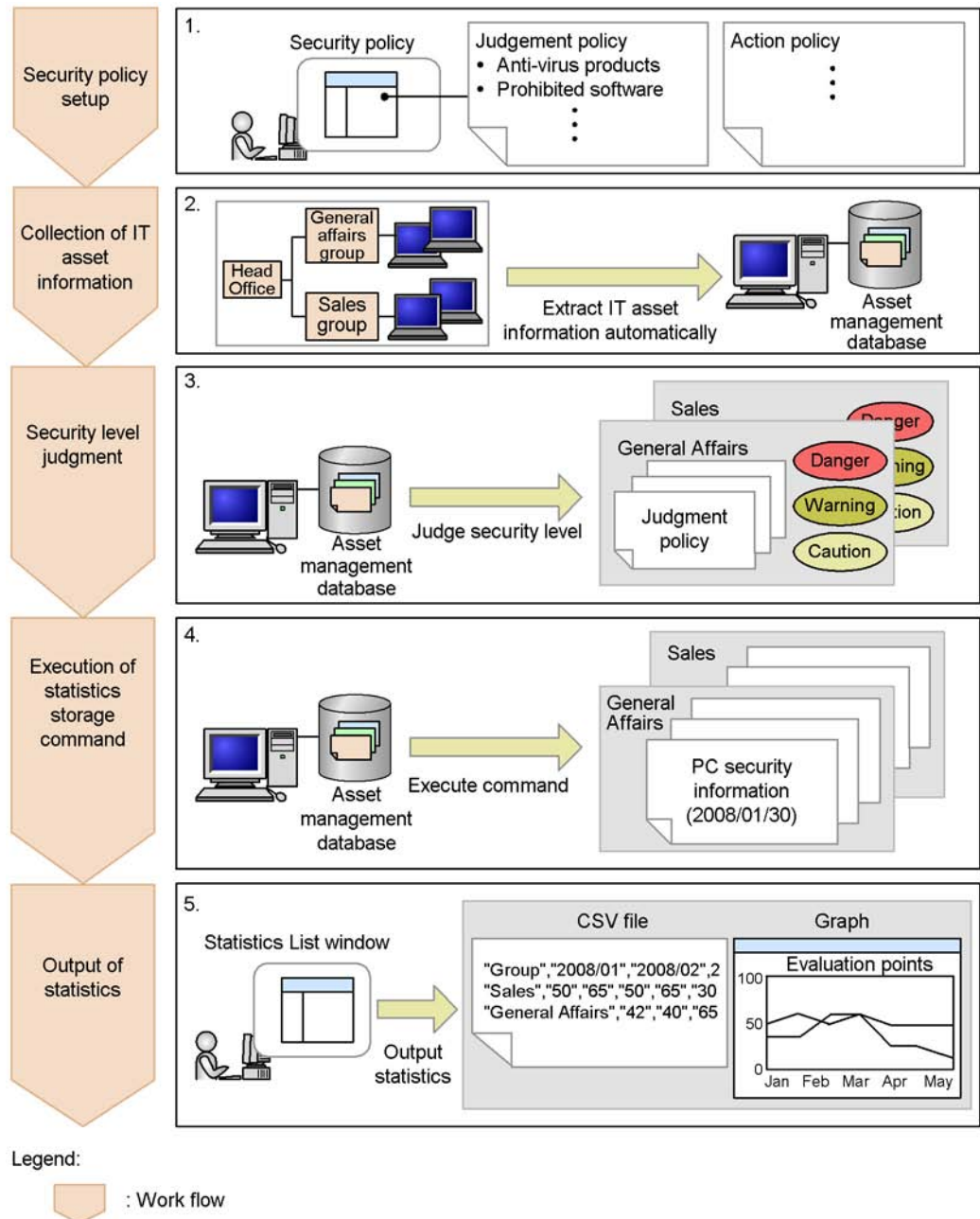
- Action command ➔ *cscaction (implements actions for a specified client) in 15. Commands*

## 1.3.8 Gauge trends in security countermeasure statuses

### ■ Overview

The example below shows how statistics are output. The administrator can use the statistics to judge whether a problem with security measures is a short-term or long-term problem.

Figure 1-18: Outputting statistics





## ■ Work flow

### 1. Security policy setup

Based on the corporate security policy, the administrator sets the judgment policy (judgment items) and the action policy (actions triggered according to the judgment result).

- Consider what needs to be in the security policy. ➔ *4.7 Considerations for security policies*
- Set the security policy. ➔ *6. Managing Security Policies*

### 2. Collection of IT asset information

The IT asset information for a client is collected and centrally managed in the asset management database.

### 3. Security level judgment

The IT asset information collected in step 2 is checked against the judgment policy set in step 1 to determine the client security level. The security levels of clients are judged one group at a time for the groups defined by the administrator.

A security level judgment can be triggered in any of three ways: Automatic judgment when inventory information is updated, periodic judgment via Scheduled Tasks in Windows, or judgment by an administrator.

- Judge the security level. ➔ *2.4 Judging security levels*

### 4. Execution of statistics storage command

When the command is executed, information about the status of security countermeasures is stored in the asset management database as statistics.

- Store statistics. ➔ *10.4.1 Storing statistics*
- Statistics storage command ➔ *cscstorecount (stores statistics about the status of security measures) in 15. Commands*

### 5. Output of statistics

Search for the statistics that you want to check. You can then check the countermeasure status by displaying the data as a graph or outputting it as a CSV file.

- Search statistics. ➔ *10.4.2 Searching statistics*
- CSV output of statistics. ➔ *10.4.3 Outputting statistics to a CSV file*
- Display graph of statistics. ➔ *10.4.4 Displaying statistics as a graph*

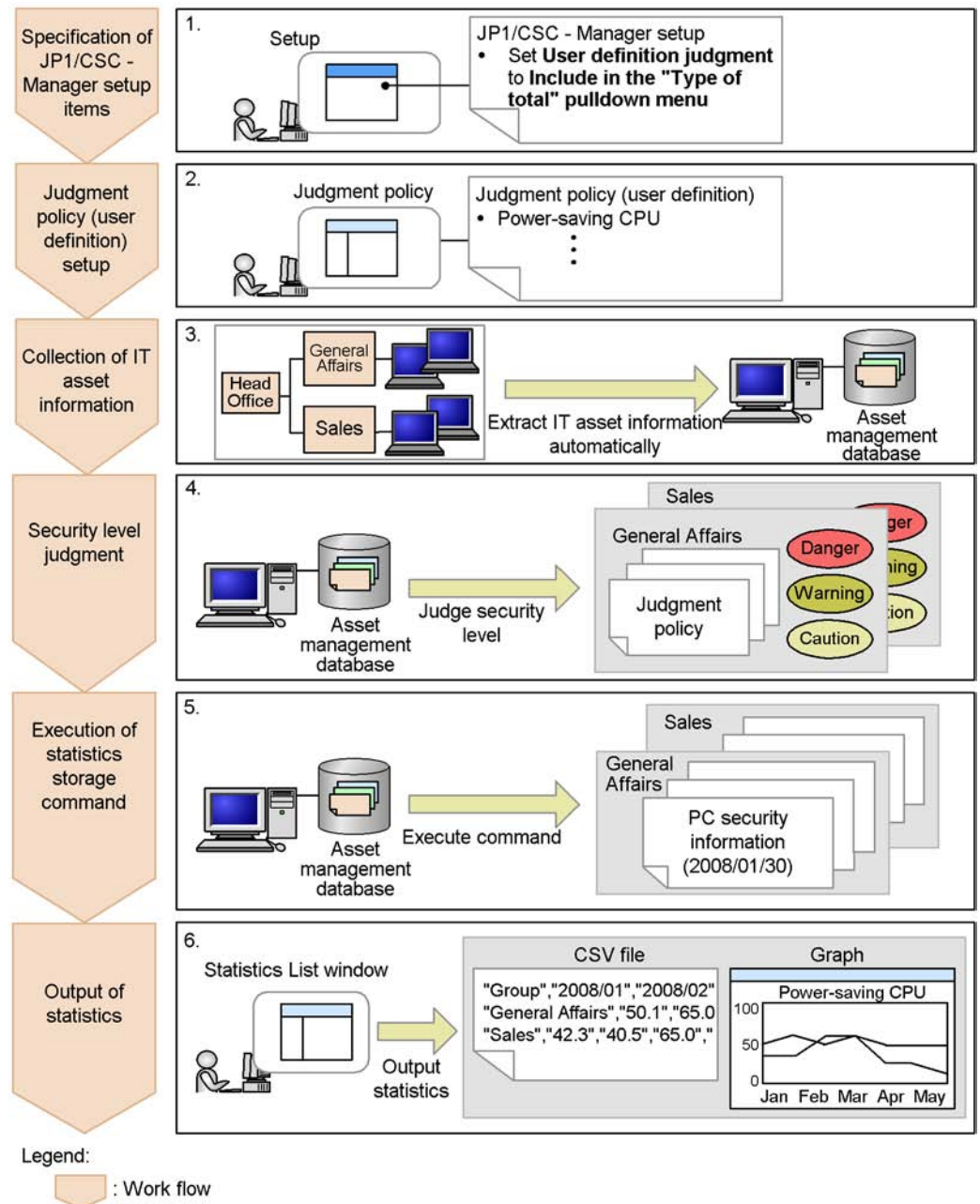
### **1.3.9 Gauge trends in countermeasure usage for user-defined judgment items**

#### **■ Overview**

The example below shows how the administrator can output statistics describing countermeasure usage for user-defined judgment items.

This operation is recommended when, for example, the administrator wants to view the trend over time in the proportion of clients running power-saving CPUs as part of an effort to reduce power consumption.

Figure 1-19: Outputting statistics (user-defined judgment items)



## ■ Work flow

### 1. Specification of JP1/CSC - Manager setup items

To output user-defined judgment items as statistics, in the JP1/CSC - Manager Setup dialog box, specify **Include in the "Type of total" pulldown menu** for **User definition judgment**.

- Set up JP1/CSC - Manager. ➔ *5.4.3 Setting up JP1/CSC - Manager*

### 2. User-defined judgment policy setup

The administrator sets the user-defined judgment policy.

- Set the user-defined judgment policy. ➔ *6.8 Editing a user-defined judgment policy*

### 3. Collection of IT asset information

The client's IT asset information is collected and centrally managed in the asset management database.

### 4. Security level judgment

To determine the client's security level, the IT asset information collected at step 3 is checked against the judgment policy set at step 2. The security levels of clients are judged one group at a time for the groups defined by the administrator.

A security level judgment can be triggered in any of three ways: Automatic judgment when inventory information is updated, periodic judgment via Scheduled Tasks in Windows, or judgment by an administrator.

- Judge the security level. ➔ *2.4 Judging security levels*

### 5. Execution of statistics storage command

When the command is executed, information about the countermeasure status of user-defined judgment items is stored in the asset management database as statistics.

- Store statistics. ➔ *10.4.1 Storing statistics*
- Statistics storage command. ➔ *cscstorecount (stores statistics about the status of security measures) in 15. Commands*

### 6. Output of statistics

Search for the statistics that you want to check. You can then check the countermeasure status by displaying the data as a graph or outputting it as a CSV file.

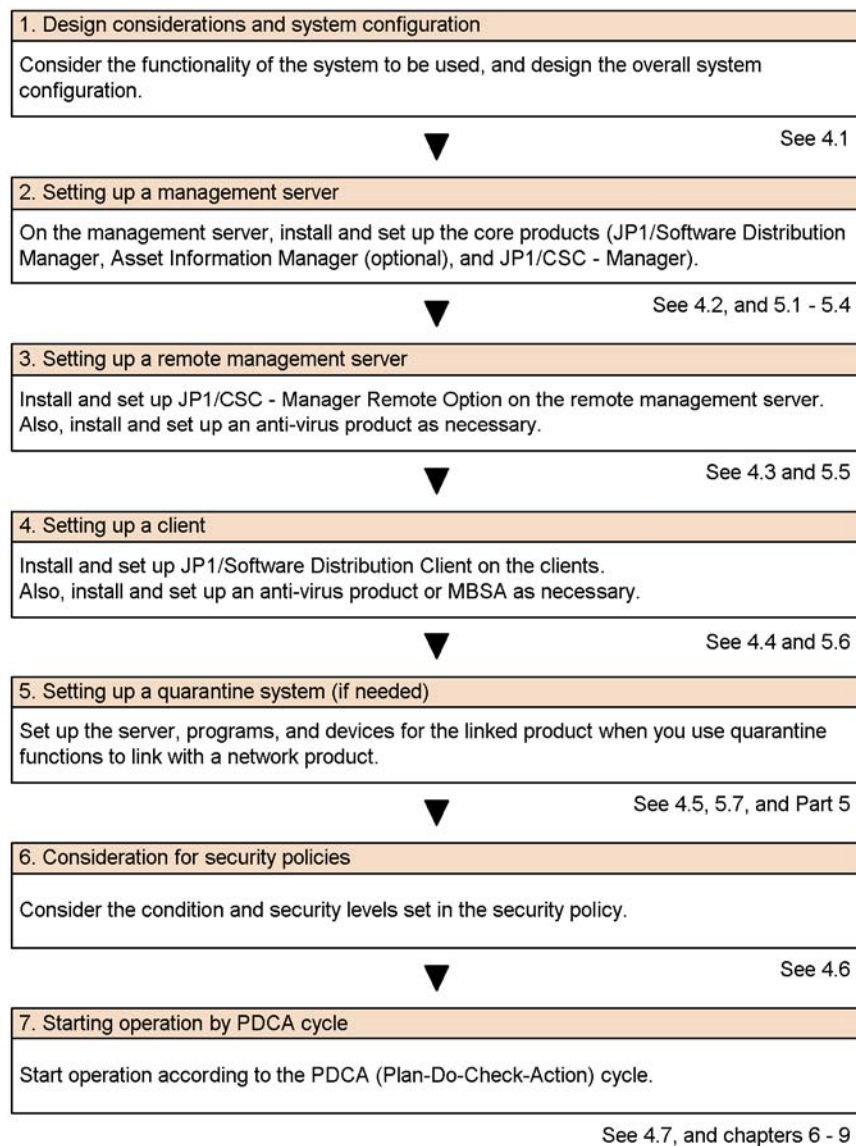
- Search statistics. ➔ *10.4.2 Searching statistics*

- CSV output of statistics. ➔ *10.4.3 Outputting statistics to a CSV file*
- Display graph of statistics. ➔ *10.4.4 Displaying statistics as a graph*

## 1.4 Work flow from installation to starting operation

The following figure shows the flow of procedures from installation of a client security control system to starting operation.

*Figure 1-20: Work flow from installation to starting operation*



## **Chapter**

---

# **2. Client Security Control System Functionality**

---

This chapter describes the functionality of a client security control system.

- 2.1 Overview of functionality
- 2.2 Managing inventory information
- 2.3 Managing security policies
- 2.4 Judging security levels
- 2.5 Implementing actions
- 2.6 Managing client security levels

---

## 2.1 Overview of functionality

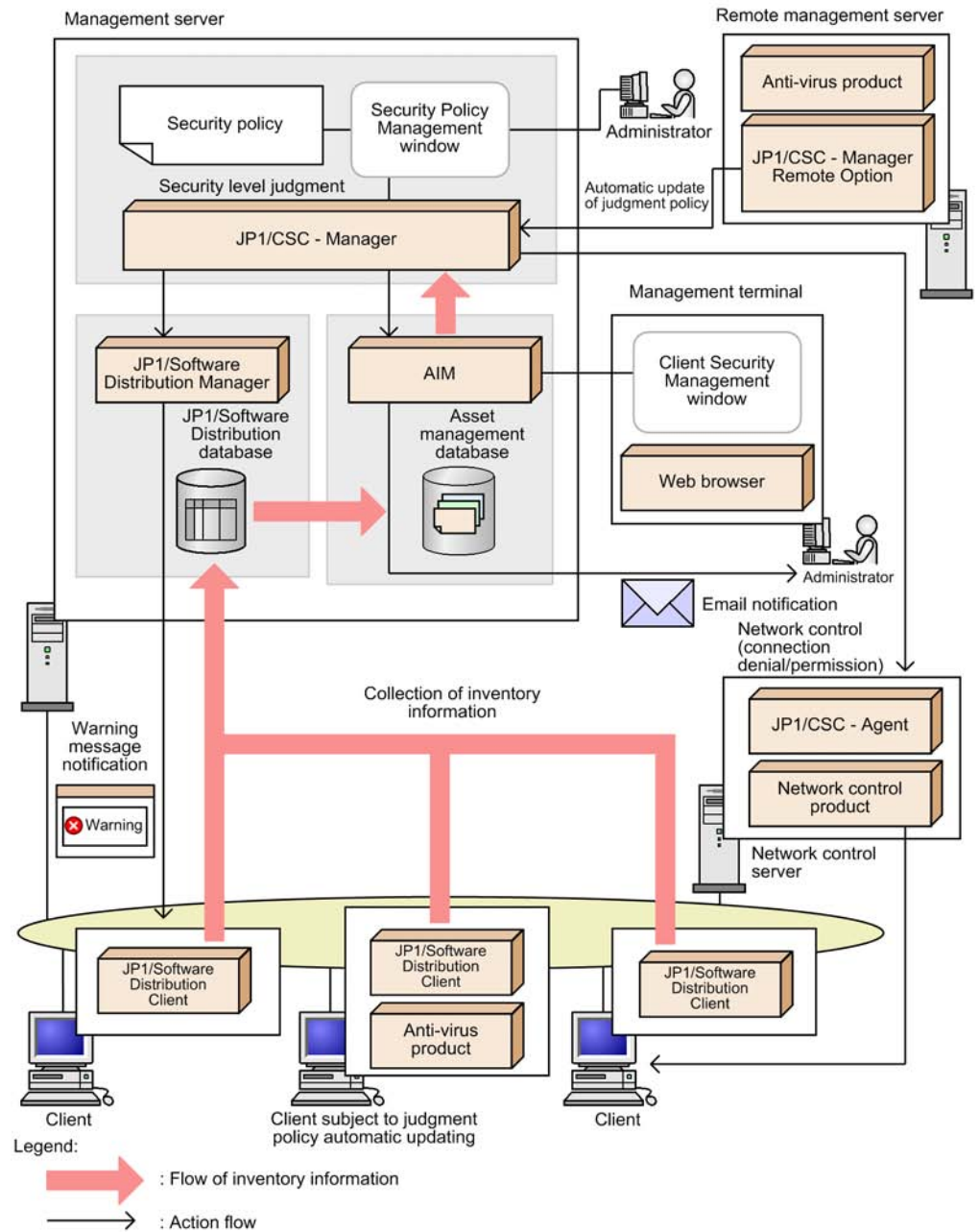
---

A client security control system can work in combination with multiple JP1 products and related products.

The following figure shows the overall configuration of a client security control system.



Figure 2-1: Overall configuration of a client security control system



Note:

In this manual, *Asset Information Manager* and *Asset Information Manager Subset Component of JP1/Software Distribution Manager* are abbreviated to *AIM*.

A client security control system provides the following primary functionality:

- **Inventory information management**  
JP1/Software Distribution collects inventory information from clients and centrally manages the information in the asset management database of AIM.
- **Security policy management**  
An administrator can edit security policies in the Security Policy Management window of JP1/CSC - Manager and assign the policies to clients.
- **Security level judgment**  
Based on a client's inventory information and security policy, JP1/CSC - Manager judges the client's security level.
- **Action implementation**  
Based on the action policy and the result of the security level judgment, JP1/CSC - Manager issues instructions which may include notifying the administrator by email, sending a message to the client, and controlling network access by the client.
- **Client security level management**  
Using the Client Security Management window of AIM, an administrator can monitor clients and evaluate whether security measures are adequate based on a points rating.

---

## 2.2 Managing inventory information

---

A client security control system can collect and centrally manage IT asset information, such as hardware information and software information, from clients.

The IT asset information sent from JP1/Software Distribution Client running on the clients to JP1/Software Distribution Manager running on the management server is known as *inventory information*. Since this inventory information is updated in real-time, an administrator can accurately assess the latest client inventory information.

The client inventory information collected by JP1/Software Distribution is managed in the client security control system via the *asset management database* of AIM. Of the inventory information collected, information about the following software is used to determine the client security level:

- Windows security update

This is used to manage information about the Windows patches and service packs not yet applied to the client.

- Anti-virus products

These are used to manage whether or not any anti-virus products are installed on the client, as well as manage the version of the virus definition file.

- Software in the **Add/Remove Programs** menu

This is used to manage whether any prohibited software is installed on the client, or whether mandatory software is installed on the client.

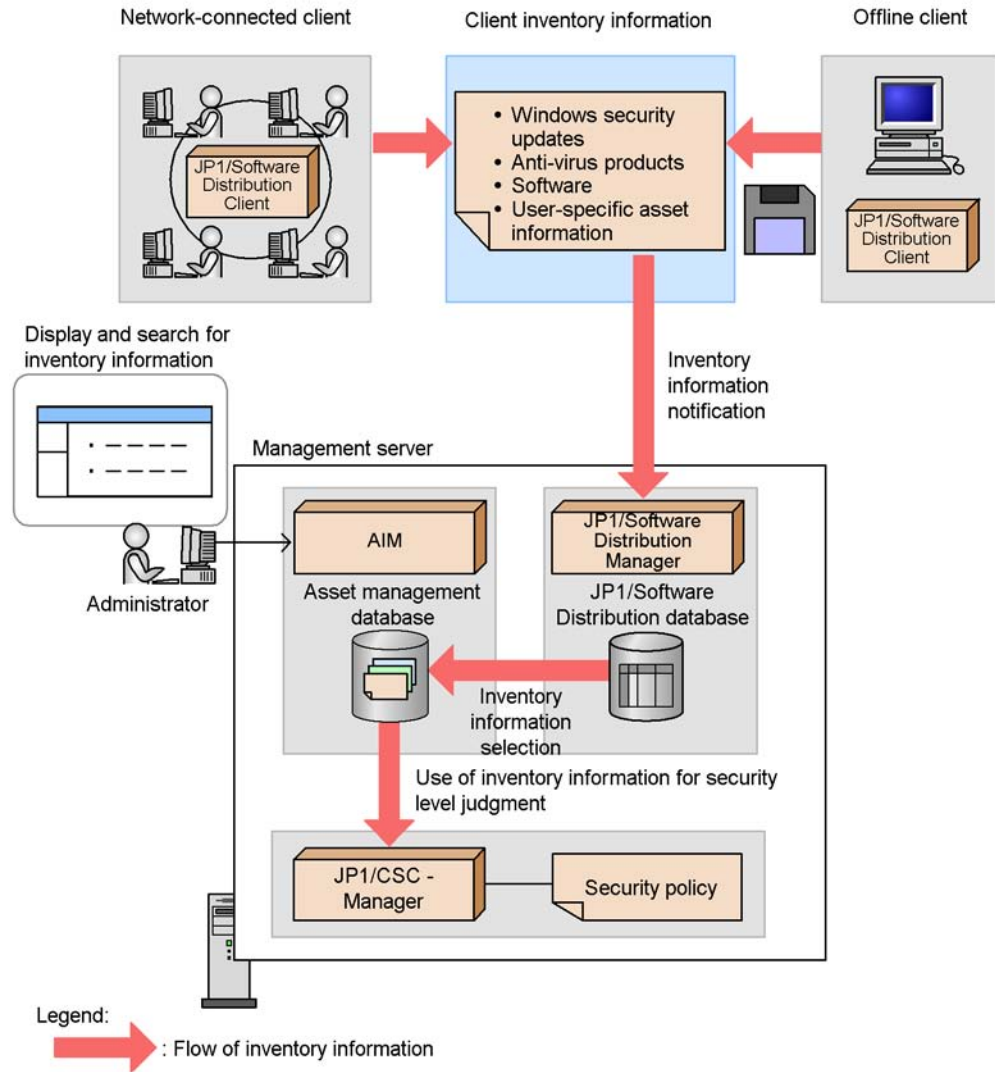
- User-specific asset information

This is used to manage information defined as asset information by the administrator, such as whether automatic login is enabled.

Inventory information can be acquired from not only clients in the network, but also from off-line machines isolated from the network.

The following figure shows an overview of inventory information.

Figure 2-2: Overview of inventory information



---

## 2.3 Managing security policies

---

The security policies needed in the client security control system are set by the administrator.

A security policy consists of a *judgment policy*, which defines conditions for evaluating client security and sets associated security levels, and an *action policy*, which defines the actions to be implemented for each security level.

Each judgment policy and each action policy is assigned to each client. Policies are defined and assigned using the Security Policy Management windows of JP1/CSC - Manager. For details about these windows, see 6. *Managing Security Policies*.

### (1) Judgment policies

In a judgment policy, the administrator can set security levels associated with parameters for determining client security levels, such as whether Windows security updates have been applied and whether anti-virus products have been installed. These parameters for determining client security levels are called *judgment items*.

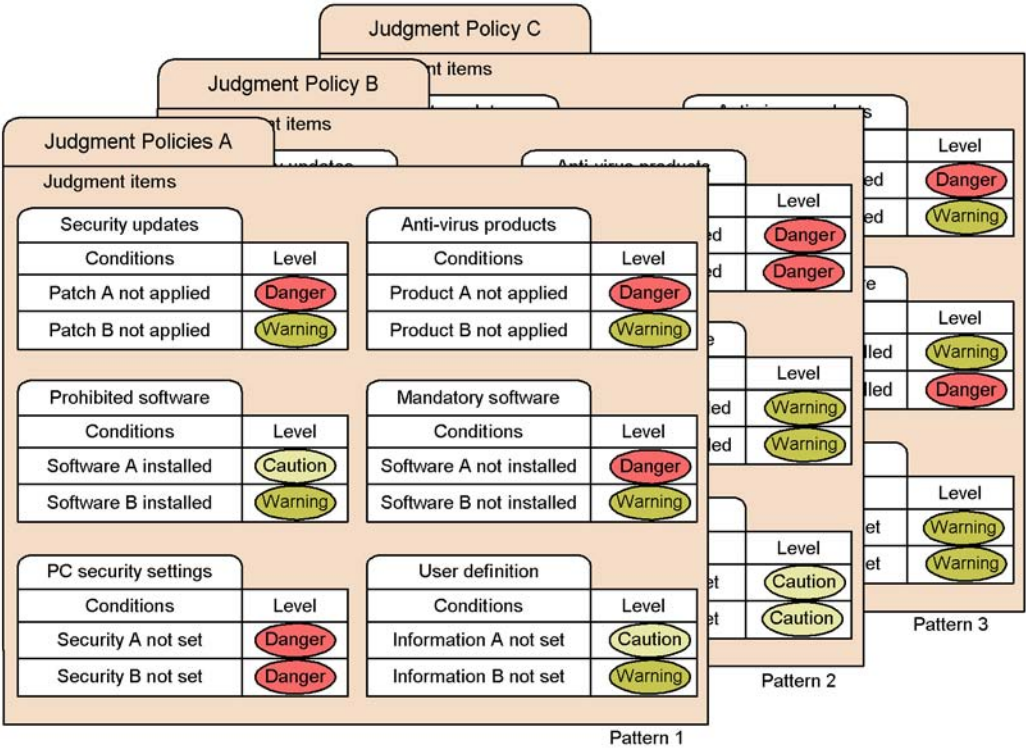
The judgment items of a judgment policy are as follows:

- Security updates
- Anti-virus products
- Prohibited software
- Mandatory software
- PC security settings
- User definition

The administrator must first decide which of these judgment items to use in determining client security levels, and then set judgment conditions for each item. The conditions can refer to security updates, anti-virus products, or software that must be installed on the client, and to user-defined judgment items optionally set by the administrator. After setting the judgment conditions, the administrator defines the client security level associated with each condition.

The following figure shows an overview of judgment policies.

Figure 2-3: Overview of judgment policies



Two methods are provided to set judgment policies:

- Using the Security Policy Management window of JP1/CSC - Manager
- Executing the judgment policy update command (`cscpolimport`)

For details about how to set judgment policies in the Security Policy Management window, see 6.2 *Managing judgment policies*. For details about how to use the command to set judgment policies, see *cscpolimport (updates judgment policy settings)* in 15. *Commands*.

Judgment policies can be preset in a variety of patterns. Alternatively, the administrator can customize the default judgment policy provided by the system.

Judgment policies relating to security updates and anti-virus programs can be updated automatically to the latest definitions. This process is described next.

**(a) Automatic update of judgment policies for security updates**

Patch information for judgment policies relating to security updates can be updated automatically by using the patch information files collected by Job Management Partner 1/Software Distribution. Patch information files contain information about

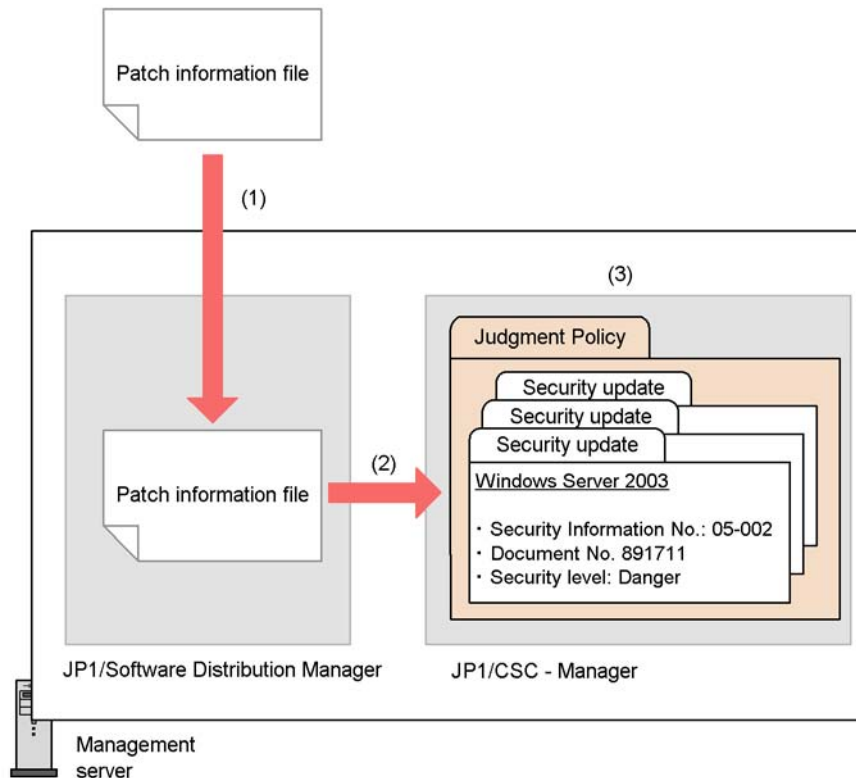
patches provided by Microsoft. This feature applies to patch information for Windows and Internet Explorer.

To update patch information for judgment policies, execute the judgment policy update command for security updates (`cscpatchupdate`). When the administrator executes this command, the judgment policy definitions for security updates are updated automatically according to the contents of the patch information file. For details about the judgment policy update command for security updates (`cscpatchupdate`), see *cscpatchupdate (updates patch information for judgment policies relating to security updates)* in *15. Commands*.

To use this feature, Job Management Partner 1/Software Distribution must be set up to acquire patch information files. For details about acquiring patch information files, see the manual *Job Management Partner 1/Software Distribution Description and Planning Guide*, for Windows systems.

The following figure shows an overview of automatically updating judgment policies for security updates.

Figure 2-4: Automatically updating judgment policies for security updates



Legend:

 : Flow of data

- (1) Acquire the patch information file.
- (2) Execute the judgment policy update command for security updates (`cscpatchupdate`)
- (3) Judgment policies relating to security updates are updated automatically.

For details about how to automatically update judgment policies for security updates, see 6.3.3 *Automatically updating judgment policies for security updates*.

#### (b) Automatic update of judgment policies for anti-virus products

Judgment policy definitions for an anti-virus product can be updated automatically by linking with the anti-virus product and collecting the latest update information for virus definition files and the engine version. You can also impose a delay between the acquisition of the latest information about the anti-virus product and the automatic update of the judgment policy definition by setting a *grace period*.

Update information for anti-virus products can be acquired either from the inventory

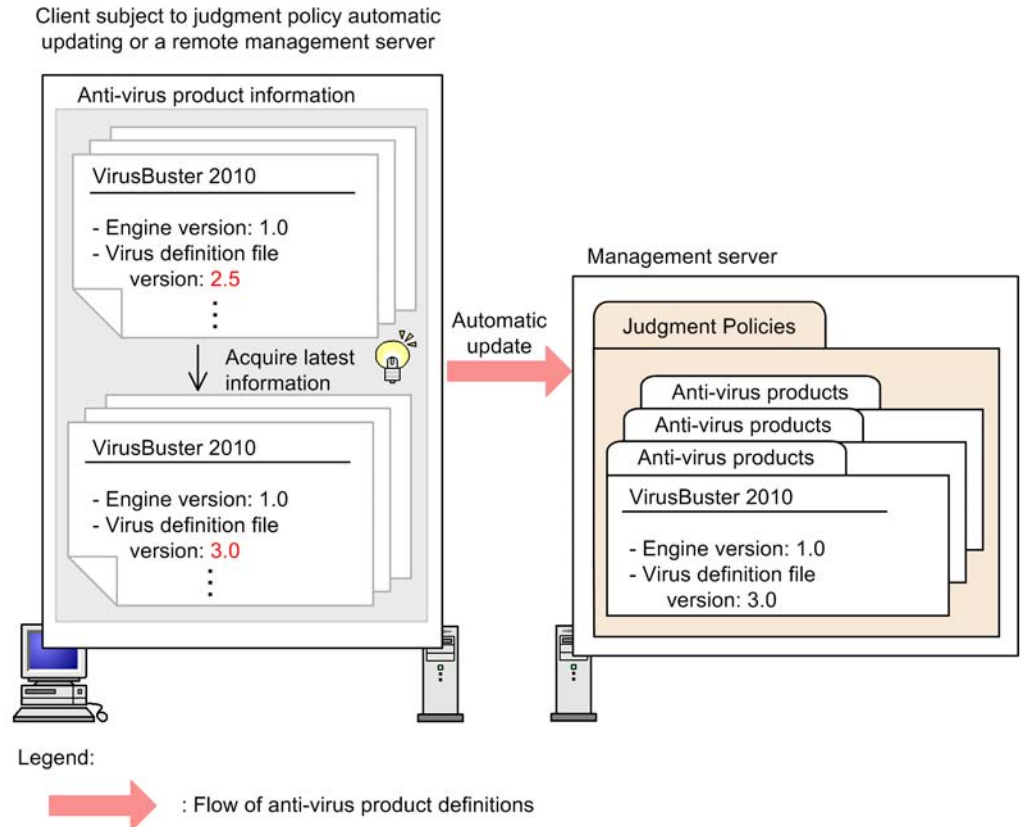


information for the specified client or by linking to JP1/CSC - Manager Remote Option on a remote management server.

For details about the system configuration when update information for anti-virus products is acquired from the inventory information for the specified client, see 3.1(2) *System configuration for automatically updating judgment policies for anti-virus products*. For details about the system configuration when update information for anti-virus products is acquired by linking with JP1/CSC - Manager Remote Option on a remote management server, see 3.1(3) *System configuration with a remote management server*.

The following figure shows an overview of automatically updating judgment policies for anti-virus products.

Figure 2-5: Automatically updating judgment policies for anti-virus products



Automatic update applies to anti-virus products supported by JP1/Software Distribution. For details about these anti-virus products, see 4.6 *Installing anti-virus products that link with automatic judgment policy updating*.

For details about how to automatically update judgment policies for anti-virus products, see *6.4.6 Updating judgment policies for anti-virus products automatically or manually*.

## **(2) Action policies**

In an action policy, the administrator can define what actions to implement on clients for each security level.

The following actions can be set for each of the four security levels (Danger, Warning, Caution, and Safe):

- Administrator notification

Send an email to the administrator.

When JP1/CSC is linked with JP1/IM, security level judgment results and implemented actions can be reported to JP1/IM.

- Client user notification

Send a pop-up warning message to the client user.

- Network connection denial or permission

JP1/CSC can be linked with a network control product to deny or permit clients to access the network. This action is available only with a quarantine system. For details on running a quarantine system, see *Part 5. Quarantine Systems*.

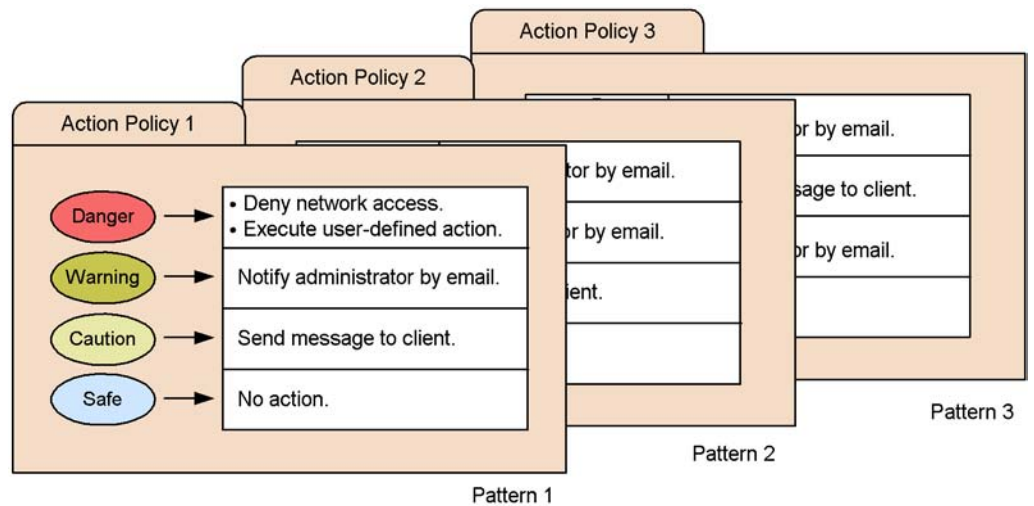
- Execution of a user-defined action

Execute a command (\*.exe or \*.bat) defined by the administrator.

Different actions can be set for each security level. For example, the administrator can specify that a message be sent to the user if a client's security level is *Warning*, or that the client be disconnected from the network when its security level is assessed as *Danger*.

The following figure shows an overview of action policies.

Figure 2-6: Overview of action policies



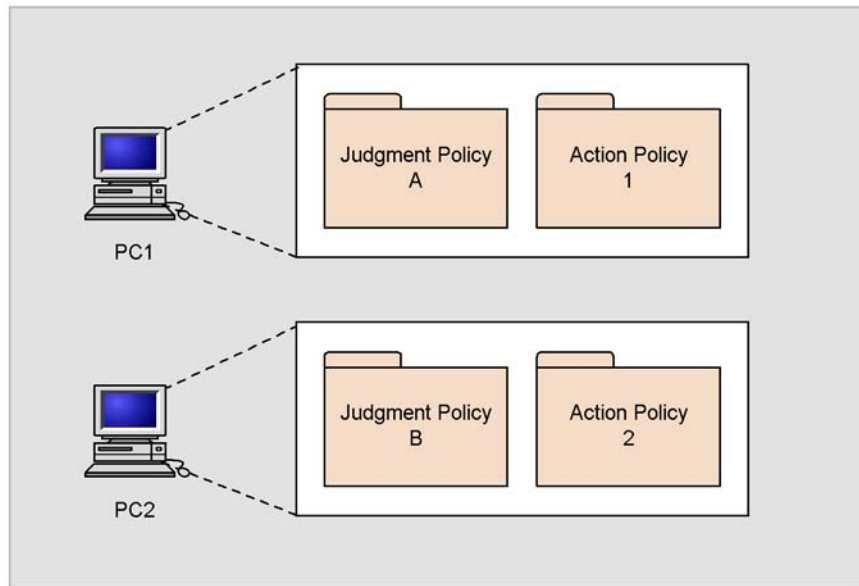
Action policies can be preset in a variety of patterns. Alternatively, the administrator can customize the default action policy provided by the system.

### (3) Assigning security policies to clients

After defining judgment and action policies, the administrator can assign them to clients. Clients can be assigned different policies.

The following figure shows an overview of assigning policies to clients.

Figure 2-7: Assigning policies to clients



You can assign policies using the Security Policy Management window of JP1/CSC - Manager or by executing the policy assignment command (`cscassign`).

For details about policy assignment in the Security Policy Management window, see *6.13 Assigning security policies to clients*. For details about policy assignment by command, see *cscassign (assigns security policies to clients)* in *15. Commands*.

Every client is assigned a default judgment policy and a default action policy in advance.

*Reference note:*

Default policies are assigned whenever a new client is configured in the system. If you add a client after starting operations with your client security control system, assign policies that the user has defined to the client as required.

---

## 2.4 Judging security levels

---

A client security level is judged based on client inventory information and the client judgment policy.

The security level is judged automatically by the judgment policy whenever inventory information is updated. In addition, the administrator can check security levels at regular intervals by registering a command for judging security levels in Scheduled Tasks in Windows, and can assess the security level of a particular client by specifying the client in the Client Security Management window of AIM.

A security level is judged for each judgment item, and the highest security level within the judgment items becomes the client security level.

The following explains how and when a security level is judged for a client.

### (1) When a security level is judged

The security level of a client is judged when the following types of judgment triggers occur:

- Automatic judgment when inventory information is updated

When client inventory information is updated, such as when software is installed on a client or a Windows security update is applied, the inventory information is reported from the client to JP1/Software Distribution Manager. The reported inventory information is reflected in the asset management database of AIM, and the client security level is determined from the applicable judgment policy and the updated inventory information.

Note that the setting of whether or not to perform an automatic judgment when inventory information is updated can be changed. By default, **Judge** is set. To prevent an automatic judgment when inventory information is updated, change this setting in the setup window of JP1/CSC - Manager. For details about this window, see *5.4.3 Setting up JP1/CSC - Manager*.

- Periodic judgment

The administrator registers the command for determining the security level (`cscjudge`) as a task in Scheduled Tasks in Windows.

A security level can be judged regularly when this task is enabled. For details about how to register a task in Scheduled Tasks, see *5.9 Procedures for setting a task in Scheduled Tasks*.

- Judgment by an administrator

Using the Client Security Management window of AIM, the administrator selects a client to judge its security level. For details about how to judge the security level

for a specified client, see *8.4 Judging a client security level*.

*Reference note:*

In the JP1/ CSC - Manager setup window, you can set whether to skip security level judgment for clients whose inventory information has not changed since the last time their security level was judged.

**(2) How a security level is judged**

In a judgment policy, the following security levels are judged in order, to determine the security level of the client.

1. Security level for each judgment condition

The security level is judged for the judgment conditions in each judgment item.

2. Security level for each judgment item

Of the security levels for each judgment condition, the highest security level becomes that of the judgment item.

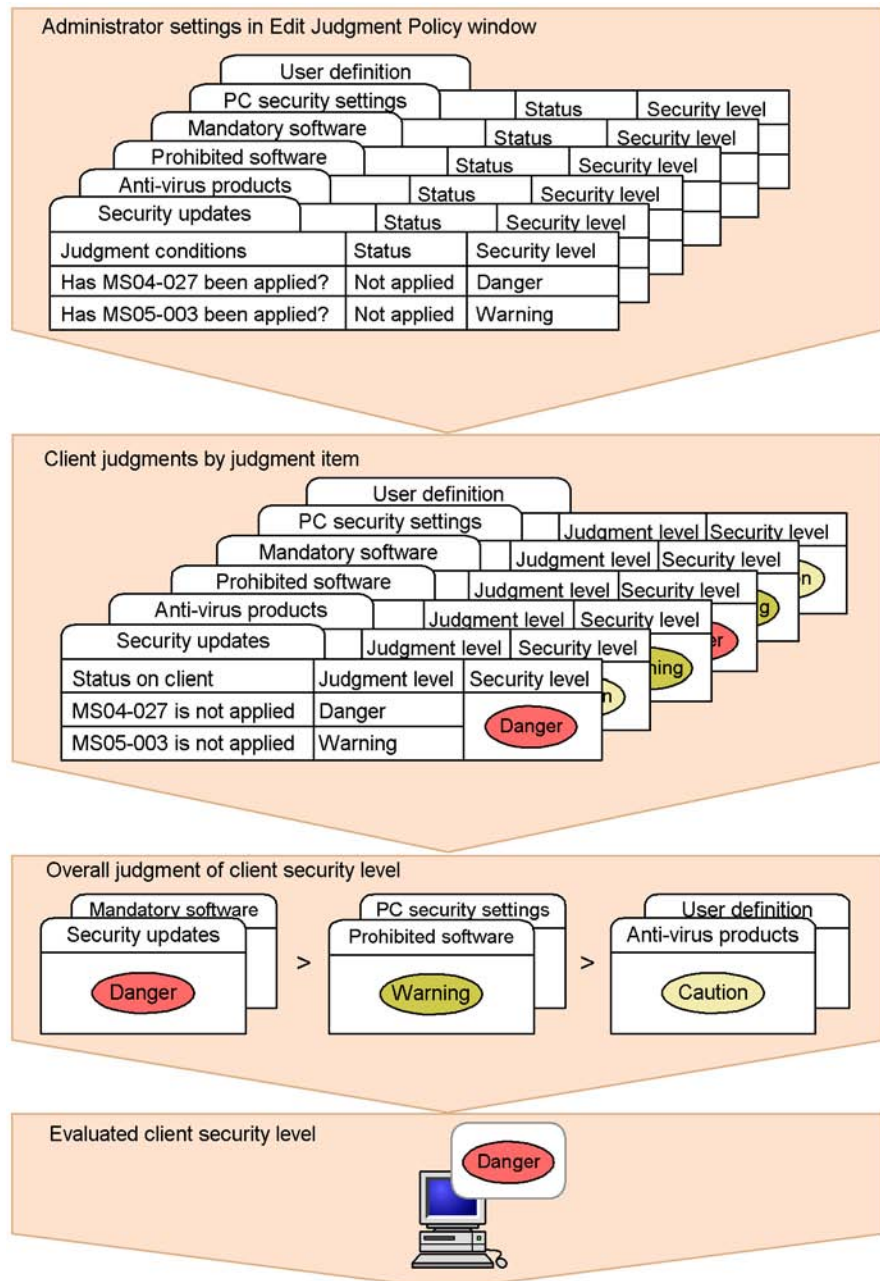
3. Client security level

Of the security levels of all judgment items to be judged, the highest security level becomes that of the client.

The security levels, in descending order, are Danger, Warning, Caution, and Safe.

The following figure shows an example of how a security level is judged.

Figure 2-8: Example of how a security level is judged



---

## 2.5 Implementing actions

---

Actions are implemented in two ways:

- As a result of security level judgment

An action is implemented according to the action policy, when a judgment trigger occurs for the security level.

- As a result of administrator instruction

An administrator implements an action manually by specifying a specific client in the Client Security Management window of AIM, in the network control command (`cscnetctrl`), or in the action command (`cscaction`).

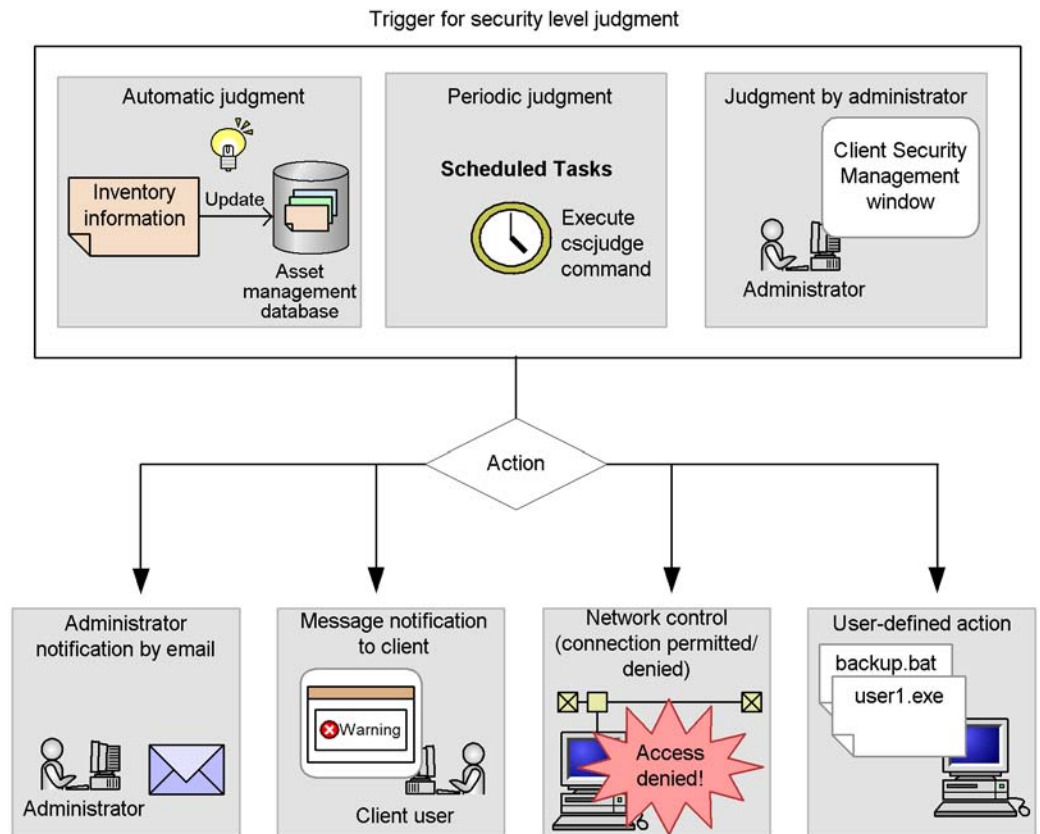
### 2.5.1 Implementing an action as a result of security level judgment

The client security level is judged when a judgment trigger occurs for the security level. The appropriate action is implemented by the action policy.

The following figure shows the actions appropriate for the security level judgment results.



Figure 2-9: Actions appropriate for the security level judgment results



### 2.5.2 Implementing an action as a result of administrator instructions

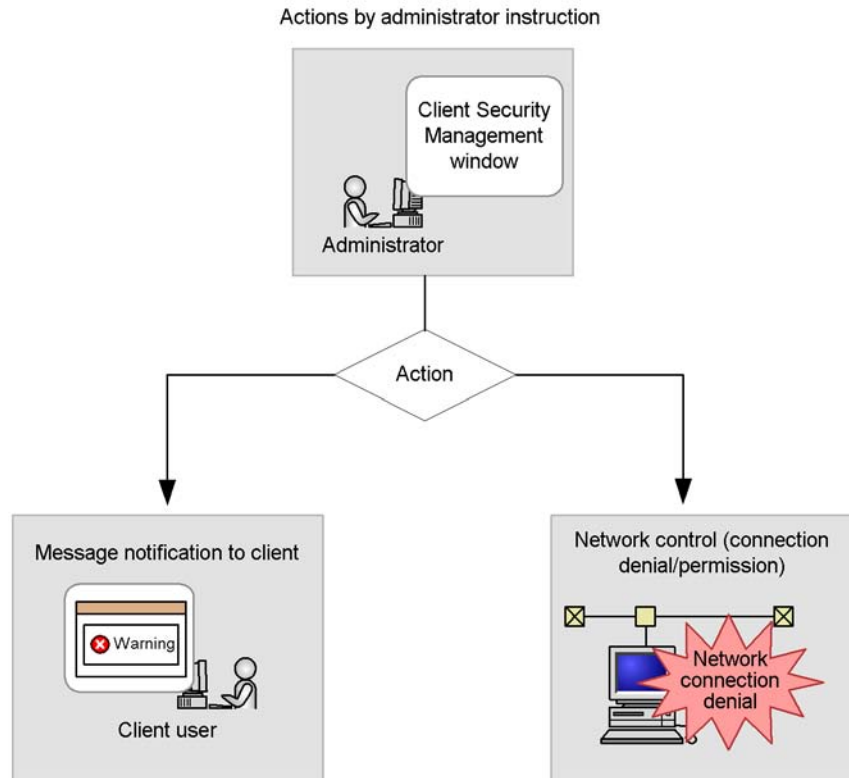
The following describes how an administrator can implement an action manually.

#### (1) Implementing an action from the Client Security Management window of AIM

Using the Client Security Management window of AIM, an administrator can execute an action on a specified client. For example if a client exists whose security level is judged as *Danger*, but no security measures have been implemented, the administrator can send a warning message to the client, or deny the client a network connection.

The following figure shows actions implemented by an administrator.

Figure 2-10: Actions implemented by an administrator



## (2) Implementing an action by the network control command (*cscnetctrl*)

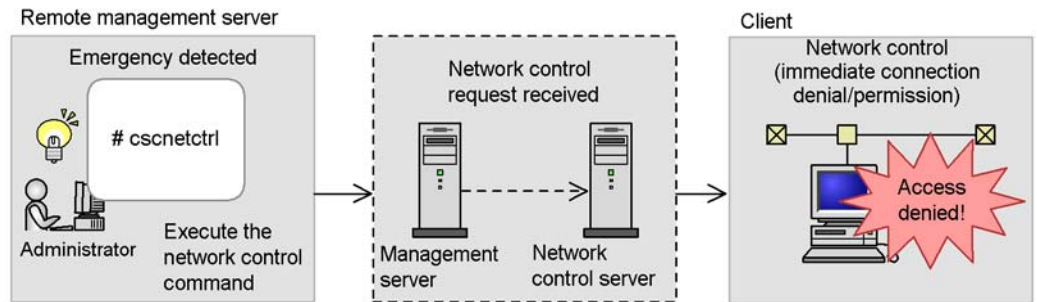
By issuing the network control command (*cscnetctrl*) from a remote system, an administrator can permit or immediately deny client connection to the network. For example, if the remote system detects that the client is infected with a virus, the administrator can immediately stop that client from accessing the network. This immediate denial by using the network control command (*cscnetctrl*) takes precedence over other actions.

To clear an immediate denial, the administrator must explicitly grant access using either the network control command (*cscnetctrl*) or the Client Security Management window. Network connection permission as the result of a subsequent security level judgment does not clear an immediate denial already in force.

A remote management server must be set up to enable linkage with the remote system.

The following figure shows an action implemented by the network control command (*cscnetctrl*).

Figure 2-11: Implementing an action by the network control command (cscnetctrl)



For details about the network control command (`cscnetctrl`), see *cscnetctrl (controls network connections)* in 15. Commands.

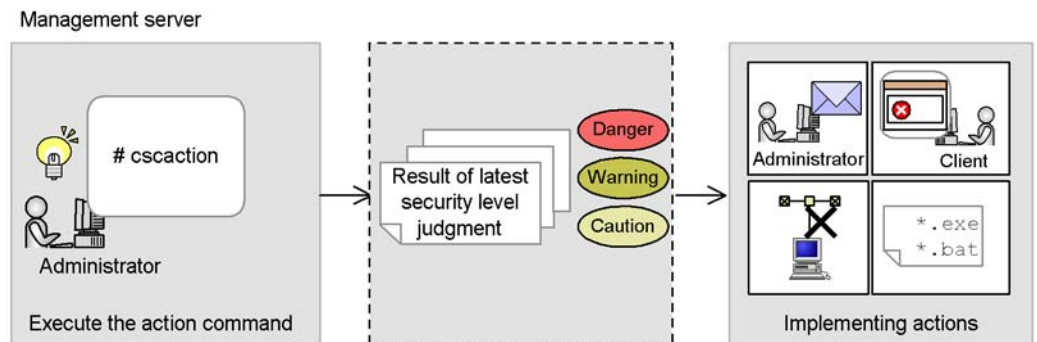
### (3) Implementing actions by the action command (cscaction)

By issuing the action command (`cscaction`) from a management server, an administrator can implement actions appropriate for the result of the latest security level judgment.

The administrator can use the `cscaction` command to implement actions when the security levels have already been judged by using the functionality that allows the judgment of security level and the implementation of actions to be performed separately, or to implement actions again for specific clients.

The following figure shows how actions are implemented by the action command (`cscaction`).

Figure 2-12: Implementing actions by the action command (cscaction)



For details about the action command (`cscaction`), see *cscaction (implements actions for a specified client)* in 15. Commands.

---

## 2.6 Managing client security levels

---

Client security levels are managed in the Client Security Management window of AIM. To open this window, choose the **Client Security Management** job category in an AIM window.

The **Client Security Management** job category contains the following job menus:

- **PC Security Level Management**

Monitors the client security levels. You can check the details about the security level for each judgment item, judge security levels, and implement actions.

- **Security Counter-Measure Evaluation**

Displays the points indicating the results of the evaluation of security measures taken on clients. The evaluation points can be used in a security audit.

- **Statistics**

Displays trends in the results of the evaluation of security measures taken on clients, on a group-by-group basis. This information can be displayed as a graph or output to a CSV file.

Users with one of the following roles can use the Client Security Management window:

- Administrator role for JP1/CSC

A JP1/CSC administrator can use the Security Policy Management window and all the job categories needed to run a client security management system in AIM.

- User role for JP1/CSC

JP1/CSC users can search for information managed by a client security control system in AIM, and can output the information to a file.

This role does not allow the user to access the Security Policy Management window, to judge security levels, or to implement actions.

- Administrator role for Asset Information Manager (optional product)

When Asset Information Manager (optional) is installed, the Asset Information Manager administrator can use all the job categories in the Security Policy Management window and in AIM. The Asset Information Manager administrator can also create JP1/CSC users. This is the highest user permission among the user roles.

For details about administrator roles, see *5.8 Creating CSC administrators and CSC users*.

The following explains each job.

### (1) PC Security Level Management

This job monitors and manages the client security levels. You can specify a search condition to search for clients with a high security risk level, and can output the search results to a CSV file. You can also judge client security levels and implement actions.

To manage client security levels, use the PC Search window. To display this window, choose **Client Security Management**, and then **PC Security Level Management**.

The following figure shows the PC Search window.

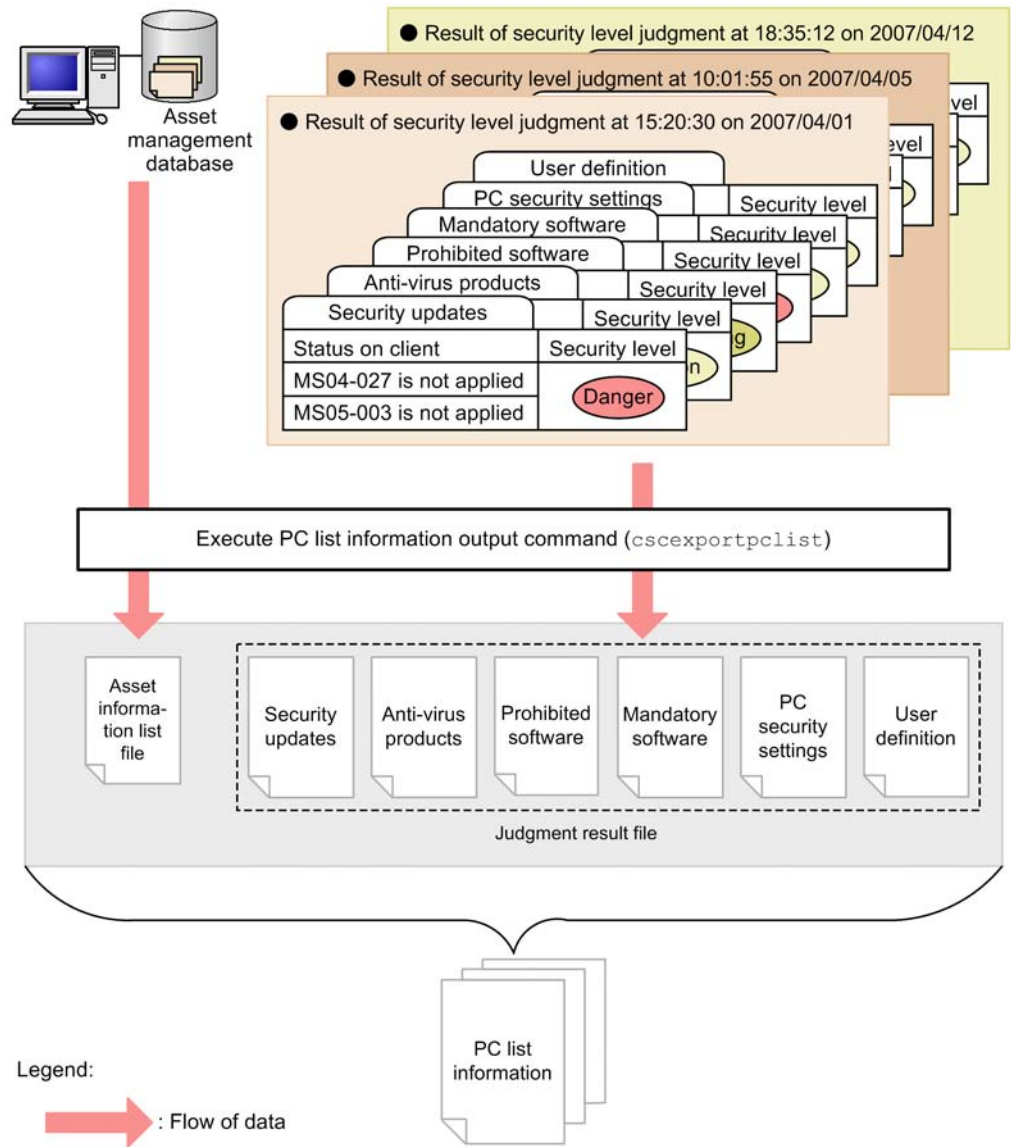
Figure 2-13: PC Search window

The screenshot shows the 'PC Search' window within the 'Asset Information Manager'. The interface includes a sidebar with a tree view containing 'Group' (Bangkok branch office, Headquarters, New York branch office) and 'Job of Asset Management' (Device Management, Software Applied Management, System Management, System Definition, Client Security Management, PC Security Level Management, Register Permitted PCs, Security Counter-Measure Evaluation, Statistics). The main area is titled 'Search' and 'CSV'. It features a 'Display' dropdown set to '200 results per page'. Below this are several search criteria with input fields and dropdown menus: 'Asset No.', 'Host name', 'IP address', 'User name', 'Group name' (with a 'Browse' button), 'PC security level' (with a 'not less than' dropdown), 'PC security level judgment date' (with a date picker), 'Number of consecutive times for the same security level' (with a 'times' dropdown), 'Number of consecutive days for the same security level' (with a 'days' dropdown), 'MAC address', 'Warning date' (with a date picker), 'Network connection status', 'Update date of network connection status' (with a date picker), 'Execution date of user definition' (with a date picker), 'Security level of security updates' (with a 'not less than' dropdown), and 'Security level of anti-virus products' (with a 'not less than' dropdown). The user 'csc\_admin' is logged in.

For details about managing PC security levels, see 8. *Monitoring Clients*.

The asset information and judgment results of clients whose security levels were judged can be output as PC list information to a CSV file. This file can be used for managing client security levels. You can also output PC list information that contains only the dates of security level judgments. To output the PC list information, use the PC list information output command (cscexportpclist).

Figure 2-14: Outputting PC list information



For details about the PC list information output command (`cscexportpclist`), see *cscexportpclist (outputs PC list information)* in 15. Commands. For details about the PC list information file, see 16.10 PC list information file.

## (2) Security Counter-Measure Evaluation

This job uses points to evaluate security measures on clients. A client for which all the

judgment items have been evaluated as **Safe** gets 100 points. On the other hand, points are deducted for a client with inadequate security measures, for example, if the latest update program has not been applied or invalid software has been installed. You can search for the evaluation results for a group or user in a window, and output the search result to a CSV file.

Use the Evaluation Condition Input window to evaluate security measures on clients. To display this window, choose **Client Security Management**, and then **Security Counter-Measure Evaluation**.

The following figure shows the Evaluation Condition Input window.

Figure 2-15: Evaluation Condition Input window

The screenshot shows the 'Evaluation Condition Input' window within the 'Asset Information Manager'. The interface includes a sidebar with a tree view under 'Job of Asset Management', where 'Client Security Management' is selected. The main panel contains search criteria fields: 'Group name' (with a 'Browse' button), 'Asset No.' (with a 'match part of the words' dropdown), 'User name' (with an 'including' dropdown), 'IP address' (with a 'match part of the words' dropdown), 'OS' (with a 'match part of the words' dropdown), 'Location' (with a 'Browse' button), 'Lowest score' (with a 'points not greater than' dropdown), 'Average score' (with a 'points not greater than' dropdown), 'Totals by' (set to 'Group'), and 'Group level' (set to '1 levels'). At the top right, there are 'Search' and 'CSV' buttons, and a 'Display 200 results per page' indicator.

For details about evaluating security measures, see *10.3 Evaluating the status of security measures on clients*.

### (3) Statistics

This job allows you to monitor trends in the status of security measures on a group-by-group basis. The following information can be displayed as statistics:

- Trends in the points indicating the results of security measure evaluation

## 2. Client Security Control System Functionality

- Trends in the proportion of clients whose security levels are satisfactory for each judgment item (countermeasure usage)
- Trends in the proportion of clients whose security levels are satisfactory for a given set of user-defined judgment items (user-defined countermeasure usage)

You can also check trends in countermeasure usage for individual judgment items. Statistics can be displayed as a graph or output to a CSV file.

To view statistics, use the Statistics Display Condition Input window. To display this window, choose **Client Security Management**, and then **Statistics**.

The following figure shows the Statistics Display Condition Input window.

Figure 2-16: Statistics Display Condition Input window

The screenshot shows a web application window titled "Asset Information Manager - Microsoft Internet Explorer". The main content area is titled "Job Management Partner 1/Asset Information Manager" and includes a user login "csc\_admin". On the left, there is a navigation pane with a tree view. The "Group" section lists "Bangkok branch office", "Headquarters", and "New York branch office". The "Location" section is empty. The "Job of Asset Management" section is expanded, showing a list of tasks: "Device Management", "Software Applied Management", "System Management", "System Definition", "Client Security Management", "PC Security Level Management", "Register Permitted PCs", "Security Counter-Measure Evaluation", and "Statistics" (which is highlighted). The main area on the right is a form titled "Search CSV". It contains several input fields: "Group name" with a "Browse" button, "Group level" set to "1 levels", "Type of totals" set to "Countermeasure usage", "Period to total" with a date picker set to "(YYYYMMDD)", "Interval to total" set to "Month", and "Start of week" set to "Sun".

For details about statistics, see *10.4 Gauging trends in security measure evaluation*.



## Chapter

---

# 3. Client Security Control System Configuration

---

This chapter describes the system configuration, product configuration, and prerequisite programs for setting up a client security control system.

- 3.1 System configuration
- 3.2 Product configuration
- 3.3 Prerequisite programs

## 3.1 System configuration

---

This section explains the system configuration for a client security control system.

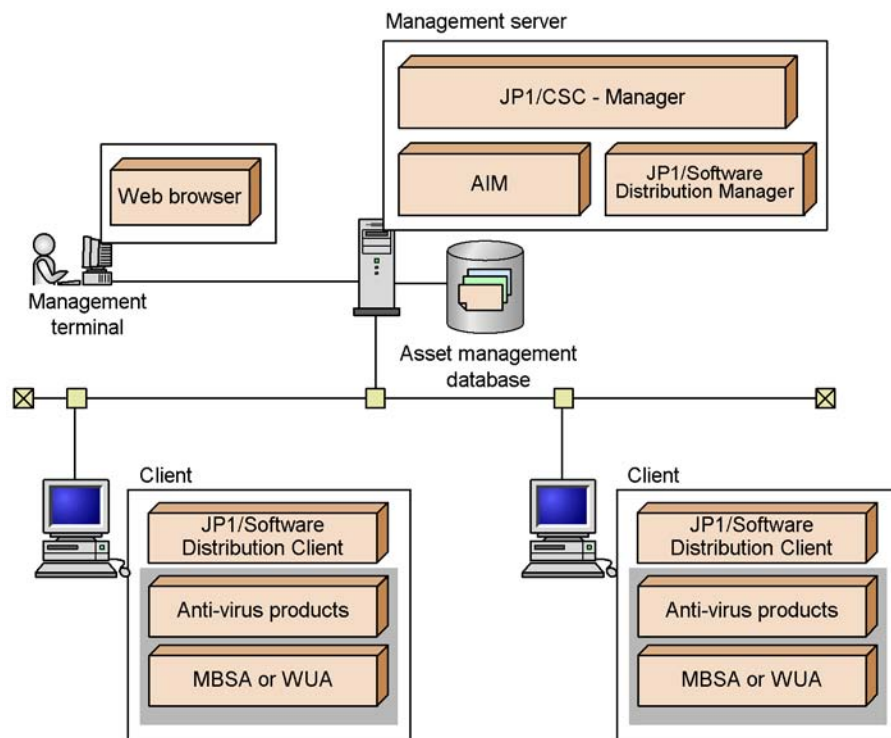
The following system configuration examples are provided:

- Using a client security control system in the basic configuration
- Automatically updating judgment policies for anti-virus products
- Operation with a remote management server
- Operation with a quarantine system

### **(1) Basic configuration**

The following figure shows the basic configuration of a client security control system.

*Figure 3-1: System configuration of a client security control system (basic configuration)*



Legend:

 : Optional product

The system components are described below.

#### Management server

A management server manages inventory information in an asset management database, and judges client security levels according to the security policy. It also implements actions appropriate to these security levels.

The following products must be installed on the management server:

- JP1/CSC - Manager
- JP1/Software Distribution Manager
- Asset Information Manager or Asset Information Manager Subset Component of JP1/Software Distribution Manager

#### Management terminal

A management terminal is used by an administrator to reference the asset management database, manage client asset information, monitor the status of client security measures, and implement actions. These tasks are performed in the AIM windows.

A Web browser must be installed on the management terminal.

#### Client

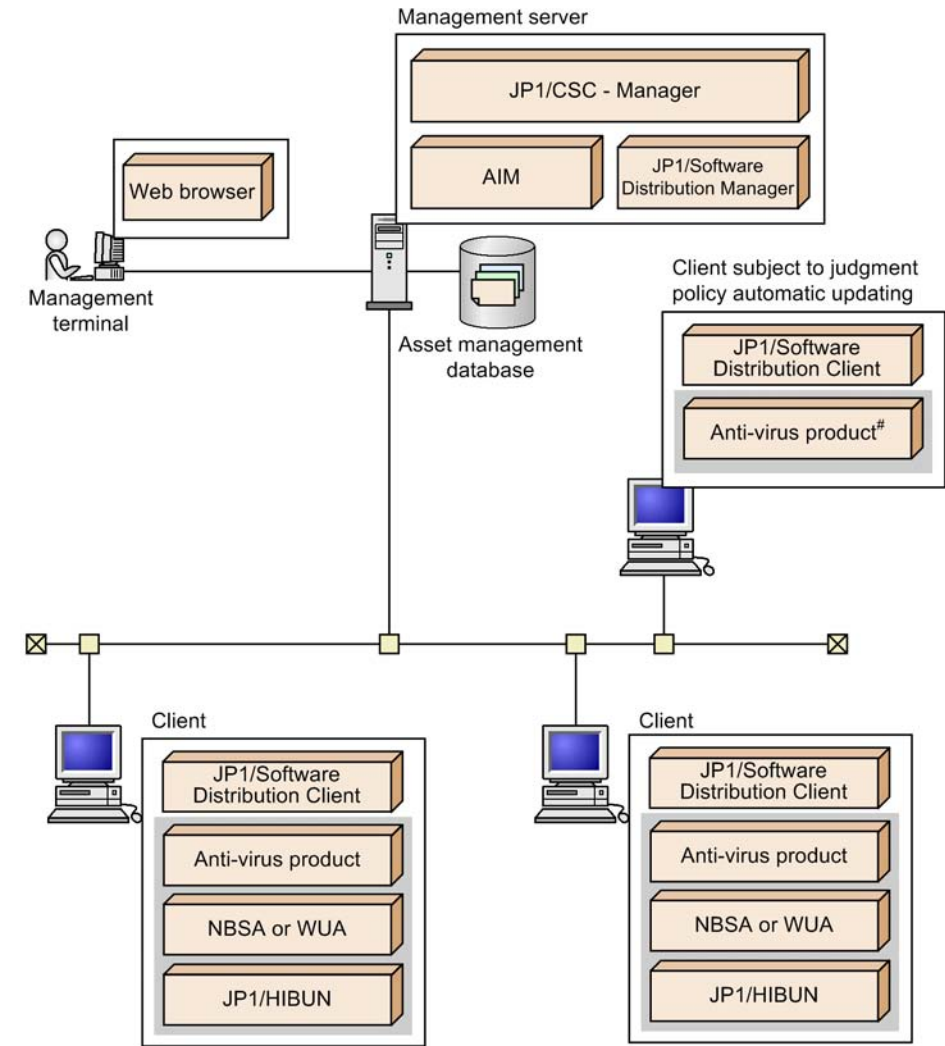
A client is the entity that is managed in a client security control system. All updates to the client inventory information are immediately notified to JP1/Software Distribution Manager on the management server.

JP1/Software Distribution Client must be installed on each client.

#### ***(2) System configuration for automatically updating judgment policies for anti-virus products***

The following figure shows the system configuration when linkage with an anti-virus product installed on a client is used to automatically update the judgment policies for anti-virus products.

Figure 3-2: System configuration for automatically updating the judgment policies for anti-virus products



Legend:

■ : Optional product

#: Anti-virus product linked with automatic judgment policy updating for anti-virus products

The system components are described below.

Management server

A management server manages inventory information in an asset management database, and judges client security levels according to the security policy. It also implements actions appropriate to these security levels.

The following products must be installed on the management server:

- JP1/CSC - Manager
- JP1/Software Distribution Manager
- Asset Information Manager Subset Component of JP1/Software Distribution, or AIM

#### Management terminal

A management terminal is used by an administrator to reference the asset management database, manage client asset information, monitor the status of client security measures, and implement actions. These tasks are performed in the AIM windows.

A Web browser must be installed on the management terminal.

#### Client subject to judgment policy automatic updating

This type of client has an anti-virus product linked with automatic judgment policy updating for anti-virus products. Judgment policy definitions for the anti-virus products are automatically updated based on the update information for the anti-virus product installed on this client.

The following products must be installed on this client:

- Windows version of JP1/Software Distribution Client
- Anti-virus product compatible with automatic judgment policy updating

For details about the anti-virus products, see *4.6 Installing anti-virus products that link with automatic judgment policy updating*.

For details about the system configuration when the judgment policies for anti-virus products are automatically updated by linkage to JP1/CSC - Manager Remote Option on a remote management server, see *(3) System configuration with a remote management server*.

#### Client

A client is an entity that is managed in a client security control system. All updates to the client inventory information are immediately reported to JP1/Software Distribution Manager on the management server.

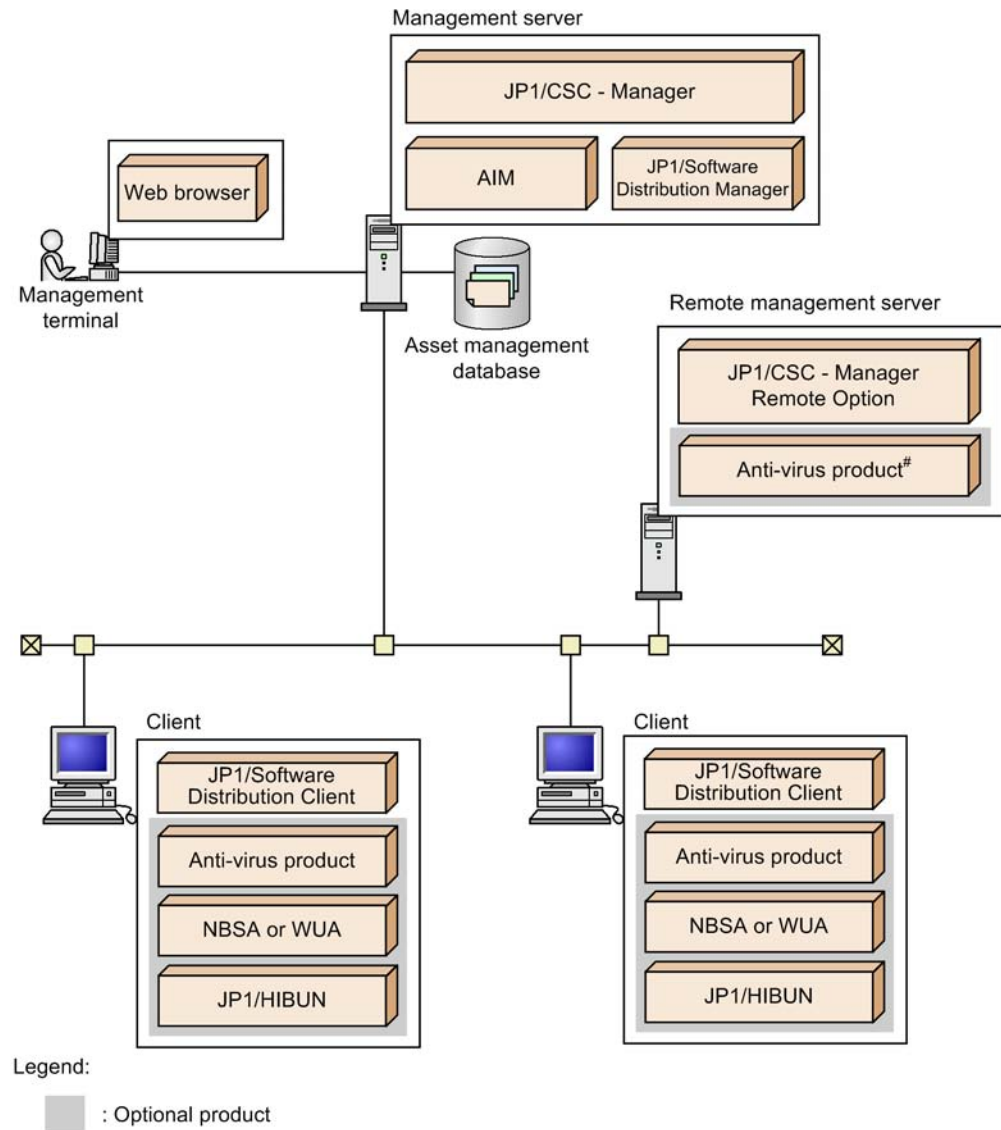
The Windows version of JP1/Software Distribution Client must be installed on each client.

**(3) System configuration with a remote management server**

This system configuration is required if you want to control client network connections from a remote system or want to automatically update the judgment policies for anti-virus products by linkage with JP1/CSC - Manager Remote Option.

JP1/CSC - Manager Remote Option must be installed on the remote management server.

Figure 3-3: System configuration with a remote management server



#: Anti-virus product linked with automatic judgment policy updating for anti-virus products

The system components are described below.

#### Management server

A management server manages inventory information in an asset management database, and judges client security levels according to the security policies. It



also implements actions appropriate to the set security levels.

The following products must be installed on the management server:

- JP1/CSC - Manager
- JP1/Software Distribution Manager
- Asset Information Manager or Asset Information Manager Subset Component of JP1/Software Distribution Manager

#### Management terminal

A management terminal is used by an administrator to reference the asset management database, manage client asset information, monitor the status of client security measures, and implement actions. These tasks are performed in the AIM windows.

A Web browser must be installed on the management terminal.

#### Remote management server

The following product must be installed on the remote management server:

- JP1/CSC - Manager Remote Option

The following products and systems are also required, depending on how the remote management server is to be used:

- To remotely control client network connections

You must incorporate a remote system and a quarantine system. For details about building a quarantine system, see *(4) System configuration with a quarantine system*.

- To automatically update judgment policies for anti-virus products by linking with JP1/CSC - Manager Remote Option

An anti-virus product compatible with automatic judgment policy updating must be installed. For details about the anti-virus products, see *4.6 Installing anti-virus products that link with automatic judgment policy updating*.

JP1/CSC - Manager Remote Option can be installed on the management server or on the quarantine system's network control server, authentication server, or treatment server.

#### Client

A client is the entity that is managed in a client security control system. All updates to the client inventory information are immediately notified to JP1/Software Distribution Manager on the management server.

JP1/Software Distribution Client must be installed on each client.

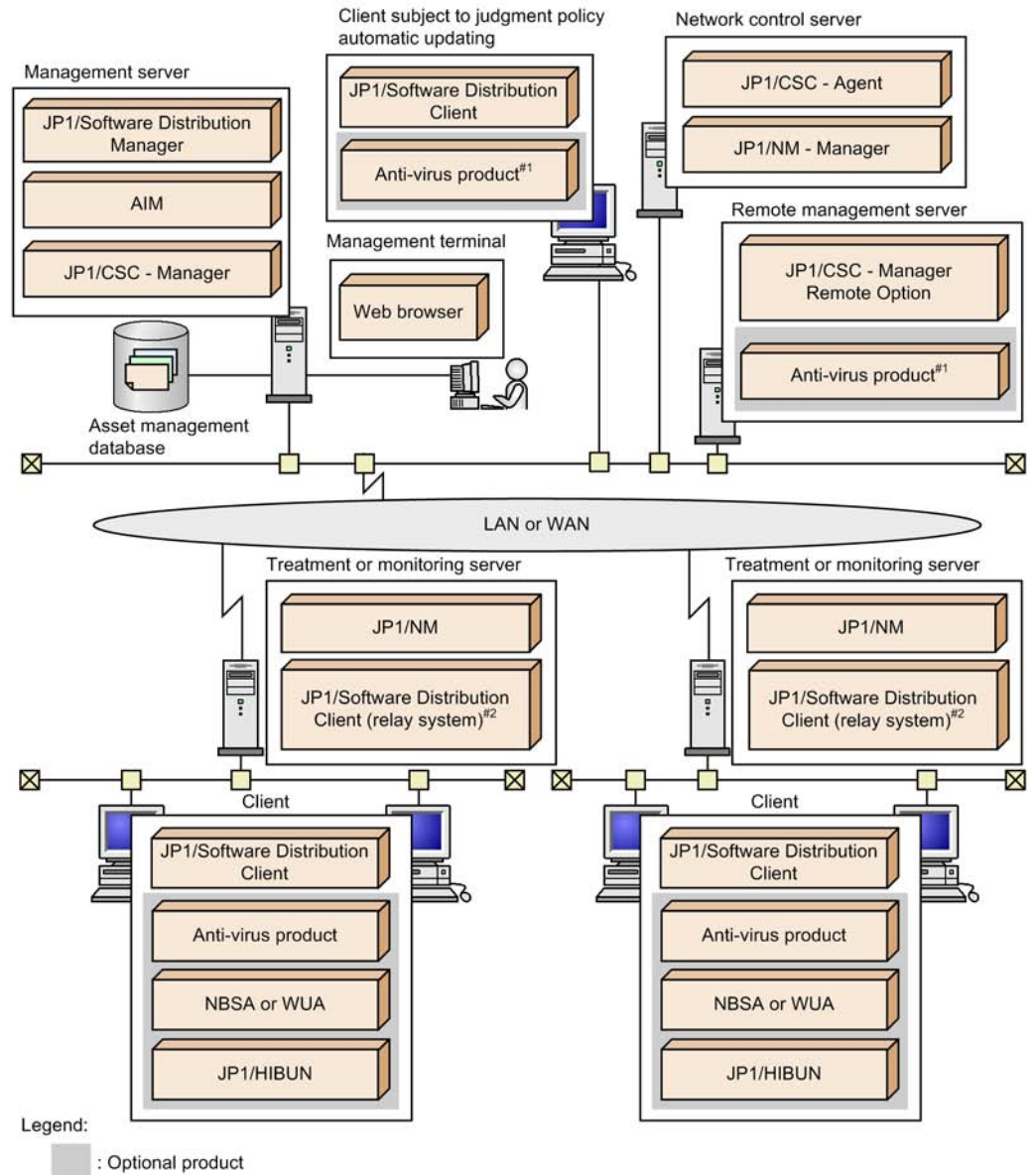
**(4) System configuration with a quarantine system**

The figures below show examples of system configurations that incorporate a quarantine system. Examples of a quarantine system linked to JP1/Network Monitor and a quarantine system linked to an authentication server are shown.

Linkage with JP1/Network Monitor:

The following figure shows JP1/CSC linked to JP1/NM.

Figure 3-4: System configuration with a quarantine system (linked to JP1/NM)



#1: Anti-virus product linked with automatic judgment policy updating for anti-virus products

#2: JP1/Software Distribution SubManager 07-05 or later can be used instead.

When the Windows version of JP1/Software Distribution 09-00 or later or the Linux version of JP1/Software Distribution 08-11 or later is used, these products can also be installed on another server.

A client security control system consists of the following components when

linked to JP1/NM:

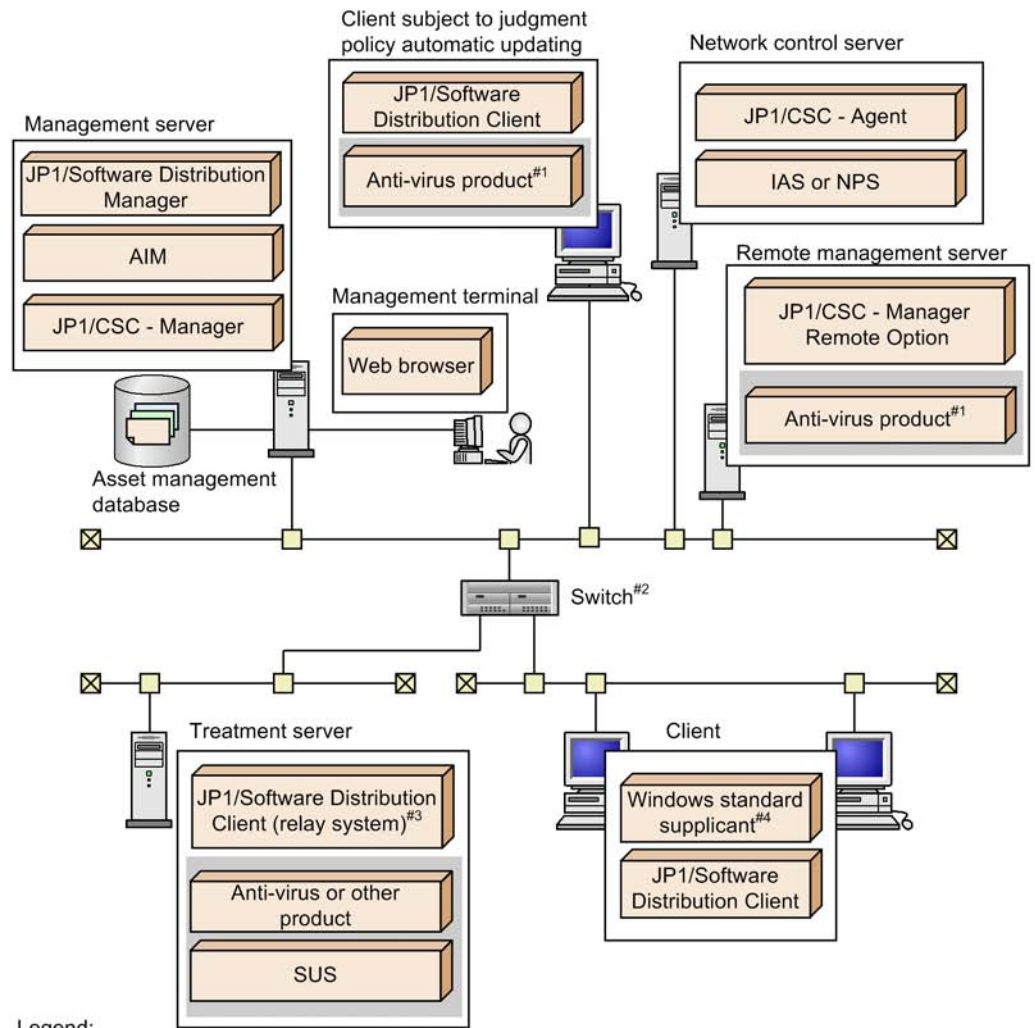
- Management server
- Management terminal
- Remote management server
- Client subject to judgment policy automatic updating
- Network control server
- Treatment and monitoring server
- Clients

For details about these components, see *12.2.1 Basic configuration of quarantine system linked to JP1/NM*.

Linkage with an authentication server:

The following figure shows JP1/CSC linked to an authentication server.

Figure 3-5: System configuration with a quarantine system (linked to an authentication server)



IAS or NPS : Microsoft Internet Authentication Service or Network Policy Server

SUS : Microsoft Software Update Services

#1: Anti-virus product linked with automatic judgment policy updating for anti-virus products.

#2: Switch supporting IEEE 802.1X or MAC authentication

#3: JP1/Software Distribution SubManager 07-05 or later can be used instead.

#4: This product is not necessary when MAC authentication is used.

If linked to an authentication server a client security control system consists of the

following components:

- Management server
- Management terminal
- Remote management server
- Client subject to judgment policy automatic updating
- Authentication server
- Treatment server
- Switch supporting IEEE 802.1X or MAC authentication
- Clients

For details about each component, see *12.3.1(1) Basic configuration of a quarantine system linked to an authentication server*.

## 3.2 Product configuration

The products used in a client security control system include basic products that must be installed and optional products that may be installed as required. Optional products can be combined to suit the user environment, and extend functionality.

The following table lists the products used in a client security control system.

*Table 3-1: Products used in a client security control system*

System configuration element	Product	Installation	Product description
Management server	JP1/CSC - Manager	Mandatory	Judges the client security level, and implements an action appropriate to the security level.
	Asset Information Manager or Asset Information Manager Subset Component of JP1/Software Distribution Manager	Mandatory	Manages the inventory information collected by JP1/Software Distribution, in an asset management database.
	JP1/Software Distribution Manager	Mandatory	Collects and manages inventory information collected from clients.
Management terminal	Microsoft Internet Explorer	Mandatory	A Web browser.
Remote management server	JP1/CSC - Manager Remote Option	Optional	A system that controls client network connections from another system or that automatically updates the judgment policies for anti-virus products.
	Anti-virus product compatible with automatic judgment policy updating <sup>#1</sup>	Optional	Software that prevents computer virus infections. This software links with JP1/CSC - Manager Remote Option to automatically update the judgment policies for anti-virus products.
Client	JP1/Software Distribution Client	Mandatory	Sends client inventory information to JP1/Software Distribution Manager.
	MBSA	Optional	A tool that detects security updates (patches and service packs) not applied to the client.

System configuration element	Product	Installation	Product description
	WUA	Optional	A tool that detects security updates (patches and service packs) not applied to the client. In addition to OS security updates, WUA can detect unapplied software security updates for Microsoft Office and other applications.
	Anti-virus product	Optional	Software that prevents computer virus infections. To automatically update judgment policies by linking with an anti-virus product installed on a client, the anti-virus product compatible with automatic judgment policy updating <sup>#1</sup> is required.
Network control server, authentication server, or treatment server <sup>#2</sup>	JP1/CSC - Agent	Optional	Receives instructions from JP1/CSC - Manager, and instructs actions to the linked network control product about actions to be taken.
	Network control product	Optional	A product that controls a client's network connection.

#1

For details about anti-virus products compatible with automatic judgment policy updating, see *4.6 Installing anti-virus products that link with automatic judgment policy updating*.

#2

These servers are required only for running a quarantine system. For details about the products needed to build and run a quarantine system, see *Part 5. Quarantine Systems*.

### (1) Mandatory products

The following programs are required to be installed on a client security control system:

- JP1/CSC - Manager
- Asset Information Manager or Asset Information Manager Subset Component of JP1/Software Distribution Manager
- JP1/Software Distribution



- JP1/Software Distribution Manager
- JP1/Software Distribution Client
- Microsoft Internet Explorer

## **(2) Optional products**

Various functions can be achieved on a client security control system by combining optional products with the mandatory ones. For details about the products needed to build and run a quarantine system, see *Part 5. Quarantine Systems*.

- JP1/CSC - Agent
- JP1/CSC - Manager Remote Option
- MBSA

MBSA can be used to detect Windows security updates that have not been applied to a client. MBSA is set on the client.

- WUA

WUA can be used to detect Windows security updates that have not been applied to a client. In addition to OS security updates, WUA can detect unapplied software security updates for Microsoft Office and other applications. WUA is set on the client.

- Anti-virus product

An anti-virus product can be used to prevent a client from becoming infected with computer viruses. A client security control system can check whether an anti-virus product is installed on a client, as well as whether the version of the virus definition file is up to date.

In addition, judgment policy definition information can be updated automatically by linking with an anti-virus product supported by JP1/Software Distribution. For details about the anti-virus products compatible with the automatic judgment policy updating, see *4.6 Installing anti-virus products that link with automatic judgment policy updating*.

Note that the anti-virus products managed by a client security control system are limited to those for which JP1/Software Distribution can collect inventory information.

---

## 3.3 Prerequisite programs

---

This subsection explains the prerequisite programs required to operate a client security control system.

### ***(1) Prerequisite programs for a management server***

OS

One of the following OSs can be used to run a management server:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

JP1 programs

- JP1/Software Distribution Manager<sup>#</sup>
- Asset Information Manager or Asset Information Manager Subset Component of JP1/Software Distribution Manager

#

This can also be installed on a separate machine. However, in this case, you must install only Remote Installation Manager on the management server, to report messages to clients.

### ***(2) Prerequisite programs for a remote management server***

OS

One of the following OSs can be used to run a remote management server:

- Windows 2000
- Windows Server 2003
- Windows XP Professional
- Windows Vista
- Windows Server 2008
- Windows Server 2008 R2
- Windows 7

### ***(3) Prerequisite programs for a management terminal***

Web browser

- Microsoft Internet Explorer

**(4) Prerequisite programs for a client**

JP1 program

- JP1/Software Distribution Client

*Reference note:*

JP1/Software Distribution SubManager or JP1/Software Distribution Manager (relay manager) may be used instead of JP1/Software Distribution Client.

**(5) Prerequisite programs for the network control server, authentication server, treatment server, and monitoring server**

For the prerequisite programs for the network control server, authentication server, treatment server, and monitoring server, see *PART 5. Quarantine Systems*.



## **Chapter**

---

# **4. Considerations for Installing and Operating a Client Security Control System**

---

This chapter explains the items that require consideration, from installation to the start of operation for a client security control system.

- 4.1 Design considerations and system configuration
- 4.2 Setting up a management server
- 4.3 Setting up a remote management server
- 4.4 Setting up a client
- 4.5 Setting up a quarantine system
- 4.6 Installing anti-virus products that link with automatic judgment policy updating
- 4.7 Considerations for security policies
- 4.8 Lifecycle of a client security control system

## 4.1 Design considerations and system configuration

When installing a client security control system, it is important to consider the functionality to be used. Then, keep the organizational structure and number of client machines in mind when setting up the system.

To implement actions involving network connection denial and permission for clients, a network control product must be installed.

### 4.1.1 Items to consider for system installation

When installing a client security control system, it is important to consider the functionality to be used. The functionality for a client security control system includes core functionality, and functionality that can be selected depending on management requirements.

#### (1) Core functionality

The core functionality of a client security control system consists of that to manage inventory information, and that to manage client security. The following table lists the products required to implement this functionality, and their respective installation destinations.

*Table 4-1: Core functionality and product installation destinations*

Core functionality	Required product	Installation destination
Management of inventory information and management of client security	JP1/CSC - Manager	Management server
	Asset Information Manager or Asset Information Manager Subset Component of JP1/Software Distribution Manager	
	JP1/Software Distribution Manager	
	JP1/Software Distribution Client	Client

#### (2) Optional functionality

A client security control system also provides optional functionality, which an administrator can choose based on the management requirements. The following table lists the optional functionality of a client security control system, and the installation destination of each product.

Table 4-2: Optional functionality and product installation destinations

No.	Optional functionality	Required product	Installation destination
1	Managing information about Windows security updates not yet applied on clients	MBSA or WUA	Client <sup>#1</sup>
2	Managing the status of anti-virus product settings (such as whether or not pattern files are up to date)	Anti-virus product supported by JP1/Software Distribution <sup>#2</sup>	Client
3	Controlling client network connections from a remote system.	JP1/CSC - Manager Remote Option	Remote management server
4	Automatically updating judgment policies for anti-virus products (including virus definition file version and engine version) (by linkage with a client).	Anti-virus product compatible with automatic judgment policy updating <sup>#3</sup>	Client
5	Automatically updating judgment policies for anti-virus products (including virus definition file version, engine version, etc.) (by linkage with JP1/CSC - Manager Remote Option).	JP1/CSC - Manager Remote Option	Remote management server
		Anti-virus product compatible with automatic judgment policy updating <sup>#3</sup>	
6	Using a quarantine system to control network connections for clients with high security risk levels and to implement security measures.	See <i>Part 5. Quarantine Systems</i>	See <i>Part 5. Quarantine Systems</i>

#1

To use MBSA, the MBSA command line interface and the MBSA database file must be set up.

To use WUA, WUA 2.0 and Windows Installer 3.0 must be installed and the WUA 2.0 database file must be set up.

For details about MBSA and WUA, see *7.4 Detecting security updates not applied to a client*.

#2

For details about anti-virus products supported by JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Description and Planning Guide*.

#3

For details about the anti-virus products compatible with automatic judgment policy updating, see 4.6 *Installing anti-virus products that link with automatic judgment policy updating*.

## 4.1.2 Designing a system configuration

After giving consideration to the functionality to be used, design a system configuration to suit the scale and environment for the system.

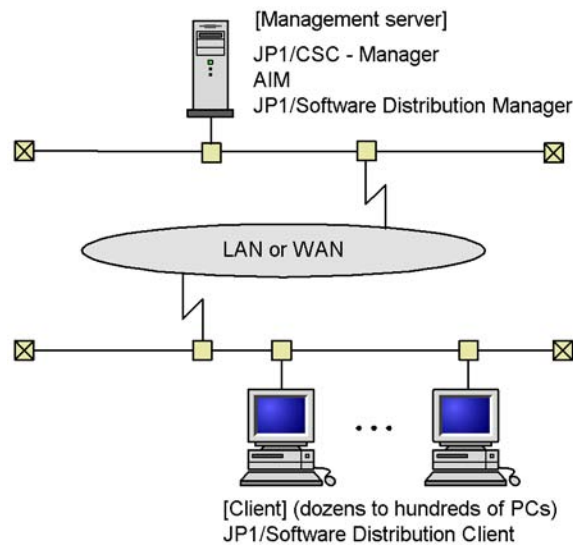
This section describes a basic configuration, and a configuration for a large-scale system. This section also describes a system configuration for operating a client security control system with a remote management server, and a configuration using a quarantine system.

### (1) Basic configuration

In a basic configuration of a client security control system, client monitoring is performed using one management server and one network control server.

The following figure shows a basic configuration.

Figure 4-1: Basic configuration



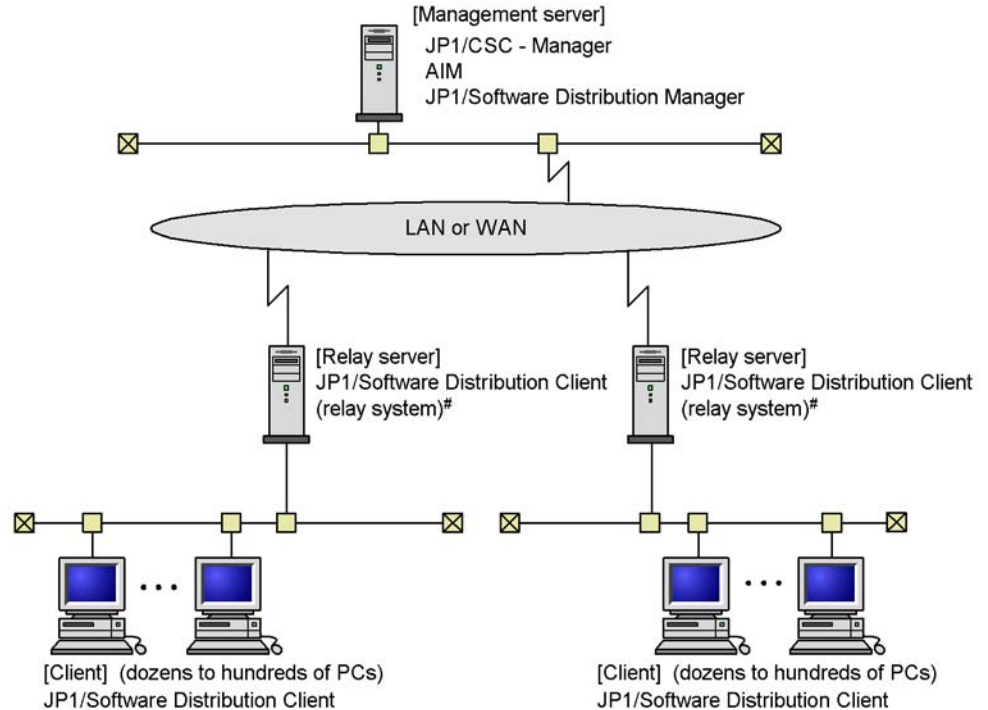


**(2) Configuration for a large-scale system**

For organizations with a large number of clients or sites, a relay system is used to achieve a hierarchical configuration. On the relay system, install either JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager.

The following figure shows a configuration for a large-scale system.

Figure 4-2: Configuration for a large-scale system



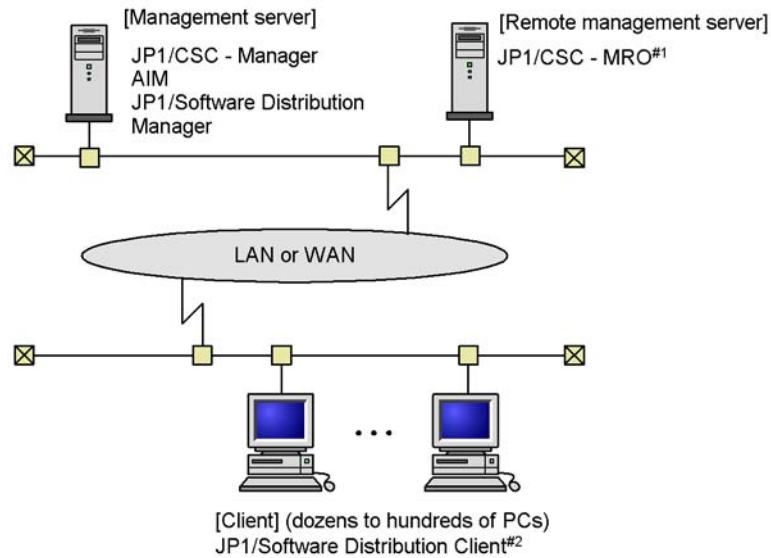
# JP1/Software Distribution SubManager may be used instead.

**(3) Configuration for operation with a remote management server**

To control client network connections from another system or to automatically update the judgment policies for anti-virus products by linkage with JP1/CSC - Manager Remote Option, you must use a system configuration that links with the other system, such as a model system for your anti-virus product. In such a configuration, JP1/CSC - Manager Remote Option must be installed on the remote management server.

The following figure shows a configuration with a remote management server.

*Figure 4-3: Configuration with a remote management server*



#1: Job Management Partner 1/Client Security Control - Manager Remote Option

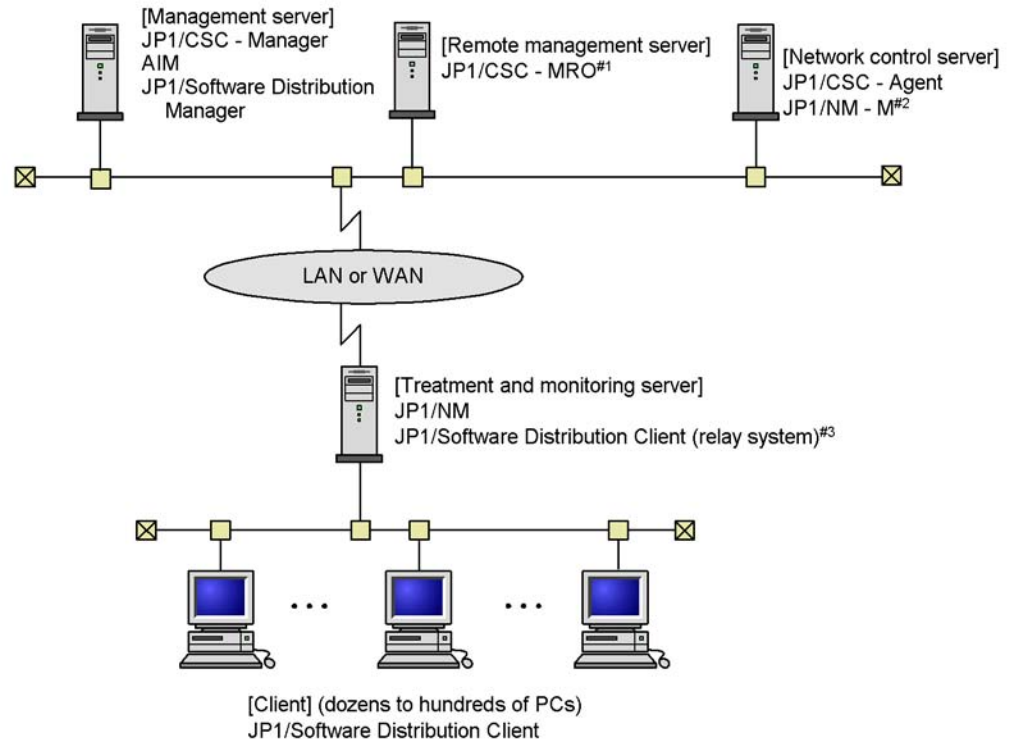
#2: In the Linux version of JP1/Software Distribution Client, the judgment policy for the antivirus product cannot be updated automatically.

#### **(4) Configuration for using a quarantine system**

If clients with a high security risk level are detected, you can use a quarantine system to take security measures on these clients.

The following figures show the configuration of a system linked to JP1/Network Monitor and the configuration of a system linked to an authentication server.

Figure 4-4: Quarantine system configuration for linkage with JP1/NM



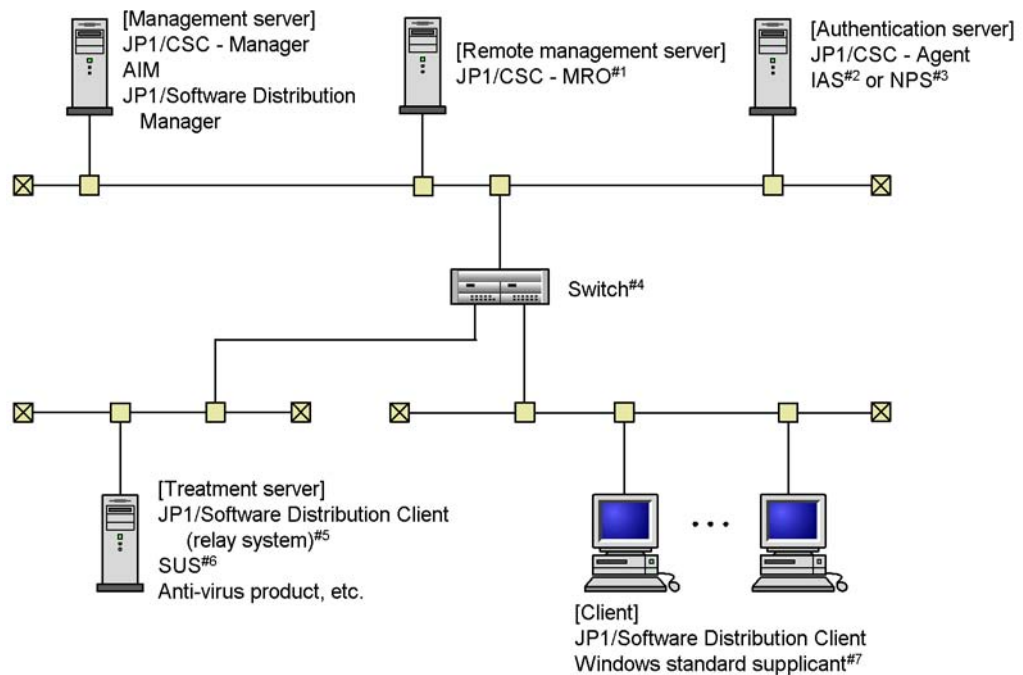
#1: Job Management Partner 1/Client Security Control - Manager Remote Option

#2: Job Management Partner 1/Network Monitor - Manager

#3: JP1/Software Distribution SubManager 07-50 or later may be used instead.

JP1/NM can also be installed on another server, depending on the version. In Windows, JP1/NM 09-00 or later can be installed on another server. In Linux, JP1/NM 08-11 or later can be installed on another server.

*Figure 4-5: Quarantine system configuration for linkage with an authentication server*



- #1: Job Management Partner 1/Client Security Control - Manager Remote Option
- #2: Microsoft Internet Authentication Service
- #3: Network Policy Server
- #4: Switch supporting IEEE 802.1X or MAC authentication
- #5: Version 07-50 or later of JP1/Software Distribution SubManager may be used instead.
- #6: Microsoft Software Update Services
- #7: This product is not necessary when MAC authentication is used.

For details about operating a quarantine system, see *Part 5. Quarantine Systems*.

### 4.1.3 Operating on a cluster system

JP1/CSC - Manager and JP1/CSC - Agent can operate on a cluster system. Operation can be performed on a configuration consisting of an active server, which performs normal operation, and a standby server, which takes on operations from the active server during failure.

For details about operating JP1/CSC - Manager and JP1/CSC - Agent on a cluster system, see *Appendix D. Operation on a Cluster System*.

For details about operating JP1/Software Distribution on a cluster system, see the

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

For details about operating Asset Information Manager and Asset Information Manager Subset Component of JP1/Software Distribution Manager on a cluster system, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

---

## 4.2 Setting up a management server

---

A management server controls the overall system.

This section explains how to set up a management server.

### 4.2.1 Procedures for program setup

Install and set up the following programs on the management server, in order:

1. JP1/Software Distribution Manager
2. Asset Information Manager (optional)
3. JP1/CSC - Manager

Note that JP1/Software Distribution Manager can also be installed on a separate machine, in which case its Remote Installation Manager component must also be installed on the management server.

*Note:*

To use AIM, either Asset Information Manager or Asset Information Manager Subset Component of JP1/Software Distribution Manager must be installed. You cannot install both products on the same management server.

For details about installation and setup, see *5. Installation and Setup*.

### 4.2.2 Setting up a database

A client security control system uses the asset management database of AIM. When estimating the size of the database, be sure to include the capacity used by JP1/CSC - Manager.

For details about estimating the size of a database used for JP1/CSC - Manager, see *E.1 Disk capacity used by JP1/CSC - Manager*.

For details about creating an asset management database for AIM, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems (when using Asset Information Manager Subset Component of JP1/Software Distribution Manager) or the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide* (when using Asset Information Manager).

For details about how to operate the database, see the manual *Job Management Partner 1/Asset Information Manager Administrator's Guide*.

### 4.2.3 Setting up a management terminal

To access the Client Security Management windows of AIM, use the following Web browser:

- Microsoft Internet Explorer

An administrator uses the Client Security Management windows displayed in the Web browser to monitor clients, perform security audits, judge client security levels, and implement actions.

Note that you must have user permissions for JP1/CSC to use the Client Security Management windows of AIM. For details about how to create user permissions for JP1/CSC, see *5.8 Creating CSC administrators and CSC users*.

---

## 4.3 Setting up a remote management server

---

Setup for a remote management server is performed after the management server is set up.

Be sure to install and set up Job Management Partner 1/Client Security Control - Manager Remote Option on each remote management server. Set up other systems such as model systems for anti-virus products as necessary.

For details about installing and setting up these products, see *5. Installation and Setup*.

### 4.3.1 Anti-virus products

You can link a remote management server with an anti-virus product compatible with automatic judgment policy updating to automatically update the judgment policies (virus definition files and engine version) for anti-virus products.

For details about the anti-virus products compatible with automatic judgment policy updating, see *4.6 Installing anti-virus products that link with automatic judgment policy updating*.



## 4.4 Setting up a client

Setup for each client is performed after the management server is set up. Be sure to install and set up JP1/Software Distribution Client on each client. Install other optional products as necessary.

### 4.4.1 Functionality limitations by the version of JP1/Software Distribution Client

When JP1/Software Distribution Client is already installed on a client, the functionality that can be used depends on the version of JP1/Software Distribution Client.

The following table lists the functionality that can be used for each version of JP1/Software Distribution Client.

*Table 4-3: Functionality that can be used for each version*

Version of JP1/Software Distribution Client <sup>#1</sup>	Whether or not security level is judged						Client notification
	Security updates	Anti-virus products	Prohibited software	Mandatory software	PC security settings	User definition	
09-50 or later	Yes	Yes	Yes	Yes	Yes	Yes	Yes <sup>#2</sup>
09-00	Yes	Yes	Yes	Yes	Yes <sup>#3</sup>	Yes	Yes <sup>#2</sup>
08-51	Yes	Yes	Yes	Yes	Yes	Yes	Yes <sup>#2</sup>
08-10	Yes	Yes	Yes	Yes	--	Yes	Yes <sup>#2</sup>
08-00	Yes	Yes	Yes	Yes	--	Yes	Yes
07-50	Yes <sup>#4,#5</sup>	Yes	Yes	Yes	--	Yes	Yes
07-00	--	Yes	Yes	Yes	--	Yes	--
Version 6	--	--	Yes	Yes	--	Yes	--

Legend:

Yes: Can be used.

--: Cannot be used.

<sup>#1</sup>

Client inventory information is not obtained automatically for JP1/Software

Distribution Client version 07-00 or earlier. Execute the *Get software information from client* job to obtain inventory information.

#2

Messages are sent to a client in either HTML or text format. Sending messages in HTML format requires JP1/Software Distribution Client version 08-10 or later. For version 08-00 or earlier, operation is as follows:

- When sending a message based on an action policy:

The message is sent in text format even if HTML format is specified.

- When sending a message from the PC List window:

HTML tags are displayed because the message is sent in HTML format.

#3

You cannot use BitLocker to manage whether drive encryption has been set.

#4

You cannot use WUA to manage which Windows security updates are applied to a client.

#5

You cannot use MBSA to manage which Windows security updates are applied to a client.

*Note:*

Table 4-3 also applies if JP1/Software Distribution SubManager or JP1/Software Distribution Manager (relay manager) is installed on the client.

#### **4.4.2 MBSA or WUA**

By linking to MBSA or WUA, JP1/Software Distribution can manage whether the latest Windows security updates have been applied to the client.

When using MBSA, you can detect any security updates not applied to the client by distributing MBSA commands and MBSA database files to the client, and then executing jobs.

When using WUA, you can detect any security updates not applied to the client by installing WUA 2.0 and Windows Installer 3.0 on the client, distributing WUA 2.0 database files to the client, and then executing jobs. In addition to OS security updates, WUA can detect unapplied software security updates for Microsoft Office and other applications.

For details about using MBSA or WUA to detect security updates that have not been applied to the client, see *7.4 Detecting security updates not applied to a client*.

### 4.4.3 Anti-virus products

An anti-virus product can be installed on a client, to prevent computer virus infections. The products that can be managed by a client security control system are limited to those supported by JP1/Software Distribution. For details about the anti-virus products supported by JP1/Software Distribution, see the manual for each version of JP1/Software Distribution.

Linkage with the anti-virus product installed on a client makes it possible for the judgment policies for anti-virus products to be updated automatically. For details about the anti-virus products compatible with automatic judgment policy updating, see *4.6 Installing anti-virus products that link with automatic judgment policy updating*.

---

## 4.5 Setting up a quarantine system

---

To set up a quarantine system, you must set up a client security control system in a basic configuration, together with the servers required by the linked product.

You can set up a quarantine system by linking JP1/CSC to either of the following products:

- JP1/NM
- Authentication server (IEEE 802.1X or MAC authentication)
- JP1/Software Distribution (AMT Linkage facility)

When setting up a quarantine system, install JP1/CSC - Agent on the server where the linked product is installed.

For details about setting up a quarantine system using these two types of linked products, see *13. Setting Up a Quarantine System*.

## 4.6 Installing anti-virus products that link with automatic judgment policy updating

An anti-virus product compatible with the automatic judgment policy update functionality can be installed on a client or remote management server. The linkage with the anti-virus product enables the judgment policies for anti-virus products (virus definition files and engine version) to be updated automatically.

The table below lists the anti-virus products compatible with automatic judgment policy update functionality. Note that the name of an anti-virus product name displayed by a client security control system might be different from the actual product name.

*Table 4-4: Anti-virus products compatible with automatic judgment policy update*

Company name	Product name / version		Display name in client security control system
Avira	Avira AntiVir Professional	9(32bit), 10(32bit)	Avira AntiVir Professional
		9(64bit), 10(64bit)	Avira AntiVir Professional 64bit
	Avira AntiVir Server	10.0.0.1824(32bit)	Avira AntiVir Server
		10.0.0.1824(64bit)	Avira AntiVir Server 64bit
ESET	ESET NOD32 Antivirus	4.2.71.2(32bit)	ESET NOD32 Antivirus
		4.2.71.2(64bit)	ESET NOD32 Antivirus 64bit
F-Secure	F-Secure Anti-Virus Client Security	5.7, 6.01	F-Secure Anti-Virus Client Security
	F-Secure Client Security	7.0, 7.1	F-Secure Client Security
		8.01(32bit)	F-Secure Client Security 8.01
		8.01(64bit)	F-Secure Client Security 8.01 64bit
		9.00(32bit)	F-Secure Client Security 9.00

#### 4. Considerations for Installing and Operating a Client Security Control System

Company name	Product name / version		Display name in client security control system
		9.00(64bit)	F-Secure Client Security 9.00 64bit
		9.01(32bit)	F-Secure Client Security 9.01
		9.01(64bit)	F-Secure Client Security 9.01 64bit
		9.10(32bit)	F-Secure Client Security 9.10
		9.10(64bit)	F-Secure Client Security 9.10 64bit
		9.11(32bit)	F-Secure Client Security 9.11
		9.11(64bit)	F-Secure Client Security 9.11 64bit
Kaspersky	Kaspersky Open Space Security	6.0.4.1424(32bit)	Kaspersky Anti-Virus 6.0 for Windows Servers
			Kaspersky Anti-Virus 6.0 for Windows Workstations
		6.0.4.1424(64bit)	Kaspersky Anti-Virus 6.0 for Windows Servers 64bit
			Kaspersky Anti-Virus 6.0 for Windows Workstations 64bit
McAfee	McAfee Managed Total Protection	4.7(32bit), 5.0(32bit)	Managed Total Protection
		4.7(64bit), 5.0(64bit)	Managed Total Protection 64bit
	McAfee VirusScan Enterprise	8.8(32bit)	VirusScan Enterprise 8.8
		8.8(64bit)	VirusScan Enterprise 8.8 64bit
	McAfee VirusScan	4.5.1	VirusScan 4.5.1
	McAfee VirusScan Enterprise	8.0i <sup>#</sup>	VirusScan Enterprise 8.0i

Company name	Product name / version		Display name in client security control system
		8.5i(32bit)	VirusScan Enterprise 8.5i
		8.5i(64bit)	VirusScan Enterprise 8.5i 64bit
		8.7i(32bit)	VirusScan Enterprise 8.7i
		8.7i(64bit)	VirusScan Enterprise 8.7i 64bit
		8.8(32bit)	VirusScan Enterprise 8.8
		8.8(64bit)	VirusScan Enterprise 8.8 64bit
Microsoft	Forefront Client Security	1.5(32bit)	Forefront Client Security
		1.5(64bit)	Forefront Client Security 64bit
Symantec	Symantec AntiVirus Corporate Edition	9.0	AntiVirus Corporate Edition 9.0
		10.0(32bit)	AntiVirus Corporate Edition 10.0
		10.1(32bit)	AntiVirus Corporate Edition 10.1
		10.2(32bit)	AntiVirus Corporate Edition 10.2
		10.0(64bit), 10.1(64bit), 10.2(64bit)	Symantec AntiVirus Win64
	Symantec Client Security	2.0(Client)	Symantec Client Security
		2.0(Server)	AntiVirus Corporate Edition 9.0
		3.0(32bit), 3.1(32bit)	Symantec Client Security
		3.0(64bit), 3.1(64bit)	Symantec AntiVirus Win64
	Symantec Endpoint Protection	11.0(32bit)	Symantec Endpoint Protection 11.0

4. Considerations for Installing and Operating a Client Security Control System

Company name	Product name / version		Display name in client security control system
		11.0(64bit)	Symantec Endpoint Protection 11.0 64bit
		12.1(32bit)	Symantec Endpoint Protection 12.1
		12.1(64bit)	Symantec Endpoint Protection 12.1 64bit
	Norton AntiVirus	2009(32bit)	Norton AntiVirus 2009
		2009(64bit)	Norton AntiVirus 2009 64bit
		2010(32bit)	Norton AntiVirus 2010
		2010(64bit)	Norton AntiVirus 2010 64bit
		2011(32bit)	Norton AntiVirus 2011
		2011(64bit)	Norton AntiVirus 2011 64bit
Trend Micro	OfficeScan Corporate Edition	5.58, 6.5, 7.0, 7.3 <sup>#</sup>	OfficeScan Corp. WinNT
		8.0(32bit)	
		8.0(64bit)	OfficeScan Corp. WinNT 64bit
		10.0(32bit)	OfficeScan Corp. WinNT 10.0
		10.0(64bit)	OfficeScan Corp. WinNT 10.0 64bit
		10.5(32bit)	OfficeScan Corp. WinNT 10.5
		10.5(64bit)	OfficeScan Corp. WinNT 10.5 64bit
	PC-cillin	2009(32bit)	PC-cillin 2009
		2009(64bit)	PC-cillin 2009 64bit
		2010(32bit)	PC-cillin 2010
		2010(64bit)	PC-cillin 2010 64bit



Company name	Product name / version		Display name in client security control system
	ServerProtect for Windows NT/ Netware	5.7(32bit), 5.8(32bit)	ServerProtect Normal Server
		5.7(64bit), 5.8(64bit)	ServerProtect Normal Server 64bit
	Trend Micro Titanium Internet Security	32bit	Trend Micro Titanium Internet Security
		64bit	Trend Micro Titanium Internet Security 64bit

#

Information about 64-bit products can also be acquired. The names displayed in client security control system are the same as for the 32-bit versions.

*Reference note:*

For anti-virus products applicable to JP1/CSC - Manager 09-50 or later, automatic judgment policy updating is possible only by acquiring update information from the inventory information for a client. Therefore, we recommend that you install an anti-virus product on a client and link it to allow judgment policies to be updated automatically.

For details about how to update the judgment policies for anti-virus products automatically, see 6.4.6 *Updating judgment policies for anti-virus products automatically or manually*.

---

## 4.7 Considerations for security policies

---

Before setting up a security policy, it is important for an administrator to consider the conditions and security levels set in the security policy.

### ■ Judgment policy

A judgment policy contains the following judgment items:

- Security updates
- Anti-virus products
- Prohibited software
- Mandatory software
- PC security settings
- User definition

Give consideration to the judgment conditions set for each judgment item, as well as the security levels set for each judgment condition.

### ■ Action policy

Give consideration to which actions to set for each security level.

The following actions can be set for each security level:

- Notify the administrator by email
- Send a message to the client
- Control client connections to the network
- Implement a user-defined action (user-specific command set by the administrator)

### ■ Assigning policies to clients

Give consideration to the combination of judgment policy and action policy assigned to each client.

For details about setting up judgment policies and action policies and assigning the policies to clients, see *6. Managing Security Policies*.

The following shows guidelines for setting security levels, and for setting judgment policies and action policies.

### 4.7.1 Guides for security level judgment standards

There are 4 security levels. The following table lists guides for which security levels

to set when setting a judgment policy.

*Table 4-5: Guides for security levels and judgment standards*

No.	Security level <sup>#</sup>	Judgment standard guide
1	Danger	Indicates a threat that could spread damage across the system if not handled immediately, with impact as significant as stoppage of operations.
2	Warning	Indicates that normal operation may be affected if the vulnerable client is not handled appropriately.
3	Caution	Indicates that normal operation is not likely affected, but measures should be taken to prevent effects on the system.
4	Safe	Indicates that no measures are necessary.

#

The Danger, Warning, and Caution security levels can be set as a judgment items.

### **(1) Security levels setting guides for each judgment item**

The following table lists guides for setting security levels for a given judgment condition.

*Table 4-6: Security levels setting guide for each judgment item*

No.	Judgment item	Judgment condition	Guide for security level settings
1	Security updates <sup>#1</sup>	The latest security update has not been applied.	Warning
2		A security update specified by the administrator has not been applied.	Warning
3	Anti-virus products	No anti-virus product has been installed.	Danger
4		No anti-virus product is running.	Danger
5		The version of the virus definition file is old.	Danger
6		The engine version of the anti-virus product is old.	Danger
7	Prohibited software	Software prohibited by the administrator is installed.	Caution

4. Considerations for Installing and Operating a Client Security Control System

No.	Judgment item		Judgment condition	Guide for security level settings
8	Mandatory software		Software required by the administrator is not installed.	Caution
9	PC security settings	Accounts <sup>#2</sup>	A Guest account is set up.	Warning
10			A Guest account is set up and active.	Warning
11		Passwords	An account with a vulnerable password exists.	Warning
12			An account has a password that never expires.	Warning
13			A password has not been changed within the number of days specified by the administrator.	Warning
14		Logon	Automatic logon is enabled.	Warning
15			Power-on password is not set. <sup>#3</sup>	Warning
16			Power-on password is not set or not installed. <sup>#3</sup>	Warning
17		Shares	A shared folder is set up on the client.	Warning
18		Anonymous connections	Anonymous connections are not restricted.	Warning
19		Services	Unnecessary services are running.	Warning
20		Firewall <sup>#4</sup>	Windows firewall is disabled.	Warning
21			Windows firewall is disabled or allows exceptions.	Warning
22		Automatic updates	Windows automatic update is disabled.	Warning
23		Screensaver	No screensaver is set.	Caution
24			Screensaver is not password-protected.	Caution
25		Drive encryption <sup>#5</sup>	The system drive is not encrypted.	Caution

No.	Judgment item	Judgment condition	Guide for security level settings
26		A drive is not encrypted.	Caution
27	User definition	A user-defined security setting specified by the administrator has not been implemented.	Caution

#1

For a security update, select either of the two judgment conditions.

#2

For an account, select either of the two judgment conditions.

#3

For power-on passwords, select either of the two judgment conditions.

#4

For a firewall, select either of the two judgment conditions.

#5

For drive encryption, select either of the two judgment conditions.

#### 4.7.2 Considerations for judgment policies

A judgment condition and security level are set for each judgment item. Note that a judgment item can also be excluded from judgment.

##### (1) *Security updates setting guide*

This policy judges the application status of Windows security updates (patches and service packs).

There are two kinds of judgment condition:

- Latest security updates

This judges whether or not the latest security update has been applied to the client. If it has not, the security level is set.

Note that specific security updates can be excluded from judgment.

- Specify security updates

This judges whether or not the security update specified by the administrator has been applied to the client. If it has not, the security level is set.

**(a) Guide for selecting "latest security update"**

Select this judgment condition to keep the Windows security update applied to the client up to date at all times.

When this judgment condition is selected, MBSA or WUA is used to judge whether the security updates applied to the client are up to date.

When as a result of judgment a client is found not to have the latest security update applied, a warning message can be sent to the client, recommending that the security update be applied. Note that security updates that do not need to apply to the client can be excluded from judgment.

**(b) Guide for selecting "specified security updates"**

Select this judgment condition to manage clients for which specific Windows security updates have not been applied.

When this judgment condition is selected, each client is judged to see whether or not an important security update specified by the administrator has been applied.

When as a result of judgment a client is found not to have the specified security update applied, linkage can be performed to the network control product to exclude the client from the network.

*Reference note:*

Automatic updating of judgment policies for security updates

Patch information for judgment policies relating to security updates can be updated automatically by using the patch information files collected by Job Management Partner 1/Software Distribution.

**(2) Anti-virus product setting guide**

This policy judges whether or not an anti-virus product is installed, as well as the application status of the engine version and virus definition file version. Whether an anti-virus product is running on the client can also be a judgment condition. A security level can be set for each anti-virus product specified.

When as a result of judgment a client is found not to have the proper anti-virus software, a warning message can be sent to the client recommending that the virus definition file be updated, or that an anti-virus program be run.

*Reference note:*

Automatic updating of judgment policies for anti-virus software

Judgment policies (virus definition file and engine version) for anti-virus products can be updated automatically by linkage with an anti-virus product compatible with automatic judgment policy updating.

**(3) Prohibited software setting guide**

This policy judges whether or not prohibited software, such as that not used for operations, or that which could cause a security risk, is installed on the client. A security level is set for each instance of prohibited software.

When as a result of judgment a client is found to have prohibited software installed, a warning message can be sent to the client recommending that software be uninstalled.

**(4) Mandatory software setting guide**

This policy judges whether the mandatory software specified by the administrator is installed on the client. Multiple versions of software are registered as a group, and a security level is set for that group. Note that JP1/Software Distribution Client is set as mandatory software by default.

When as a result of judgment a client is found not to have mandatory software installed, a warning message can be sent to the client recommending that software be installed.

**(5) PC security setting guide**

This policy judges whether any settings on the client PC may lead to a reduced security level. Settings judged in this policy include account, password, and other settings. A security level is set for each judgment item that matches a judgment condition.

The following table lists the judgment conditions for judgment items in the PC security setting policy.

*Table 4-7: Judgment conditions for PC security settings*

No.	Judgment item		Judgment conditions
1	Accounts	Guest account settings	Select one of the following judgment conditions: <ul style="list-style-type: none"> <li>• Guest account exists.</li> <li>• Guest account exists and is enabled.</li> </ul>
2	Passwords	Vulnerable password	An account with a vulnerable password exists.
3		Password that never expires	An account has a password that never expires.
4		Days since the password was updated <sup>#1</sup>	A password has not been updated within the period specified by the administrator.
5	Logon	Automatic logon	Automatic logon is enabled.
6		Power-on password	Select one of the following judgment conditions: <ul style="list-style-type: none"> <li>• Power-on password is not set.</li> <li>• Power-on password is not set or not installed.</li> </ul>

No.	Judgment item		Judgment conditions
7	Shares	Shared folder settings	A shared folder is set up on the client.
8	Anonymous connections	Restrictions on anonymous connections	Anonymous connections are not restricted.
9	Services	Status of unnecessary services	Unnecessary services are running.
10	Firewall	Windows Firewall settings	Select one of the following judgment conditions: <ul style="list-style-type: none"> <li>Windows firewall is disabled.</li> <li>Windows firewall is disabled or allows exceptions.</li> </ul>
11	Automatic updates	Windows automatic update settings	Automatic update is disabled.
12	Screensaver #1	Screensaver settings	No screensaver is set.
13		Password protection	Screensaver is not password-protected.
14	Drive encryption	Drive encryption by BitLocker	Select one of the following judgment conditions: <ul style="list-style-type: none"> <li>The system drive is not encrypted.</li> <li>A drive is not encrypted.</li> </ul>

#1

The administrator sets the number of days within which the password must be updated.

#2

Whether the screensaver is password-protected is judged irrespective of the screensaver settings. If password protection is enabled, the screensaver will be judged *Safe* even if the screensaver settings are disabled.

When as a result of judgment a client is found to match a judgment condition, a warning message can be sent to the client recommending that the setting associated with the judgment item be amended.

#### **(6) User definition setting guide**

This policy judges whether a user definition specified by the administrator has been set on the client. A user definition can refer to any item in the asset management database of Asset Information Manager, such as whether the client is running a power-saving CPU or automatic logon is enabled. It can also define security levels for those items.



When the judgment result shows that a user-defined security setting has not been implemented, a warning message can be sent to the client recommending that the setting be implemented.

### 4.7.3 Considerations for action policies

After considering which security level to apply to each judgment item, give consideration to which action to implement for each security level.

#### (1) Which action to implement

In the action policy, set which action to implement for each of the security levels Danger, Warning, Caution, and Safe.

The actions that can be set for each security level are as follows:

- Notify the administrator by email
- Send a message to the client
- Control (permit or deny) client connections to the network
- Implement a user-defined action (user-specific command set by the administrator)

The actions in the action policy are implemented automatically according to the security level judgment based on the judgment policy.

After an automated action is implemented by the action policy, an administrator can manually implement another action for any clients that fail to take appropriate measures. Use the Client Security Management window of AIM to perform an action manually on a specific client.

#### (2) How to implement the action

Consider which of the following two methods for implementing actions is more beneficial:

- Implementing an action immediately following judgment of the security level  
This method automatically implements the action as soon as the security levels are judged for each of the groups specified by the administrator. For client security control systems, this method is set by default.
- Judging the security level and implementing actions separately

In this method, at some time after security levels have been judged, the action command (`cscaction`) is executed to implement the actions. This method is useful when the security levels of many clients are judged and time is needed to complete the judgments and implement the actions, or when you want to create a report on the judgment results before implementing any actions.

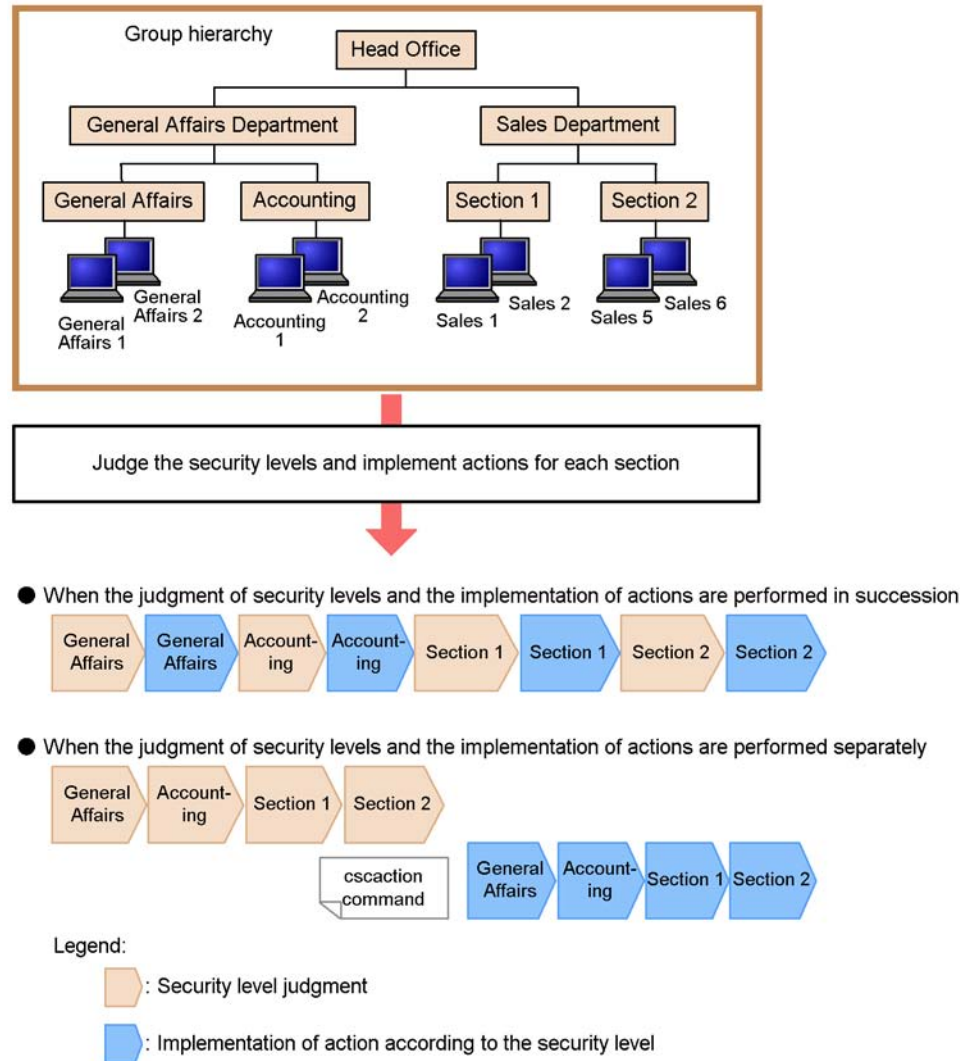
To implement actions at a separate time from the judgment of security level, you must specify that implementation of an action immediately after judging the

security level be skipped. To do so, in the **Basic Settings** page of the Client Security Control - Manager Setup dialog box, specify **Skip** for **Action execution**. For details about the Client Security Control - Manager Setup dialog box, see *5.4.3 Setting up JPI/CSC - Manager*.

For details about the action command (`cscaction`), see *cscaction (implements actions for a specified client)* in *15. Commands*.

The following figure shows an example of implementing actions when the judgment of security levels and the implementation of actions are performed section by section.

Figure 4-6: Example of implementing actions



### (3) When to implement the action

The implementation conditions you can set depend on the security level.

#### (a) Implementation conditions for security levels Danger, Warning and Caution

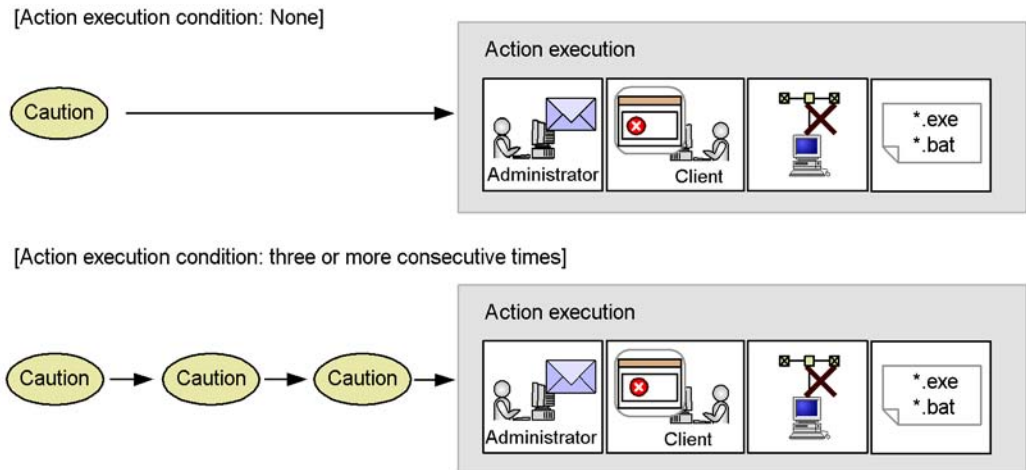
In the action policies for the security levels Danger, Warning, and Caution, you can use the number of consecutive days or times the client has remained at the same security level as a condition for implementing an action.

### ■ Number of consecutive days and times

An action policy can execute an action when the security level is judged to be the same for a specified number of days or times.

The following figure shows an example with no action execution conditions set for the security level *Caution*, and an example when three or more consecutive times is used as an action execution condition.

Figure 4-7: Examples of action execution conditions



When no action execution condition is specified, the action is implemented as soon as the security level is judged *Caution*. On the other hand, when three or more consecutive times is specified as an action execution condition, the action is implemented after the security level is judged as *Caution* three consecutive times.

When you specify three or more as the number of consecutive days, the action is implemented even if the security level has been judged the same only two consecutive times, provided that there are at least three days between the dates of the two judgments.

You can specify a number of consecutive days and times for each security level in the Edit Action Policy window. For example, suppose you specify the following action policy for the *Warning* security level: send a notification message to the client (no consecutive days or times specified); send a notification email to the administrator after two or more consecutive times; and deny network connections after three or more consecutive times. In this case, after the first time the security level is judged *Warning*, a message will be sent to the client. After the second time, a message is sent to the client and an email is sent to the administrator. After the third time, a message is sent to the client, an email is sent to the administrator, and the client network connections are denied.

You can also set both a number of consecutive days and a number of consecutive times for the same action. For example, if you specify that network connections be denied after the security level is judged `Warning` for three or more consecutive days or five or more consecutive times, the action is implemented as soon as either condition is met.

#### ■ Method for counting the number of consecutive days and times

When you specify a number of consecutive days or times, you can also specify which of the following counting methods to use:

- Increase the count when the security level is the same

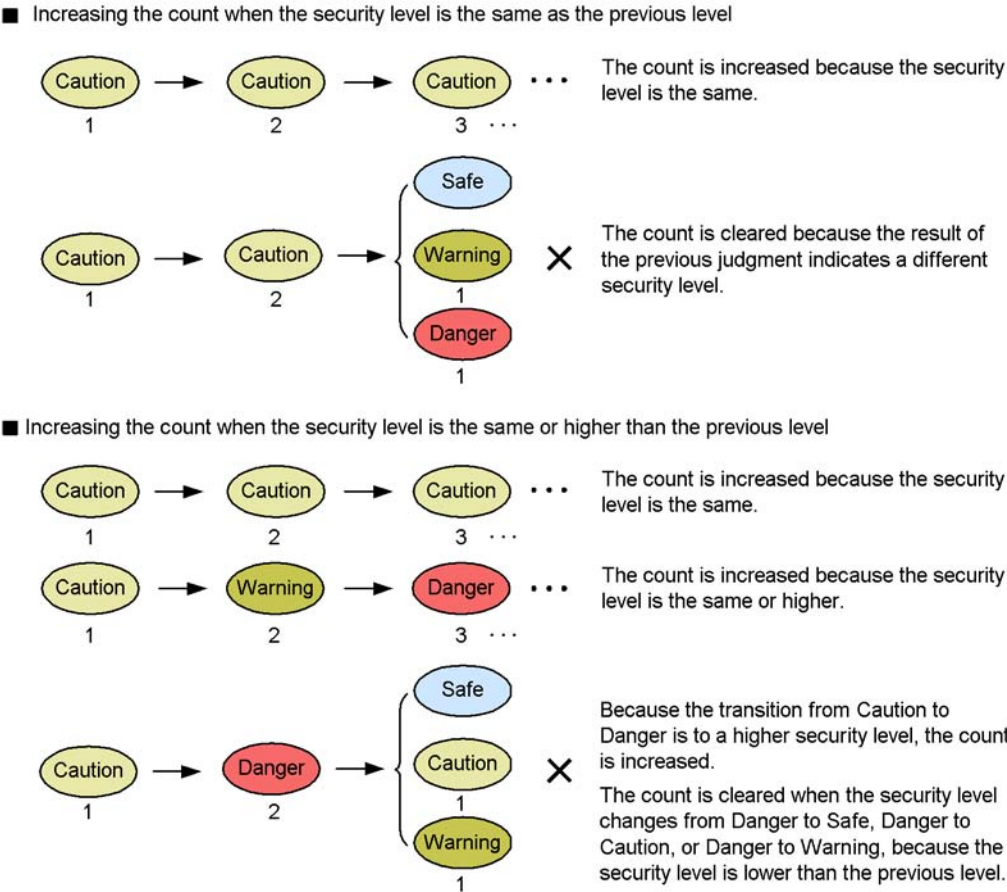
The count is increased when the security level is the same as the previous judgment, and cleared when it is different.

- Increase the count when the security level is the same or higher

The count is increased when the security level is the same or higher than the previous judgment, and cleared when it is lower. It is also cleared when the security level is judged not to be `Danger`, `Warning`, or `Caution`.

The following figure shows an example of each counting method.

Figure 4-8: Examples of counting security levels



You can set the counting method in the **Basic Settings** page of the Client Security Control - Manager Setup dialog box. For details about the Client Security Control - Manager Setup dialog box, see 5.4.3 *Setting up JPI/CSC - Manager*.

*Note:*

If you choose to increase the count when the security level is the same or higher, depending on your settings the action may not be implemented when intended.

The following table shows an example of action execution when the conditions are six or more consecutive times for Danger, four or more consecutive times for Warning, and two or more consecutive times for Caution.

Judgment result	No. of consecutive times	Action execution
Caution	1	Not implemented.
Warning	2	Not implemented. A higher security level than the previous level is judged, and the count is increased to two for the security level <code>Warning</code> . Because the action execution condition for <code>Warning</code> (four or more consecutive times) has not been met, the action is not implemented.
Warning	3	Not implemented.
Caution	1	Not implemented. Because the judgment result indicates a lower security level than the previous level, the count is cleared and restarted from 1.
Warning	2	Not implemented.
Warning	3	Not implemented.
Warning	4	The action for <code>Warning</code> is implemented.
Caution	1	Not implemented.
Warning	2	Not implemented.
Warning	3	Not implemented.
Danger	4	Not implemented. A higher security level than the previous level is judged, and the count is increased to four for the security level <code>Danger</code> . Because the action execution condition for <code>Danger</code> (six or more consecutive times) has not been met, the action is not implemented.
Danger	5	Not implemented.
Danger	6	The action for <code>Danger</code> is implemented.

If you choose to increase the count when the security level is the same or higher, you must set the same number of consecutive days or times as the action execution condition for each security level.

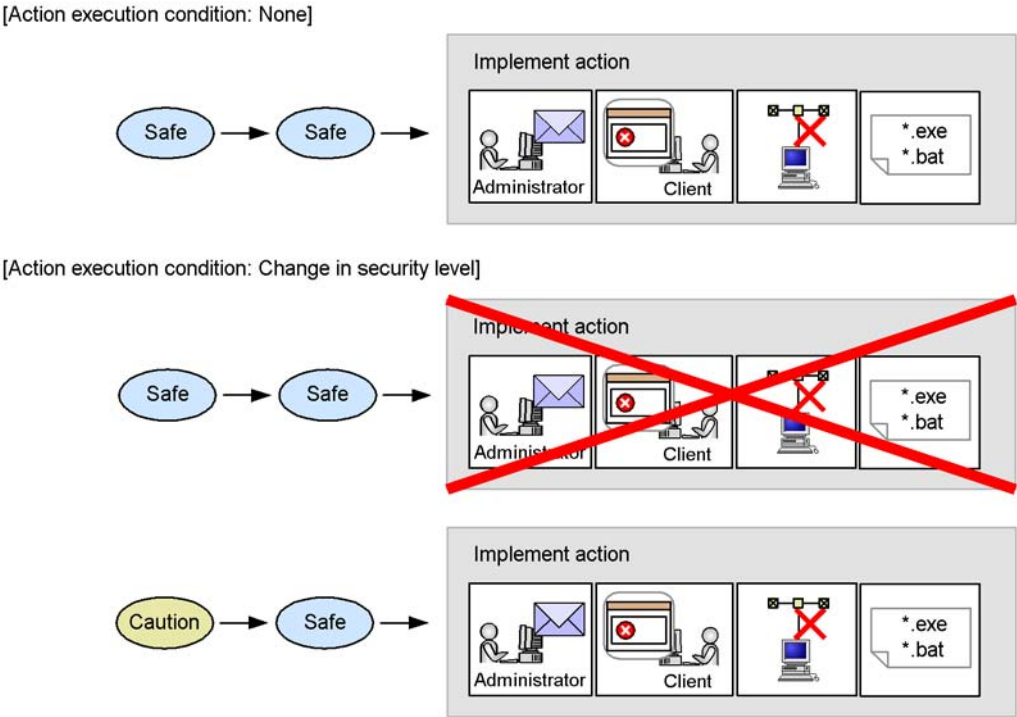
#### (b) Execution condition for `Safe`

You can set up the action policy for `Safe` in such a way that an action is implemented

when the security level changes.

The following figure shows an example where no action execution condition is set, and an example where the action policy implements an action in response to a change in the security level.

Figure 4-9: Examples of action execution conditions



When no action execution condition is specified, the action is implemented as soon as the security level is judged *Safe*. The action is also implemented when the security level is judged *Safe*, and then judged *Safe* again at the next judgment.

If you specify that the action be implemented when the security level changes, the security level is compared with the previous judgment result, and the action is implemented if the security level is found to have changed. Therefore, if the security level is judged *Safe*, and is then judged *Safe* again at the next judgment, no action is implemented. The action is implemented only when the security level changes to *Safe* from another security level.

**(4) Example action settings**

The following table lists example action policies, and examples of actions implemented by an administrator after an automated action is implemented by the



action policy.

*Table 4-8: Example action settings*

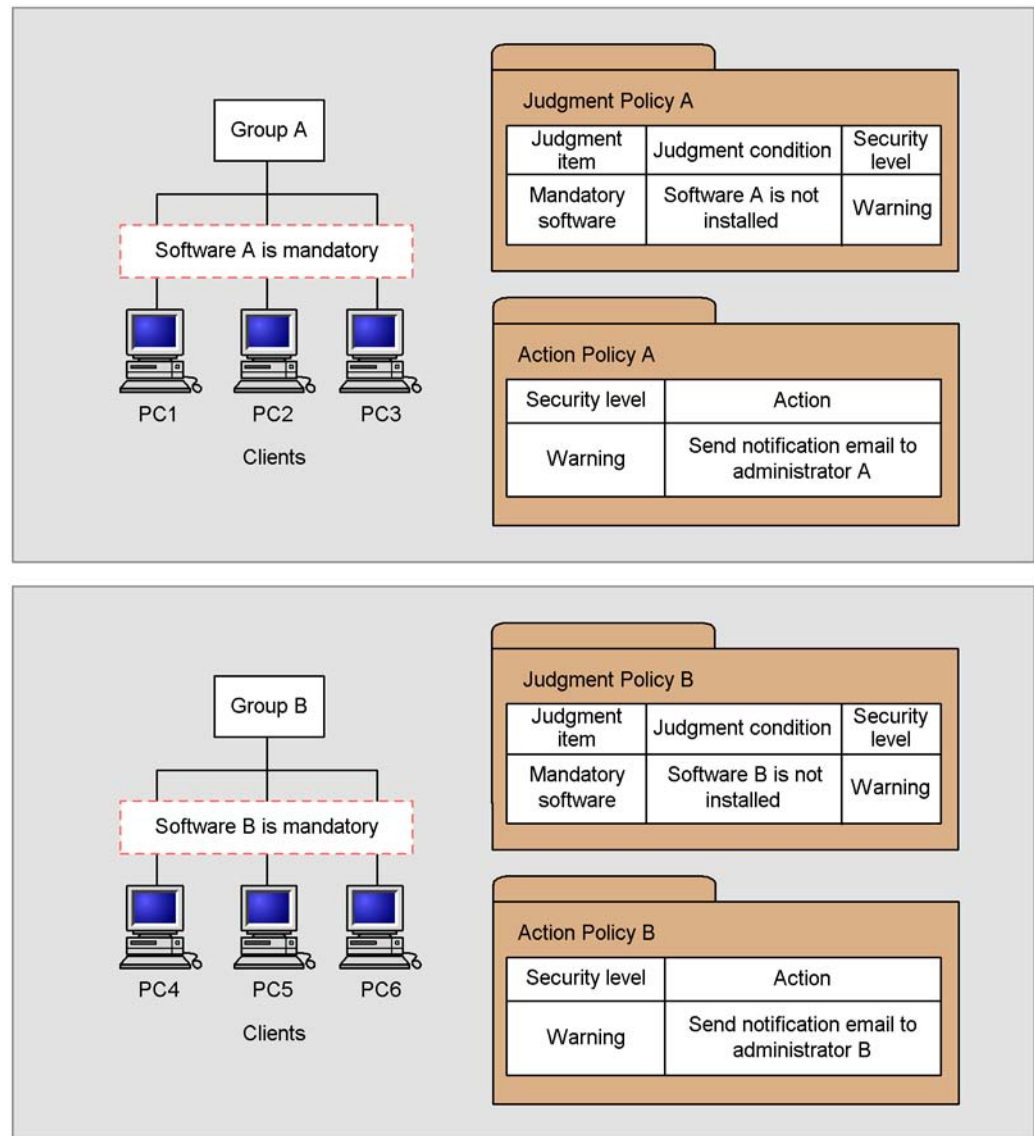
No.	Security level	Example action policy setting	Automated action and response
1	Danger	Deny network connections.	Network connections are denied to clients with <code>Danger</code> security level. The administrator implements security measures for those clients denied access to the network. When a client is subsequently judged <code>Safe</code> , its network connections are restored.
2	Warning	<ul style="list-style-type: none"> <li>Send a message to the client user.</li> <li>Notify the administrator by email (action execution condition: two or more consecutive times).</li> <li>Deny network connections (action execution condition: three or more consecutive times).</li> </ul>	A message is sent to clients with <code>Warning</code> security level. When the client's security level is <code>Warning</code> in two consecutive judgments, an email is sent to the administrator. After the third consecutive judgment, the client network connections are denied. The administrator implements security measures for those clients denied access to the network. When a client is subsequently judged <code>Safe</code> , its network connections are restored.
3	Caution	<ul style="list-style-type: none"> <li>Notify the administrator by email</li> <li>Send a message to the user.</li> </ul>	A message is sent to clients with <code>Caution</code> security level. An email is also sent to the administrator. The administrator implements security measures for those clients with <code>Caution</code> security level.
4	Safe	Network connections are permitted.	No measures are necessary.

#### 4.7.4 Considerations for assigning security policies to clients

It is important to consider which policies to assign to each client.

The following figure shows an example of assigning policies to clients in two groups, group A and group B.

Figure 4-10: Example of assigning security policies to clients



For example, if the clients in group A and group B require different software as shown in the figure, each group must be assigned a different judgment policy. Because the software A must be installed on the clients in group A, the clients in this group are assigned judgment policy A, which includes the software A as mandatory software. The clients in group B are assigned judgment policy B, which includes the software B as mandatory software.

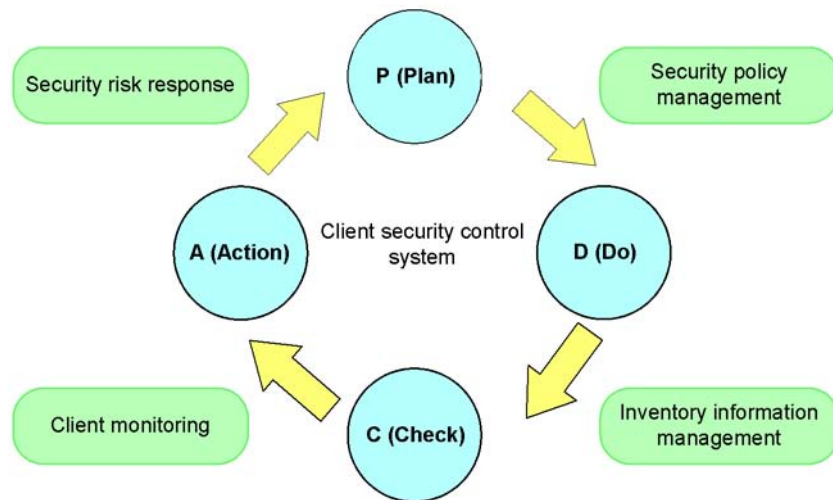
Also, to set a different recipient for the notification email sent when the judgment result for a client is `Warning`, each group must be assigned a different action policy. To ensure that administrator A is notified when the security level of a client in group A is judged `Warning`, action policy A is assigned to group A. This policy specifies administrator A as the recipient of the notification email. Action policy B, which specifies administrator B as the recipient of the notification email, is assigned to group B.

## 4.8 Lifecycle of a client security control system

A client security control system can be operated according to the PDCA (Plan-Do-Check-Action) cycle. Operation using a PDCA cycle facilitates management of a series of operations, from system planning to execution, client monitoring, and measures against security risk. Operations revisions and improvements can also be performed.

The following figure shows a PDCA cycle.

Figure 4-11: PDCA cycle



The following shows what is implemented in each phase of a PDCA cycle.

- Plan

Judge the client security level, and set a security policy that implements an action for the security level.

For details about how to set a security policy, see *6. Managing Security Policies*.

- Do

Automatically collect client inventory information, and manage the application status of Windows security updates and anti-virus products, as well as the installation status of software.

For details about managing inventory information, see *7. Managing Inventory Information*.

- Check

Monitor the managed clients. Find clients that meet the conditions specified by the administrator, and check details about the security level of each client.

For details about monitoring clients, see 8. *Monitoring Clients*.

- Action

Send warning messages to client users, or deny client network connections as instructed by the action policy or administrator.

For details about actions, see 9. *Dealing with Security Risks*.



## Chapter

---

# 5. Installation and Setup

---

This chapter explains the operations for installing and setting up each program for a client security control system.

- 5.1 Procedures for installation and setup
- 5.2 Installing and setting up JP1/Software Distribution Manager
- 5.3 Installing and setting up Asset Information Manager (optional)
- 5.4 Installing and setting up JP1/CSC - Manager
- 5.5 Installing and setting up JP1/CSC - Manager Remote Option
- 5.6 Installing and setting up JP1/Software Distribution Client
- 5.7 Installing and setting up JP1/CSC - Agent
- 5.8 Creating CSC administrators and CSC users
- 5.9 Procedures for setting a task in Scheduled Tasks

---

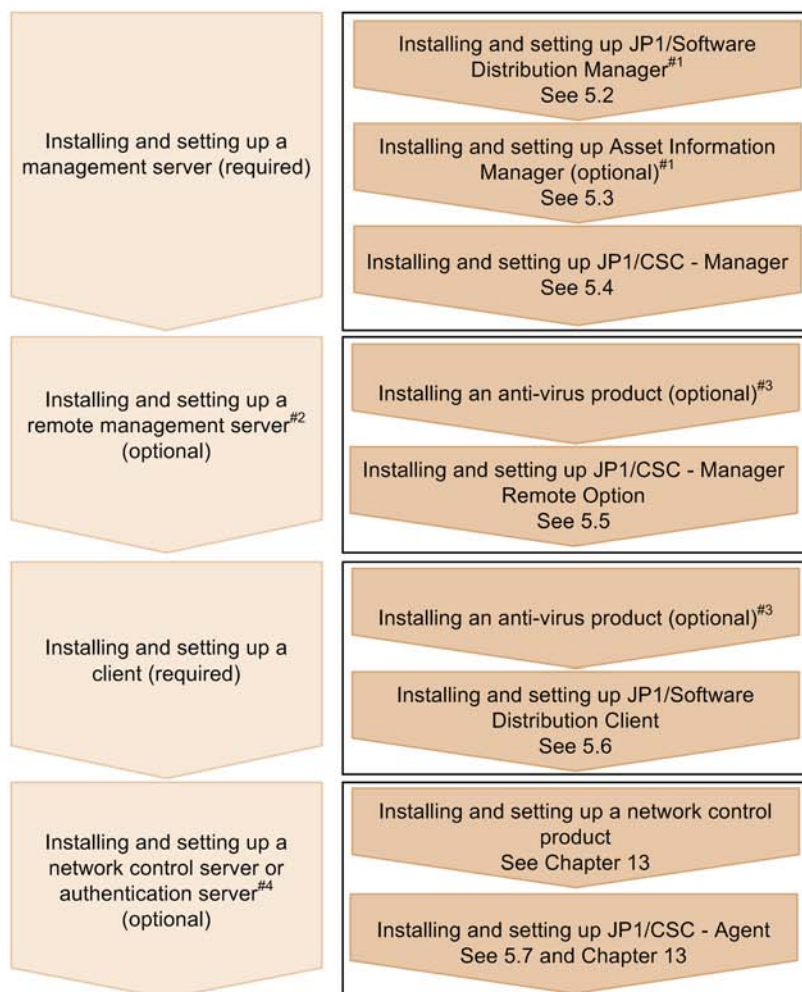
## 5.1 Procedures for installation and setup

---

The following figure shows the procedures for installation and setup.



Figure 5-1: Procedures for installation and setup



#1

To configure a management server, either Asset Information Manager or Asset Information Manager Subset Component of JP1/Software Distribution Manager must be installed and set up.

#2

Set up a remote management server if you want to automatically update judgment policies by linking with an anti-virus product installed on that server or to control network connections via an external server. For details, see 4. *Considerations for Installing and Operating a Client Security Control System*.

#3

Install an anti-virus product if you want to automatically update judgment policies by linking with it. For details, see 4.6 *Installing anti-virus products that linked with automatic judgment policy updating*.

#4

Set up a network control server or authentication server if you want to run a quarantine system that uses a product linked with JP1/CSC.

Installation and setup are performed on the management server, remote management server, and clients, in that order. Installation and setup may also be performed on the

network control server or authentication server as necessary.

For details about the order in which programs should be installed on the network control server and authentication server, see *13. Setting Up a Quarantine System*.

---

## 5.2 Installing and setting up JP1/Software Distribution Manager

---

This section explains how to install and set up JP1/Software Distribution Manager.

For details about installing and setting up JP1/Software Distribution Manager, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems.

### 5.2.1 Installing JP1/Software Distribution Manager

Install JP1/Software Distribution Manager on the management server.

Note that the conditions indicated for the following cases must be met:

When installing JP1/Software Distribution Manager on another machine

You must install Remote Installation Manager, which is a JP1/Software Distribution Manager component, on the management server.

When using Asset Information Manager Subset Component of JP1/Software Distribution Manager to set up a management server

You must also install Asset Information Manager Subset Component of JP1/Software Distribution Manager on the management server.

*Note:*

If you are setting up a management server using Asset Information Manager (optional), do not install Asset Information Manager Subset Component of JP1/Software Distribution Manager.

When setting up a quarantine system linked to the AMT Linkage facility of JP1/Software Distribution

Before you can use the AMT Linkage facility of JP1/Software Distribution, you must install the following program on the management server:

- .NET Framework 1.1 or 2.0

You must also install AMT Linkage facility Component of JP1/Software Distribution.

For details about the quarantine system linked to the AMT Linkage facility of JP1/Software Distribution, see *12.4 Quarantine system linked to JP1/Software Distribution (AMT Linkage facility)*.

### 5.2.2 Setting up JP1/Software Distribution Manager

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

### **(1) Setting up to detect non-Software Distribution clients**

To detect clients for which JP1/Software Distribution has not been installed, specify the following setting during JP1/Software Distribution Manager setup:

- In the **Server Customization** page, select the **Hold the newly detected results** check box.

For details about detecting non-Software Distribution clients, see 7.2 *Detecting non-Software Distribution clients*.

### **(2) Setting up for automatic notification of inventory information to AIM**

To automatically notify AIM of new inventory information, specify the following settings in JP1/Software Distribution Manager:

- In the **System Configuration** page, select the **Automatically apply the system configuration** check box.
- In the **System Configuration** page, select the **Save deletion history** check box.

For details about how to automatically notify AIM of inventory information, see 7.3 *Automatically obtaining client inventory information*.

### **(3) Setting up for automatic deletion of message notification job results**

When you execute a job that sends a notification message to a client, the status of the job appears in the Job Status window of Remote Installation Manager, and the execution history is saved to the CSCSendMessage folder. To automatically delete the execution results of successful message notification jobs, specify the following settings in JP1/Software Distribution Manager:

- On the **JP1/CSC - Agent linkage** panel, select the **Delete Successful Jobs** check box.

### **(4) Setting up for a quarantine system linked to the AMT Linkage facility**

Setting up a quarantine system linked to the AMT Linkage facility of JP1/Software Distribution is required only when you want to change the settings specified during installation.

To perform the setup, specify the following setting in JP1/Software Distribution Manager:

- On the **AMT Linkage** page, specify the user ID and password of the AMT management user.

For details about the setting, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems.

### **(5) Setup when Asset Information Manager Subset Component of JP1/Software Distribution Manager is installed**

When you install Asset Information Manager Subset Component of JP1/Software Distribution Manager, you must set up the following items:

#### **(a) Setting up to detect non-Software Distribution clients**

To detect information about non-Software Distribution clients, reflect this information in AIM, and use JP1/CSC for judgment processing, specify the following setting during setup of the server for Asset Information Manager Subset:

- In **Link with JP1/SD** in the Setup dialog box, set **Take machines without SD installed** to **Take** (default).

For details about how to detect non-Software Distribution clients, see *7.2 Detecting non-Software Distribution clients*.

#### **(b) Setting up to automatically obtain inventory information from JP1/Software Distribution Manager**

To automatically obtain inventory information from JP1/Software Distribution Manager, start the following Asset Information Manager service:

- Asset Information Synchronous Service

*Note:*

When starting Asset Information Synchronous Service, use the following service start order:

- Client Security Control - Manager
- Asset Information Synchronous Service

You must also specify the following setting during setup of the server for Asset Information Manager Subset:

- In **Link with JP1/SD** of the Setup dialog box, set **Type of information to acquire** to **Hardware and software and software inventory information**.

For details about how to automatically obtain inventory information from JP1/Software Distribution Manager, see *7.3 Automatically obtaining client inventory information*.

#### **(c) Setting up to scrap clients**

When you scrap clients, you might want to delete the asset information about the scrapped clients from the AIM asset management database. To delete this information, specify the following setting during setup of the Asset Information Manager Subset server.

- In **Link with JP1/SD** in the Setup dialog box, set **Status of machines deleted with JP1/SD** to **Erase** (default).

**(6) Setting up for acquiring patch information files**

To automatically update the judgment policy for security updates, JP1/Software Distribution must be set up to acquire patch information files. To enable this feature, enter the following information during setup of JP1/Software Distribution Manager:

- Enter network information in the **Network Settings** page displayed from the Software Update Management dialog box.

For details about acquiring patch information files, see the manual *Job Management Partner 1/Software Distribution Description and Planning Guide*, for Windows systems.

---

## 5.3 Installing and setting up Asset Information Manager (optional)

---

This section explains how to install and set up Asset Information Manager.

For details about installing and setting up Asset Information Manager, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

These steps are unnecessary if you are setting up a management server using Asset Information Manager Subset Component of JP1/Software Distribution Manager.

### 5.3.1 Installing Asset Information Manager

Install Asset Information Manager on the management server.

### 5.3.2 Setting up Asset Information Manager

This subsection explains how to set up Asset Information Manager.

#### (1) *Setting up to detect non-Software Distribution clients*

To detect client information for non-Software Distribution clients, reflect this information for Asset Information Manager, and perform judgment using JP1/CSC, specify the following setting during Asset Information Manager setup:

- In **Link with JP1/SD** in the Setup dialog box, set **Take machines without SD installed** to **Take**.

For details about how to detect non-Software Distribution clients, see 7.2 *Detecting non-Software Distribution clients*.

#### (2) *Setting up to automatically obtain inventory information from JP1/Software Distribution Manager*

To automatically obtain inventory information from JP1/Software Distribution Manager, start the following Asset Information Manager service:

- Asset Information Synchronous Service

*Note:*

When starting Asset Information Synchronous Service, use the following service start order:

- Client Security Control - Manager
- Asset Information Synchronous Service

You must also specify the following setting during setup of Asset Information Manager:

- In **Link with JP1/SD** in the Setup dialog box, set **Type of information to**

**acquire to Hardware and software and software inventory information.**

For details about how to automatically obtain inventory information from JP1/Software Distribution Manager, see *7.3 Automatically obtaining client inventory information*.

**(3) Setting up to scrap clients**

When you scrap clients, you might want to delete the asset information about the scrapped clients from the AIM asset management database. To delete this information, specify the following settings during the Asset Information Manager setup:

- In **Link with JP1/SD** in the Setup dialog box, set **Status of machines deleted with JP1/SD** to **Erase**.
- Set the **Data maintenance** task to periodic execution.

**(4) Setting the device type**

A client security control system uses the Asset Information Manager device type to judge whether or not a machine is to be managed. For `MachineKind` in the `HardwareInfo` class displayed in the Code window of AIM, do not change or delete the following device types:

- PC (code: 100)
- PC server (code: 101)



---

## 5.4 Installing and setting up JP1/CSC - Manager

---

This section explains how to install and setup JP1/CSC - Manager.

### 5.4.1 Installing JP1/CSC - Manager

Install JP1/CSC - Manager on the management server.

This subsection explains the procedures for installing JP1/CSC - Manager, for both a new installation and an overwrite installation.

#### (1) *Performing a new installation of JP1/CSC - Manager*

The following explains the procedures for performing a new installation of JP1/CSC - Manager. To install JP1/CSC - Manager, use the provided CD-ROM. Alternatively, use JP1/Software Distribution to perform remote installation. For details about remote installation using JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems. If the remote installation failed, use the provided CD-ROM to install JP1/CSC - Manager.

#### *Note:*

Before installing JP1/CSC - Manager, you must have completed the installation and setup of Asset Information Manager or Asset Information Manager Subset Component of JP1/Software Distribution Manager. If neither of these products has been set up, you will be unable to set up the JP1/CSC - Manager environment. For details about how to install and set up Asset Information Manager Subset Component of JP1/Software Distribution Manager, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems. For details about how to install and set up Asset Information Manager, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

To install JP1/CSC - Manager using the provided CD-ROM:

1. Log on to Windows as a member of the Administrators group.
2. Insert the provided CD-ROM in the drive.

When the installer starts, a dialog box prompting you to select a component is displayed, so select the JP1/CSC - Manager component.

3. Click the **Install** button.

A dialog box is displayed prompting you to confirm the start of installation.

4. Click the **OK** button.

A dialog box is displayed indicating that JP1/CSC - Manager installation has

started.

5. Click the **Next** button.

A dialog box is displayed, in which you can enter user information.

6. Enter the user name and company name.

7. Click the **Next** button.

A dialog box is displayed in which you can specify the installation folder.

8. Specify the installation folder.

Installation is performed in the specified folder. The default installation destinations are as follows (when the OS is installed under C:\):

For a 64-bit edition of Windows:

C:\Program Files(x86)\HITACHI\jplnetmcscm

For other OSs

C:\Program Files\HITACHI\jplnetmcscm

9. Click the **Next** button.

A dialog box is displayed, in which you can select the program folder.

10. Specify the program folder.

Specify the folder to which the program icon is added. The default folder name is Client Security Control.

11. Click the **Next** button.

A dialog box is displayed in which automatic setup can be selected. To perform automatic setup, select the **Perform setup processing** check box.

*Note:*

If you select automatic setup, stop the World Wide Web Publishing Service.

12. Click the **Next** button.

A dialog box is displayed confirming the current contents. Check the settings.

13. Click the **Next** button.

Installation begins.

When installation is finished, a dialog box confirming whether or not to open the README file is displayed. Skip to step 15 if you click the **No** button.

14. Read and then close the README file.

When the README file is read and closed, a dialog box indicating that installation is complete is displayed.

15. Click the **Finish** button.

Installation is complete.

16. Restart Windows.

If the installation finished successfully, restart Windows.

*Note:*

If automatic setup was not selected in step 11, restart the system after installation, stop the World Wide Web Publishing Service, and execute the `cscsetup` command. If automatic setup was selected in step 11 and an error occurred, check the log information, restart the system, and execute the `cscsetup` command. For details about the `cscsetup` command, see *cscsetup (sets up JP1/CSC - Manager)* in 15. *Commands*.

## **(2) Performing an overwrite installation of JP1/CSC - Manager**

An overwrite installation of JP1/CSC - Manager can be performed when the version to be installed is the same or later than the existing one.

*Note:*

Before you perform an overwrite installation, stop services in the following order:

- World Wide Web Publishing Service
- Asset Information Synchronous Service
- Client Security Control - Manager
- Client Security Control - Manager Remote Service

To perform an overwrite installation:

1. Log on to Windows as a member of the Administrators group.
2. Insert the provided CD-ROM in the drive.

When the installer starts, a dialog box appears, prompting you to select a component. Select the JP1/CSC - Manager component.

3. Click the **Install** button.

A dialog box appears, prompting you to confirm the start of overwrite installation.

4. Click the **OK** button.

A dialog box appears, in which you can select automatic setup. To perform automatic setup, select the **Perform an automatic setup** check box.

5. Click the **Next** button.

Installation begins.

When installation finished, a dialog box appears, asking whether you want to open the README file. Skip to step 7 if you click the **No** button.

6. Read and then close the README file.

When the README file is read and closed, a dialog box appears, indicating that installation is completed.

7. Click the **Finish** button.

Installation is complete. For an overwrite installation, you do not have to restart Windows.

Note that an overwrite installation cannot be performed if the version to be installed is earlier than the current version of JP1/CSC - Manager.

*Note:*

If you did not select automatic setup in step 4, restart the system after installation, stop the World Wide Web Publishing Service, and then execute the `cscsetup` command. If you selected automatic setup in step 4 and an error occurred, check the log information, restart the system, and then execute the `cscsetup` command. For details about the `cscsetup` command, see *cscsetup (sets up JP1/CSC - Manager)* in 15. Commands.

## 5.4.2 Uninstalling JP1/CSC - Manager

This subsection explains the procedures for uninstalling JP1/CSC - Manager. Before performing uninstallation, be sure to terminate all JP1/CSC - Manager services.

To uninstall JP1/CSC - Manager:

1. In the Control Panel, open **Add/Remove Programs**, select **Client Security Control - Manager**, and then click the **Change/Remove** button.

A dialog box is displayed, confirming deletion.

2. Click the **Yes** button.

JP1/CSC - Manager is uninstalled.

Note that the files and folders created after installation are not deleted, and must be deleted manually by an administrator.

Once uninstallation is finished, a dialog box indicating that uninstallation is complete is displayed.

3. Click the **Finish** button.

Uninstallation is complete.

4. Restart Windows.

If the uninstallation finished successfully, restart Windows.

*Note:*

When uninstalling Asset Information Manager or Asset Information Manager Subset Component of JP1/Software Distribution Manager, be sure to also uninstall JP1/CSC - Manager.

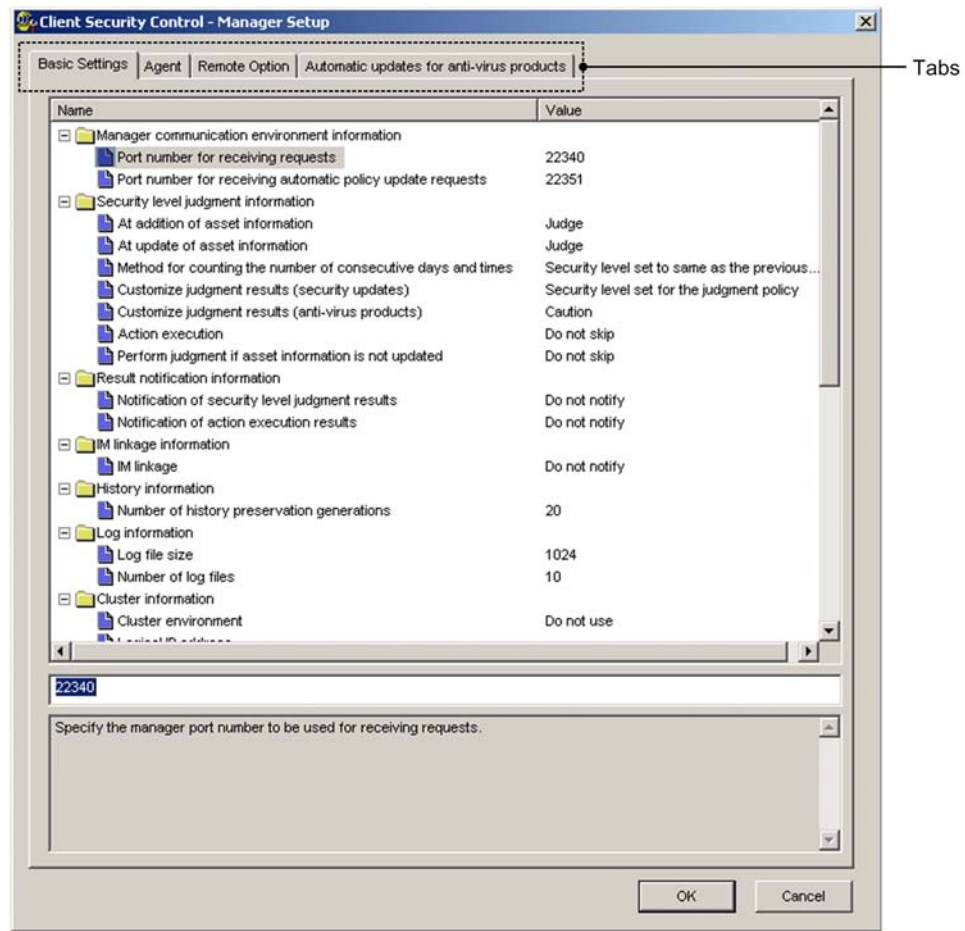
### 5.4.3 Setting up JP1/CSC - Manager

When automatic setup is selected during installation of JP1/CSC - Manager, the installer automatically sets up JP1/CSC - Manager. When automatic setup is not selected, an administrator must execute the `cscsetup` command to set up JP1/CSC - Manager. To change the option specified during setup, use the Client Security Control - Manager Setup dialog box.

The Client Security Control - Manager Setup dialog box has three panes, which can be selected by clicking the corresponding tab.

The following figure shows the Client Security Control - Manager Setup dialog box.

Figure 5-2: Client Security Control - Manager Setup dialog box



The following table describes the contents set in the Client Security Control - Manager Setup dialog box.

Table 5-1: Contents set in the Client Security Control - Manager Setup dialog box

Tab selected	Description
Basic Settings tab	This tab is used to display settings information for JPI/CSC - Manager environments already set up, and to change environment settings information.

Tab selected	Description
<b>Agent tab</b>	This tab is used to display the IP address and port number of the JP1/CSC - Agent that connects to JP1/CSC - Manager. You can also add and delete IP addresses and port numbers for JP1/CSC - Agent.
<b>Remote Option tab</b>	This tab is used to display the IP address of the JP1/CSC - Manager Remote Option that connects to JP1/CSC - Manager. You can also add and delete IP addresses for the JP1/CSC - Manager Remote Option.
<b>Automatic updates for anti-virus products tab</b>	This tab is used to display the setting information required to link with an anti-virus product installed on a client in order to enable the automatic updating of judgment policies for anti-virus products. You can also add and delete a client on which an anti-virus product to be linked is installed. You can also set a period of time following which the update information for the anti-virus product is applied to the judgment policies.

To display the Client Security Control - Manager Setup dialog box and edit the setting items:

1. Click the **Start** button, and then choose **Programs**, then **Client Security Control**, and **Manager setup**.

The dialog box is displayed.

2. Click the tabs to set the item values.

When an item is selected, a box is displayed below the item list, in which you can either enter a value or string, or select a value from the drop-down list.

3. Click the **OK** button.

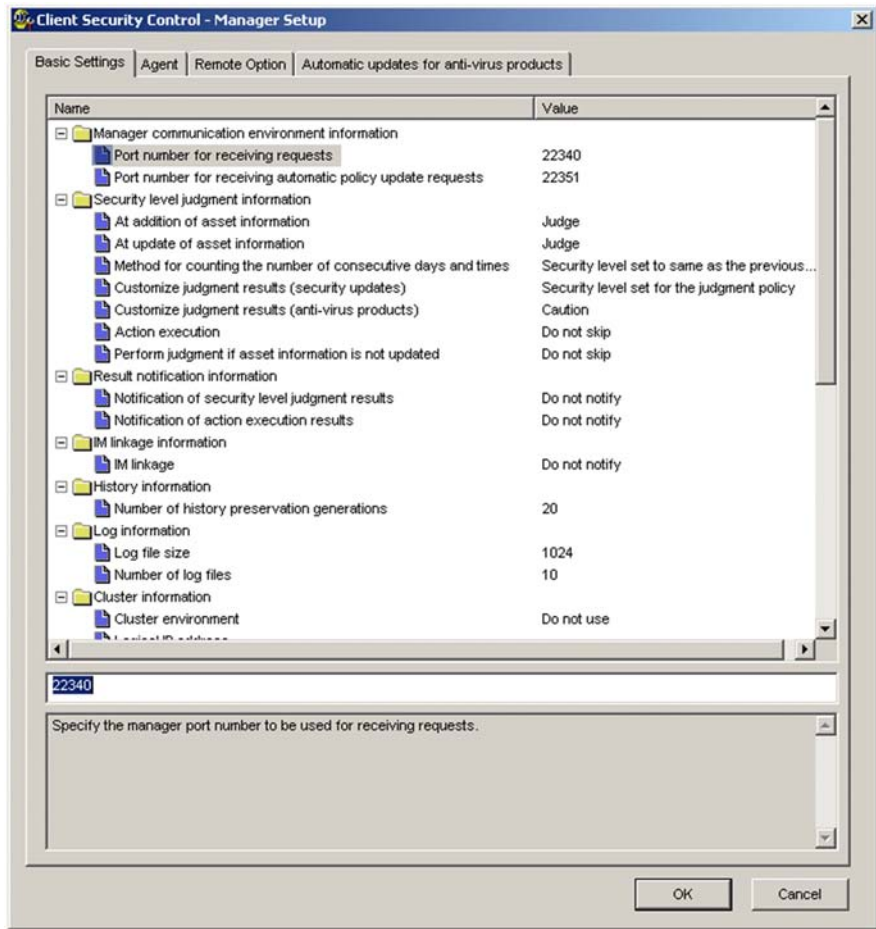
The specified contents are set for the JP1/CSC - Manager environment. The Client Security Control - Manager Setup dialog box closes. To close the dialog box without performing environment settings, click the **Cancel** button.

#### **(1) Using the Basic Settings page**

Use the **Basic Settings** page to display and change the environment settings information for JP1/CSC - Manager.

The following figure shows the **Basic Settings** page.

Figure 5-3: Basic Settings page



The following table describes and lists the items that can be checked and set in the **Basic Settings** page.



Table 5-2: Items that can be set and checked in the Basic Settings page

Item		Description	Specifiable values	Default for initial environment setup
Manager communication environment information	Port number for receiving requests	The port number of the JP1/CSC - Manager used for request reception. Enter the same port number as specified in <b>Port number</b> for Manager communication environment information, in the Client Security Control - Agent Setup dialog box.	1024 to 65535	22340
	Port number for receiving automatic policy update requests	The port number of the JP1/CSC - Manager used for request reception when the automatic policy update feature is enabled. Enter the same port number as specified for <b>Port number</b> under <b>Manager communication environment information</b> in the Client Security Control - Manager Remote Option Setup dialog box.	1024 to 65535	22351
Security level judgment information	At addition of asset information	Specify whether or not to judge the security level when a new client is added to the network.	Judge / Do not Judge	Judge
	At update of asset information	Specify whether or not to judge the security level when client inventory information is updated.	Judge / Do not Judge	Judge

Item		Description	Specifiable values	Default for initial environment setup
	<b>Method for counting the number of consecutive days and times</b>	Specify the method of counting the number of consecutive days and times for the security level. <ul style="list-style-type: none"> <li><b>Security level set to same as the previous level</b> The count is increased when the security level is the same as the previous judgment, and cleared when it is different.</li> <li><b>Security level set to higher than the previous level</b> The count is increased when the security level is the same or higher than the previous judgment, and cleared when it is lower.</li> </ul>	<b>Security level set to same as the previous level / Security level set to higher than the previous level</b>	<b>Security level set to same as the previous level</b>
	<b>Customize judgment results (security updates)<sup>#1</sup></b>	Specify the security level to be used when, as a result of the security update judgment, the specified patch is not found in the list of installed software or in the unapplied patch information.	<b>Unknown / Safe / Security level set for the judgment policy</b>	<b>Security level set for the judgment policy</b>
	<b>Customize judgment results (anti-virus products)</b>	Specify the security level to be used for anti-virus product judgment when a product other than the specified anti-virus product is installed.	<b>Safe / Caution / Warning / Danger / Not applicable</b>	<b>Not applicable</b>
	<b>Action execution</b>	Specify whether or not to skip implementation of the action as soon as the security level has been judged.	<b>Skip / Do not skip</b>	<b>Do not skip</b>
	<b>Perform judgment if asset information is not updated</b>	Specify whether or not to skip security level judgment for assets whose asset information has not changed since the last time their security level was judged. Actions are not implemented for assets for which judgment is skipped.	<b>Skip / Do not skip</b>	<b>Do not skip</b>

Item		Description	Specifiable values	Default for initial environment setup
<b>Result notification information</b>	<b>Notification of security level judgment results</b>	Specify whether or not to notify JP1/IM of security level judgment results.	<b>Notify / Do not notify</b>	<b>Do not notify</b>
	<b>Notification of action execution results</b>	Specify whether or not to notify JP1/IM of action implementation results.	<b>Notify / Do not notify</b>	<b>Do not notify</b>
<b>IM linkage information</b>	<b>IM linkage<sup>#2</sup></b>	Specify whether or not to notify JP1/IM of JP1/CSC messages.	<b>Notify / Do not notify</b>	<b>Do not notify</b>
<b>History information</b>	<b>Number of history preservation generations<sup>#3</sup></b>	Specify the maximum number of generations of security level judgment history and action history to save in the database.	1 to 99	20
<b>Log information</b>	<b>Log file size</b>	Specify the maximum size (in kilobytes) of the JP1/CSC - Manager log files.	1 to 2097151	1024
	<b>Number of log files</b>	Specify the maximum number of JP1/CSC - Manager log files to be created.	1 to 999	10
<b>Cluster information<sup>#3</sup></b>	<b>Cluster environment</b>	Specify whether or not to run JP1/CSC - Manager in a cluster environment.	<b>Use / Do not use</b>	<b>Do not use</b>
	<b>Logical IP address</b>	Specify a logical IP address to use in the cluster environment.	IPv4 format (xxx.xxx.xxx.x)	N/A
	<b>Logical host</b>	Specify the logical host name for JP1/IM linkage, as used in the cluster environment.	Host name	N/A
	<b>Shared disk</b>	Specify the shared disk name used in the cluster environment.	Full path	N/A
<b>Software Distribution information</b>	<b>Software Distribution SubManager<sup>#4</sup></b>	Specify whether to judge the security level and implement actions for servers on which Software Distribution SubManager is installed.	<b>Do not subject to judgment or action for the security level / Subject to judgment and action for the security level</b>	<b>Do not subject to judgment or action for the security level</b>

Item		Description	Specifiable values	Default for initial environment setup
	<b>Software Distribution manager (relay manager)</b>	Specify whether to judge the security level and implement actions for servers on which Software Distribution Manager (relay manager) is installed.	<b>Do not subject to judgment or action for the security level / Subject to judgment and action for the security level</b>	<b>Do not subject to judgment or action for the security level</b>
<b>Asset deletion information</b>	<b>Automatic refusal of network connection<sup>#5</sup></b>	Specify whether to automatically deny a client's network connections when the client is removed from the client security control system.	<b>Execute / Do not execute</b>	<b>Execute<sup>#6</sup></b>
<b>Policy update information</b>	<b>Anti-Virus products</b>	Specify whether to automatically update anti-virus product judgment policies (the virus definition file and engine version) by linking with an anti-virus product that is compatible with automatic judgment policy updating.	<b>Update automatically / Do not update automatically</b>	<b>Do not update automatically</b>
<b>Message notification information</b>	<b>"Safe" or "Not applicable" results</b>	Specify whether or not to include <b>Safe</b> and <b>Not applicable</b> in the judgment results displayed in the message.	<b>Include / Do not include</b>	<b>Include</b>
	<b>Display position of the judgment results</b>	Specify whether to display PC judgment results at the beginning or end of the message.	<b>Display at the end of the message / Display at the beginning of the message</b>	<b>Display at the end of the message</b>

Item		Description	Specifiable values	Default for initial environment setup
	<b>Notification method</b>	Specify the message notification method to be used for security level judgment. <ul style="list-style-type: none"> <li>• <b>Synchronous method</b> The existing notification method. When message notification processing is completed, another request is executed.</li> <li>• <b>Asynchronous method</b> Message notification processing and another request are executed concurrently.</li> </ul>	<b>Synchronous method / Asynchronous method</b>	<b>Synchronous method</b>
<b>Audit log information</b>	<b>Audit log</b>	Specify whether or not to output audit logs.	<b>Output / Do not output</b>	<b>Do not output</b>
<b>Statistics information</b>	<b>User definition judgment</b>	Specify whether or not to include user-defined judgment items when compiling statistics.	<b>Do not include in the "Type of total" pulldown menu / Include in the "Type of total" pulldown menu</b>	<b>Do not include in the "Type of total" pulldown menu</b>
<b>Mail notification information</b>	<b>Email sender address<sup>#8</sup></b>	Specify the email sender address to be used for email notification. Use no more than 64 bytes.	Email address	manager@csc.message

N/A: Not applicable

#1

The **Customize judgment results (security updates)** setting is valid when the following conditions are satisfied.

- In the Edit Judgment Policy (Security Update) window, **Specify security updates** is selected for the judgment condition, and patch information is defined.
- The patch information specified for installed software information is not found.

- The client is linked to MBSA or WUA.
- The patch information specified as security update information not applied to the client (unapplied patch information) is not found.

#2

When **Do not notify** is set for **IM linkage** in the IM linkage information, JP1/IM notification is not performed even when **Notify** is for **Notification of security level judgment results** and **Notification of action execution results**. To report results to JP1/IM, be sure to set **IM linkage** to **Notify**. Also, when selecting the **Notify IM** check box in the Edit Action Policy window, be sure to set **IM linkage** to **Notify**.

#3

The set value cannot be changed when the JP1/CSC - Manager service is running. To change the set value, first stop the JP1/CSC - Manager service.

#4

Servers on which JP1/Software Distribution Client (relay system) is installed are subject to judgment and execution of an action for the security level even if **Do not subject to judgment or action for the security level** is set. If you do not want these servers to be subject to judgment and execution of an action, you need to disable security management. For details about how to disable security management, see 8.5 *Enabling and disabling security management for a client*.

#5

This function can only be used on clients with JP1/Software Distribution installed.

#6

If you upgrade from version 07-51 of JP1/CSC - Manager, the default will be **Do not execute** when you set up the initial environment.

#7

If you do not specify anything for **Email sender address**, the default email address (manager@csc.message) is set.

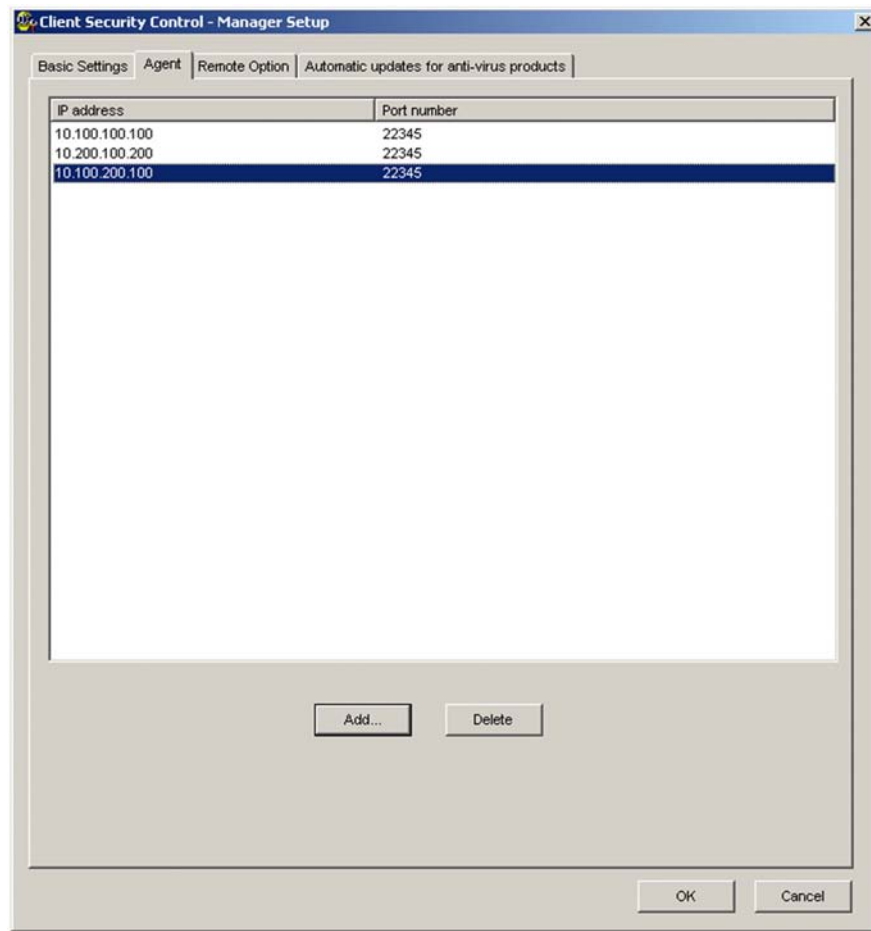
*Reference note:*

- The log information contains information about startup and termination of JP1/CSC, as well as security level judgment results and action implementation results.
- If you specify **Execute** for the **Automatic refusal of network connection** item, the administrator is not required to deny the client connection to the network before the client is removed. Note that you cannot use JP1/CSC to deny a client connection to the network once its asset information has been deleted from AIM. In this case you must change the settings directly from the network control product. For details, see *14. Operating a Quarantine System*.
- If you specify **Asynchronous method** for **Notification method** for **Message notification information**, you can implement important actions such as network control and judge the security level irrespective of the status of message notification processing.

**(2) Using the Agent page**

From the **Agent** page, you can add or delete information about the IP addresses and port numbers for JP1/CSC - Agent.

The following figure shows the **Agent** page.

*Figure 5-4: Agent page*

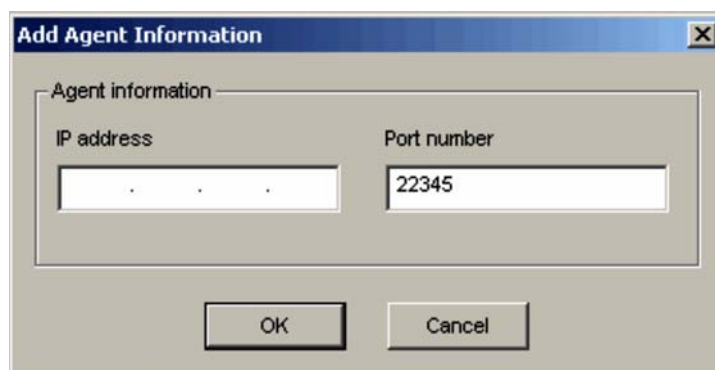
**(a) Adding agent information**

To add information about JP1/CSC - Agent, click the **Add** button on the **Agent** page to display the Add Agent Information window, and use the window to register the IP address and port number of a JP1/CSC - Agent.

The following figure shows the Add Agent Information window.



Figure 5-5: Add Agent Information window



To register the IP address and port number of a JP1/CSC - Agent in the Add Agent Information window:

1. Enter an IP address.

Specify the IP address of the JP1/CSC - Agent to be added, in IPv4 format (xxx.xxx.xxx.xxx).

2. Enter a port number.

Specify the port number of the JP1/CSC - Agent to be added. 22345 is set by default, and the specifiable range is 1024 to 65535. Enter the same port number as that specified for **Port number in Agent communication environment information**, in the Client Security Control - Agent Setup dialog box.

3. Click the **OK** button.

The IP address and port number are added, and the Add Agent Information window closes. To cancel addition of JP1/CSC - Agent information, click the **Cancel** button.

#### (b) Deleting agent information

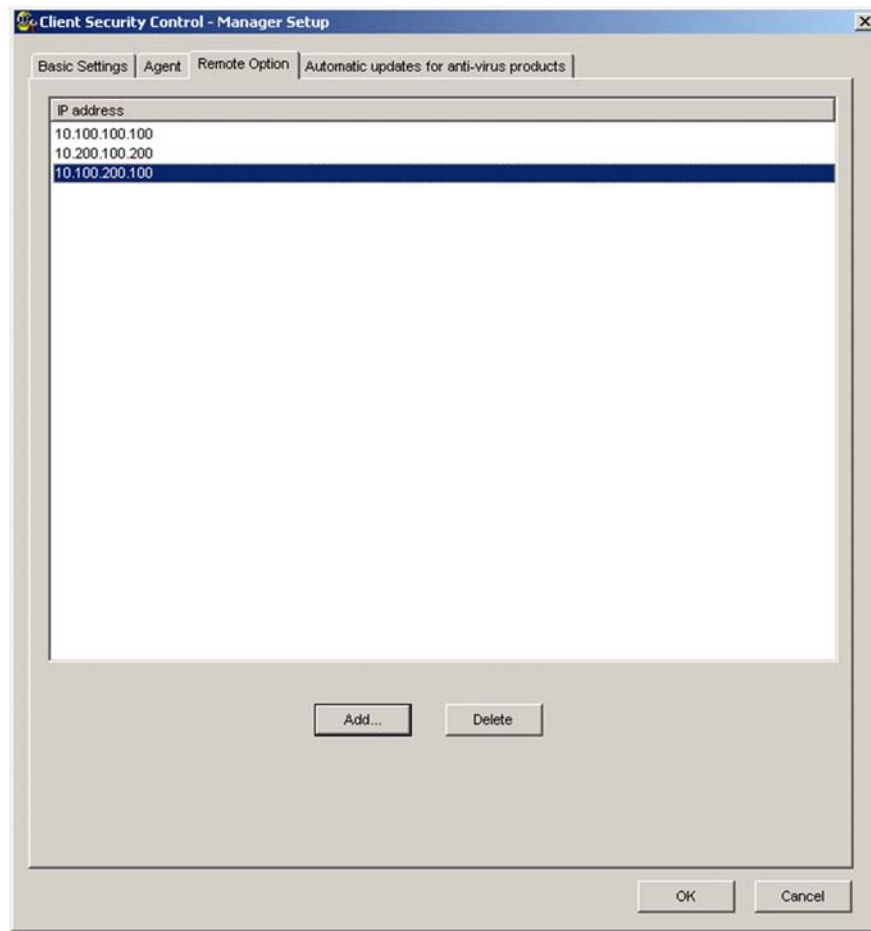
To delete the IP address and port number of a JP1/CSC - Agent, from the **Agent** page, select the IP address and port number you want to delete, and then click **Delete**.

### (3) Using the Remote Option page

Use the **Remote Option** page to add or delete IP addresses used by JP1/CSC - Manager Remote Option to connect to JP1/CSC - Manager.

The following figure shows the **Remote Option** page.

Figure 5-6: Remote Option page

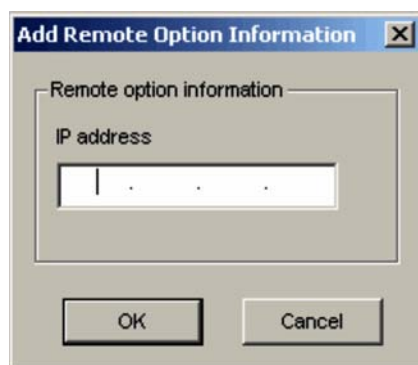


**(a) Adding remote option information**

To add an IP address of JP1/CSC - Manager Remote Option, click the **Add** button on the **Remote Option** page. In the displayed Add Remote Option Information window, add the IP address of the JP1/CSC - Manager Remote Option.

The following figure shows the Add Remote Option Information window.

Figure 5-7: Add Remote Option Information window



To register an IP address of JP1/CSC - Manager Remote Option in the Add Remote Option Information window:

1. Enter an IP address.

Specify the IP address of the JP1/CSC - Manager Remote Option to be added, in IPv4 format (xxx.xxx.xxx.xxx).

2. Click the **OK** button.

The IP address is added, and the Add Remote Option Information window closes. To close the window without adding information about JP1/CSC - Manager Remote Option, click **Cancel**.

#### (b) Deleting remote option information

To delete information about JP1/CSC - Manager Remote Option, select the IP address you want to delete in the **Remote Option** page, and then click **Delete**.

We recommend that you delete the relevant IP address in the following cases.

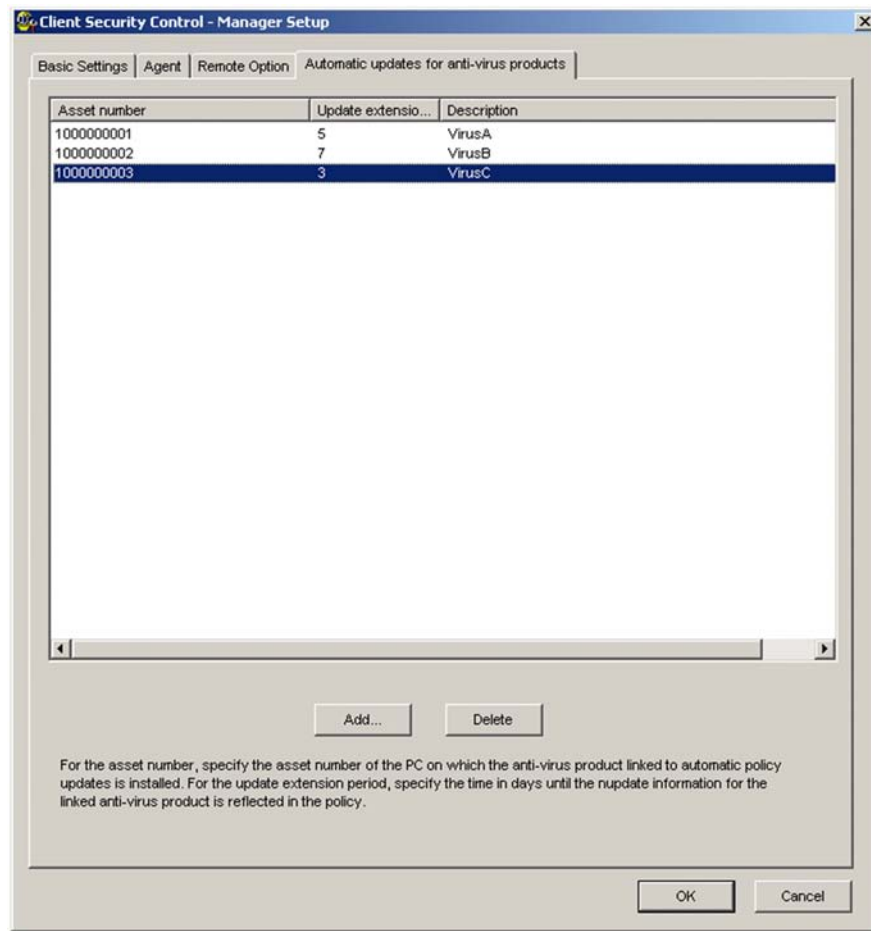
- The method of automatically updating judgment policies for anti-virus products by linkage with a remote management server has changed to the method that links with a client.
- The network control command (`cscnetctrl`) is not used.

#### (4) Using the Automatic updates for anti-virus products page

Use the **Automatic updates for anti-virus products** page to add or delete clients that have anti-virus products that link with automatic judgment policy updating for anti-virus products. You can also set the period of time following which the update information for the anti-virus products is applied to the judgment policies.

The following figure shows the **Automatic updates for anti-virus products** page.

Figure 5-8: Automatic updates for anti-virus products page



The following table describes the items that can be checked on the **Automatic updates for anti-virus products** page.

Table 5-3: Items that can be checked on the Automatic updates for anti-virus products page

Item	Description
<b>Asset number</b>	The asset number of the client on which the anti-virus product linked with automatic judgment policy updating for anti-virus products is installed.
<b>Update extension period</b>	The period (in days) following which the update information for the anti-virus product is applied to the judgment policies.

Item	Description
Description	Comment on the automatic update information ( <b>Asset number</b> and <b>Update extension period</b> ).

### (a) Adding automatic update information

To link an anti-virus product installed on the client in order to automatically update judgment policies for anti-virus products, click the **Add** button on the **Automatic updates for anti-virus products** page to open the Additional automatic update information window. In this window, set the asset number of the client on which the anti-virus product to be linked is installed and the update extension period following which the update information for the anti-virus product is applied to the judgment policies.

The following figure shows the Additional automatic update information window.

Figure 5-9: Additional automatic update information window

The screenshot shows a dialog box titled "Additional automatic update information". It contains a group box labeled "Automatic update information". Inside this group box, there are two input fields: "Asset number" (containing "1000000004") and "Update extension period" (containing "5"). Below these is a "Description" field (containing "VirusD"). At the bottom of the dialog are "OK" and "Cancel" buttons.

To register automatic update information in the Additional automatic update information window:

1. Enter an asset number.  
Specify the asset number of the client on which the anti-virus product to be linked is installed. Use 1 to 60 bytes of alphanumeric characters. This item must be specified.
2. Enter an update extension period.  
Specify the period (in days) following which the update information for the anti-virus product is applied to the judgment policies. Use a value in the range

from 0 to 100. The default is 0. This item must be specified.

3. Enter a description (optional).

Enter a comment for the automatic update information to be added. Use a string from 0 to 300 bytes. This item is optional.

4. Click the **OK** button.

The automatic update information is added, and the Additional automatic update information window closes. To cancel addition of the automatic update information, click **Cancel**.

#### **(b) Deleting automatic update information**

To delete automatic update information, select the automatic update information you want to delete in the **Automatic updates for anti-virus products** page, and then click **Delete**.

### **5.4.4 Setting up JP1/CSC - Manager and the remote service to start automatically**

This subsection explains how to start JP1/CSC - Manager and the remote service automatically when the OS starts. The remote service must be running if you want to update policies automatically.

#### **(1) Setting up JP1/CSC - Manager to start automatically**

This subsection explains how to start JP1/CSC - Manager automatically when the OS starts.

Open Windows **Services**, and set **Startup type** to **Automatic** for **Client Security Control - Manager**.

To stop automatic start for JP1/CSC - Manager once set, perform the following.

Open Windows **Services**, and set **Startup type** to **Manual** for **Client Security Control - Manager**.

#### **■ Notes on setting up the Client Security Control - Manager service and the Asset Information Synchronous Service service to start automatically**

If you want the services Client Security Control - Manager and Asset Information Synchronous Service to start automatically, the dependencies must be configured so that the services start in a particular order.

The services must start in the following order:

1. Client Security Control - Manager
2. Asset Information Synchronous Service

To set the dependency of JP1/Client Security Control - Manager and the Asset

## Information Synchronous Service:

1. Start the registry editor (`regedt32.exe`).
2. Add dependency information to the registry.

Add dependency information for Client Security Control - Manager and the Asset Information Synchronous Service.

Add the following information to the registry:

*Table 5-4:* Information to be added to the registry

Item	Value
Registry key	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AssetInformationSynchronousService
Name	DependOnService
Type	Multi-string value (REG_MULTI_SZ)
Data	JP1_NETM_CSCM

3. Set the startup method for each service.

Open Windows **Services**. Set the **Startup type** to **Manual** for **Client Security Control - Manager**, and the **Startup type** to **Automatic** for **Asset Information Synchronous Service**.

4. Restart Windows.

**(2) Setting up the remote service to start automatically**

Open Windows **Services**, and set **Startup type** to **Automatic** for **Client Security Control - Manager Remote Service**.

To stop automatic start for the remote service once set, perform the following:

Open Windows **Services**, and set **Startup type** to **Manual** for **Client Security Control - Manager Remote Service**.

---

## 5.5 Installing and setting up JP1/CSC - Manager Remote Option

---

This section explains how to install and set up JP1/CSC - Manager Remote Option.

### 5.5.1 Installing JP1/CSC - Manager Remote Option

Install JP1/CSC - Manager Remote Option on the remote management server.

Install JP1/CSC - Manager Remote Option by copying the installation files from JP1/CSC - Manager. You cannot perform a remote installation of JP1/CSC - Manager Remote Option.

This subsection explains the procedures for installing JP1/CSC - Manager Remote Option, for both a new installation and an overwrite installation.

#### (1) *Performing a new installation of JP1/CSC - Manager Remote Option*

To perform a new installation of JP1/CSC - Manager Remote Option:

1. Log on to Windows as a member of the Administrators group.
2. Copy the JP1/CSC - Manager Remote Option package (`cscmremotepkg.exe`) from JP1/CSC - Manager to a folder on the remote management server.

The package (`cscmremotepkg.exe`) can be found in the following location:

*JP1/CSC - Manager-installation-folder\remote*

The default installation location for JP1/CSC - Manager is as follows (when the OS is installed under `C:\`):

For a 64-bit edition of Windows:

`C:\Program Files(x86)\HITACHI\jplnetmcscm`

For other OSs:

`C:\Program Files\HITACHI\jplnetmcscm`

3. Run the JP1/CSC - Manager Remote Option package (`cscmremotepkg.exe`).

A dialog box for the Hitachi self-expanding program appears.

When using Windows Server 2008 or Windows Vista as your operating system, run the package (`cscmremotepkg.exe`) as an administrator.

4. Click the **Install** button.

A dialog box is displayed prompting you to confirm the start of installation.

Note that when the OS is Windows Vista or Windows 7, the User Account Control dialog is displayed. To continue the installation, click the **Allow** button in Windows Vista. In Windows 7, click the **Yes** button.



Note: Alternatively, you can install JP1/CSC - Manager Remote Option by clicking the **Expand** button after you run the package (`cscmremotepkg.exe`). To install JP1/CSC - Manager Remote Option using the **Expand** button:

1. Click the **Expand** button.

A dialog box is displayed in which you can specify the destination folder.

2. Specify the destination folder, and then click the **OK** button.

The files are expanded into the folder you specified.

3. Navigate to the folder that contains the expanded files, and run the JP1/CSC - Manager Remote Option installation file (`Setup.exe`).

The installer starts, and a dialog box is displayed prompting you to confirm the start of installation.

5. Click the **OK** button.

A dialog box is displayed indicating that JP1/CSC - Manager Remote Option installation has started.

6. Click the **Next** button.

A dialog box is displayed, in which you can enter user information.

7. Enter the user name and company name.

8. Click the **Next** button.

A dialog box is displayed, in which you can specify the installation folder.

9. Specify the installation folder.

Installation is performed in the specified folder. The default installation folder is as follows (when the OS is installed under `C:\`):

For a 64-bit edition of Windows:

```
C:\Program Files(x86)\HITACHI\jplnetmcscm\remote
```

For other OSs:

```
C:\Program Files\HITACHI\jplnetmcscm\remote
```

Note that when JP1/CSC - Manager Remote Option is installed on the same system as JP1/CSC - Manager, the default installation folder is as follows:

*JP1/CSC - Manager-installation-folder*\remote

10. Click the **Next** button.

A dialog box is displayed, in which you can select the program folder.

11. Specify the program folder.

Specify the folder to which the program icon is to be added. The default folder name is `Client Security Control`.

12. Click the **Next** button.

A dialog box is displayed prompting you to confirm the current settings. Check the settings before proceeding.

13. Click the **Next** button.

Installation begins. When installation is finished, a dialog box indicating that installation is complete is displayed.

Note that when the OS is Windows 7, the Program Compatibility Assistant dialog box might be displayed. If this dialog box is displayed, click the **This program installed correctly** button because JP1/CSC - Manager Remote Option has been installed normally.

14. Click the **Finish** button.

Installation is complete.

15. Restart Windows.

If installation was successful, restart Windows.

## **(2) Performing an overwrite installation of JP1/CSC - Manager Remote Option**

An overwrite installation of JP1/CSC - Manager Remote Option can be performed when the version to be installed is the same or later than the existing one. When performing an overwrite installation, be sure to first terminate all JP1/CSC - Manager Remote Option services.

To perform an overwrite installation of JP1/CSC - Manager Remote Option:

1. Log on to Windows as a member of the Administrators group.
2. Copy the JP1/CSC - Manager Remote Option package (`cscmremotepkg.exe`) from JP1/CSC - Manager to a folder on the remote management server.

The package (`cscmremotepkg.exe`) can be found in the following location:

*JP1/CSC - Manager-installation-folder*\remote

The default installation location for JP1/CSC - Manager is as follows (when the OS is installed under `C:\`):

For a 64-bit edition of Windows:

`C:\Program Files(x86)\HITACHI\jplnetmcsm`

For other OSs:

C:\Program Files\HITACHI\jplnetmcscm

3. Run the JP1/CSC - Manager Remote Option package (cscmremotepkg.exe).

A dialog box for the Hitachi self-expanding program appears.

4. Click the **Install** button.

A dialog box is displayed prompting you to confirm the start of the overwrite installation.

Note that when the OS is Windows Vista or Windows 7, the User Account Control dialog is displayed. To continue the installation, click the **Allow** button in Windows Vista. In Windows 7, click the **Yes** button.

Note: Alternatively, you can install JP1/CSC - Manager Remote Option by clicking the **Expand** button after you run the package (cscmremotepkg.exe). To install JP1/CSC - Manager Remote Option using the **Expand** button:

1. Click the **Expand** button.

A dialog box is displayed in which you can specify the destination folder.

2. Specify the destination folder, and then click the **OK** button.

The files are expanded into the folder you specified.

3. Navigate to the folder that contains the expanded files, and run the JP1/CSC - Manager Remote Option installation file (Setup.exe).

The installer starts, and a dialog box is displayed prompting you to confirm the start of installation.

5. Click the **OK** button.

Installation begins. When installation is finished, a dialog box indicating that installation is complete is displayed.

Note that when the OS is Windows 7, the Program Compatibility Assistant dialog box might be displayed. If this dialog box is displayed, click the **This program installed correctly** button because JP1/CSC - Manager Remote Option has been installed normally.

6. Click the **Finish** button.

Installation is complete. You do not need to restart Windows after an overwrite installation.

Note that overwrite installation cannot be performed when the version to be installed

is earlier than the existing version of JP1/CSC - Manager Remote Option.

### 5.5.2 Uninstalling JP1/CSC - Manager Remote Option

This subsection explains the procedures for uninstalling JP1/CSC - Manager Remote Option. Before performing uninstallation, be sure to terminate all JP1/CSC - Manager Remote Option services.

1. In the Control Panel, open **Add/Remove Programs**, select **Client Security Control - Manager Remote Option**, and then click the **Change/Remove** button.

A dialog box is displayed, confirming deletion.

2. Click the **Yes** button.

JP1/CSC - Manager Remote Option is uninstalled.

Note that the files and folders created after installation are not deleted, and must be deleted manually by an administrator.

Once uninstallation is finished, a dialog box indicating that uninstallation is complete is displayed.

3. Click the **Finish** button.

Uninstallation is complete.

4. Restart Windows.

If uninstallation was successful, restart Windows.

#### *Reference note:*

We recommend that you uninstall JP1/CSC - Manager Remote Option in the following cases:

- The method of automatically updating judgment policies for anti-virus products by linkage with a remote management server has changed to the method that links with a client.
- The network control command (`cscnetctrl`) is not used.

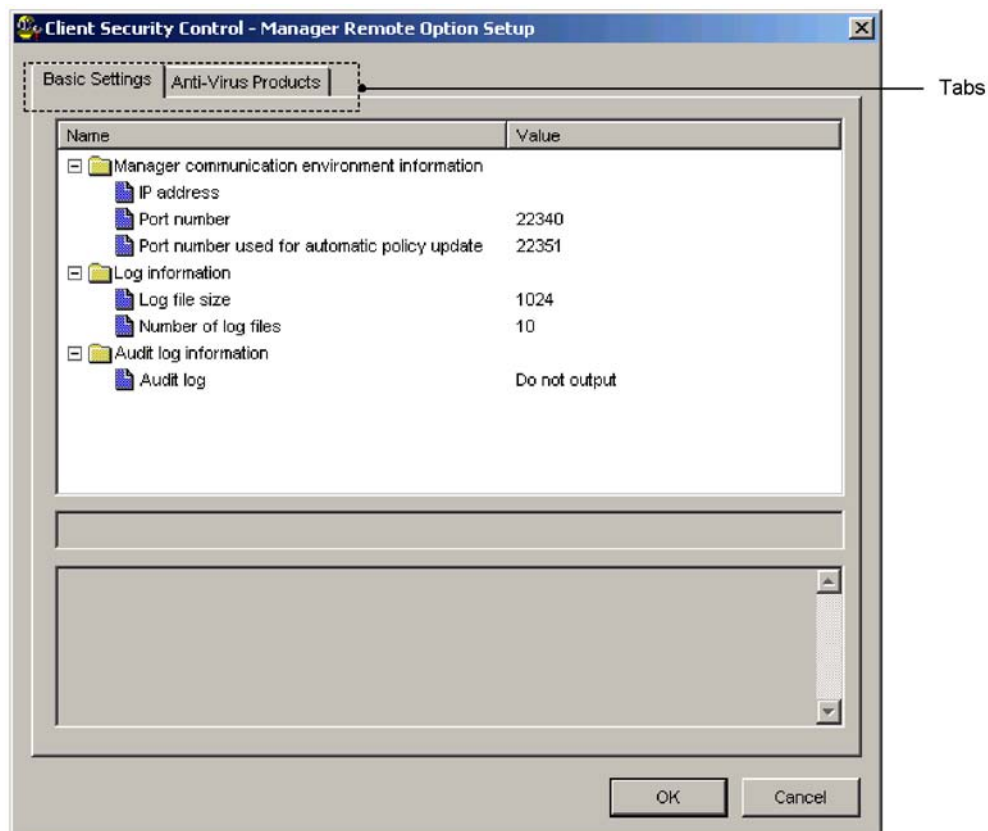
### 5.5.3 Setting up JP1/CSC - Manager Remote Option

This subsection explains the procedures for setting up JP1/CSC - Manager Remote Option.

The Client Security Control - Manager Remote Option Setup dialog box has two tabbed pages, which can be selected by clicking the corresponding tab.

The following figure shows the Client Security Control - Manager Remote Option Setup dialog box.

Figure 5-10: Client Security Control - Manager Remote Option Setup dialog box



The following table lists the items that can be set in the Client Security Control - Manager Remote Option Setup dialog box.

Table 5-5: Items that can be set in the Client Security Control - Manager Remote Option Setup dialog box

Tab selected	Description
<b>Basic Settings</b> tab	This tab is used to display settings for JP1/CSC - Manager Remote Option environments already set up, and to change environment settings information.
<b>Anti-Virus Products</b> tab	This tab is used to specify the settings required for linking with an anti-virus product installed on a remote management server in order to automatically update judgment policies for the anti-virus products and to display information about the linked anti-virus products.

To display the Client Security Control - Manager Remote Option Setup dialog box and edit the setting items:

1. Click the **Start** button, and then choose **Programs, Client Security Control, and Remote Option setup**.

The dialog box is displayed.

2. Click the tabs to set the item values.

When an item is selected, a box is displayed below the item list, in which you can either enter a value or string, or select a value from the drop-down list.

3. Click the **OK** button.

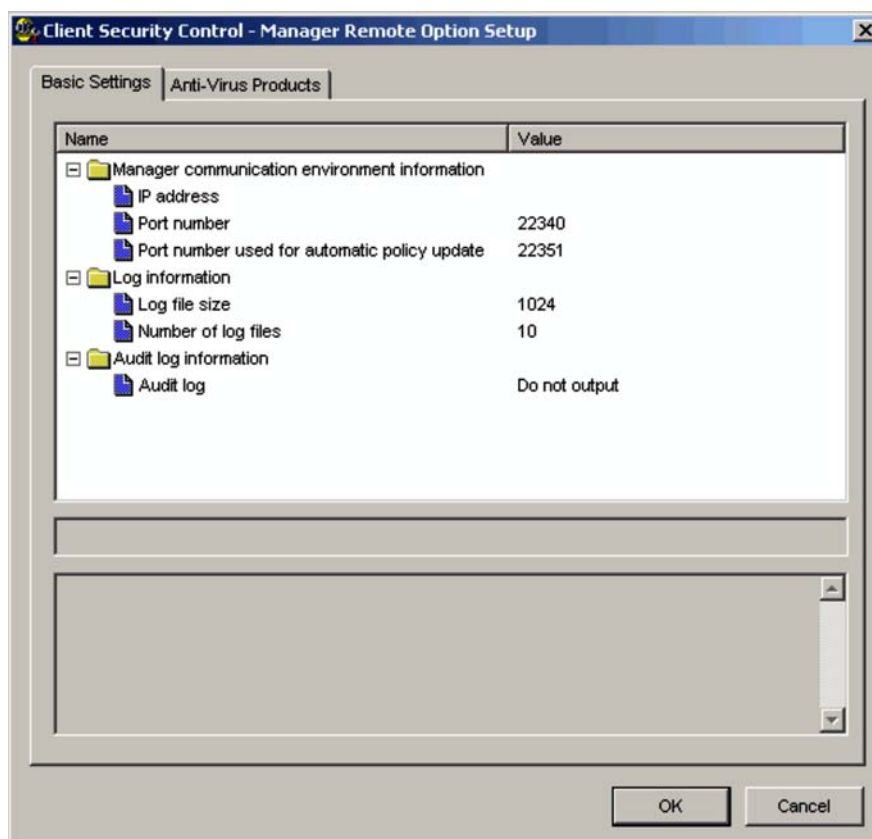
The specified contents are set for the JP1/CSC - Manager Remote Option environment. The Client Security Control - Manager Remote Option Setup dialog box closes. To close the dialog box without making any settings, click the **Cancel** button.

#### **(1) Using the Basic Settings page**

Use the **Basic Settings** page to display and change the environment settings information for JP1/CSC - Manager Remote Option.

The following figure shows the **Basic Settings** page.

Figure 5-11: Basic Settings page



The following table describes the items that can be viewed and set in the **Basic Settings** page.

Table 5-6: Items that can be viewed and set in the Basic Settings page

Item		Description	Specifiable values	Default
Manager communication environment information	IP address	Specify the IP address of JP1/CSC - Manager.	IPv4 format (xxx.xxx.xxx.xxx)	N/A

Item		Description	Specifiable values	Default
	<b>Port number</b>	The port number used by JP1/CSC - Manager. Enter the same port number as specified for <b>Port number for receiving requests</b> under <b>Manager communication environment information</b> in the Client Security Control - Manager Setup dialog box.	1024 to 65535	22340
	<b>Port number used for automatic policy update</b>	Specify the port number used by JP1/CSC - Manager to communicate with JP1/CSC - Manager Remote Option.	1024 to 65535	22351
<b>Log information</b>	<b>Log file size</b>	Specify the maximum size (in kilobytes) of the JP1/CSC - Manager Remote Option log files.	1 to 2097151	1024
	<b>Number of log files</b>	Specify the maximum number of JP1/CSC - Manager Remote Option log files to be created.	1 to 999	10
<b>Audit log information</b>	<b>Audit log</b>	Specify whether or not to output audit logs.	<b>Output / Do not output</b>	<b>Do not output</b>

Legend:

N/A: Not applicable

*Reference note:*

The log information contains information about startup and termination of JP1/CSC - Manager Remote Option, as well as the results of implementing automatic policy updates and network connection control.

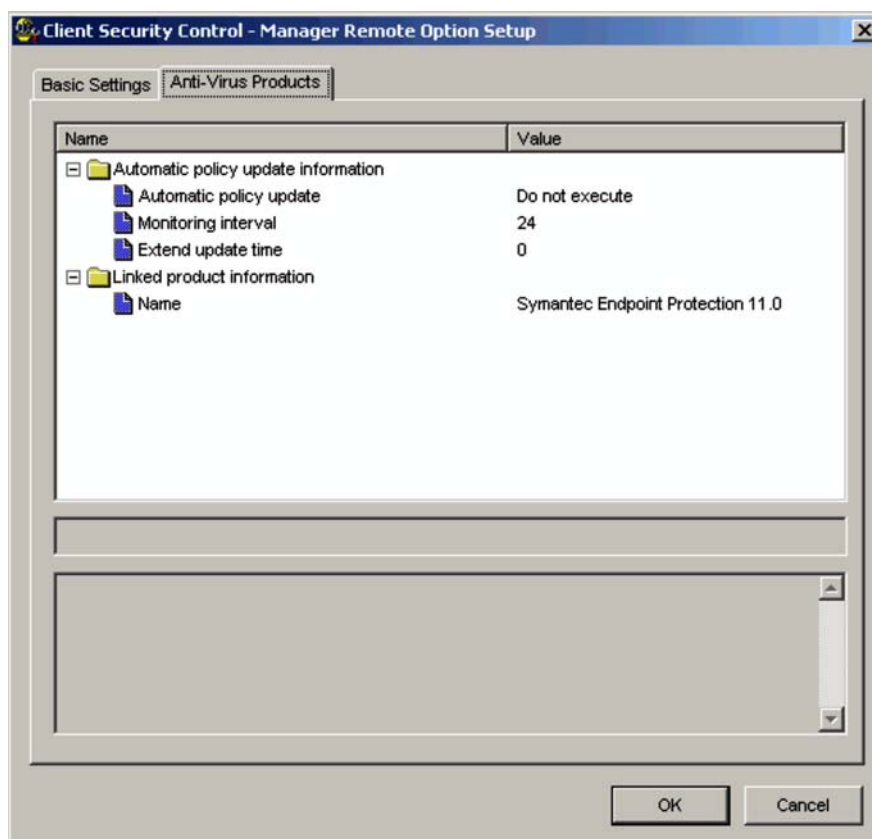
## **(2) Using the Anti-Virus Products page**

Use the **Anti-Virus Products** page to make settings related to automatic policy update information, and to display information about linked anti-virus products.

The following figure shows the **Anti-Virus Products** page.



Figure 5-12: Anti-Virus Products page



The following table describes the items that can be viewed and set in the **Anti-Virus Products** page.

Table 5-7: Items that can be viewed and set in the Anti-Virus Products page

Item		Description	Specifiable values	Default
Automatic policy update information	Automatic policy update	Specify whether to automatically update the judgment policies for anti-virus products by linkage with the anti-virus product installed on a remote management server.	Execute/Do not execute	Do not execute
	Monitoring interval	Specify (in hours) the interval for monitoring the information for linked anti-virus products.	1 to 99999	24

Item		Description	Specifiable values	Default
	<b>Extend update time</b>	Specify the interval (in days) between the acquisition of the latest information about the anti-virus product and the automatic update of the judgment policy definition.	1 to 100	0
<b>Linked product information</b>	<b>Name</b>	Select the name of the anti-virus product installed on the remote management server.	Name of the anti-virus product <sup>#</sup>	Symantec Endpoint Protection 11.0

#

The name of an anti-virus product listed in Table 4-4 in *4.6 Installing anti-virus products that link with automatic judgment policy updating* is displayed.

*Note:*

- To automatically update judgment policies by linkage with the anti-virus product installed on the client rather than the anti-virus product installed on the remote management server, set **Do not execute** for **Automatic policy update**.
- For the **Name** item under **Linked product information**, select the name of the anti-virus product installed on the remote management server. If you select the wrong name, the judgment policy may not be updated as intended.

Note that the name of an anti-virus product displayed by a client security management system might be different from the actual product name. For details about the correspondence between the anti-virus product names and the names displayed by the client security management system, see *4.6 Installing anti-virus products that link with automatic judgment policy updating*.

#### 5.5.4 Setting up the virus definition information monitoring service to start automatically

This subsection explains how to start the virus definition information monitoring service of JP1/CSC - Manager Remote Option automatically when the OS starts. The virus definition information monitoring service must be running when judgment policies for anti-virus products are automatically activated by linkage with the remote management server.

■ **Setting up the virus definition information monitoring service to start automatically**

Open Windows **Services**, and set **Startup type** to **Automatic** for **Client Security Control - Manager for AntiVirus**.

To stop automatic start for the virus definition information monitoring service once set, perform the following:

Open Windows **Services**, and set **Startup type** to **Manual** for **Client Security Control - Manager for AntiVirus**.

---

## 5.6 Installing and setting up JP1/Software Distribution Client

---

This section explains how to install and set up JP1/Software Distribution Client. For details about installing and setting up JP1/Software Distribution Client, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems.

### (1) Installing JP1/Software Distribution Client

Install JP1/Software Distribution Client on the client.

Before you can set up a quarantine system linked to the AMT Linkage facility of JP1/Software Distribution, you must install AMT Linkage facility Component.

### (2) Setting up JP1/Software Distribution Client

To automatically notify JP1/Software Distribution Manager of changes to inventory information on a client, such as when new software is installed or security updates are applied, specify the following settings during setup of the JP1/Software Distribution Client:

- On the **System Monitoring** page, select the **When the system is changed, inventory information is notified to Higher System** check box.
- On the **Connection Destination** page, select the **Automatically register this computer in the system configuration** and **Also report this computer's inventory to the server** check boxes.
- On the **Default Running Status/Polling** page, select the **Client will poll the managing server** check box.

JP1/Software Distribution Manager is notified of changes to inventory information when the client connects to the server at polling or job execution. For details about automatic notification of inventory information, see 7.3 *Automatically obtaining client inventory information*.

When you want to use JP1/Software Distribution Client as a relay system to set up a quarantine system linked to the AMT Linkage facility of JP1/Software Distribution to change the settings specified during installation, you must specify the following setting:

Specify the following setting during setup of JP1/Software Distribution Client (relay system):

- On the **AMT Linkage** page, specify the user ID and password of the AMT management user.

For details about the setting, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems.

---

## 5.7 Installing and setting up JP1/CSC - Agent

---

This section explains how to install and set up JP1/CSC - Agent.

### 5.7.1 Installing JP1/CSC - Agent

Install JP1/CSC - Agent on a network control server or an authentication server.

This subsection explains the procedures for installing JP1/CSC - Agent, for both a clean installation and an overwrite installation.

#### (1) *Performing a new installation of JP1/CSC - Agent*

The following explains the procedures for performing a new installation of JP1/CSC - Agent.

Install JP1/CSC - Agent either from the provided media, or by using JP1/Software Distribution to perform a remote installation. For details about remote installation using JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems. If remote installation fails, perform installation again using the provided media.

*Note:*

If you intend to use a network control product, install the network control product before installing JP1/CSC - Agent.

To perform installation using the provided media:

1. Log on to Windows as a member of the Administrators group.
2. Insert the provided CD-ROM in the drive.

When the installer starts, a dialog box prompting you to select a component is displayed, so select the JP1/CSC - Agent component.

3. Click the **Install** button.

A dialog box is displayed prompting you to confirm the start of installation.

4. Click the **OK** button.

A dialog box is displayed indicating that JP1/CSC - Agent installation has started.

5. Click the **Next** button.

A dialog box is displayed, in which you can enter user information.

6. Enter the user name and company name.
7. Click the **Next** button.

A dialog box is displayed in which you can specify the installation folder.

8. Specify the installation folder.

Installation is performed in the specified folder. The default installation destinations are as follows (when the OS is installed under C:\):

For a 64-bit edition of Windows:

C:\Program Files(x86)\HITACHI\jplnetmcsca

For other OSs:

C:\Program Files\HITACHI\jplnetmcsca

9. Click the **Next** button.

A dialog box is displayed, in which you can select the program folder.

10. Specify the program folder.

Specify the folder to which the program icon is added. The default folder name is Client Security Control.

11. Click the **Next** button.

A dialog box is displayed confirming the current contents. Check the set contents.

12. Click the **Next** button.

Installation begins.

When installation is finished, a dialog box confirming whether or not to open the README file is displayed. Skip to step 14 if you click the **No** button.

13. Read and then close the README file.

When the README file is read and closed, a dialog box indicating that installation is complete is displayed.

14. Click the **Finish** button.

Installation is complete.

15. Restart Windows.

If the installation finished successfully, restart Windows.

## **(2) Performing an overwrite installation of JP1/CSC - Agent**

An overwrite installation of JP1/CSC - Agent can be performed when the version to be installed is the same or later than the existing one. When performing an overwrite installation, be sure to first terminate the JP1/CSC - Agent service.

When an overwrite installation is performed, Windows does not need to be restarted.

Note that overwrite installation cannot be performed when the version to be installed

is earlier than the existing version of JP1/CSC - Agent.

### 5.7.2 Uninstalling JP1/CSC - Agent

This subsection explains the procedures for uninstalling JP1/CSC - Agent. Before performing uninstallation, be sure to terminate all JP1/CSC - Agent services.

*Note:*

If you are using a network control product, be sure to terminate all services of the network control product before uninstalling JP1/CSC - Agent.

1. In the Control Panel, open **Add/Remove Programs**, select **Client Security Control - Agent**, and then click the **Change/Remove** button.

A dialog box is displayed, confirming deletion.

2. Click the **Yes** button.

JP1/CSC - Agent is uninstalled.

Note that the files and folders created after installation are not deleted, and must be deleted manually by an administrator.

Once uninstallation is finished, a dialog box indicating that uninstallation is complete is displayed.

3. Click the **Finish** button.

Uninstallation is complete.

4. Restart Windows.

If the uninstallation finished successfully, restart Windows.

### 5.7.3 Setting up JP1/CSC - Agent

After installing JP1/CSC - Agent, be sure to set up JP1/CSC - Agent before starting it.

Note that the procedures for setting up JP1/CSC - Agent differ depending on the linked network control product. For details, see *13. Setting Up a Quarantine System*.

### 5.7.4 Setting up JP1/CSC - Agent to start automatically

To start JP1/CSC - Agent automatically when the OS starts, open Windows **Services**, and set **Startup type** to **Automatic** for **Client Security Control - Agent**.

To stop automatic start for JP1/CSC - Agent once set, perform the following.

Open Windows **Services**, and set **Startup type** to **Manual** for **Client Security Control - Agent**.

---

## 5.8 Creating CSC administrators and CSC users

---

When JP1/CSC - Manager is installed, a user with the administrator role for JP1/CSC is set by default. This user is called a *CSC administrator*. CSC administrators can use the Client Security Management window and the Security Policy Management window.

When users other than CSC administrators want to use information managed by the client security control system, an administrator can create users with restricted permissions. A user who can use the restricted functionality is called a *CSC user*. CSC users are created by a *CSC administrator*.

The following shows the types of user roles for a client security control system.

- CSC administrator

A user with the administrator role for JP1/CSC. A CSC administrator can use the Security Policy Management window and the windows for all the job categories of AIM needed to run a client security management system.

- CSC user

A user with the user role for JP1/CSC. CSC users can search for information managed by the client security control system and can output the search results to a file. CSC users cannot judge security levels, implement actions, or edit security policies.

- Asset Information Manager administrator (optional)

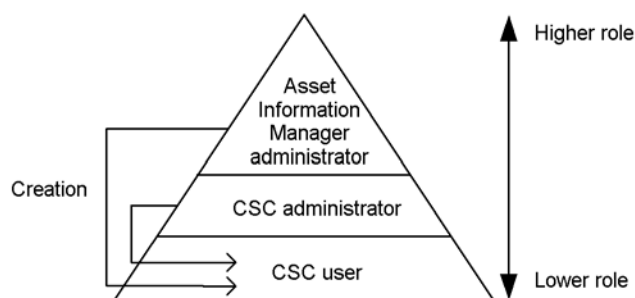
An asset administrator designated when installing Asset Information Manager. An Asset Information Manager administrator has the highest user role, and can use all the job categories of Asset Information Manager and the Security Policy Management window.

Note that you cannot create an Asset Information Manager administrator if you configure the management server using Asset Information Manager Subset Component of JP1/Software Distribution Manager.

The following figure shows the role hierarchy for Asset Information Manager administrators, CSC administrators, and CSC users.



Figure 5-13: Administrator role hierarchy



The following table lists the windows that can be used based on the corresponding user role.

Table 5-8: Operations available for each user role

Application	Window	Asset Information Manager administrator	CSC administrator	CSC user
AIM	All job categories	Yes	Yes*	--
	Client Security Management window	Yes <sup>#</sup>	Yes	Yes*
JP1/CSC	Security Policy Management window	Yes	Yes	--

Legend:

Yes: Can be used.

Yes\*: Can be used but with partial functionality.

--: Cannot be used.

#

The Security Counter-Measure Evaluation and Statistics job menus are disabled by default. You can enable these menus from the Customize Job Menu window in AIM. For details about this window, see the manual *Job Management Partner 1/ Asset Information Manager Planning and Setup Guide*.

The following subsections explain the roles and user information available for the CSC administrator that is set up during installation, and also explain how to create CSC users.

### 5.8.1 Setting up CSC administrators during installation

When JP1/CSC - Manager is installed with automatic setup specified or when an administrator executes the `cscsetup` command after installing JP1/CSC - Manager without specifying automatic setup, the JP1/CSC administrator role and an administrator user are created by default.

#### (1) CSC administrator role

The following is information about the CSC administrator role:

- Role ID  
`csc_admin`
- Role name  
CSC administrator

The following table lists the job categories of AIM that a CSC administrator can execute.

*Table 5-9: Functionality that a CSC administrator can execute*

No.	AIM job category#	AIM job menu	Functionality
1	Device Management	Device Totals	Finds the total number of devices
2		Device List	Search for devices
3		Unused Device List	Search for unused devices
4		Batch Update	Update device management information
5	Software Applied Management	Software Applied	Manage the application status of software
6		Distribution Status	Check the distribution status of software
7	System Management	Group and User	Update group and user information
8		Search Users	Search for users
9		Location	Update location information
10		IP Group	Update IP group information
11		Installed Software	Update information about installed software
12		Code	Add or update type and status information

No.	AIM job category <sup>#</sup>	AIM job menu	Functionality
13		Individual Information	View and update individual information
14		Log	Check inventory information acquisition
15	System Definition	Role	Change user roles
16		Customize Managed Items	Change managed items
17		Customize Job Windows	Change the window operations each user role can perform
18		Customize Job Menu	Change the tasks users can execute
19		Assign Inventory	Assign inventory items
20	Client Security Management	PC Security Level Management	Monitor and manage client security levels
21		Register Permitted PCs	Add a new client
22		Security Counter-Measure Evaluation	Evaluates and assigns a score to the status of security measures taken
23		Statistics	Check trends in the status of security countermeasures on a group-by-group basis

#

The jobs that a user with the CSC administrator role can use with the AIM job categories are limited to those listed in Table 5-9. If Asset Information Manager is installed on the management server, you can use other jobs by logging in to Asset Information Manager as a user with the Asset Information Manager administrator role.

The following table describes the AIM client security management functionality that a CSC administrator can use.

*Table 5-10:* Client security management functions that a CSC administrator can execute

No.	AIM job category	AIM job menu	Button name for the Customize Job Windows window <sup>#</sup>	Functionality
1	Client Security Management	PC Security Level Management	<b>Judge</b>	Security level judgment
2			<b>Message</b>	Warning message notification
3			<b>Permit</b>	Network connection permission
4			<b>Refuse</b>	Network connection denial
5			<b>Valid</b>	Security management activation
6			<b>Invalid</b>	Security management deactivation
7			<b>History CSV</b>	CSV output of judgment action history
8			<b>Search</b>	Search
9			<b>CSV</b>	CSV output of search results
10		Registration Authorized PC	<b>OK</b>	PC registration permission
11		Security Counter-Measure Evaluation	<b>Search</b>	Search
12			<b>CSV</b>	CSV output of search results
13		Statistics	<b>Search</b>	Search
14			<b>CSV</b>	CSV output of search results
15			<b>Select all</b>	Select all groups
16			<b>Clear all</b>	Deselect all groups
17			<b>Graph</b>	Display search results as graph

#

For details about the Customize Job Windows window, see 5.8.2(4) *Limiting the*

*GUI buttons that CSC users can use.*

*Note:*

The CSC administrator role can execute everything shown in the job menu in Table 5-10. Unexecutable job menus only exist for the CSC user role. Note that the CSC user role cannot log in to the Security Policy Management window.

## **(2) CSC administrator user**

The user information for the CSC administrator created during JP1/CSC - Manager setup is as follows:

- User ID  
csc\_admin
- Password  
csc\_admin

Change the password as necessary.

You can create additional CSC administrators.

For details about how to change the password and how to create additional CSC administrators, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

### **5.8.2 Creating a CSC user**

CSC users are created by a CSC administrator or an Asset Information Manager administrator. CSC users can only execute some of the client security management functionality for AIM.

The following table describes a recommended example of the AIM client security management functionality available to CSC users.

*Table 5-11: Example of functionality that a CSC user can use (recommended)*

No.	AIM job category	AIM job menu	Button name for the Customize Job Windows window <sup>#</sup>	Functionality
1	Client Security Management	PC Security Level Management	<b>History CSV</b>	CSV output of judgment action history
2			<b>Search</b>	Search
3			<b>CSV</b>	CSV output of search results
4		Security Counter-Measure Evaluation	<b>Search</b>	Search
5			<b>CSV</b>	CSV output of search results
6		Statistics	<b>Search</b>	Search
7			<b>CSV</b>	CSV output of search results
8			<b>Select all</b>	Select all groups
9			<b>Clear all</b>	Deselect all groups
10			<b>Graph</b>	Display search results as graph

#

For details about the Customize Job Windows window, see (4) *Limiting the GUI buttons that CSC users can use*.

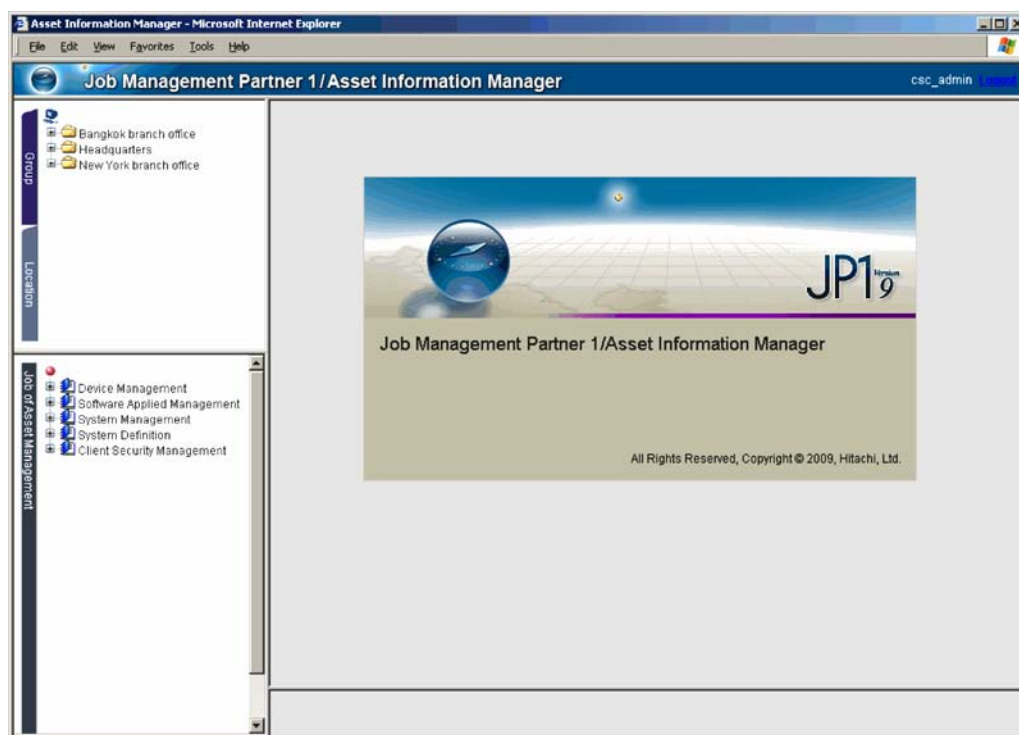
Note that CSC users can be created by users with the CSC administrator or Asset Information Manager administrator roles, using the AIM windows.

The following subsections describe how a CSC administrator or an Asset Information Manager administrator creates a CSC user, based on the recommended example given in Table 5-11.

### **(1) Logging in to AIM**

1. Log in from the Login window of AIM, as a user with either the CSC administrator role or the Asset Information Manager administrator role.

The initial window of AIM appears.



## (2) Creating a new user role for a CSC user

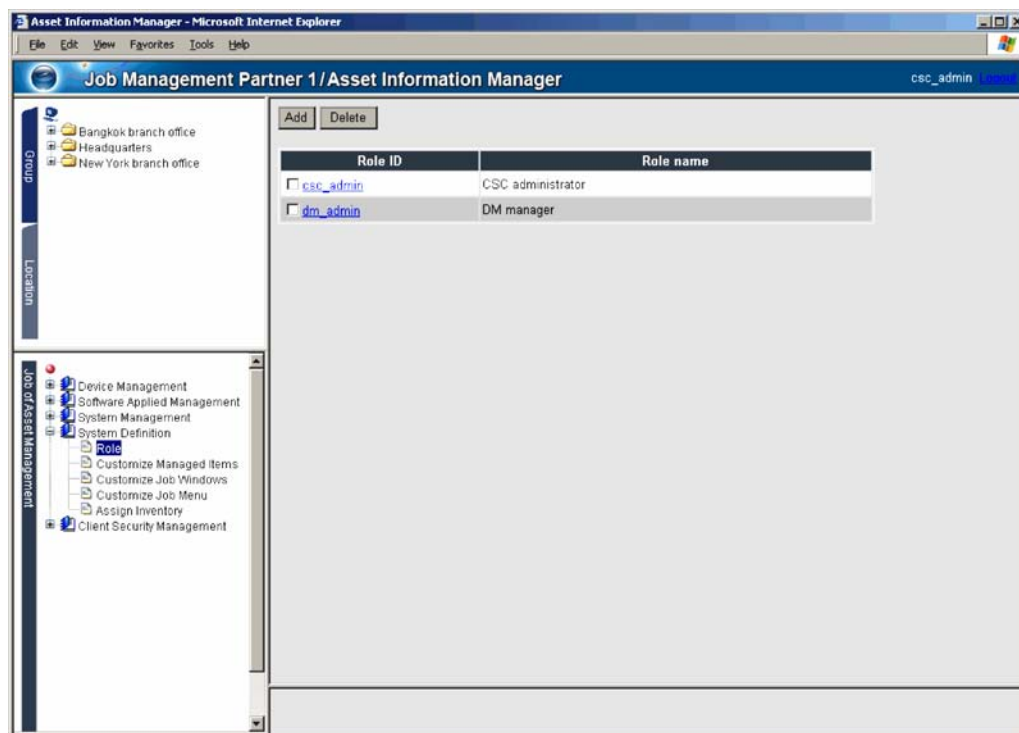
Create a user role from the Role window of AIM. For details about the Role window, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

To create a user role:

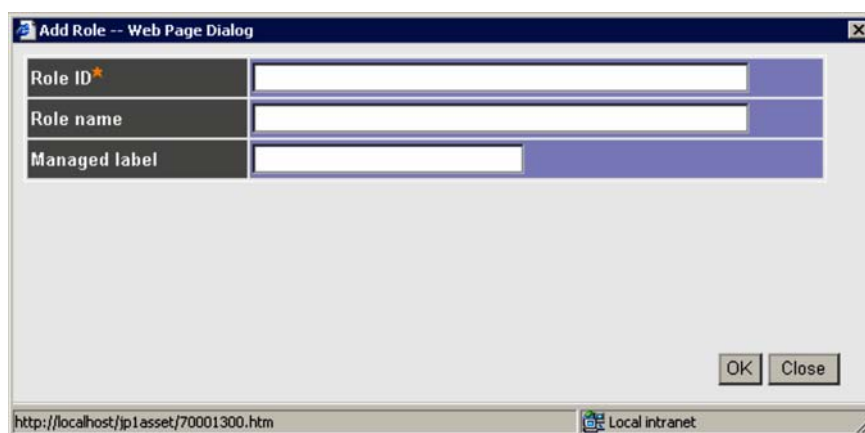
1. From **System Definition** in the job menu, click **Role**.

The Role window is displayed.

## 5. Installation and Setup



2. In the Role window, click the **Add** button.  
The Add Role dialog box is displayed.



Enter each item:

**Role ID**



Enter the role ID for the CSC user. This setting is required.

**Role name**

Enter the role name for the CSC user. A role with an existing name cannot be created. If this item is omitted, the value set for **Role ID** is used for the name.

**Managed label**

Set this to limit access to each group hierarchy.

3. Click the **OK** button.

The user role for the CSC user is created.

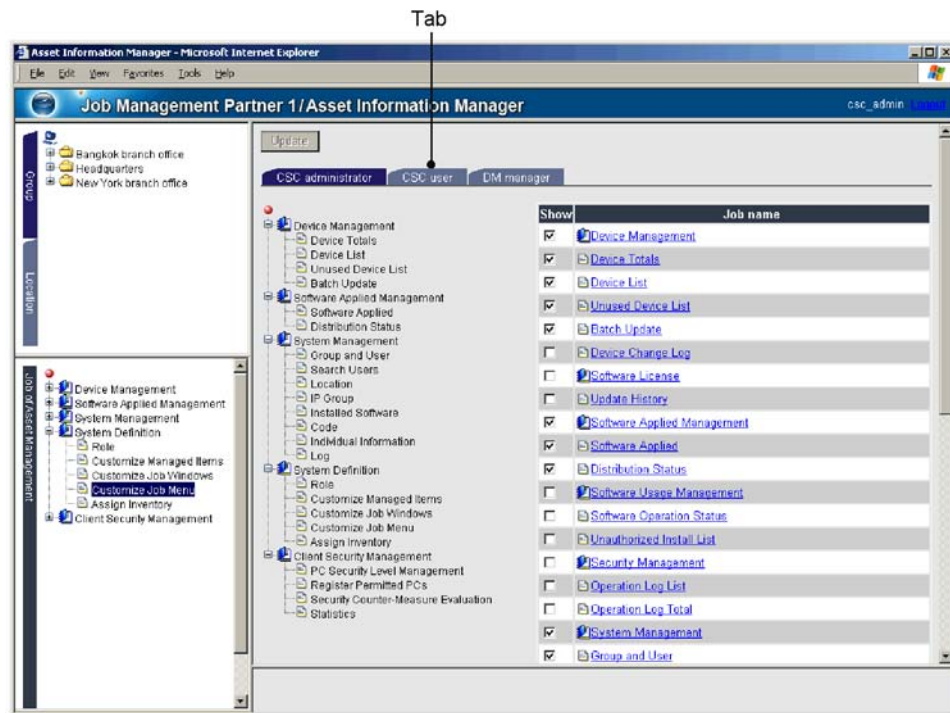
**(3) Assigning jobs that a CSC user can use**

Assign jobs for the CSC user to use. You can assign jobs from the Customize Job Menu window of AIM. For details about this window, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

To allocate a job to a CSC user:

1. From **System Definition** in the job menu, click **Customize Job Menu**.

The Customize Job Menu window is displayed.



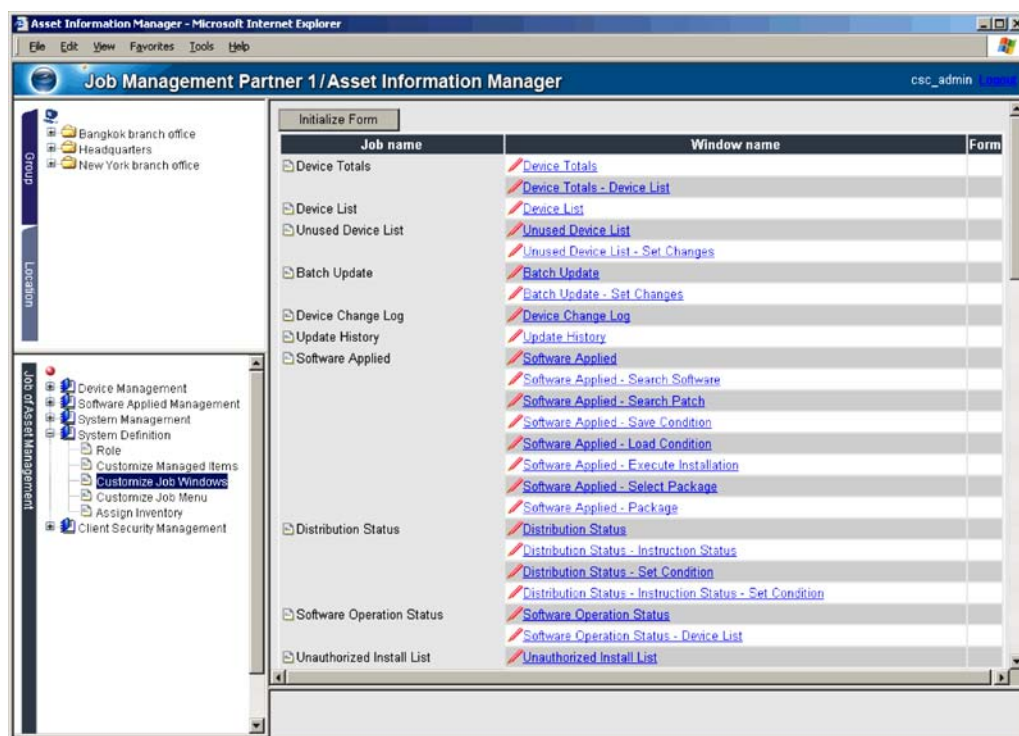
2. Click the new **CSC user** tab created for the user role of the CSC user.  
A window is displayed for allocating CSC user jobs.
3. Select the **Show** check boxes for the job names **PC Security Level Management**, **Security Counter-Measure Evaluation**, and **Statistics**.  
Make sure that the **Show** check boxes for all other job names are cleared.
4. Click the **Update** button.  
In the operation window for users with the CSC user role, only the job names **PC Security Level Management**, **Security Counter-Measure Evaluation**, and **Statistics** are displayed.

#### (4) Limiting the GUI buttons that CSC users can use

By limiting the GUI buttons that are shown, the window operations of CSC users can be restricted. You can change the buttons that are shown by using the Customize Job Windows window of AIM. For details about this window, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

To change the display of the GUI buttons used for **PC Security Level Management**:

1. From **System Definition** in the job menu, click **JobCustomize Job Windows**.  
The Customize Job Windows window is displayed.



2. Click the anchor (underlined link) for which the window name is **PC Security Level Management**.  
The Edit Form window is displayed.

The screenshot shows the 'Edit of PC Security Level Management' window. It has a title bar with 'Edit of PC Security Level Management - Microsoft Internet Explorer'. Below the title bar are buttons: OK, Add Form, Copy Form, Rename Form, Delete Form, and Cancel. The main content area is divided into three sections: 'Object role', 'Button', and 'Condition'. Each section has two lists and transfer buttons. In the 'Object role' section, the 'Do not apply' list contains 'CSC administrator' and the 'Apply' list contains 'CSC user'. In the 'Button' section, the 'Hide' list contains 'Permit', 'Invalid', 'Judge', 'Message', 'Refuse', and 'Valid', and the 'Show' list contains 'CSV', 'Search', and 'History CSV'. In the 'Condition' section, the 'Hide' list is empty and the 'Show' list contains 'Asset No.(Asset information)', 'Host name(Hardware information)', 'IP address(Hardware information)', 'User name(Asset information)', 'Group name(Group information)', and 'PC security level'.

3. From the list in **Do not apply** for **Object role**, select **CSC user**, and then click the **Apply** button.

**CSC user** is moved to the **Apply** list, and the object role is set.

4. From the list in **Show** for **Button**, select the following buttons, and then click the **Hide** button.

See Table 5-10 *Client security management functions that a CSC administrator can execute*, and select the buttons not to be used by the CSC user. We recommend the following buttons to be selected:

- **Judge**
- **Message**
- **Permit**
- **Refuse**
- **Valid**

- **Invalid**

The selected buttons are moved to the **Hide** list, and will be hidden from user window operations for the CSC user role.

5. Click the **OK** button.

The changed form is reflected in the window.

You do not need to limit the GUI buttons shown in the windows for the **Security Counter-Measure Evaluation** and **Statistics** jobs, because these jobs use functions that only reference data.

*Note:*

When you upgrade the version of JP1/CSC - Manager, you must delete all the forms of **Customize Job Windows** for **PC Security Level Management**, and then set them again. To delete a form, in the Edit Form window shown in step 2, choose the form tab you want to delete, and click the **Delete form** and then the **OK** buttons.

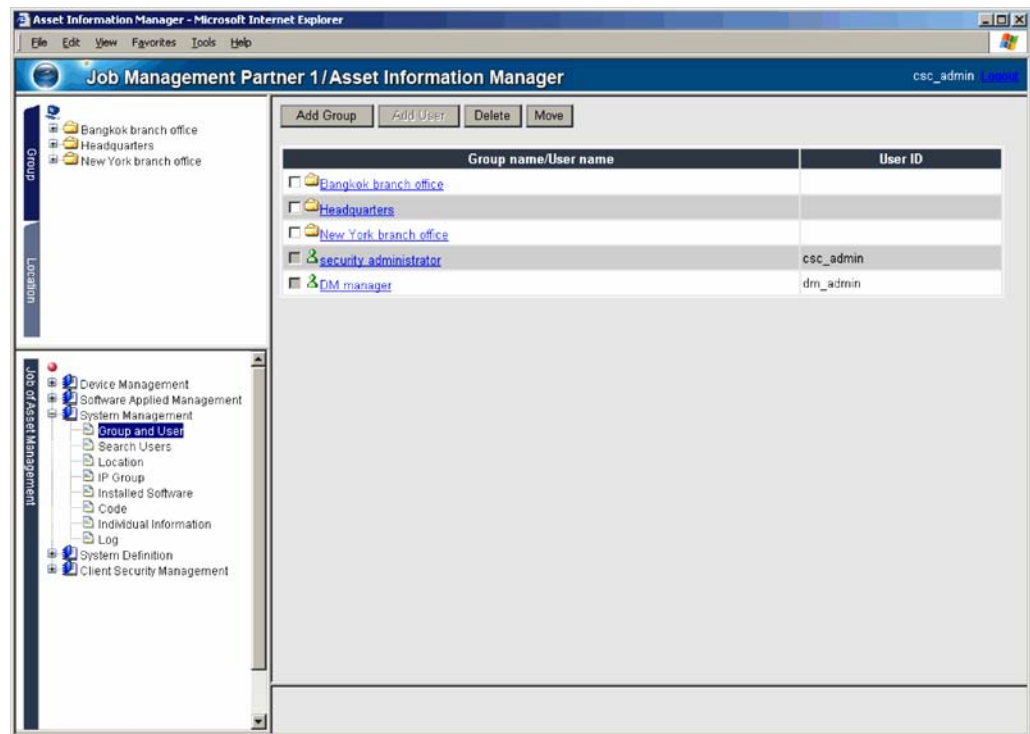
### **(5) Registering a CSC user**

Register a user with the CSC user role. You can register a user from the Group and User window of AIM. For details about this window, see the manual *Job Management Partner 1/Asset Information Manager Administrator's Guide*.

To register a new user:

1. From **System Management** in the job menu, click **Group and User**.

The Group and User window is displayed.



2. Select the group to which you would like to add a user, from **simple search condition**.

Users cannot be registered in the highest level group.

3. Click the **Add User** button.

The Add User dialog box is displayed.

Be sure to set the following items:

- **User ID**  
Specify a user ID that is unique among users.
- **Password**  
For confirmation, specify the same password twice.
- **User name**  
Specify the user name.

4. Select the CSC user from **Role**.

5. Click the **Add** button.

A user is added with the contents specified.

### 5.8.3 Preventing update processing for detailed device information

A CSC administrator or Asset Information Manager administrator can use the Client Security Management window of AIM to update and view the detailed device information for each client. Update processing for detailed device information needs to be prevented for CSC administrators and CSC users, so that they can only view the information.

To prevent CSC users from updating detailed device information, a CSC administrator or Asset Information Manager administrator can use the Customize Job Windows window of AIM to hide the **Update** button in the Device Details dialog box. For details about the Customize Job Windows window, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

The following table lists the button display settings for the Device Details dialog box that a CSC administrator or Asset Information Manager administrator can set in the Customize Job Windows window.

Table 5-12: Button display settings in the Device Details dialog box

Page name	Detail dialog box name	Button name	Display
<b>Device</b>	None	<b>Update</b>	Hide
		<b>NNM</b>	Hide
		<b>Close</b>	Show
<b>Network</b>	None	<b>Add</b>	Hide
		<b>Delete</b>	Hide
		<b>Close</b>	Show
	Network Details	<b>Update</b>	Hide
		<b>Delete</b>	Hide
		<b>Close</b>	Show
	IP Address	<b>Search</b>	Show
		<b>OK</b>	Hide
		<b>Close</b>	Show
<b>Software</b>	None	<b>Add</b>	Hide
		<b>Delete</b>	Hide
		<b>Close</b>	Show

Page name	Detail dialog box name	Button name	Display
	Installed Software Details	Update	Hide
		Delete	Hide
		Close	Show
Patch	None	Add	Hide
		Delete	Hide
		Show	Show
		Close	Show
Anti-Virus	None	Add	Hide
		Delete	Hide
		Show	Show
		Close	Show
License <sup>#</sup>	None	Assign	Hide
		Cancel	Hide
		Close	Show
Inventory	None	Close	N/A
Contract <sup>#</sup>	None	Add	Hide
		Cancel	Hide
		Close	Show
Maintenance <sup>#</sup>	None	Add	Hide
		Delete	Hide
		Close	Show
	Maintenance Log Details	Edit	Hide
		Delete	Hide
		Close	Show
Update Records <sup>#</sup>	None	Close	N/A

N/A: Not applicable



#

Not displayed if the management server uses Asset Information Manager Subset Component of JP1/Software Distribution Manager.

For details about client detailed device information, see 8.3.7 *Checking device details for a client*.

---

## 5.9 Procedures for setting a task in Scheduled Tasks

---

To periodically judge security levels or assign security policies to clients, set the following commands as tasks in Windows Scheduled Tasks:

- To periodically judge security levels:  
Security level judgment command (`cscjudge`)
- To periodically assign security policies to clients:  
Policy assignment command (`cscassign`)
- To periodically store statistics relating to the status of security countermeasures:  
Statistics storage command (`cscstorecount`)
- To periodically update the judgment policy for security updates:  
Judgment policy update command for security updates (`cscpatchupdate`)

To set a command as a task in Windows Scheduled Tasks:

1. In the Windows Control Panel, choose **Tasks**, and then **Add Scheduled Task**.

The Scheduled Task Wizard window is displayed.

2. Click the **Next** button.

The Scheduled Task Wizard dialog box is displayed.

3. Click the **Browse** button, and select the following program:

To periodically judge security levels:

*JP1/CSC - Manager-installation-folder\bin\cscjudge.exe*

To periodically assign security policies to clients:

*JP1/CSC - Manager-installation-folder\bin\cscassign.exe*

To periodically store statistics relating to the status of security countermeasures:

*JP1/CSC - Manager-installation-folder\bin\cscstorecount.exe*

To periodically update the judgment policy for security updates:

*JP1/CSC - Manager-installation-folder\bin\cscpatchupdate.exe*

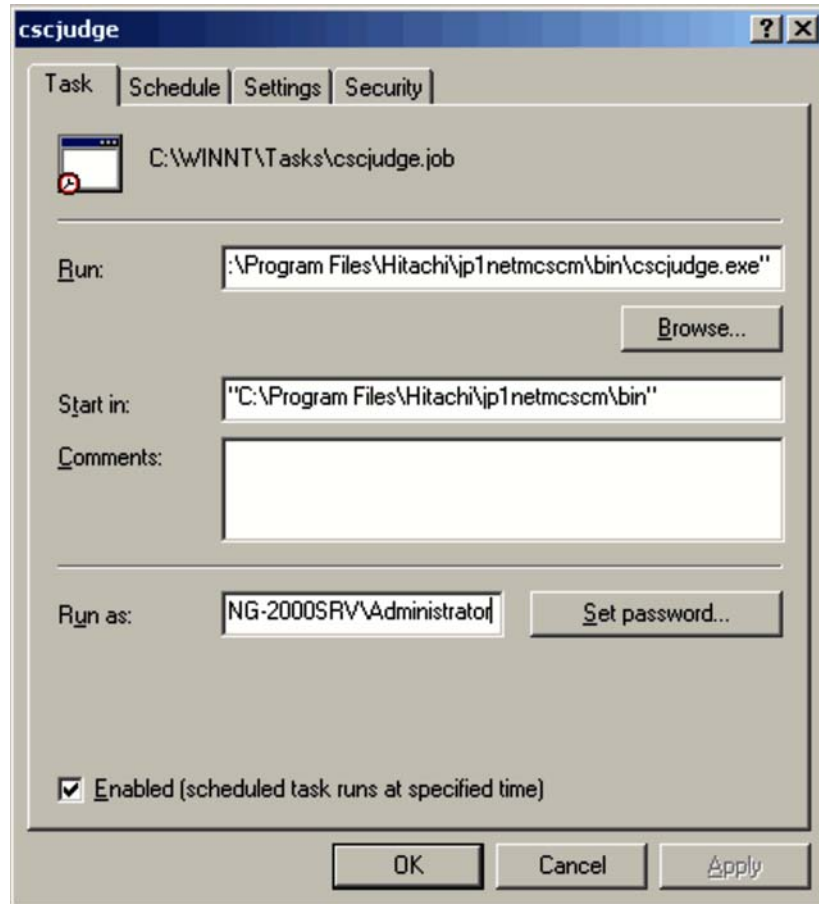
4. Click the **Open** button.

A dialog box is displayed in which the task name can be entered and the task execution unit can be selected.

5. Enter a task name, and select the task execution unit.

6. Click the **Next** button.  
A dialog box is displayed in which the task schedule information can be entered.
7. Enter the task schedule information.  
Enter the start time, execution interval, and start day for the task.
8. Click the **Next** button.  
A dialog box is displayed in which the user name can be entered.
9. Enter the user name.  
Enter the name and password of a user with Administrator permissions.
10. Click the **Next** button.  
A dialog box is displayed in which the scheduled task can be checked.
11. Select the **Open advanced properties for this task when I click Finish** check box.
12. Click the **Finish** button.  
The following window is displayed.

Figure 5-14: Name of the file to be executed (when setting the security level judgment command `cscjudge` as a task)



13. Specify the arguments of the command, for the name of the file to be executed.

To periodically judge security levels:

For details about the `cscjudge` command, see *cscjudge (judges security levels)* in 15. Commands.

To periodically assign security policies to clients:

For details about the `cscassign` command, see *cscassign (assigns security policies to clients)* in 15. Commands.

To periodically store statistics relating to the status of security countermeasures:

For details about the `cscstorecount` command, see *cscstorecount (stores*

*statistics about the status of security measures)* in *15. Commands*.

To periodically update the judgment policy for security updates:

For details about the `cscpatchupdate` command, see *cscpatchupdate (updates patch information for judgment policies relating to security updates)* in *15. Commands*.

14. Click the **OK** button.

A settings dialog box is displayed for account information. Check the name of the execution account, and enter the password.

15. Click the **OK** button.

The task settings are complete.



## Chapter

---

# 6. Managing Security Policies

---

This chapter describes how to manage and edit security policies (judgment policies and action policies) and how to assign them to clients.

- 6.1 Procedures and window transitions for policy settings
- 6.2 Managing judgment policies
- 6.3 Editing a security update judgment policy
- 6.4 Editing an anti-virus product judgment policy
- 6.5 Editing a prohibited software judgment policy
- 6.6 Editing a mandatory software judgment policy
- 6.7 Editing a PC security setting judgment policy
- 6.8 Editing a user-defined judgment policy
- 6.9 Managing action policies
- 6.10 Setting an action for each security level
- 6.11 Editing an administrator notification email
- 6.12 Editing a client user notification message
- 6.13 Assigning security policies to clients
- 6.14 Displaying clients that meet specified conditions

---

## 6.1 Procedures and window transitions for policy settings

---

To manage client security, an administrator sets a security policy based on the security objectives. A security policy consists of *judgment policies* to judge the security level of the client, and *action policies* to implement actions based on the corresponding security level.

After setting the judgment policies and action policies, the administrator assigns them to clients.

The steps involved in setting a security policy and assigning it to clients are as follows:

1. Create a judgment policy

Create a judgment policy as required.

This step is unnecessary if you intend using the default judgment policy.

2. Edit the judgment policy

Set a judgment condition and security level for each judgment item.

The judgment items for a judgment policy are as follows:

- Security updates
- Anti-virus products
- Prohibited software
- Mandatory software
- PC security settings
- User definition

Note that the security levels that can be set for a judgment policy are Danger, Warning, or Caution.

You can also use the judgment policy update command (`cscpolimport`) to set judgment policies. For details about how to use the `cscpolimport` command, see *cscpolimport (updates judgment policy settings)* in 15. Commands.

3. Create an action policy

Create an action policy as required.

This step is unnecessary if you intend using the default action policy.

4. Edit the action policy

Set an action for each security level. The security levels are as follows:

- Danger



- Warning
- Caution
- Safe

You can set any of the following actions for each security level:

- Notify the administrator by email
- Send a message to the client
- Control client connections to the network
- Implement a user-defined action (user-specific command set by the administrator)

You can customize the text of the messages sent to the administrator and client.

#### 5. Assign the policies

Assign the created judgment policy and action policy to clients.

A default judgment policy and a default action policy are pre-assigned to every client.

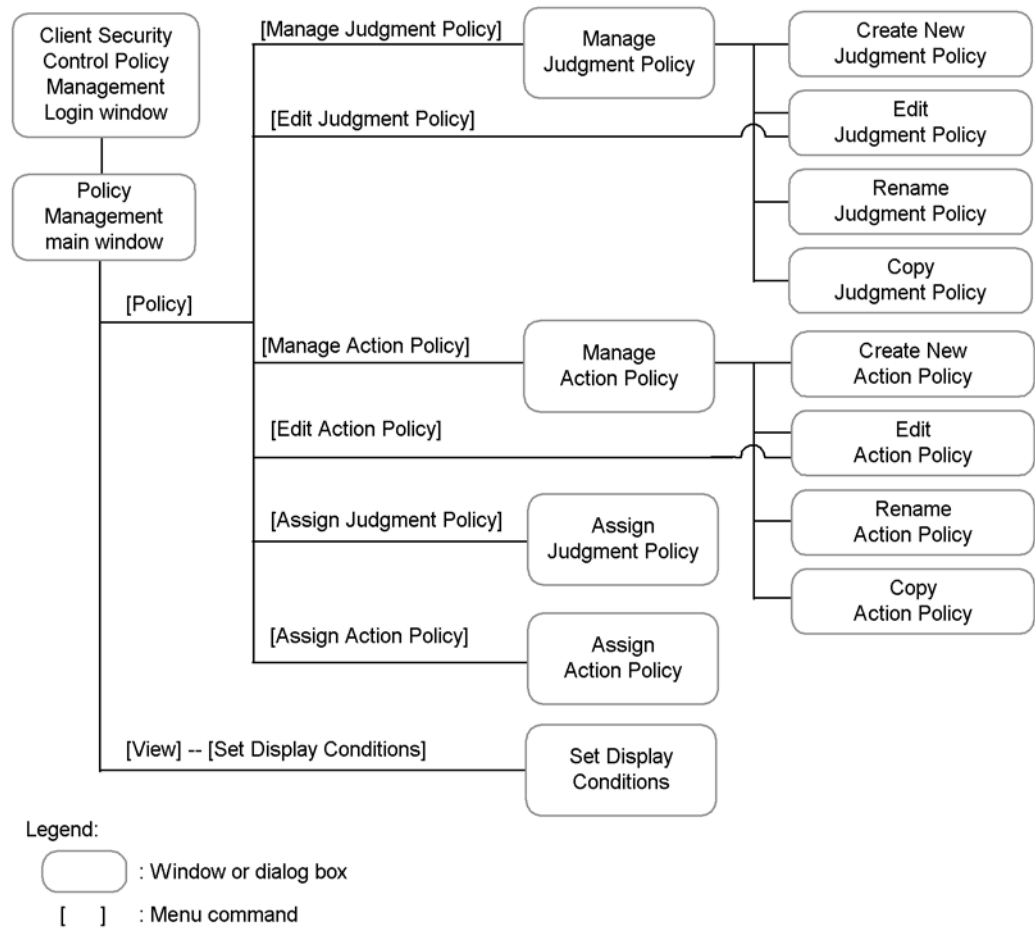
#### *Reference note:*

Default policies are assigned whenever a new client is configured in the system. If you add a client after starting operations with your client security control system, assign policies to that client as required.

Security policies are set and assigned from the Policy Management main window.

The following figure shows the window transitions for the Policy Management main window.

Figure 6-1: Windows transitions for the Policy Management main window



To log in to the Policy Management main window:

1. Log on to Windows as a user with Administrators permissions.
2. Click the **Start** menu, and choose **Programs, Client Security Control**, and then **Policy Management**.

After a splash window is displayed, the Client Security Control Policy Management Login window is displayed.



3. Set each item.

The items to set are as follows:

**User ID** text box

Enter the user ID of the CSC administrator.

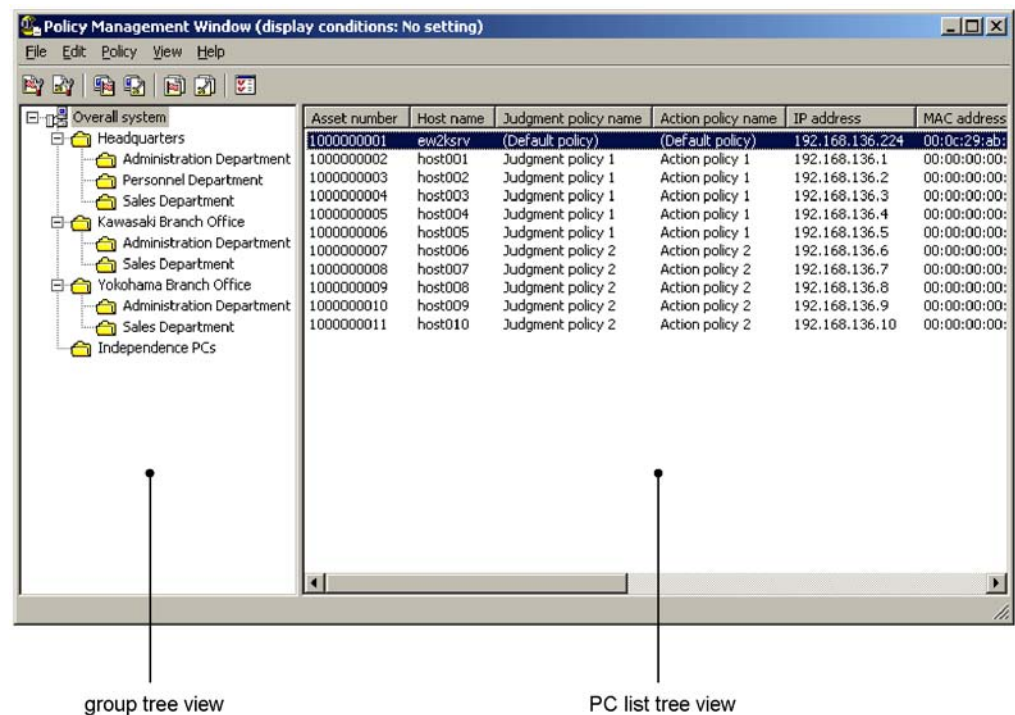
**Password** text box

Enter the password of the CSC administrator.

4. Click the **OK** button.

If user authentication is successful, you are logged in to JP1/CSC - Manager and the Policy Management main window appears.

Figure 6-2: Policy Management main window



The following describes the Policy Management main window.

The Policy Management main window is for managing the security policies in the system. It consists of two panes: a *group tree view* and a *PC list tree view*.

The display items in the Policy Management main window are as follows.

Group tree view

The group tree view shows the hierarchy of departments and sections to which the clients belong, based on the asset information managed in AIM.

The tree root is shown as **Overall system**. Clients that do not belong to any department are grouped under **Independence PCs**.

PC list tree view

The PC list tree view shows client asset information and details about the policies assigned to clients, based on the asset information managed in AIM. The policy information includes the asset number, host name, judgment policy name, action policy name, IP address, MAC address, OS information, group name, user name, and location of each client in list format.

The following information is displayed in PC list tree view, depending on what you select in the group tree view:




- Select **Overall system**:  
To view information for all clients.
- Select a group name:  
To view information for the clients belonging to that group.
- Select **Independence PCs**:  
To view information for the clients that do not belong to any group.





When you click a column header, the PC information in that column is sorted in ascending or descending order.

By setting display conditions in the Set Display Conditions dialog box, you can view asset information for only those clients that meet the set conditions. When display conditions are set, **Policy Management Window (display conditions: Setting)** appears in the title bar of the Policy Management main window. Before you set any display conditions, **Policy Management Window (display conditions: No setting)** appears in the title bar.

The menus in the Policy Management main window are shown below.

*Table 6-1: Menus in the Policy Management main window*

Menu	Command	Purpose
<b>File</b>	<b>Exit</b>	Closes the Policy Management main window.
<b>Edit</b>	<b>Copy</b>	Copies asset information (text in CSV format) to the clipboard. This command is available when you select a single client in the PC list tree view.
	<b>Select All</b>	Selects all the clients in the PC list tree view.
<b>Policy</b>	<b>Manage Judgment Policy</b>  button)	Displays the Manage Judgment Policy dialog box. In this dialog box, you can create, edit, delete, rename, and copy judgment policies.
	<b>Manage Action Policy</b> (  button)	Displays the Manage Action Policy dialog box. In this dialog box, you can create, edit, delete, rename, and copy action policies.
	<b>Edit Judgment Policy</b> (  button)	Displays the Edit Judgment Policy window for editing a judgment policy assigned to a selected group or PC. This command is available when you select a single client in the PC list tree view.

Menu	Command	Purpose
	<b>Edit Action Policy</b> (  button)	Displays the Edit (Action Policy) window for editing an action policy assigned to a group or PC. This command is available when you select a single client in the PC list tree view.
	<b>Assign Judgment Policy</b> (  button)	Displays the Assign Judgment Policy dialog box for assigning a judgment policy to a selected group or client. This command is available when you select a group in the group tree view, or one or more clients in the PC list tree view.
	<b>Assign Action Policy</b> (  button)	Displays the Assign Action Policy dialog box for assigning an action policy to a selected group or client. This command is available when you select a group in the group tree view, or one or more clients in the PC list tree view.
<b>View</b>	<b>Set Display Conditions</b> (  button)	Displays the Set Display Conditions dialog box for setting conditions for displaying clients in the PC list tree view. This command is available when you select a group in the group tree view.
	<b>Refresh</b>	Collects asset information managed in AIM, and updates the information displayed in the group tree view and PC list tree view.
<b>Help</b>	<b>Version</b>	Displays version information.

Legend:

The buttons shown in parentheses appear in the tool bar.

The following commands also appear in the shortcut menu of the Policy Management main window:

- **Edit Judgment Policy**
- **Edit Action Policy**
- **Assign Judgment Policy**
- **Assign Action Policy**
- **Set Display Conditions**
- **Copy**

## 6.2 Managing judgment policies

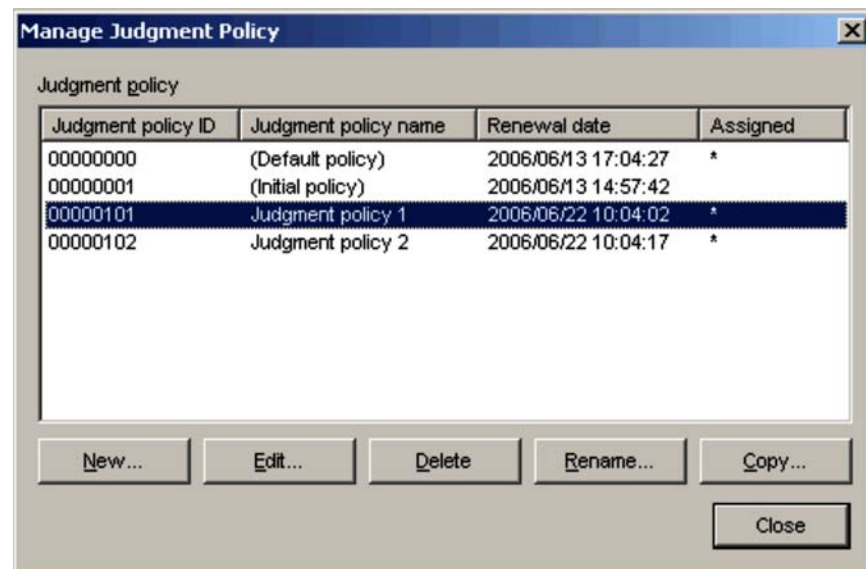
A judgment policy can be managed in the Manage Judgment Policy dialog box.

In this dialog box, you can create, edit, delete, rename, and copy judgment policies.

To open the Manage Judgment Policy dialog box, in the Policy Management main window choose **Policy** and then **Manage Judgment Policy**.

The following figure shows the Manage Judgment Policy dialog box.

Figure 6-3: Manage Judgment Policy dialog box



The display items and buttons in the Manage Judgment Policy dialog box are as follows.

### Judgment policy

Lists information about created judgment policies, including the ID and name of each policy, latest update time, and whether the policy has been assigned (indicated by an asterisk (\*) if so). The following two judgment policies are preset by the system:

No.	Judgment policy name	Judgment policy ID	Description
1	Default policy	00000000	A policy initially assigned to every client. You can customize this policy.

No.	Judgment policy name	Judgment policy ID	Description
2	Initial policy	00000001	A judgment policy for saving the default settings. You cannot edit, delete, or rename this policy. By copying the contents of this policy, you can change a modified default policy back to its original contents.

Like clicking the **Edit** button, double-clicking a judgment policy in the list displays a window that allows you to edit the judgment policy. For details, see *6.2.2 Editing a judgment policy*.

#### **New** button

Opens the Create New Judgment Policy dialog box. Use this button to create a new judgment policy. For details, see *6.2.1 Creating a judgment policy*.

#### **Edit** button

Opens a window for editing a judgment policy selected in the list. You can have multiple Edit Judgment Policy windows open at the same time. Note that the **Edit** button is disabled when multiple judgment policies are selected in the list. For details, see *6.2.2 Editing a judgment policy*.

#### **Delete** button

Deletes a judgment policy selected in the list. You can select multiple judgment policies. When you delete an assigned judgment policy, the system assigns the default policy to that client. For details, see *6.2.3 Deleting a judgment policy*.

#### **Rename** button

Opens the Rename Judgment Policy dialog box. Use this button to rename a judgment policy selected in the list. Note that the **Rename** button is disabled when multiple judgment policies are selected in the list. For details, see *6.2.4 Renaming a judgment policy*.

#### **Copy** button

Opens the Copy Judgment Policy dialog box. Use this button to copy the contents of a particular judgment policy to another judgment policy. For details, see *6.2.5 Copying a judgment policy*.

The operations you can perform depend on the type of policy you select, as shown in the table below.



Table 6-2: Operations that can be performed on each type of policy

No.	Judgment policy type	Edit	Delete	Rename	Copy
1	Default policy	Yes	No	No	Yes
2	Initial policy	No	No	No	Yes <sup>#</sup>
3	Created judgment policy	Yes	Yes	Yes	Yes

Legend:

Yes: The operation can be performed.

No: The operation cannot be performed.

#

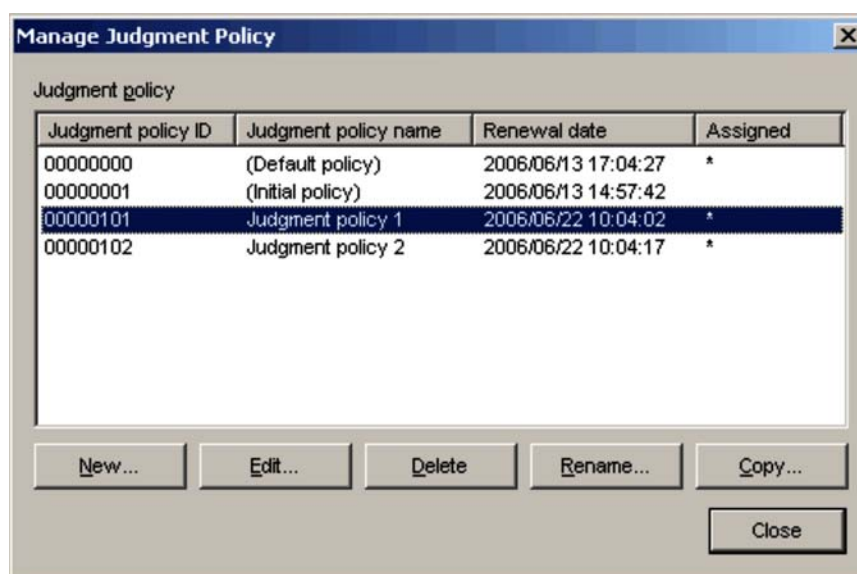
Can be performed only when the initial policy is selected as the copy source, not the copy destination.

### 6.2.1 Creating a judgment policy

To create a new judgment policy, follow the steps below. If you use the default policy, this operation is unnecessary.

1. In the Policy Management main window, choose **Policy** and then **Manage Judgment Policy**.

The Manage Judgment Policy dialog box appears.



- Click the **New** button.

The Create New Judgment Policy dialog box appears.

*Figure 6-4: Create New Judgment Policy dialog box*

**Create New Judgment Policy**

Judgment policy name:

☒ Create a copy from an existing judgment policy

Judgment policy for the copy source

Judgment policy ID	Judgment policy name	Renewal date	Assigned
00000000	(Default policy)	2006/07/19 18:58:12	*
00000001	(Initial policy)	2006/07/19 18:58:12	
00000101	Judgment policy 1	2006/07/19 20:44:27	*
00000102	Judgment policy 2	2006/07/19 20:44:29	*

OK Cancel

The items to set in the Create New Judgment Policy dialog box are as follows.

#### **Judgment policy name**

Specify the name of the new judgment policy as a character string of no more than 128 bytes.

You cannot duplicate the name of an existing judgment policy.

#### **Create a copy from an existing judgment policy**

Select this check box to create a new judgment policy based on the initial policy or other existing policy. This check box is selected by default.

#### **Judgment policy for the copy source**

If you selected the **Create a copy from an existing judgment policy** check box, select the source judgment policy from this list.

- Click the **OK** button.

You are returned to the Manage Judgment Policy dialog box. The new policy is

added to the listed judgment policies.

### 6.2.2 Editing a judgment policy

To edit a judgment policy, follow the steps below. You can set the following judgment items in a judgment policy:

#### ■ Security updates

This policy judges whether a Windows security update (patch or service pack) has been applied to a client. There are two kinds of judgment condition:

- Latest security update
- Specified security update

#### ■ Anti-virus products

This policy judges the installation status of an anti-virus product, and whether an engine version and virus definition file version have been applied to a client.

#### ■ Prohibited software

This policy judges whether any prohibited software is installed on a client.

#### ■ Mandatory software

This policy judges whether mandatory software is installed on a client.

#### ■ PC security settings

This policy judges whether security-related items have been set correctly on client PCs. There are ten judgment items:

- Accounts
- Passwords
- Logon
- Shares
- Anonymous connections
- Services
- Firewall
- Automatic updates
- Screensaver
- Drive encryption

#### ■ User definition

This policy judges items defined by the administrator, such as power-saving CPU

usage, automatic logon settings, and other information contained in the asset management database of AIM.

The administrator can set judgment conditions and security levels for each of the above judgment items.

To edit a judgment policy:

1. Perform either of the following operations.

To edit a judgment policy selected from the list:

In the Policy Management main window, choose **Policy** and then **Manage Judgment Policy**. The Manage Judgment Policy dialog box appears.

From the list of judgment policies in the dialog box, click to select the judgment policy you want to edit and then click the **Edit** button.

Alternatively, from the list of judgment policies in the Manage Judgment Policy dialog box, double-click the judgment policy you want to edit.

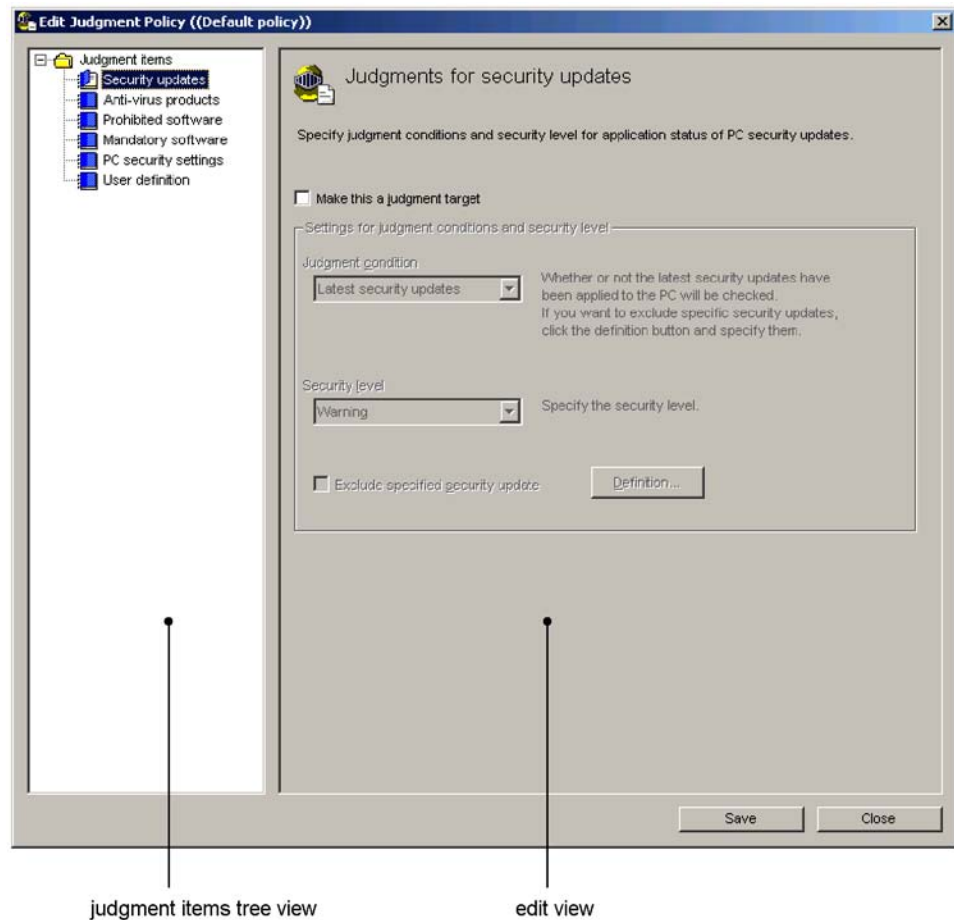
Note that the **Edit** button is disabled if you select multiple judgment policies in the list in the Manage Judgment Policy dialog box.

To edit a judgment policy assigned to a client:

In the Policy Management main window, select a client who has been assigned the judgment policy you want to edit. Then choose **Policy** and **Edit Judgment Policy**.

The Edit Judgment Policy window appears.

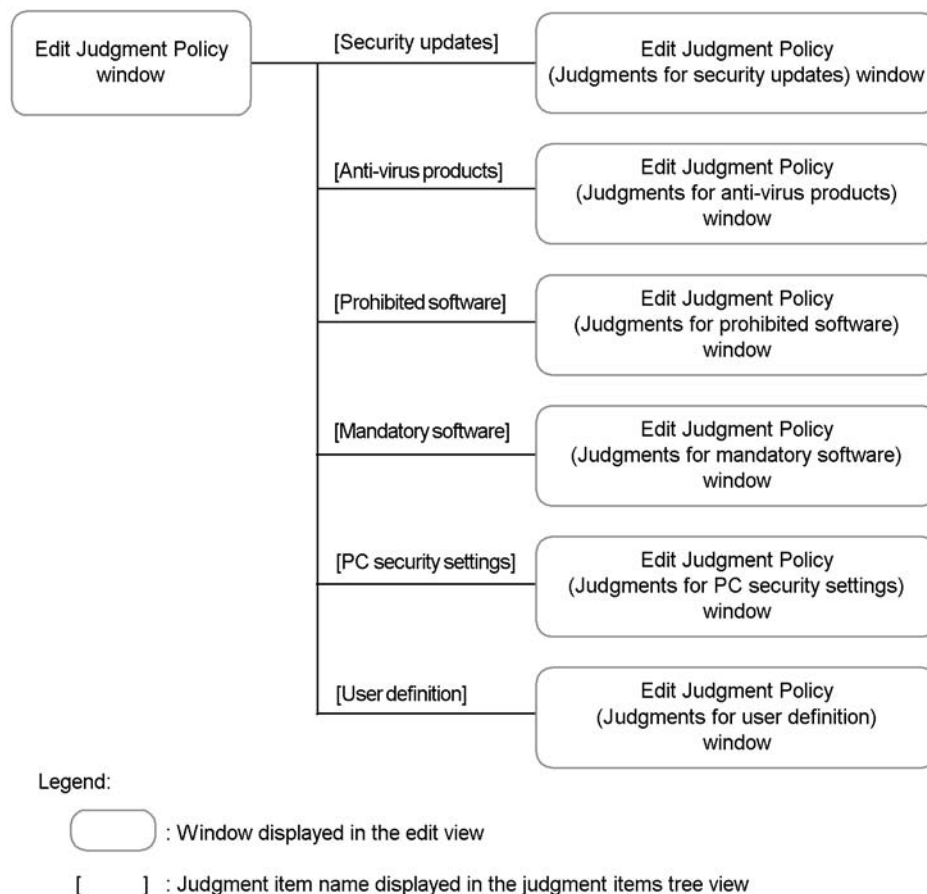
Figure 6-5: Edit Judgment Policy window



The Edit Judgment Policy window consists of the *judgment items tree view* and the *edit view*. Select an item from the judgment items tree view, and use the edit view to edit the judgment conditions and security level.

The following figure shows the window transitions for the Edit Judgment Policy window.

Figure 6-6: Windows transitions for the Edit Judgment Policy window



2. In the **Judgment items** tree view, select a judgment item to edit.  
An edit window for the selected judgment item appears in the edit view.
3. In the edit window for the selected judgment item, select the **Make this a judgment target** check box.

You can now edit the judgment item you selected.

For details about editing each judgment item, see the following sections:

- Security updates: See 6.3 *Editing a security update judgment policy*.
- Anti-virus products: See 6.4 *Editing an anti-virus product judgment policy*.
- Prohibited software: See 6.5 *Editing a prohibited software judgment policy*.

- Mandatory software: See 6.6 *Editing a mandatory software judgment policy*.
- PC security settings: See 6.7 *Editing a PC security setting judgment policy*.
- User definition: See 6.8 *Editing a user-defined judgment policy*.

*Note:*

You cannot edit the initial policy settings.

### 6.2.3 Deleting a judgment policy

To delete a judgment policy:

1. In the Policy Management main window, choose **Policy** and then **Manage Judgment Policy**.

The Manage Judgment Policy dialog box appears.

2. In the policy list in the Manage Judgment Policy dialog box, select the judgment policy you want to delete.

You can select multiple judgment policies.

3. Click the **Delete** button.

A message box appears, asking if you are sure you want to delete the policy.

4. Click the **OK** button in the message box.

The judgment policy is deleted. If the judgment policy you selected at step 1 has been assigned to any clients, the default policy will be assigned to those clients.

*Note:*

You cannot delete a default policy or initial policy.

### 6.2.4 Renaming a judgment policy

To rename a judgment policy:

1. In the Policy Management main window, choose **Policy** and then **Manage Judgment Policy**.

The Manage Judgment Policy dialog box appears.

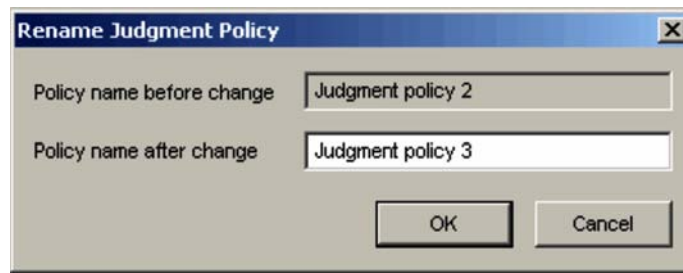
2. In the policy list in the Manage Judgment Policy dialog box, select a judgment policy to rename and then click the **Rename** button.

The Rename Judgment Policy dialog box appears.

Note that the **Rename** button is disabled if you select multiple judgment policies

in the list in the Manage Judgment Policy dialog box.

Figure 6-7: Rename Judgment Policy dialog box



3. In the **Policy name after change** box, type the new name as a character string of no more than 128 bytes.
4. Click the **OK** button.

The new policy name is listed in the Manage Judgment Policy dialog box.

*Note:*

Note these points when renaming a judgment policy:

- You cannot rename a default policy or initial policy.
- You cannot duplicate the name of an existing judgment policy, but you can specify the same name as an existing action policy.

### 6.2.5 Copying a judgment policy

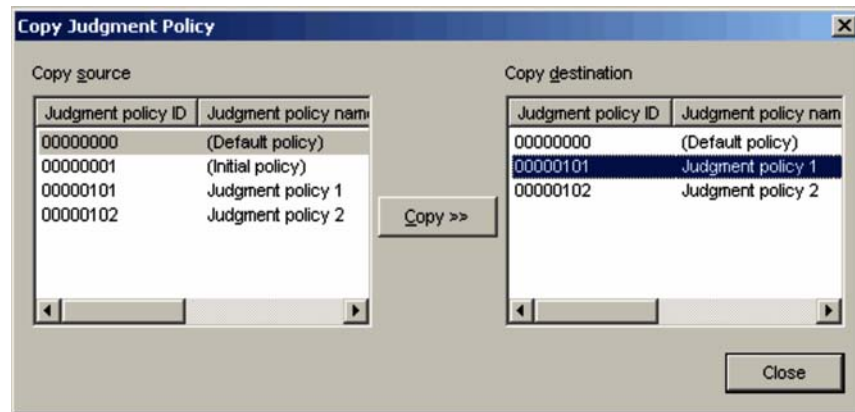
To copy a judgment policy, follow the steps below. This operation writes the contents of an existing policy to another judgment policy, replacing its contents.

1. In the Policy Management main window, choose **Policy** and then **Manage Judgment Policy**.  
The Manage Judgment Policy dialog box appears.
2. In the policy list in the Manage Judgment Policy dialog box, click the **Copy** button.

The Copy Judgment Policy dialog box appears.



Figure 6-8: Copy Judgment Policy dialog box



3. Select one judgment policy from the **Copy source** list and one from **Copy destination** list, and then click the **Copy>>** button.

A message box asks if you are sure you want to copy the policy.

4. Click the **OK** button in the message box.

The contents of the judgment policy you selected in the **Copy source** list are copied to the judgment policy you selected in the **Copy destination** list.

*Note:*

You cannot specify the initial policy as the copy destination.

*Reference note:*

If you have modified the default policy and want to reset it to the defaults, select the initial policy as the copy source.

## 6.3 Editing a security update judgment policy

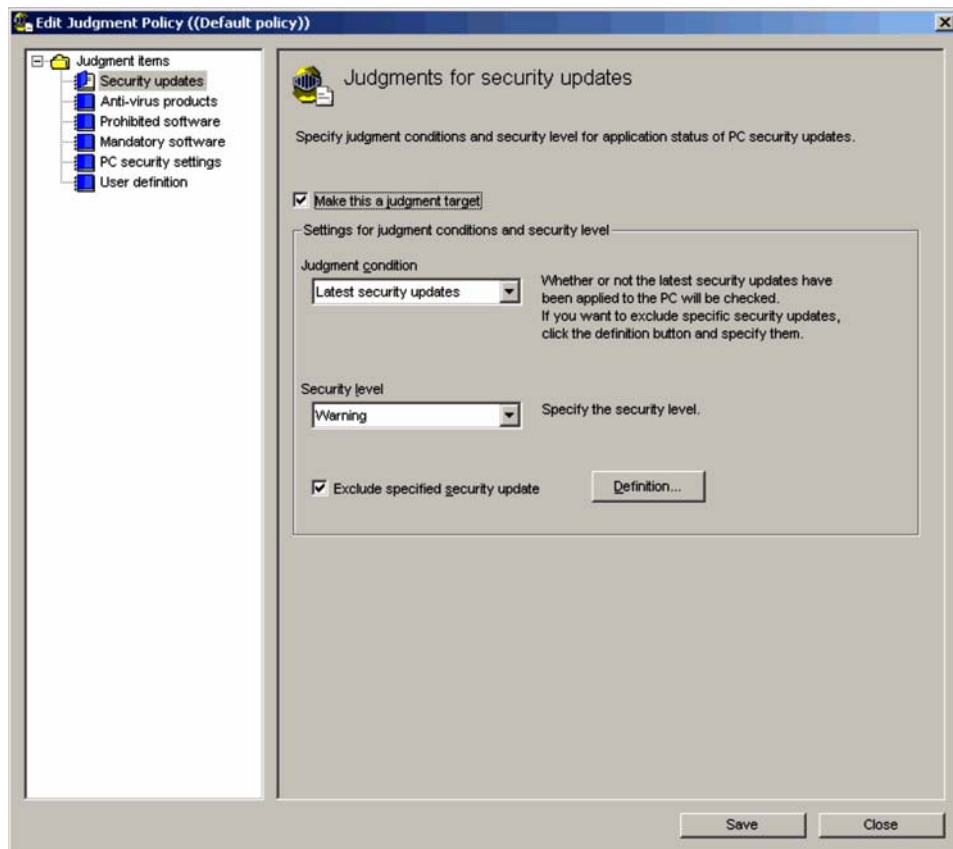
In the Edit Judgment Policy (Judgments for security updates) window, set information about the patches and service packs that must be applied to clients, as well as the client security level when the patches and service packs are not applied.

Note that judgments for security updates require the client to have JP1/Software Distribution Client 07-50 or later installed.

To display the Edit Judgment Policy (Judgments for security updates) window, select **Security updates** from the judgment items tree view in the Edit Judgment Policy window.

The following figure shows the Edit Judgment Policy (Judgments for security updates) window.

Figure 6-9: Edit Judgment Policy (Judgments for security updates) window



The items to be set in the Edit Judgment Policy (Judgments for security updates) window are as follows:

#### **Make this a judgment target**

Select the check box to make the security update a judgment policy target. If the check box is selected, the window items are activated. This is cleared by default.

#### **Judgment condition**

Select the judgment condition from the pull-down menu. The items that can be selected are as follows:

- **Latest security updates**

Select this condition to determine whether the latest security updates from Microsoft have been applied to the client, using MBSA or WUA.

#### **Security level**

Select a security level from the pull-down menu. The items that can be selected are as follows:

Danger

Warning

Caution

#### **Exclude specified security update**

Select this check box to exclude specific security updates from judgment. This is cleared by default. Click the **Definition** button to display the Definition of Excluded Security Updates dialog box, and set the security update to be excluded.

- **Specify security updates**

Select this to judge whether security updates specified by the administrator are applied to the client.

#### **Definition of mandatory security updates**

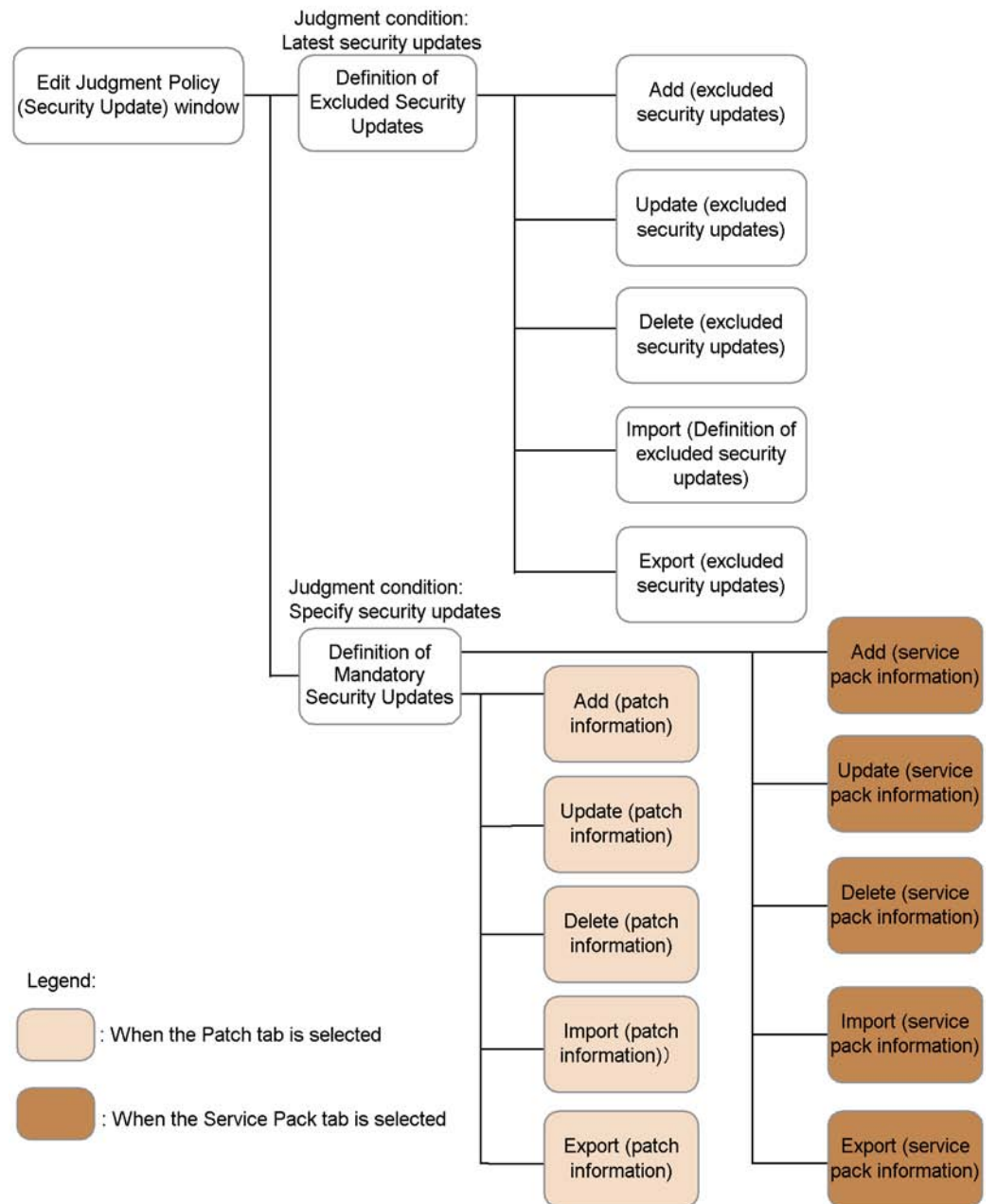
Click the **Definition** button to display the Definition of Mandatory Security Updates box and set the security updates that must be applied to clients.

*Reference note:*

When you select **Latest security updates** as the judgment condition, MBSA or WUA looks for security updates that have not been applied to the client. If any security updates are found to be missing, the specified security level is judged for the client. If not all security updates need to be applied, certain security updates can be excluded.

The following figure shows the window transitions for the Edit Judgment Policy (Judgments for security updates) window.

Figure 6-10: Window transitions for the Edit Judgment Policy (Judgments for security updates) window



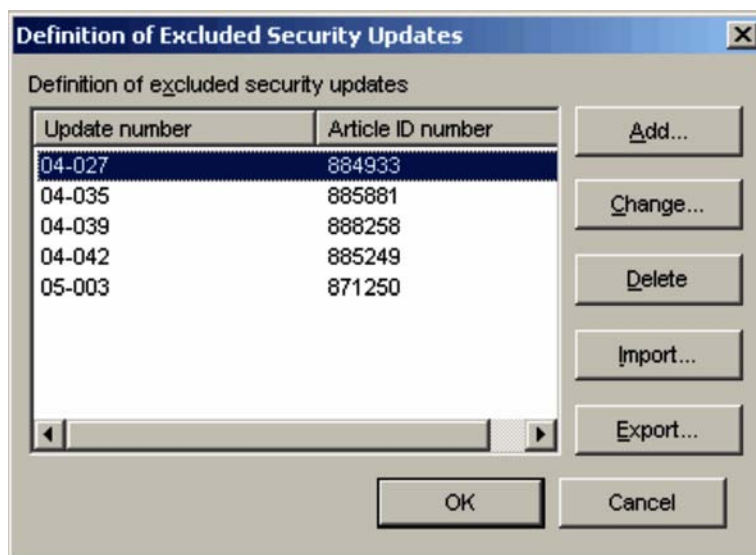
The following explains procedures for when **Judgment condition** is set to **Latest**

**security updates**, and for when it is set to **Specify security updates**.

### 6.3.1 Performing judgment by the latest security updates

To perform judgment when **Latest security updates** is selected for **Judgment condition**:

1. Select the **Make this a judgment target** check box.  
The items in the Edit Judgment Policy (Judgments for security updates) window are activated.
2. For **Judgment condition**, select **Latest security updates**.  
Select **Latest security updates** from the **Judgment condition** pull-down menu.
3. For **Security level**, select the security level to be set.  
Select **Danger**, **Warning**, or **Caution** from the **Security level** pull-down menu.  
Skip to step 8 if not excluding a specific security update from security level judgment.
4. To exclude a specific security update from security level judgment, select the **Exclude specified security update** check box.  
The **Definition** button is activated.
5. Click the **Definition** button.  
The Definition of Excluded Security Updates dialog box is displayed.



6. In the Definition of Excluded Security Updates dialog box, define the security

update to be excluded from judgment.

You can add, change, and delete information about the security updates to be excluded from judgment. You can also import and export security update information as a CSV file. Click the corresponding button to edit the information in the displayed dialog box.

7. In the Definition of Excluded Security Updates dialog box, click **OK**.

The Edit Judgment Policy (Judgments for security updates) window is displayed again.

8. In the Edit Judgment Policy (Judgments for security updates) window, click the **Save** button.

The set contents are saved as a judgment policy.

The following table lists the names of the dialog boxes and message boxes displayed when the corresponding buttons are clicked in the Definition of Excluded Security Updates dialog box.

*Table 6-3:* Names of the dialog boxes and message boxes displayed from the Definition of Excluded Security Updates dialog box

No.	Button	Dialog box name or message box name
1	<b>Add</b>	Add (excluded security updates) dialog box
2	<b>Change</b>	Update (excluded security updates) dialog box
3	<b>Delete</b>	Delete (excluded security updates) message box
4	<b>Import</b>	Import (excluded security updates) dialog box
5	<b>Export</b>	Export (excluded security updates) dialog box

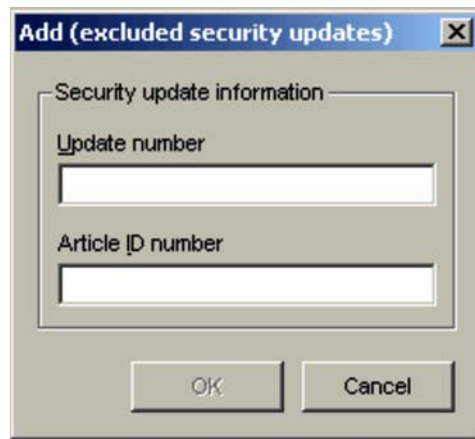
The following explains the procedures for adding, changing, deleting, importing, and exporting information.

#### **(1) Adding information about an excluded security update**

To add information about an excluded security update:

1. In the Definition of Excluded Security Updates dialog box, click the **Add** button.

The Add (excluded security updates) dialog box is displayed.



2. Enter the update number and article ID number.

Enter both the update number and article ID number to be excluded from judgment.

**Update number**

Check the Web page for Microsoft security information, and enter the update number to be added. Make sure that you do not enter the prefix MS.

**Article ID number**

Check the Web page for Microsoft security information, and enter the article ID number to be added. Make sure that you do not enter the prefix, such as KB or Q.

*Note:*

Enter the update number and article ID number as published by Microsoft. If the security update you specify in a judgment policy does not have an update number, enter the article ID number of the security update in the text box used for the update number.

3. Click the **OK** button.

The Add (excluded security updates) dialog box is closed, and the Definition of Excluded Security Updates dialog box is displayed again. The entered information about an excluded security update is added.

**(2) Changing information about an excluded security update**

To change security update information:



1. In the Definition of Excluded Security Updates dialog box, select the security update you wish to change, and click the **Change** button. Alternatively, double-click the security update you wish to change.

The Update (excluded security updates) dialog box is displayed.

Note that the **Change** button is disabled if you select multiple security updates.



2. Check and change the update number and article ID number.

The update number and article ID number for the security update information to be changed are displayed, so check and change them as necessary.

#### **Update number**

Check the Web page for Microsoft security information, and enter the update number to be changed. Make sure that you do not enter the prefix MS.

#### **Article ID number**

Find the new article ID number on the Microsoft Web page that provides the security information, and enter the new article ID number. Make sure that you do not enter the prefix, such as KB or Q.

#### *Note:*

Enter the update number and article ID number as published by Microsoft. If the security update you specify in a judgment policy does not have an update number, enter the article ID number of the security update in the text box used for the update number.

3. Click the **OK** button.

The Update (excluded security updates) dialog box is closed, and the Definition of Excluded Security Updates dialog box is displayed again. The information

about the excluded security update is changed to the entered contents.

### (3) **Deleting information about excluded security update**

To delete security update information:

1. In the Definition of Excluded Security Updates dialog box, click to select the security update you wish to delete.

You can select multiple security updates.

2. Click the **Delete** button.

The Delete (excluded security updates) message box appears.



3. Check the message, and click the **OK** button.

The Delete (excluded security updates) message box is closed, and the Definition of Excluded Security Updates dialog box is displayed again. The selected security update information is deleted.

### (4) **Importing information about an excluded security update**

For a large number of excluded security updates, an administrator can create a definition file of excluded security updates in CSV format, and import the file.

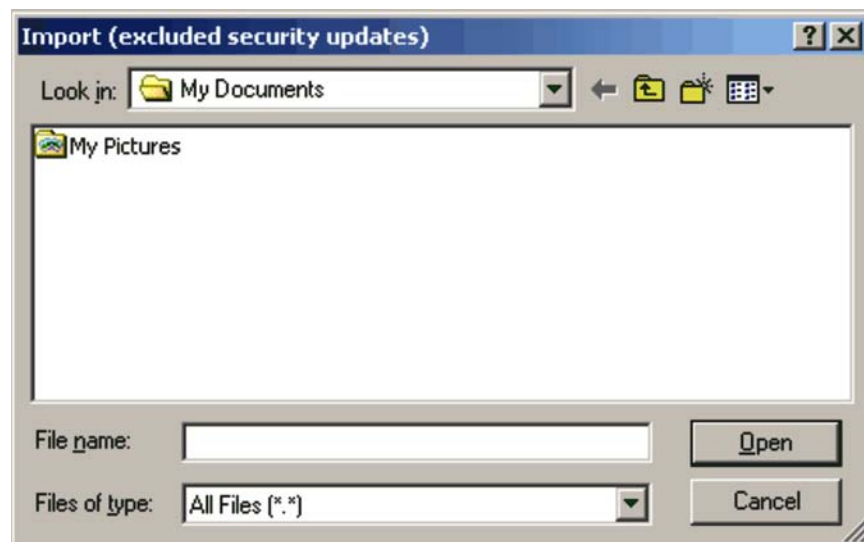
The client security control system provides a sample of a definition file of excluded security updates. The administrator can customize the sample file to create a definition file based on the security objectives and then import it. For details about the sample of this definition file, see *A.4(1) Sample of a definition file for excluded security updates*.

For details about the format of the definition file of excluded security updates, see *16.2.3 Definition file of excluded security updates*.

To import information about excluded security updates:

1. In the Definition of Excluded Security Updates dialog box, click the **Import** button.

The Import (excluded security updates) dialog box is displayed.



2. Specify **Look in**.

Specify the location of the definition file of excluded security updates to be imported.

3. Specify the name of the definition file of excluded security updates, and then click the **Open** button.

The specified file is read, and the Definition of Excluded Security Updates dialog box is displayed again.

If the specified file does not contain information for the excluded security updates (the file is empty), an error message appears and the import is canceled.

### **(5) Exporting information about an excluded security update**

Information about excluded security updates can be exported to a CSV file.

To export excluded security updates:

1. In the Definition of Excluded Security Updates dialog box, click the **Export** button.

The Export (excluded security updates) dialog box is displayed.

Note that the **Export** button is disabled when no definition has been registered in the Export (excluded security updates) dialog box.



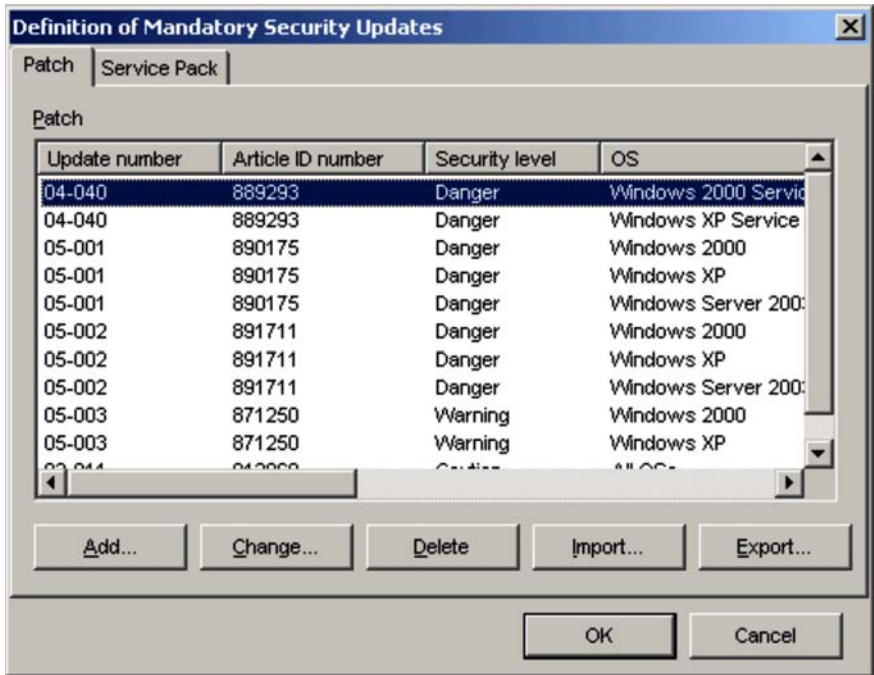
2. Specify **Save in**.  
Specify the location in which to save the exported file.
3. Specify the name of the CSV file to be exported for the file name, and click the **Save** button.  
The specified file is saved, and the Definition of Excluded Security Updates dialog box is displayed again.

### 6.3.2 Performing judgment by a specified security update

This subsection explains all of the procedures for performing judgment when **Specify security updates** is specified for **Judgment condition**. Note that you can use the tabs to specify a patch or service pack, when a security update is specified.

To specify a security update:

1. Select the **Make this a judgment target** check box.  
The items in the Edit Judgment Policy (Judgments for security updates) window are activated.
2. Select **Specify security updates** from **Judgment condition**.  
Select **Specify security updates** from the **Judgment condition** pull-down menu.
3. Click the **Definition** button.  
The Definition of Mandatory Security Updates dialog box is displayed.



- In the Definition of Mandatory Security Updates dialog box, define the patch or service pack.

In the Definition of Mandatory Security Updates dialog box, there are two tabs: the **Patch** tab and the **Service Pack** tab. Select one to define information.

- In the Definition of Mandatory Security Updates dialog box, click the **OK** button.

The Edit Judgment Policy (Judgments for security updates) window is displayed again.

- In the Edit Judgment Policy (Judgments for security updates) window, click the **Save** button.

The set contents are saved as a judgment policy.

The following table lists the names of the dialog boxes and message boxes displayed when the corresponding buttons are clicked in the Definition of Mandatory Security Updates dialog box.

*Table 6-4:* Names of the dialog boxes and message boxes displayed from the Definition of Mandatory Security Updates dialog box

No.	Tab name	Button	Dialog box name or message box name
1	<b>Patch</b>	<b>Add</b>	Add (patch information) dialog box
2		<b>Change</b>	Update (patch information) dialog box
3		<b>Delete</b>	Delete (patch information) message box
4		<b>Import</b>	Import (patch information) dialog box
5		<b>Export</b>	Export (patch information) dialog box
6	<b>Service Pack</b>	<b>Add</b>	Add (service pack information) dialog box
7		<b>Change</b>	Update (service pack information) dialog box
8		<b>Delete</b>	Delete (service pack information) message box
9		<b>Import</b>	Import (service pack information) dialog box
10		<b>Export</b>	Export (service pack information) dialog box

The following explains the edit operations for each page.

### **(1) Defining patch information**

To define patch information:

1. In the Definition of Mandatory Security Updates dialog box, select the **Patch** tab.
2. In the **Patch** page, define patch information.

You can add, change, and delete information about patches that must be applied to the client, in the **Patch** page. You can also import or export patch information as a CSV file.

Edit the information in the dialog boxes displayed by clicking the corresponding buttons.

3. When editing operations are complete, in the Definition of Mandatory Security Updates dialog box, click the **OK** button.

The Definition of Mandatory Security Updates dialog box closes, and the Edit Judgment Policy (Judgments for security updates) window is displayed again.

*Reference note:*

When JP1/Client Security Control - Manager is upgraded from version 08-00 or earlier, the update number, article ID number, security level, and OS settings are also inherited without change. Note, however, that the comparison condition becomes blank.

*Reference note:*

You can specify **Unknown**, **Security level set for the judgment policy**, and **Safe** for the judgment result that is used when one of the following conditions is satisfied:

- Patch information is defined with **Specify security updates** specified for **Judgment condition** in the Edit Judgment Policy (Judgments for security updates) window.
- The patch information specified in **Installed software information** is not found.
- The client is linked to MBSA or WUA.
- The specified patch information is not found in the security update information that has not been applied to the client (unapplied patch information).

You can set the judgment result in **Customize judgment results (security updates)** on the **Basic Settings** page of the Client Security Control - Manager Setup dialog box. For details about setting the judgment result, see 5.4.3 *Setting up JP1/CSC - Manager*.

The following explains how to add, change, delete, import, and export patch information.

**(a) Adding patch information**

To add patch information:

1. In the Definition of Mandatory Security Updates dialog box, click the **Add** button.

The Add (patch information) dialog box is displayed.

**Add (patch information)**

Patch information

Update number: 05-003

Article ID number: 871250

Object

OS: Windows Server 2003, Enterprise Edition

OS service pack: No specification

Product name: No specification

Comparison condition: Match all the words

Product version:

Product service pack: No specification

Security level: Warning

Set the patch information and add it to the patch list by clicking the Add button.

Add

Patch

Update number	Article ID number	Security level	OS
05-003	871250	Warning	Windows Server 2003, Er

OK Cancel

2. Enter the update number and article ID number.

Enter both the update number and article ID number for the patch information to be added.



**Update number**

Check the Web page for Microsoft security information, and enter the update number to be added. Make sure that you do not enter the prefix **MS**.

**Article ID number**

Check the Web page for Microsoft security information, and enter the article ID number to be added. Make sure that you do not enter the prefix, such as **KB** or **Q**.

*Note:*

Enter the update number and article ID number as published by Microsoft. If the security update you specify in a judgment policy does not have an update number, enter the article ID number of the security update in the text box used for the update number.

3. Enter the information in **Object**.

Enter information about the target OS and target product for the patch information to be added. The following table lists the target setting items.

*Table 6-5: Target setting items (when adding information)*

No.	Window item name	Description	Default
1	<b>OS</b>	Select an OS from the pull-down menu.	<b>All OSs</b>
2	<b>OS service pack</b>	Select an OS service pack from the pull-down menu. <ul style="list-style-type: none"> <li>• <b>No specification</b> It is determined that no service packs have been applied.</li> <li>• <b>All</b> All service packs are judged no matter whether a service pack is applied.</li> </ul> This item cannot be selected when <b>All OSs</b> is specified for <b>OS</b> in No. 1.	<b>No specification</b>
3	<b>Product name<sup>#</sup></b>	Select a product name from the combo box or enter a character string. <ul style="list-style-type: none"> <li>• When selecting from the combo box: Select a product name from the combo box. You can select <b>No specification</b>, <b>Microsoft Internet Explorer</b>, or a product name registered in the product name definition file.</li> <li>• When entering a product name: Use a character string of no more than 255 bytes to specify a product name.</li> </ul>	<b>No specification</b>

No.	Window item name	Description	Default
4	<b>Comparison condition</b>	If a product name other than <b>No specification</b> or <b>Microsoft Internet Explorer</b> is selected for <b>Product name</b> , select a comparison condition from the pull-down menu. You can select <b>Match all the words</b> or <b>Match the beginning of the words</b> .	<b>Match all the words</b>
5	<b>Product version</b>	Enter the product version number. Versions are judged by forward matching.	<b>None</b> (No default is provided.)
6	<b>Product service pack</b>	If <b>Microsoft Internet Explorer</b> is selected for <b>Product name</b> , select the product service pack from the pull-down menu. This item is disabled when a product name other than <b>Microsoft Internet Explorer</b> is selected.	<b>No specification</b>

#

- When defining IE patch information, be sure to select **Microsoft Internet Explorer** for **Product name**.
  - When you enter a product name, specify a software name registered as asset information in AIM.
  - The combo box of product names contains the product names that have been registered in the product name definition file by the administrator. However, if a product name is entered in step 3, that product name is automatically registered in the product name definition file and will be added to the combo box of product names next time it is displayed. If the product name definition file does not exist, the file is created automatically. For details about the product name definition file, see *16.4 Product name definition file*.
4. Select the security level.  
Select a security level from the pull-down menu. The default is **Warning**.
  5. Click the **Add** button.  
The set information is added to the patch list in the Add (patch information) dialog box. If there are multiple target OSs and target products for the patch information to be added, add them as necessary.
  6. Click the **OK** button.  
The Add (patch information) dialog box closes, and the Definition of Mandatory Security Updates dialog box is displayed again. The entered patch information is added.

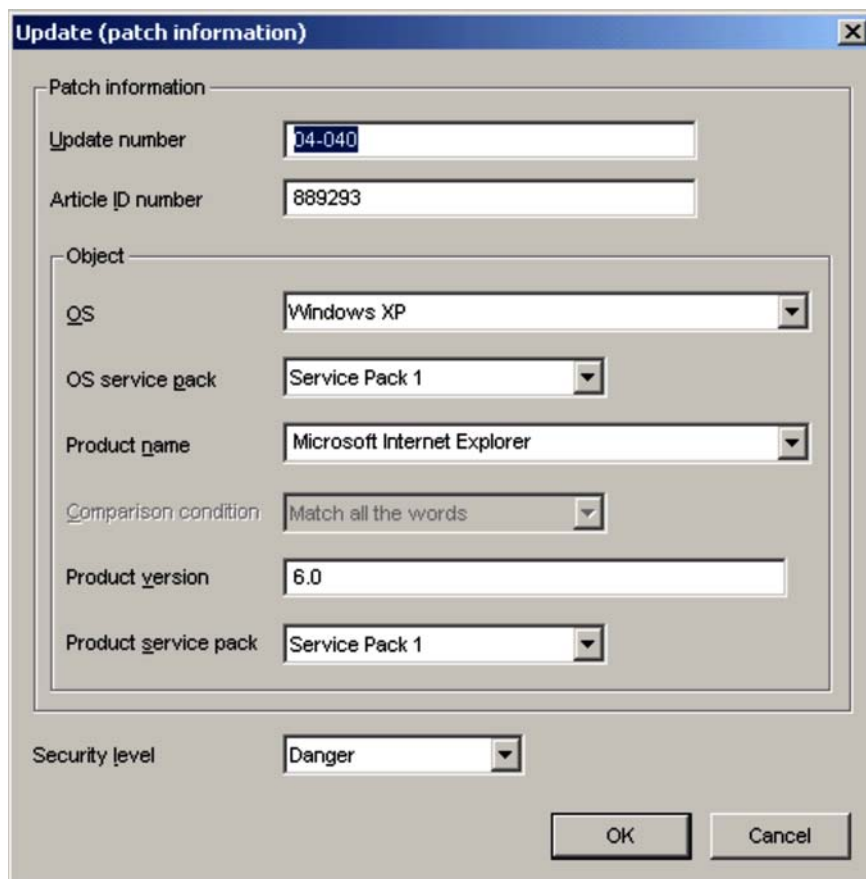
**(b) Changing patch information**

To change patch information:

1. In the Definition of Mandatory Security Updates dialog box, select the patch information to be changed, and click the **Change** button. Alternatively, double-click the patch information you want to change.

The Update (patch information) dialog box is displayed.

Note that the **Change** button is disabled if you select multiple patches.



The image shows a Windows-style dialog box titled "Update (patch information)". It contains several input fields and dropdown menus. The "Patch information" section has "Update number" (04-040) and "Article ID number" (889293). The "Object" section has "OS" (Windows XP), "OS service pack" (Service Pack 1), "Product name" (Microsoft Internet Explorer), "Comparison condition" (Match all the words), "Product version" (6.0), and "Product service pack" (Service Pack 1). The "Security level" is set to "Danger". At the bottom right are "OK" and "Cancel" buttons.

Field	Value
Update number	04-040
Article ID number	889293
OS	Windows XP
OS service pack	Service Pack 1
Product name	Microsoft Internet Explorer
Comparison condition	Match all the words
Product version	6.0
Product service pack	Service Pack 1
Security level	Danger

2. Check or change the update number and article ID number.

Check the update number and article ID number displayed for the patch information to be changed. Enter both the update number and article ID number to change the patch information.

**Update number**

Enter the update number to be updated. Make sure that you do not enter the prefix MS.

**Article ID number**

Enter the article ID number to be updated. Make sure that you do not enter the prefix, such as KB or Q.

*Note:*

Enter the update number and article ID number as published by Microsoft. If the security update you specify in a judgment policy does not have an update number, enter the article ID number of the security update in the text box used for the update number.

3. Enter the information in **Object**.

4. Select the security level.

Select a security level from the pull-down menu.

5. Click the **OK** button.

The Update (patch information) dialog box closes, and the Definition of Mandatory Security Updates dialog box is displayed again. The patch information is updated to reflect the entered contents.

**(c) Deleting patch information**

To delete patch information in the Definition of Mandatory Security Updates dialog box:

1. In the Definition of Mandatory Security Updates dialog box, click to select the patch information you want to delete.
2. Click the **Delete** button.

The Delete (patch information) message box is displayed.



3. Check the message, and click the **OK** button.

The Delete (patch information) message box closes, and the Definition of

Mandatory Security Updates dialog box is displayed again. The selected patch information is deleted.

#### (d) Importing patch information

For a significant amount of patch information, an administrator can create a definition file for mandatory security updates in CSV format, and import the file.

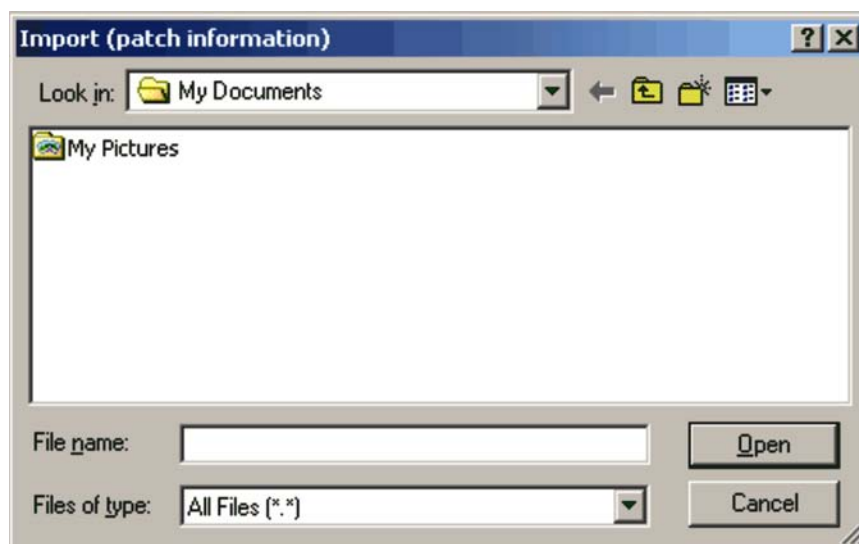
The client security control system provides a sample of a definition file for mandatory security updates. The administrator can customize the sample file to create a definition file based on the security objectives and then import it. For details about the sample of this definition file, see *A.4(2) Sample of a definition file for mandatory security updates*.

For details about the format of the definition file for mandatory security updates, see *16.2.4 Definition file for mandatory security updates*.

To import patch information:

1. In the Definition of Mandatory Security Updates dialog box, click the **Import** button.

The Import (patch information) dialog box is displayed.



2. Specify **Look in**.  
Specify the location of the definition file for mandatory security updates to be imported.
3. Specify the name of the definition file for mandatory security updates, and then click the **Open** button.

The specified file is read, and the Definition of Mandatory Security Updates dialog box is displayed again.

If the specified file does not contain information for the mandatory security updates (the file is empty), an error message appears and the import is canceled.

### (e) Exporting patch information

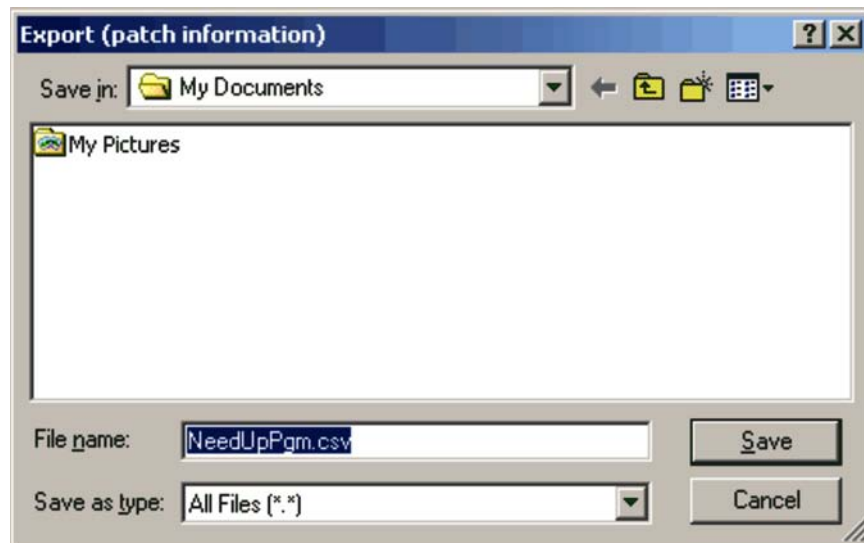
Patch information can be exported to a CSV file.

To export patch information:

1. In the Definition of Mandatory Security Updates dialog box, click the **Export** button.

The Export (patch information) dialog box is displayed.

Note that the **Export** button is disabled when no definition has been registered in the Definition of Mandatory Security Updates dialog box.



2. Specify **Save in**.
3. Specify the name of the CSV file to be exported for the file name, and click the **Save** button.

The specified file is saved, and the Definition of Mandatory Security Updates dialog box is displayed again.

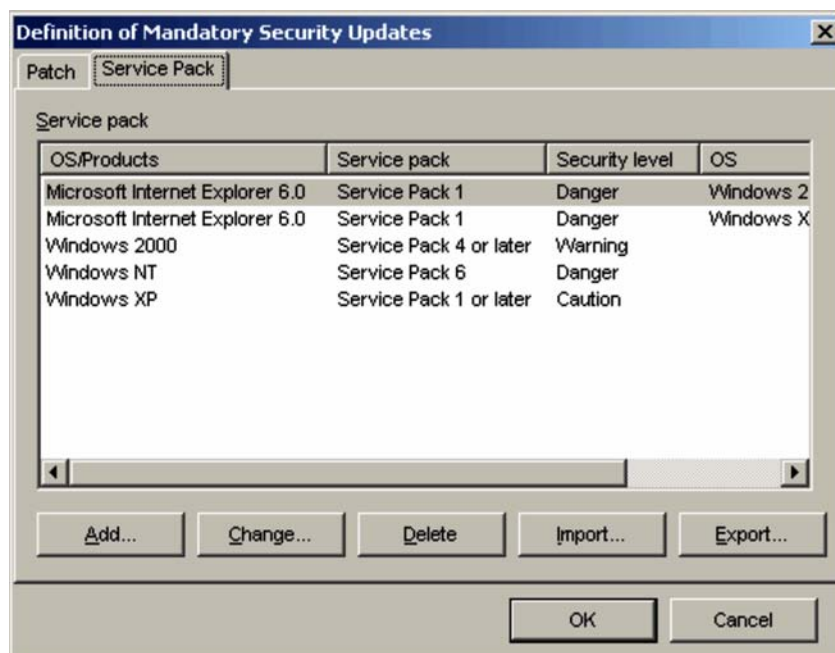
### (2) Defining service pack information

For details about the OSs and products that can be defined in the **Service Pack** tab, see

### 16.2.2 List of setting values.

To define service pack information:

1. In the Definition of Mandatory Security Updates dialog box, select the **Service Pack** tab.



2. In the **Service Pack** page, define the service pack.

You can add, change, and delete information about service packs that must be applied to the client, in the **Service Pack** page. You can also import or export service pack information as a CSV file.

Edit the information in the dialog boxes displayed by clicking the corresponding buttons.

3. When editing operations are complete, in the Definition of Mandatory Security Updates dialog box, click the **OK** button.

The Definition of Mandatory Security Updates dialog box closes, and the Edit Judgment Policy (Judgments for security updates) window is displayed again.

*Note:*

The OS and product name you define in the service pack information must be names registered as asset information in AIM.

The following explains how to add, change, delete, import, and export service pack information.

**(a) Adding service pack information**

To add service pack information:

1. In the Definition of Mandatory Security Updates dialog box, click the **Add** button.

The Add (service pack information) dialog box is displayed.

The screenshot shows the 'Add (service pack information)' dialog box. It has a title bar with a close button. The main area contains two radio buttons: 'OS' (selected) and 'Product'. Below this is a section for 'OS service pack' with a dropdown menu showing 'Windows NT Workstation'. Below that is a 'Service pack' dropdown showing 'Service Pack 1', a 'Match' dropdown, and a '(E)' label. At the bottom is a 'Security level' dropdown showing 'Warning'. There are 'OK' and 'Cancel' buttons at the bottom right.

2. Use the radio buttons to select either **OS** or **Product**.  
Select either an OS service pack or a product service pack.



3. Enter information for either **OS service pack** or **Product service pack**.

The set information differs between OSs and products. The following table describes the setting items.

*Table 6-6: Setting Items for the Add (service pack information) dialog box*

No.	OS or product	Window item name		Description	Default
1	OS	<b>OS</b>		Select an OS from the pull-down menu.	<b>Windows NT Workstation</b>
2		<b>Service pack</b>		Select an OS service pack from the pull-down menu.	<b>Service Pack 1</b>
3				Select <b>Match</b> or <b>or later</b> from the pull-down menu.	<b>Match</b>
4	Product	<b>Product name</b>		Select a product name from the pull-down menu.	<b>Microsoft Internet Explorer</b>
5		<b>Product version</b>		Enter the product version.	None (No default is provided.)
6		<b>Service pack</b>		Select the product service pack from the pull-down menu.	<b>Service Pack 1</b>
7				Select <b>Match</b> or <b>or later</b> from the pull-down menu.	<b>Match</b>
8		<b>OS specification<sup>#</sup></b>	<b>OS</b>	Select an OS from the pull-down menu.	<b>All OSs</b>
9			<b>Service pack</b>	Select an OS service pack from the pull-down menu. <ul style="list-style-type: none"> <li>• <b>No specification</b> It is determined that no service packs have been applied.</li> <li>• <b>All</b> All service packs are judged no matter whether a service pack is applied.</li> </ul>	<b>No specification</b>

<sup>#</sup>

Specify the prerequisite OS and service pack for the product.

## 4. Specify the security level.

Select a security level from the pull-down menu. The default is **Warning**.

5. Click the **OK** button.

The Add (service pack information) dialog box closes, and the Definition of Mandatory Security Updates dialog box is displayed again. The entered service pack information is added.

#### (b) Changing service pack information

To change service pack information:

1. In the Definition of Mandatory Security Updates dialog box, click to select the service pack information you want to change, and then click the **Change** button. Alternatively, double-click the service pack information you want to change.

The Update (service pack information) dialog box is displayed.

Note that the **Change** button is disabled if you select more than one item of service pack information.

The screenshot shows the 'Update (service pack information)' dialog box. It has a title bar with a close button. The main area is divided into three sections. The first section, 'Target of service pack', has two radio buttons: 'OS' (which is selected) and 'Product'. The second section, 'OS service pack', has three dropdown menus: 'OS' (showing 'Windows XP'), 'Service pack' (showing 'Service Pack 1'), and 'Or later' (showing '(E)'). The third section, 'Security level', has a dropdown menu showing 'Caution'. At the bottom right of the dialog are two buttons: 'OK' and 'Cancel'.

2. Use the radio buttons to select either **OS** or **Product**.

Select either an OS service pack or a product service pack.

3. Change the information for either **OS service pack** or **Product service pack**.
4. Change the security level.

Select from the pull-down menu to change the security level.

5. Click the **OK** button.

The Update (service pack information) dialog box closes, and the Definition of Mandatory Security Updates dialog box is displayed again. The service pack information is changed to reflect the entered contents

### (c) Deleting service pack information

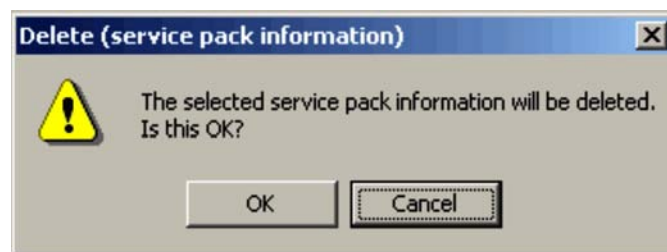
To delete service pack information:

1. In the Definition of Mandatory Security Updates dialog box, click to select the service pack information you want to delete.

You can select more than one item of service pack information.

2. Click the **Delete** button.

The Delete (service pack information) message box is displayed.



3. Check the message, and click the **OK** button.

The Delete (service pack information) message box closes, and the Definition of Mandatory Security Updates dialog box is displayed again. The selected service pack information is deleted.

### (d) Importing service pack information

For a significant amount of service pack information, an administrator can create a definition file for mandatory service packs in CSV format, and import the file.

The client security control system provides a sample of a definition file for mandatory service packs. The administrator can customize the sample file to create a definition file based on the security objectives and then import it. For details about the sample of this definition file, see *A.4(3) Sample of a definition file for mandatory service packs*.

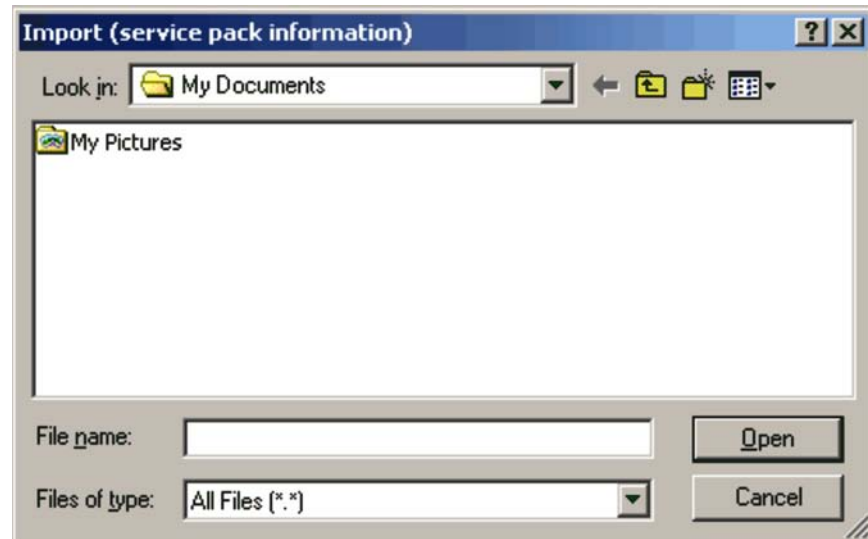
For details about the format of the definition file for mandatory service packs, see

### 16.2.5 Definition file for mandatory service packs.

To import service pack information:

1. In the Definition of Mandatory Security Updates dialog box, click the **Import** button.

The Import (service pack information) dialog box is displayed.



2. Specify **Look in**.

Specify the location of the definition file for mandatory service packs to be imported.

3. Specify the name of the definition file for mandatory service packs, and then click the **Open** button.

The specified file is read, and the Definition of Mandatory Security Updates dialog box is displayed again.

If the specified file does not contain information for the mandatory service packs (the file is empty), an error message appears and the import is canceled.

#### (e) Exporting service pack information

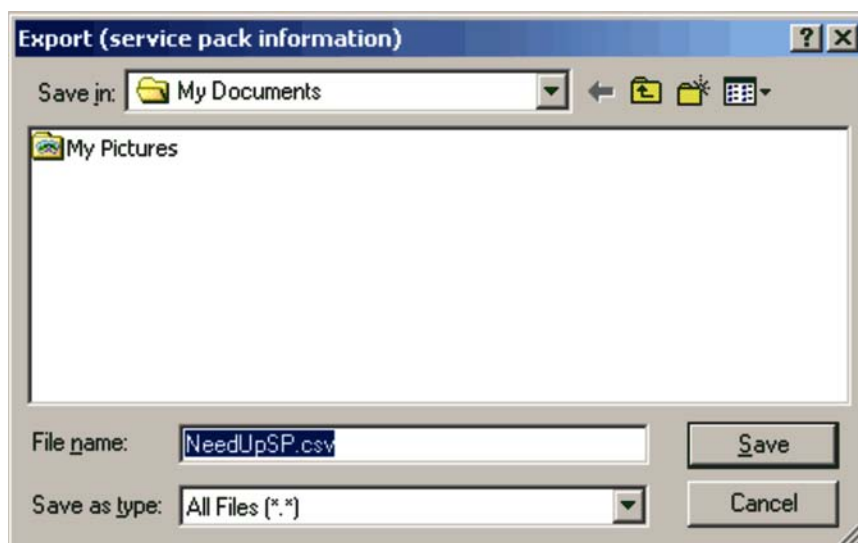
Service pack information can be exported to a CSV file. In the Definition of Mandatory Security Updates dialog box, click the **Export** button to display the Export (service pack information) dialog box. Use this dialog box to output service pack information in CSV format.

To export service pack information:

1. In the Definition of Mandatory Security Updates dialog box, click the **Export** button.

The Export (service pack information) dialog box is displayed.

Note that the **Export** button is disabled when no definition has been registered in the Definition of Mandatory Security Updates dialog box.



2. Specify **Save in**.  
Specify the location in which to save the exported file.
3. Specify the name of the CSV file to be exported for the file name, and click the **Save** button.

The specified file is saved, and the Definition of Mandatory Security Updates dialog box is displayed again.

### 6.3.3 Automatically updating judgment policies for security updates

This subsection describes the procedures for updating the judgment policies relating to security updates without using the Edit Judgment Policy (Judgments for security updates) window.

By running the judgment policy update command for security updates (`cscpatchupdate`), you can automatically update patch information for judgment policies relating to security updates by using the patch information files collected by Job Management Partner 1/Software Distribution.

For details about the judgment policy update command for security updates (`cscpatchupdate`), see *cscpatchupdate (updates patch information for judgment*

*policies relating to security updates) in 15. Commands.*

**(1) Types of patch included in automatic update**

The judgment policy update command for security updates can update patch information for the programs listed in the table below. Note that automatic update of patch information applies to the OSs or service packs supported by Microsoft.

*Table 6-7: Programs for which automatic update of patches is supported*

Program	Type or version
Windows	Windows 7
	Windows Server 2008
	Windows Vista
	Windows Server 2003
	Windows XP
	Windows 2000
Microsoft Internet Explorer	6.0, 7.0, 8.0, 9.0

Of the patches provided for these programs, automatic update applies to the following classes of patch:

- Critical updates
- Security updates
- Security rollups

*Note:*

The result of security level judgment may be **Unknown** if patch information meets any of the conditions listed below. If this occurs, review the relevant patch information from the Edit Judgment Policy (Judgments for security updates) window.

- The patch information is specific to a 32 bit (x86) or 64 bit (x64) version of Windows (for example Windows Server 2003 (x64)).
- The patch information is specific to a particular edition of the operating system (for example Windows Server 2003, Enterprise Edition).
- The patch information has already been applied by way of a cumulative security update or other means.
- The patch information depends on the status of a particular Windows service or component.

## ***(2) Using Scheduled Tasks to automatically update judgment policies for security updates***

To periodically update the judgment policy for security updates, we recommend that you register the judgment policy update command for security updates in Windows Scheduled Tasks.

To automatically update judgment policies for security updates using Windows Scheduled Tasks:

1. In JP1/Software Distribution Manager, configure the network for acquiring patch information files.

For information about setting up JP1/Software Distribution Manager to acquire patch information files, see 5.2.2(6) *Setting up for acquiring patch information files* and the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows Systems.

2. Create a patch update condition file as required.

Use the judgment policy update command for security updates (`cscpatchupdate`) to create a patch update condition file containing updated patch information.

For details about patch update condition files, see 16.11 *Patch update condition file*.

3. Define the judgment policy update command for security updates as a task in Scheduled Tasks.

Set up periodic execution of the judgment policy update command for security updates (`cscpatchupdate`) by defining it as a task in Windows Scheduled Tasks. For details about how to register commands in Scheduled Tasks, see 5.9

*Procedures for setting a task in Scheduled Tasks.*

4. Acquire the latest patch information file.

Using JP1/Software Distribution, acquire the latest patch information file. You must do so before executing the judgment policy update command for security updates (`cscpatchupdate`).

For details about how to acquire patch information files, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows Systems.

5. Execute the judgment policy update command for security updates as a scheduled task.

The judgment policy for security updates is updated based on the contents of the patch information file and the patch update condition file. You can then use the Policy Management window of JP1/Client Security Control - Manager to check whether the judgment policy has been updated.



---

## 6.4 Editing an anti-virus product judgment policy

---

The Edit Judgment Policy (Judgments for anti-virus products) window can be used to set up all anti-virus products installed on a client. Set the engine version, definition file, and resident status of the anti-virus product, as well as the client security level when they are not applied. Also, be sure to delete any unused anti-virus products set up during installation.

*Reference note:*

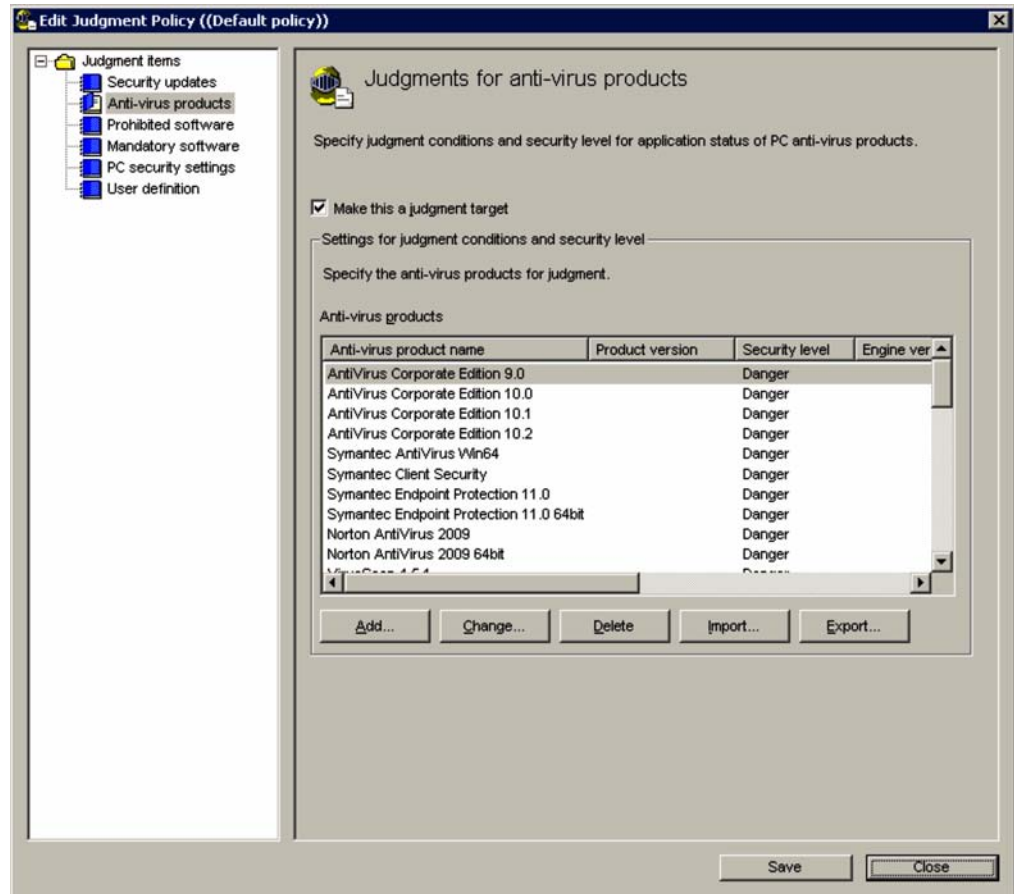
Updating anti-virus product judgment policies manually or automatically

Judgment policies relating to anti-virus products can be updated automatically, or manually by the administrator at any time, without using the Edit Judgment Policy (Judgments for anti-virus products) window. For details about the procedures for updating an anti-virus product judgment policy manually or automatically, see *6.4.6 Updating judgment policies for anti-virus products automatically or manually*.

To display the Edit Judgment Policy (Judgments for anti-virus products) window, from the judgment items tree view in the Edit Judgment Policy window, select **Anti-virus products**.

The following figure shows the window.

Figure 6-11: The Edit Judgment Policy (Judgments for anti-virus products) window



Information about the anti-virus products supported by JP1/Software Distribution can be set in the Edit Judgment Policy (Judgments for anti-virus products) window. For details about the anti-virus products supported by JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Description and Planning Guide*, for Windows systems.

The items set in the Edit Judgment Policy (Judgments for anti-virus products) window are as follows.

#### Make this a judgment target

Select the check box to make the anti-virus product a judgment policy target. If the check box is selected, the window items are activated. This is selected by default.

## Anti-virus products

Set the anti-virus product to be judged.

To edit anti-virus product information:

1. In the Edit Judgment Policy (Judgments for anti-virus products) window, select the **Make this a judgment target** check box.

All items in the Edit Judgment Policy (Judgments for anti-virus products) window are activated.

2. Set the anti-virus product information.

You can add, change, and delete information about the set anti-virus products. You can also import and export anti-virus product information as a CSV file. Click the corresponding button to edit the information in the dialog box displayed.

3. When editing operations are complete, in the Edit Judgment Policy (Judgments for anti-virus products) window, click the **Save** button.

The set contents are saved as a judgment policy.

### Note:

The anti-virus product name, product version, engine version, and virus definition file version that you define in the Edit Judgment Policy (Judgments for anti-virus products) window must be names registered as asset information in AIM.

The following table lists the names of the dialog boxes and message boxes displayed when the corresponding buttons are pressed in the Edit Judgment Policy (Judgments for anti-virus products) window.

*Table 6-8:* Names of the dialog boxes and message boxes displayed from the Edit Judgment Policy (Judgments for anti-virus products) window

No.	Button	Dialog box name or message box name
1	<b>Add</b>	Add (anti-virus product information) dialog box
2	<b>Change</b>	Update (anti-virus product information) dialog box
3	<b>Delete</b>	Delete (anti-virus product information) message box
4	<b>Import</b>	Import (anti-virus product information) dialog box
5	<b>Export</b>	Export (anti-virus product information) dialog box

The following explains the procedures for adding, changing, deleting, importing, and

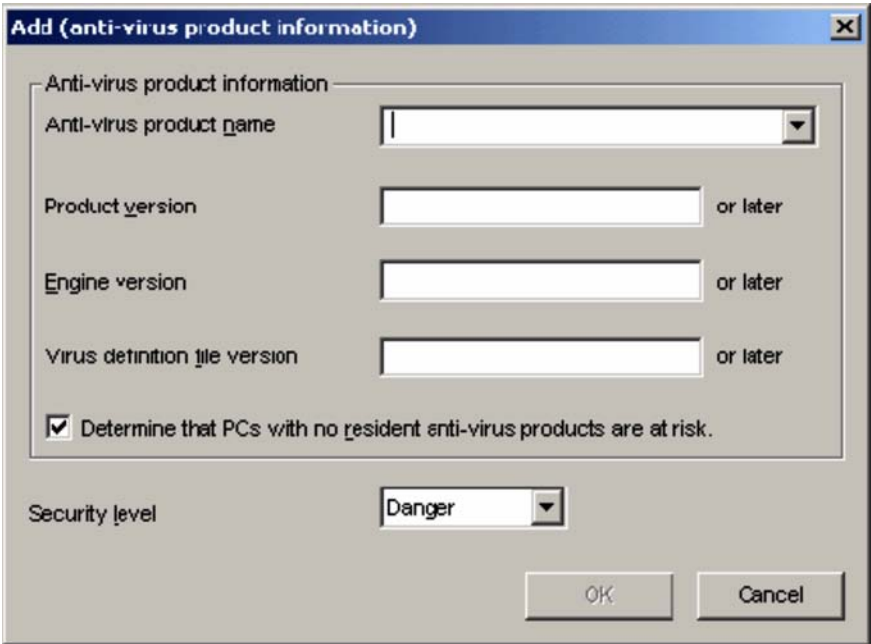
exporting information.

6.4.1 Adding anti-virus product information

To add anti-virus product information:

- 1. In the Edit Judgment Policy (Judgments for anti-virus products) window, click the **Add** button.

The Add (anti-virus product information) dialog box is displayed.



- 2. Enter the anti-virus product information.

Enter the anti-virus product information. The following table describes the setting items.

Table 6-9: Setting items for the Add (anti-virus product information) dialog box

No.	Window item name	Description	Default
1	Anti-virus product name <sup>#</sup>	Select the anti-virus product name from the combo box. Alternatively enter a string in 255 or fewer bytes. This setting is required.	None
2	Product version	Enter the anti-virus product version in 255 or fewer bytes, using alphanumeric characters and symbols.	None

No.	Window item name	Description	Default
3	<b>Engine version</b>	Enter the anti-virus product engine version in 255 or fewer bytes, using alphanumeric characters and symbols.	None
4	<b>Virus definition file version</b>	Enter the virus definition file version of the anti-virus product in 255 or fewer bytes, using alphanumeric characters and symbols.	None
5	<b>Determine that PCs with no resident anti-virus products are at risk.</b>	Specify whether or not security levels are to be judged for clients with no resident anti-virus product.	Selected
6	<b>Security level</b>	Select a security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	<b>Danger</b>

#

The name of the anti-virus product is judged by a complete match.

*Note:*

Use periods ( . ) to separate the groups of digits in the product version, engine version, and virus definition file version. The security level is judged by comparing the size of each value set in the judgment policy with the corresponding value registered as asset information in AIM. Use the following format to specify values set for the judgment policy. The security level may not be judged correctly if the specified value does not conform to the following format.

- Make sure the period-separated format matches the format registered as asset information in AIM.
- Make sure the number of digits in the specified value matches the number of digits in the values registered as asset information in AIM.

For some anti-virus products, some of the following items cannot be acquired:

- Product version
- Engine version
- Virus definition file version
- Whether the product is resident

If you set an item that cannot be acquired for the judgment policy and judgment is performed, the judgment result will be **Unknown**. Do not specify the version of such items for the judgment policy. Instead, specify that whether or not products are resident is not to be judged.

3. Click the **OK** button.

The Add (anti-virus product information) dialog box closes, and the Edit Judgment Policy (Judgments for anti-virus products) window is displayed again. The entered anti-virus product information is added.

## 6.4.2 Changing anti-virus product information

To change anti-virus product information:

1. In the Edit Judgment Policy (Judgments for anti-virus products) window, click the anti-virus product to be changed, and then click **Change** button. Alternatively, double-click the anti-virus product to be changed.

The Update (anti-virus product information) dialog box is displayed.

Note that the **Change** button is disabled if you select multiple anti-virus products.

2. Change the anti-virus product information.
3. Click the **OK** button.

The Update (anti-virus product information) dialog box closes, and the Edit Judgment Policy (Judgments for anti-virus products) window is displayed again. The anti-virus product information is changed to reflect the entered contents.

### 6.4.3 Deleting anti-virus product information

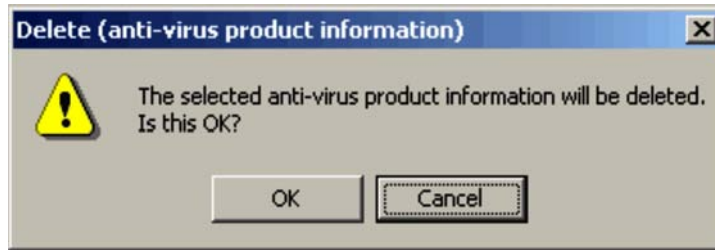
To delete anti-virus product information:

1. In the Edit Judgment Policy (Judgments for anti-virus products) window, click to select the anti-virus product you want to delete.

You can select multiple anti-virus products.

2. Click the Delete button.

The Delete (anti-virus product information) message box is displayed.



3. Check the contents of the message, and then click the **OK** button.

The Delete (anti-virus product information) message box closes, and the Edit Judgment Policy (Judgments for anti-virus products) window is displayed again. The selected anti-virus product is deleted.

#### 6.4.4 Importing anti-virus product information

For a large number of anti-virus products, an administrator can create an anti-virus products definition file in CSV format, and import the file.

The client security control system provides a sample of an anti-virus products definition file. The administrator can customize the sample file to create a definition file based on the security objectives and then import it. For details about a sample of this definition file, see *A.4(4) Sample of an anti-virus product definition file*.

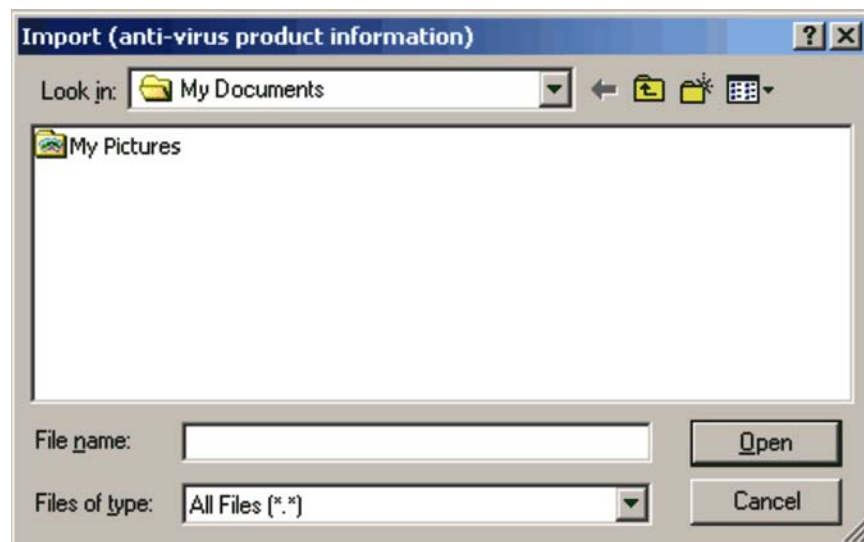
For details about this file, see *16.2.6 Anti-virus products definition file*.

To import anti-virus product information:

1. In the Edit Judgment Policy (Judgments for anti-virus products) window, click the **Import** button.

The Import (anti-virus product information) dialog box is displayed.





2. Specify **Look in**.

Specify the location of the anti-virus products definition file to be imported.

3. Specify the name of the anti-virus products definition file, and then click the **Open** button.

The specified file is read, and the Edit Judgment Policy (Judgments for anti-virus products) window is displayed again.

If the specified file does not contain anti-virus product information (the file is empty), an error message appears and the import is canceled.

#### 6.4.5 Exporting anti-virus product information

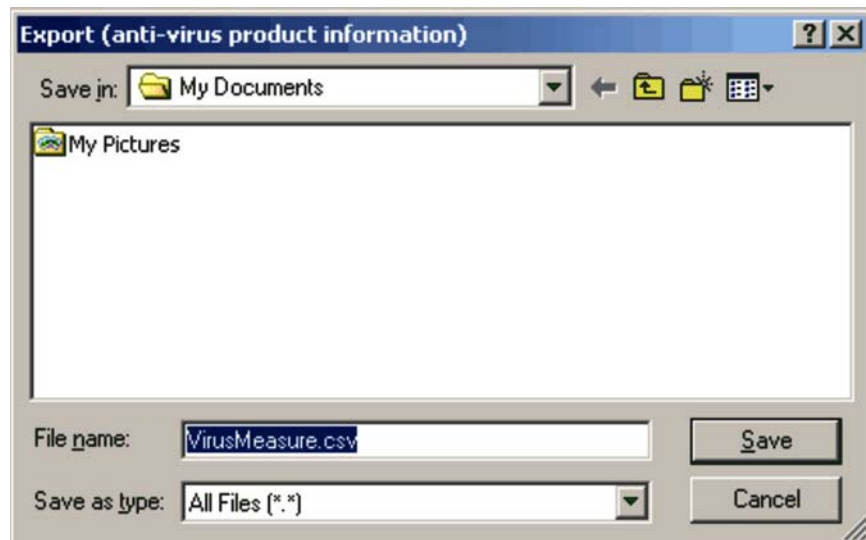
Information about anti-virus products can be exported to a CSV file.

To export anti-virus product information:

1. In the Edit Judgment Policy (Judgments for anti-virus products) window, click the **Export** button.

The Export (anti-virus product information) dialog box is displayed.

Note that the **Export** button is disabled when no definition has been registered in the Edit Judgment Policy (Judgments for anti-virus products) window.



2. Specify **Save in**.

Specify the location in which to save the exported file.

3. Specify the name of the CSV file to be exported for the file name, and click the **Save** button.

The specified file is saved, and the Edit Judgment Policy (Judgments for anti-virus products) window is displayed again.

#### 6.4.6 Updating judgment policies for anti-virus products automatically or manually

The following describes how to update a judgment policy for an anti-virus product without using the Edit Judgment Policy (Judgments for anti-virus products) window.

##### ***(1) Installing an anti-virus product on a client in order to update judgment policies***

When an anti-virus product compatible with automatic judgment policy updating is installed on a client, the judgment policies for the anti-virus products can be updated automatically based on the update information for the virus definition file and engine version.

To update judgment policies by linkage with a client:

1. Install an anti-virus product on the client.

For details about anti-virus products compatible with automatic judgment policy updating, see *4.6 Installing anti-virus products that link with automatic judgment*

*policy updating.*

2. Set up JP1/Client Security Control - Manager.

In the Client Security Control - Manager Setup dialog box, complete the following settings so that judgment policies will be updated automatically:

- In the Additional automatic update information window that is opened from the **Automatic updates for anti-virus products** page, set automatic update information such as the asset number of the client on which the anti-virus product is installed and the update extension period.

For details about how to use the **Automatic updates for anti-virus products** page, see 5.4.3(4) *Using the Automatic updates for anti-virus products page*.

3. Start **JP1/Client Security Control - Manager Remote Service**, which is the remote service of JP1/CSC - Manager.

When JP1/CSC - Manager detects an update to the anti-virus product information (virus definition file and engine version), the judgment policy update command (`cscpolimport`) is automatically executed to automatically update the judgment policies.

For details about the judgment policy update command (`cscpolimport`), see *cscpolimport (updates judgment policy settings)* in 15. *Commands*.

*Reference note:*

You can set up the remote service to start automatically when the OS starts. For details about setting up the remote service to start automatically, see 5.4.4 *Setting up JP1/CSC - Manager and the remote service to start automatically*.

**(2) Installing an anti-virus product on a remote management server to update judgment policies**

When an anti-virus product compatible with automatic judgment policy updating is installed on a remote management server, the judgment policies for the anti-virus products can be updated automatically whenever the virus definition file or engine version is updated. Alternatively, the administrator can update the judgment policy manually at any time. Updating manually allows you to postpone updating for a set time rather than updating immediately after the updates become available.

The following describes the procedure for updating judgment policies by linkage with a remote management server.

**(a) Updating judgment policies automatically by linkage with a remote management server**

1. Set up a remote management server.

In the Client Security Control - Manager Setup dialog box, complete the

following settings to update judgment policies automatically:

- In the **Basic Settings** page, under **Policy update information**, set **Anti-virus products** to **Update automatically**.
- In the **Remote Option** page, register the IP address of the remote management server.

In the Client Security Control - Manager Remote Option Setup dialog box, complete the following settings:

- In the **Anti-Virus Products** page, under **Automatic policy update information**, set **Automatic policy update** to **Execute**.
- In the **Anti-Virus Products** page, under **Automatic policy update information**, specify a grace period in **Extend update time** to apply between the acquisition of the latest information about the anti-virus product and the automatic update of the judgment policy definition.
- In the **Anti-Virus Products** page, under **Linked product information**, select the anti-virus product name in **Name**.

For details about setting up a remote management server, see *5.4 Installing and setting up JP1/CSC - Manager* and *5.5 Installing and setting up JP1/CSC - Manager Remote Option*.

2. Install the anti-virus product on the remote management server.

For details about anti-virus products compatible with automatic judgment policy updating, see *4.6 Installing anti-virus products that link with automatic judgment policy updating*.

3. Start **Client Security Control - Manager Remote Service**, the remote service of JP1/CSC - Manager.
4. Start **Client Security Control - Manager for AntiVirus**, the virus definition information monitoring service of JP1/CSC - Manager Remote Option.

When the remote management server detects an update of anti-virus product information (virus definition file and engine version), the judgment policy update command (`cscpolimport`) is automatically executed to automatically update the judgment policies.

For details about the judgment policy update command (`cscpolimport`), see *cscpolimport (updates judgment policy settings)* in *15. Commands*.

*Reference note:*

You can set up the remote service and virus definition information monitoring service to start automatically when the OS starts. For details about setting up the remote service to start automatically, see *5.4.4 Setting up JP1/CSC - Manager and the remote service to start automatically*. For details about setting up the virus definition information monitoring service to start automatically, see *5.5.4 Setting up the virus definition information monitoring service to start automatically*.

**(b) Updating judgment policies manually whenever the administrator chooses**

1. Set up a remote management server.

In the Client Security Control - Manager Setup dialog box, complete the following settings to update judgment policies at any time the administrator chooses:

- In the **Basic Settings** page, under **Policy update information**, set **Anti-virus products** to **Do not update automatically**.
- In the **Remote Option** page, register the IP address of the remote management server.

In the Client Security Control - Manager Remote Option Setup dialog box, complete the following settings:

- In the **Anti-Virus Products** page, under **Automatic policy update information**, set **Automatic policy update** to **Execute**.
- In the **Anti-Virus Products** page, under **Linked product information**, select the anti-virus product name in **Name**.

For details about setting up a remote management server, see *5.4 Installing and setting up JP1/CSC - Manager* and *5.5 Installing and setting up JP1/CSC - Manager Remote Option*.

2. Install the anti-virus product on the remote management server.
3. Start **Client Security Control - Manager Remote Service**, the remote service of JP1/CSC - Manager.
4. Start **Client Security Control - Manager for AntiVirus**, the virus definition information monitoring service of JP1/CSC - Manager Remote Option.

When the remote management server detects that information about the anti-virus product (for example the version of the virus definition file or detection engine) has been updated, a policy import execution file (manual) (`cscmpolimport.dat`) is created. For the name and location of this file, see *16.14 Policy import execution file (manual)*.

5. Execute the judgment policy update command (`cscpolimport`) with the policy import execution file (manual) (`cscmpolimport.dat`) specified.

Execute the command as follows:

```
cscpolimport -v JPI/CSC -
Manager-installation-folder\spool\cscmpolimport.dat
```

The judgment policies are updated.

For details about the judgment policy update command (`cscpolimport`), see *cscpolimport (updates judgment policy settings)* in *15. Commands*.

*Reference note:*

You can set up the remote service and virus definition information monitoring service to start automatically when the OS starts. For details about setting up the remote service to start automatically, see *5.4.4 Setting up JPI/CSC - Manager and the remote service to start automatically*. For details about setting up the virus definition information monitoring service to start automatically, see *5.5.4 Setting up the virus definition information monitoring service to start automatically*.

### **(3) Creating a policy import file for anti-virus products to update judgment policies manually**

By creating a *policy import file for anti-virus products*, an administrator can manually update the relevant judgment policies. A policy import file for anti-virus products defines update information (for example information about the version of the virus definition file or detection engine) for anti-virus products. For details about this file, see *16.13 Anti-virus product policy import file*.

This method can be used when an administrator wants to update judgment policies with specific information.

To update judgment policies manually:

1. Create a policy import file for anti-virus products.
2. Execute the judgment policy update command (`cscpolimport`) with the anti-virus product policy import file specified.

Execute the command as follows:

```
cscpolimport -v anti-virus-product-policy-import-file-name
```

The judgment policies are updated.

For details about the judgment policy update command (`cscpolimport`), see *cscpolimport (updates judgment policy settings)* in *15. Commands*.

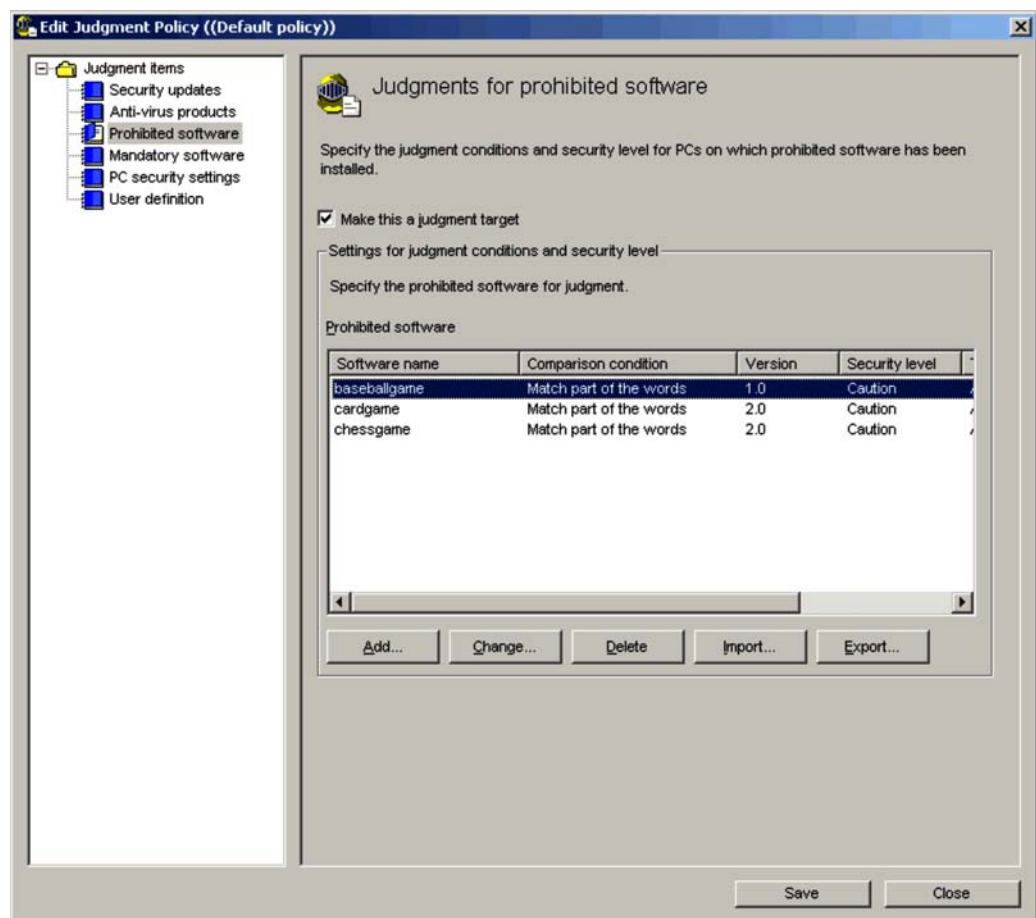
## 6.5 Editing a prohibited software judgment policy

The Edit Judgment Policy (Judgments for prohibited software) window can be used to set information about prohibited software that is not allowed to be installed on a client, as well as the security level when such software is installed on a client.

The Edit Judgment Policy (Judgments for prohibited software) window is displayed by selecting **Prohibited software** from the judgment items tree view, in the Edit Judgment Policy window.

The following figure shows the Edit Judgment Policy (Judgments for prohibited software) window.

Figure 6-12: Edit Judgment Policy (Judgments for prohibited software) window





The items set in the Edit Judgment Policy (Judgments for prohibited software) window are as follows.

### Make this a judgment target

Select the check box to make the prohibited software a judgment policy target. If the check box is selected, the window items are activated. This is cleared by default.

### Prohibited software

Set the prohibited software to be judged.

To edit prohibited software information:

1. In the Edit Judgment Policy (Judgments for prohibited software) window, select the **Make this a judgment target** check box.

All items in the Edit Judgment Policy (Judgments for prohibited software) window are activated.

2. Set the prohibited software.

You can add, change, and delete the set prohibited software. You can also import and export prohibited software information as a CSV file. Click the corresponding button to edit the information in the dialog box displayed.

3. When editing operations are complete, in the Edit Judgment Policy (Judgments for prohibited software) window, click the **Save** button.

The set contents are saved as a judgment policy.

#### Note:

The software names you define in the Edit Judgment Policy (Judgments for prohibited software) window must be names registered as asset information in AIM.

The following table lists the names of the dialog boxes and message boxes displayed when the corresponding buttons are pressed in the Edit Judgment Policy (Judgments for prohibited software) window.

*Table 6-10:* Names of dialog boxes and message boxes displayed from the Edit Judgment Policy (Judgments for prohibited software) window

No.	Button	Dialog box name or message box name
1	<b>Add</b>	Add (prohibited software information) dialog box
2	<b>Change</b>	Update (prohibited software information) dialog box
3	<b>Delete</b>	Delete (prohibited software information) message box

No.	Button	Dialog box name or message box name
4	<b>Import</b>	Import (prohibited software information) dialog box
5	<b>Export</b>	Export (prohibited software information) dialog box

*Reference note:*

When JP1/Client Security Control - Manager is upgraded from version 08-00 or earlier, the software name, version, security level, and OS settings are also inherited without change. Note, however, that the comparison condition is set to **Match the beginning of the words**.

The following explains the procedures for adding, changing, deleting, importing, and exporting information.

### 6.5.1 Adding prohibited software information

To add prohibited software information:

1. In the Edit Judgment Policy (Judgments for prohibited software) window, click the **Add** button.

The Add (prohibited software information) dialog box is displayed.

2. Enter the prohibited software information.  
Enter the prohibited software information. The following table lists the setting

items.

*Table 6-11:* Setting items for the Add (prohibited software information) dialog box

No.	Window item name	Description	Default
1	<b>Software name</b>	Enter the name of the prohibited software, in 255 or fewer bytes. This setting is required.	None
2	<b>Comparison condition</b>	Select the software name comparison condition from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• <b>Match all the words</b></li> <li>• <b>Match part of the words</b></li> <li>• <b>Match beginning of the words</b></li> <li>• <b>Match end of the words</b></li> </ul>	<b>Match part of the words</b>
3	<b>Version<sup>#</sup></b>	Enter the version of the prohibited software, in 60 or fewer bytes.	None
4	<b>OS</b>	Select the type of OS from the pull-down menu.	<b>All OSs</b>
5	<b>Security level</b>	Select the security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	<b>Caution</b>

#

Versions are judged by forward matching. If the version registered as asset information in AIM is 0000, and you enter something other than 0000, the security level judgment result will be **Unknown**.

3. Click the **OK** button.

The Add (prohibited software information) dialog box closes, and the Edit Judgment Policy (Judgments for prohibited software) window is displayed again. The entered prohibited software information is added.

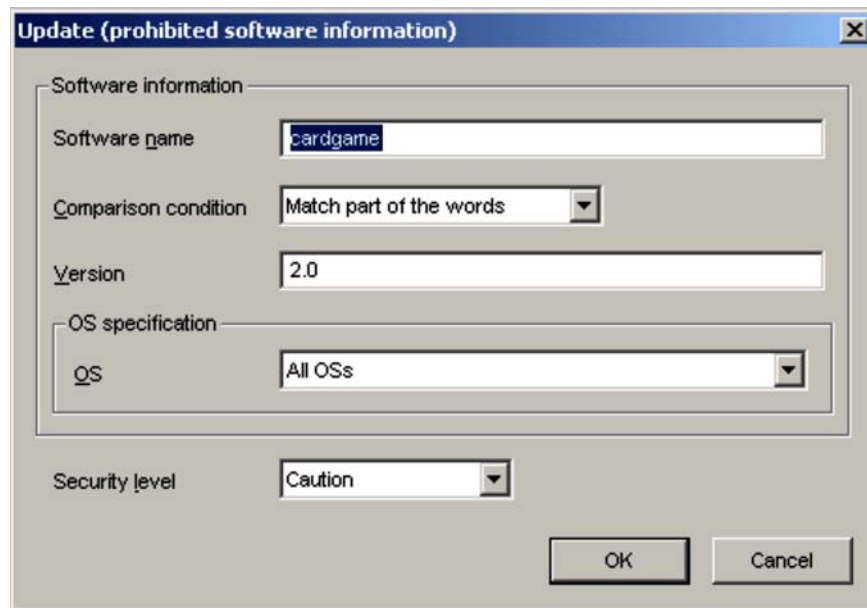
## 6.5.2 Changing prohibited software information

To change prohibited software information:

1. In the Edit Judgment Policy (Judgments for prohibited software) window, click the prohibited software to be changed, and then click the **Change** button. Alternatively, double-click the prohibited software to be changed.

The Update (prohibited software information) dialog box is displayed.

Note that the **Change** button is disabled if you select multiple prohibited software products.



2. Change the prohibited software information.
3. Click the **OK** button.

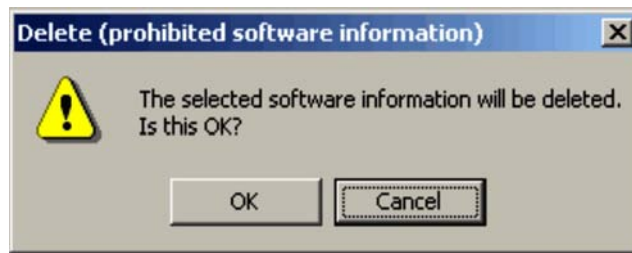
The Update (prohibited software information) dialog box closes, and the Edit Judgment Policy (Judgments for prohibited software) window is displayed again. The prohibited software information is changed to reflect the entered contents.

### 6.5.3 Deleting prohibited software information

To delete prohibited software information:

1. In the Edit Judgment Policy (Judgments for prohibited software) window, click to select the prohibited software you want to delete.  
You can select multiple prohibited software products.
2. Click the **Delete** button.

The Delete (prohibited software information) message box is displayed.



3. Check the contents of the message, and then click the **OK** button.

The Delete (prohibited software information) message box closes, and the Edit Judgment Policy (Judgments for prohibited software) window is displayed again. The selected prohibited software is deleted.

#### 6.5.4 Importing prohibited software information

For a large amount of prohibited software, an administrator can create a prohibited software definition file in CSV format, and import the file.

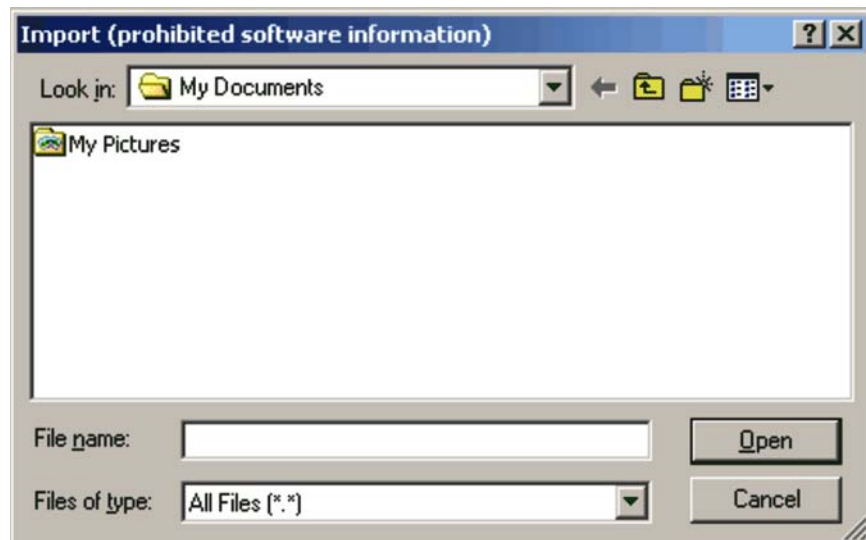
The client security control system provides a sample of a prohibited software definition file. The administrator can customize the sample file to create a definition file based on the security objectives and then import it. For details about a sample of this definition file, see *A.4(5) Sample of a prohibited software definition file*.

For details about the format of this file, see *16.2.7 Prohibited software definition file*.

To import prohibited software information:

1. In the Edit Judgment Policy (Judgments for prohibited software) window, click the **Import** button.

The Import (prohibited software information) dialog box is displayed.



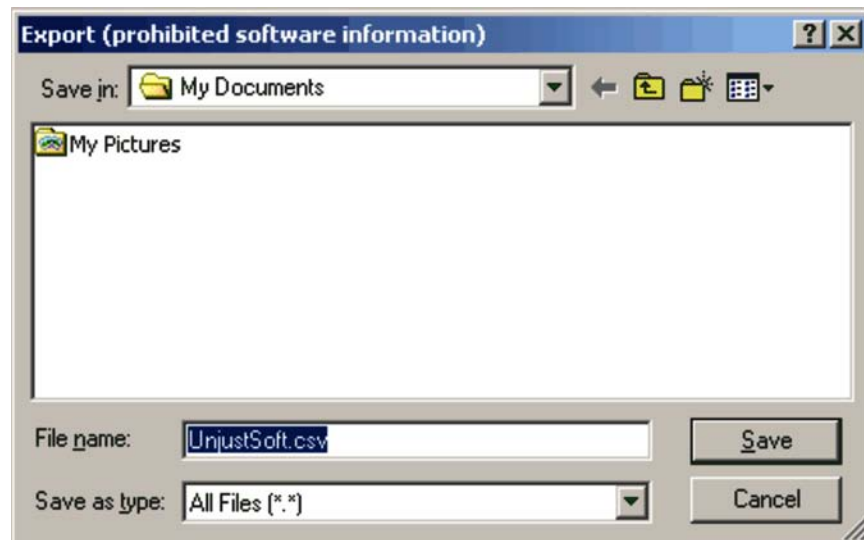
2. Specify **Look in**.  
Specify the location of the prohibited software definition file to be imported.
3. Specify the name of the prohibited definition file, and then click the **Open** button.  
The specified file is read, and the Edit Judgment Policy (Judgments for prohibited software) window is displayed again.  
If the specified file does not contain prohibited software information (the file is empty), an error message appears and the import is canceled.

### 6.5.5 Exporting prohibited software information

Information about prohibited software can be exported to a CSV file.

To import prohibited software information:

1. In the Edit Judgment Policy (Judgments for prohibited software) window, click the **Export** button.  
The Export (prohibited software information) dialog box is displayed.  
Note that the **Export** button is disabled when no definition has been registered in the Edit Judgment Policy (Judgments for prohibited software) window.



2. Specify **Save in**.  
Specify the location in which to save the exported file.
3. Specify the name of the CSV file to be exported for the file name, and click the **Save** button.

The specified file is saved, and the Edit Judgment Policy (Judgments for prohibited software) window is displayed again.

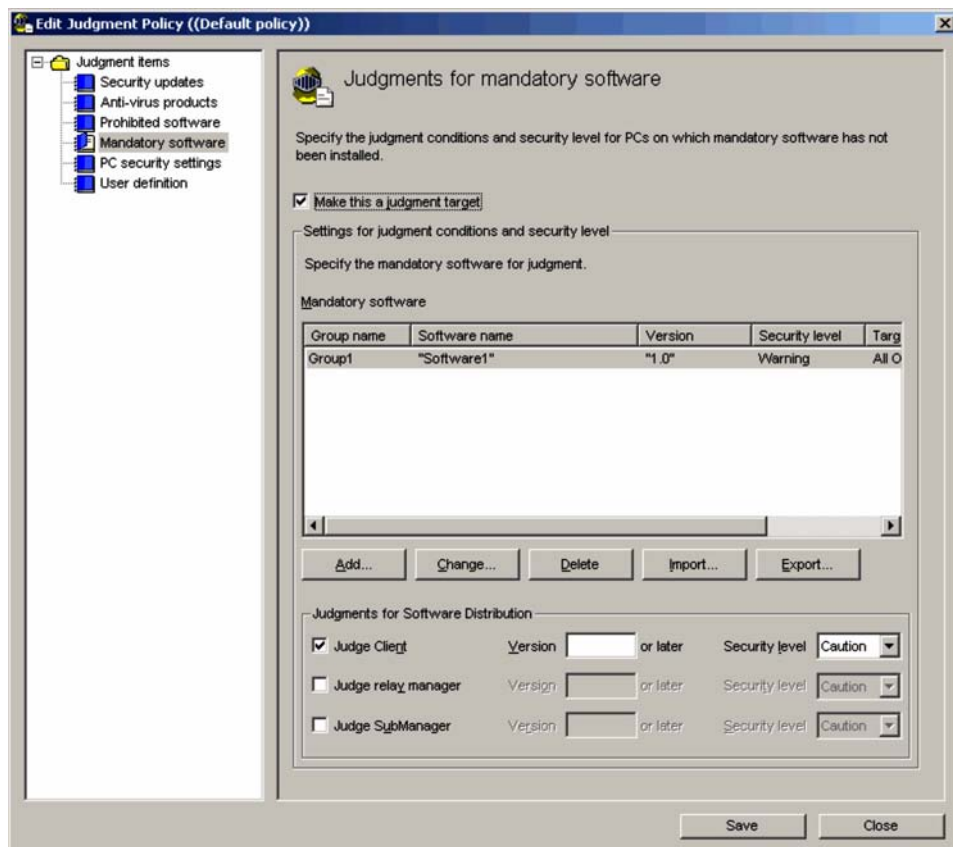
## 6.6 Editing a mandatory software judgment policy

The Edit Judgment Policy (Judgments for mandatory software) window can be used to set information about mandatory software that must be installed on a client, as well as the security level when such software is not installed on a client.

The Edit Judgment Policy (Judgments for mandatory software) window is displayed by selecting **Mandatory software** from the judgment items tree view, in the Edit Judgment Policy window.

The following figure shows the Edit Judgment Policy (Judgments for mandatory software) window.

*Figure 6-13:* Edit Judgment Policy (Judgments for mandatory software) window



The items set in the Edit Judgment Policy (Judgments for mandatory software)



window are as follows.

### **Make this a judgment target**

Select the check box to make the mandatory software a judgment policy target. If the check box is selected, the window items are activated. This is cleared by default.

### **Mandatory software**

Set the mandatory software to be judged. Multiple versions of software with different names can be registered as a group. If any one of the software names in the group matches the name of software installed on the client, the client is judged to be *Safe*.

When multiple groups are set, the security level of the client will be judged using an AND conditions.

#### *Note:*

Do not define JP1/Software Distribution Client, JP1/Software Distribution SubManager, or JP1/Software Distribution Manager (relay manager) as mandatory software. If you define these products as mandatory software, JP1/Software Distribution Client, JP1/Software Distribution SubManager, and JP1/Software Distribution Manager (relay manager) will appear more than once in the judgment results in the Mandatory Software Details window of the Client Security Management window.

### **Judgments for Software Distribution**

Set whether to include JP1/Software Distribution Client, JP1/Software Distribution SubManager, and JP1/Software Distribution Manager (relay manager) in the judgment policy.

#### **Judge client**

Select this check box to include JP1/Software Distribution Client as a judgment target. The check box is selected by default. When this check box is cleared, the **Version** and **Security level** items are rendered inactive.

#### **Judge relay manager**

Select this check box to include JP1/Software Distribution Manager (relay manager) as a judgment target. The check box is cleared by default. When this check box is cleared, the **Version** and **Security level** items are rendered inactive.

If you specify JP1/Software Distribution Manager (relay manager) as a judgment target, **Software Distribution manager (relay manager)** must be set to **Subject to judgment and action for the security level** in the setup

dialog box for JP1/CSC - Manager. For details about setting up JP1/CSC - Manager, see *5.4.3 Setting up JP1/CSC - Manager*.

### Judge SubManager

Select this check box to include JP1/Software Distribution SubManager as a judgment target. The check box is cleared by default. When this check box is cleared, the **Version** and **Security level** items are rendered inactive.

If you specify JP1/Software Distribution SubManager as a judgment target, **Software Distribution SubManager** must be set to **Subject to judgment and action for the security level** in the setup dialog box for JP1/CSC - Manager. For details about setting up JP1/CSC - Manager, see *5.4.3 Setting up JP1/CSC - Manager*.

### Version

Specify the version of each software product. This item is optional.

### Security level

From the pull-down menu, select a security level to be applied when the software product is not installed. The default is **Caution**.

#### Note:

The information you set in **Judgments for Software Distribution** also applies to the security level for JP1/Software Distribution Client (relay system). Include information applicable to JP1/Software Distribution Client (relay system) when you set these items.

To edit mandatory software information:

1. In the Edit Judgment Policy (Judgments for mandatory software) window, select the **Make this a judgment target** check box.  
All items in the Edit Judgment Policy (Judgments for mandatory software) window are activated.
2. Set the mandatory software.  
You can add, change, and delete the set mandatory software. You can also import and export mandatory software information as a CSV file. Click the corresponding button to edit the information displayed in the dialog box.
3. Set judgment information for JP1/Software Distribution Client.  
Set the version and security level for judging JP1/Software Distribution Client.
4. Set judgment information for JP1/Software Distribution SubManager as required.

Set the version and security level for judging JP1/Software Distribution SubManager.

5. Set judgment information for JP1/Software Distribution Manager (relay manager) as required.

Set the version and security level for judging JP1/Software Distribution Manager (relay manager).

6. When you have finished editing, in the Edit Judgment Policy (Judgments for mandatory software) window, click the **Save** button.

The set contents are saved as a judgment policy.

*Reference note:*

A warning message may appear when you click the **Save** button. Read the message, and review your settings if necessary. Click the **OK** button to save the settings, or the **Cancel** button to discard them.

*Note:*

The software names you define in the Edit Judgment Policy (Judgments for mandatory software) window must be names registered as asset information in AIM.

The following table lists the names of the dialog boxes and message boxes displayed when the corresponding buttons are clicked in the Edit Judgment Policy (Judgments for mandatory software) window.

*Table 6-12:* Names of dialog boxes and message boxes displayed from the Edit Judgment Policy (Judgments for mandatory software) window

No.	Button	Dialog box name or message box name
1	<b>Add</b>	Add (mandatory software information) dialog box
2	<b>Change</b>	Update (mandatory software information) dialog box
3	<b>Delete</b>	Delete (mandatory software information) message box
4	<b>Import</b>	Import (mandatory software information) dialog box
5	<b>Export</b>	Export (mandatory software information) dialog box

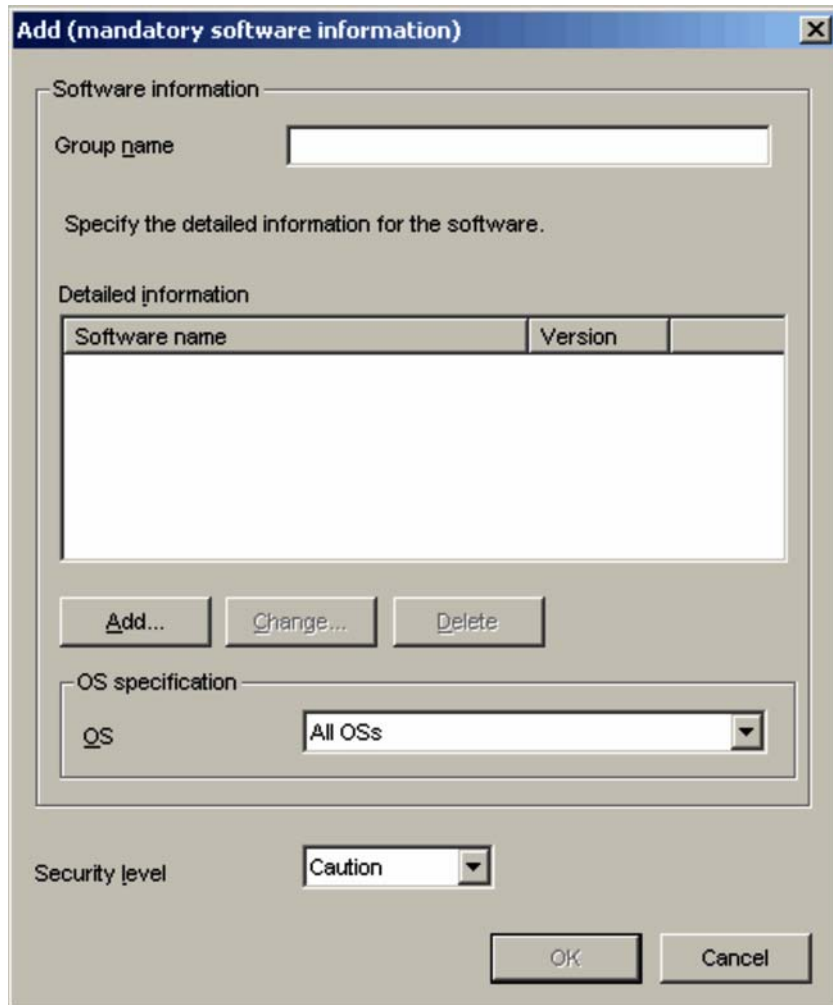
The following explains the procedures for adding, changing, deleting, importing, and exporting information.

### 6.6.1 Adding mandatory software information

To add mandatory software information:

1. In the Edit Judgment Policy (Judgments for mandatory software) window, click the **Add** button.

The Add (mandatory software information) dialog box is displayed.



The dialog box is titled "Add (mandatory software information)". It contains the following fields and controls:

- Software information** section:
  - Group name**: A text input field.
  - Specify the detailed information for the software.**: A label.
  - Detailed information** section:
    - A table with two columns: **Software name** and **Version**.
    - A large empty text area below the table headers.
  - Buttons: **Add...**, **Change...**, and **Delete**.
- OS specification** section:
  - OS**: A dropdown menu currently showing "All OSs".
- Security level**: A dropdown menu currently showing "Caution".
- OK** and **Cancel** buttons at the bottom right.

2. Enter the group name.

To register multiple software names and versions as a group, enter the group name to be registered, using a string of 255 or fewer bytes. This item is required. The group name must be registered even if only one software item is registered.

## 3. Define detailed information about the mandatory software.

Add, change, or delete detailed information about the mandatory software to be registered. Click the button for the desired operation, and then use the displayed dialog box to edit the detailed information.

## 4. Select an OS.

Select an OS from the pull-down menu. The default is **All OSs**.

## 5. Select a security level.

Select a security level from the pull-down menu. The default is **Caution**.

6. Click the **OK** button.

The Add (mandatory software information) dialog box closes, and the Edit Judgment Policy (Judgments for mandatory software) window is displayed again.

The following table shows the names of the dialog boxes and message box displayed when the corresponding buttons are clicked in the Add (mandatory software information) dialog box.

*Table 6-13:* Names of dialog boxes and message box displayed from the Add (mandatory software information) dialog box

No.	Button	Dialog box name or message box name
1	<b>Add</b>	Add (mandatory software detailed information) dialog box
2	<b>Change</b>	Update (mandatory software detailed information) dialog box
3	<b>Delete</b>	Delete (mandatory software detailed information) message box

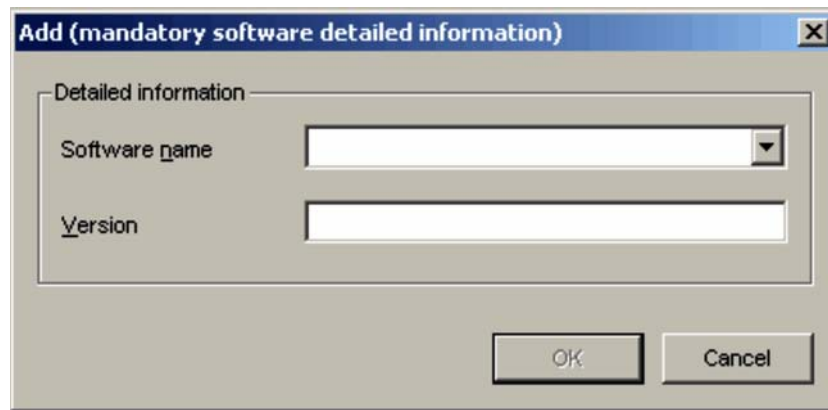
The following subsections explain how to add, change, and delete detailed information to be registered in the mandatory software group.

**(1) Adding detailed mandatory software information**

To add detailed mandatory software information in the Add (mandatory software information) dialog box:

1. In the Add (mandatory software information) dialog box, click the **Add** button.

The Add (mandatory software detailed information) dialog box is displayed.



2. Enter detailed mandatory software information.

The following table lists the setting items.

*Table 6-14: Setting items for the Add (mandatory software detailed information) dialog box*

No.	Window item name	Description	Default
1	<b>Software name</b> <sup>#1</sup>	Select the mandatory software name from the combo box. Alternatively, enter a string of 255 or fewer bytes. This setting is required.	The name entered in <b>Group name</b>
2	<b>Version</b> <sup>#2</sup>	Enter the version of the mandatory software in 60 or fewer bytes.	None

#1

The name of the software is judged by partial matching.

#2

Versions are judged by forward matching. If the version registered as asset information in AIM is 0000, and you enter something other than 0000, the security level judgment result will be **Unknown**.

3. Click the **OK** button.

The Add (mandatory software detailed information) dialog box closes, and the Add (mandatory software information) dialog box is displayed again. The detailed information entered for the mandatory software is added.

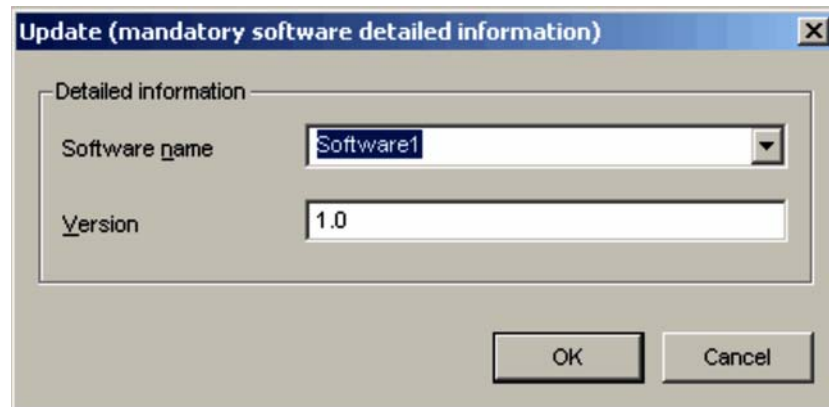
## **(2) Changing detailed mandatory software information**

To change detailed mandatory software information in the Add (mandatory software information) dialog box:

1. In the Add (mandatory software information) dialog box, select the detailed mandatory software information you want to change, and then click the **Change** button. Alternatively, double-click the detailed mandatory software information you want to change.

The Update (mandatory software detailed information) dialog box is displayed.

Note that the **Change** button is disabled if you select more than one item of mandatory software detailed information.



2. Change the detailed mandatory software information.
3. Click the **OK** button.

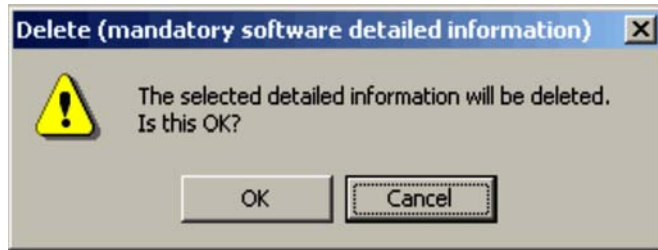
The Update (mandatory software detailed information) dialog box closes, and the Add (mandatory software information) dialog box is displayed again. The detailed information entered for the mandatory software is changed.

### **(3) Deleting detailed mandatory software information**

To delete detailed mandatory software information in the Add (mandatory software information) dialog box:

1. In the Add (mandatory software information) dialog box, click to select the detailed mandatory software information.  
You can select more than one item of detailed mandatory software information.
2. Click the **Delete** button.

The Delete (mandatory software detailed information) message box is displayed.



3. Check the message, and then click the **OK** button.

The Delete (mandatory software detailed information) message box closes, and the Add (mandatory software information) dialog box is displayed again. The detailed mandatory software information you selected is deleted.

### 6.6.2 Changing mandatory software information

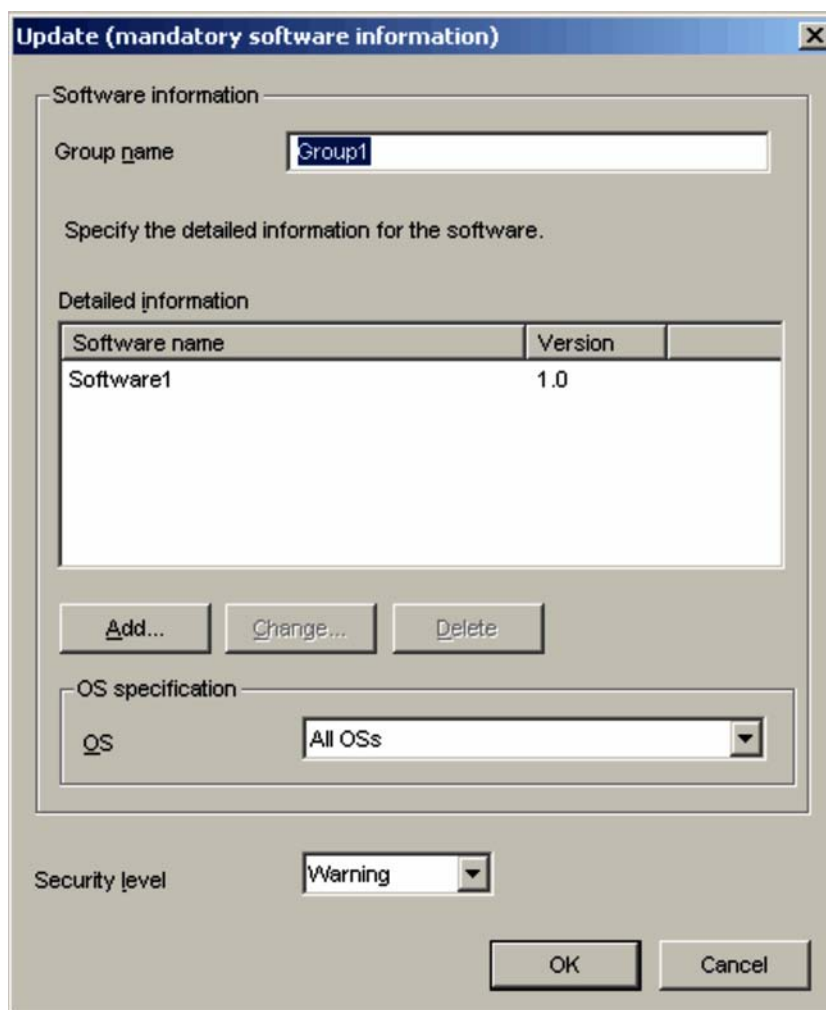
To change mandatory software information:

1. In the Edit Judgment Policy (Judgments for mandatory software) window, click the mandatory software to be changed, and click the **Change** button. Alternatively, double-click the mandatory software you want to change.

The Update (mandatory software information) dialog box is displayed.

Note that the **Change** button is disabled if you select more than one item of mandatory software for modification.





The dialog box is titled "Update (mandatory software information)". It contains the following elements:

- Software information** section:
  - A text box labeled "Group name" containing the text "Group1".
  - A label "Specify the detailed information for the software."
- Detailed information** section:
  - A table with two columns: "Software name" and "Version".
  - A single row with the values "Software1" and "1.0".
- Three buttons: "Add...", "Change...", and "Delete".
- OS specification** section:
  - A label "OS" followed by a dropdown menu currently showing "All OSs".
- Security level** section:
  - A dropdown menu currently showing "Warning".
- At the bottom right, "OK" and "Cancel" buttons.

2. Enter the group name.  
Enter the group name of the mandatory software to be changed, using a string of 255 or fewer bytes. This item is required.
3. Define detailed information about the mandatory software.  
Add, change, or delete detailed information about the mandatory software to be changed. Click the button for the desired operation, and then use the displayed dialog box to edit the detailed information.
4. Select an OS.

Select an OS for each group from the pull-down menu.

5. Select a security level.

Select a security level for each group from the pull-down menu.

6. Click the **OK** button.

The Update (mandatory software information) dialog box closes, and the Edit Judgment Policy (Judgments for mandatory software) window is displayed again.

The following table shows the names of the dialog boxes and message box displayed when the corresponding buttons are clicked in the Update (mandatory software information) dialog box.

*Table 6-15:* Names of dialog boxes and message box displayed from the Update (mandatory software information) dialog box

No.	Button	Dialog box name or message box name
1	<b>Add</b>	Add (mandatory software detailed information) dialog box
2	<b>Change</b>	Update (mandatory software detailed information) dialog box
3	<b>Delete</b>	Delete (mandatory software detailed information) message box

In the Update (mandatory software information) dialog box, you can add, change, and delete detailed information for mandatory software, using the same procedures as in the Add (mandatory software information) dialog box. See the following for each procedure:

- For details about adding detailed information, see *6.6.1(1) Adding detailed mandatory software information*.
- For details about changing detailed information, see *6.6.1(2) Changing detailed mandatory software information*.
- For details about deleting detailed information, see *6.6.1(3) Deleting detailed mandatory software information*.

### 6.6.3 Deleting mandatory software information

To delete mandatory software information:

1. In the Edit Judgment Policy (Judgments for mandatory software) window, click the mandatory software information you want to delete.

You can select more than one item of mandatory software information.

2. Click the **Delete** button.

The Delete (mandatory software information) message box is displayed.



3. Check the contents of the message, and then click the **OK** button.

The Delete (mandatory software information) message box closes, and the Edit Judgment Policy (Judgments for mandatory software) window is displayed again. The selected mandatory software is deleted.

#### 6.6.4 Importing mandatory software information

For a large amount of mandatory software, an administrator can create a mandatory software definition file in CSV format, and import the file.

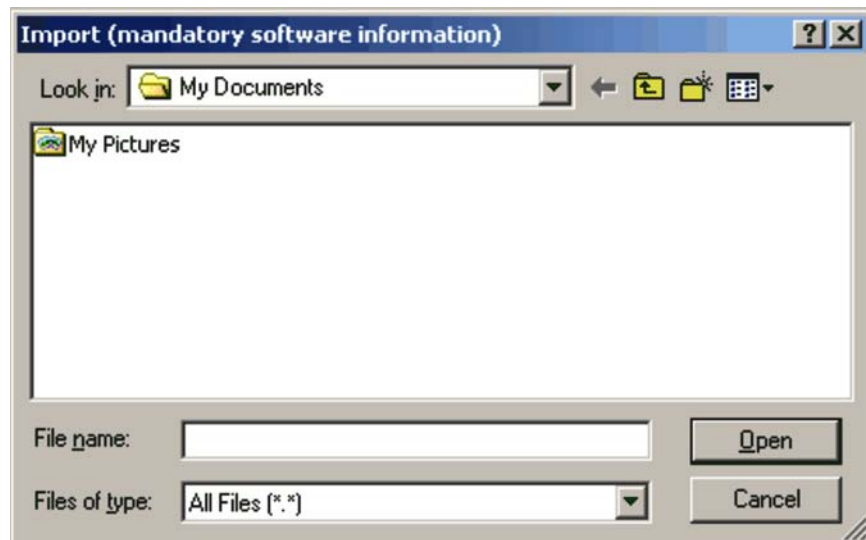
The client security control system provides a sample of a mandatory software definition file. The administrator can customize the sample file to create a definition file based on the security objectives and then import it. For details about a sample of this definition file, see *A.4(6) Sample of a mandatory software definition file*.

For details about the format of this file, see *16.2.8 Mandatory software definition file*.

To import mandatory software information:

1. In the Edit Judgment Policy (Judgments for mandatory software) window, click the **Import** button.

The Import (mandatory software information) dialog box is displayed.



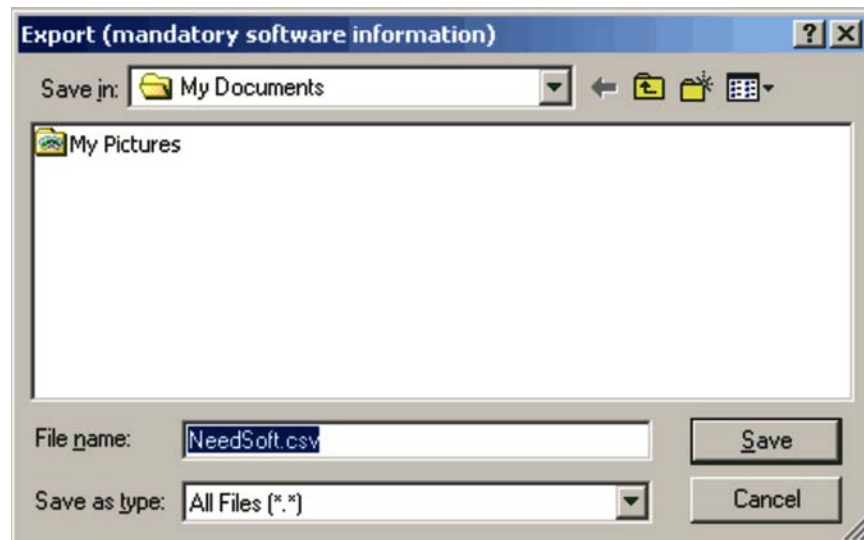
2. Specify **Look in**.  
Specify the location of the mandatory software definition file to be imported.
3. Specify the name of the mandatory definition file, and then click the **Open** button.  
The specified file is read, and the Edit Judgment Policy (Judgments for mandatory software) window is displayed again.  
If the specified file does not contain mandatory software information (the file is empty), an error message appears and the import is canceled.

### 6.6.5 Exporting mandatory software information

Information about mandatory software can be exported to a CSV file.

To export mandatory software information:

1. In the Edit Judgment Policy (Judgments for mandatory software) window, click the **Export** button.  
The Export (mandatory software information) dialog box is displayed.  
Note that the **Export** button is disabled when no definition has been registered in the Edit Judgment Policy (Judgments for mandatory software) window.



2. Specify **Save in**.  
Specify the location in which to save the exported file.
3. Specify the name of the CSV file to be exported for the file name, and click the **Save** button.

The specified file is saved, and the Edit Judgment Policy (Judgments for mandatory software) window is displayed again.

---

## 6.7 Editing a PC security setting judgment policy

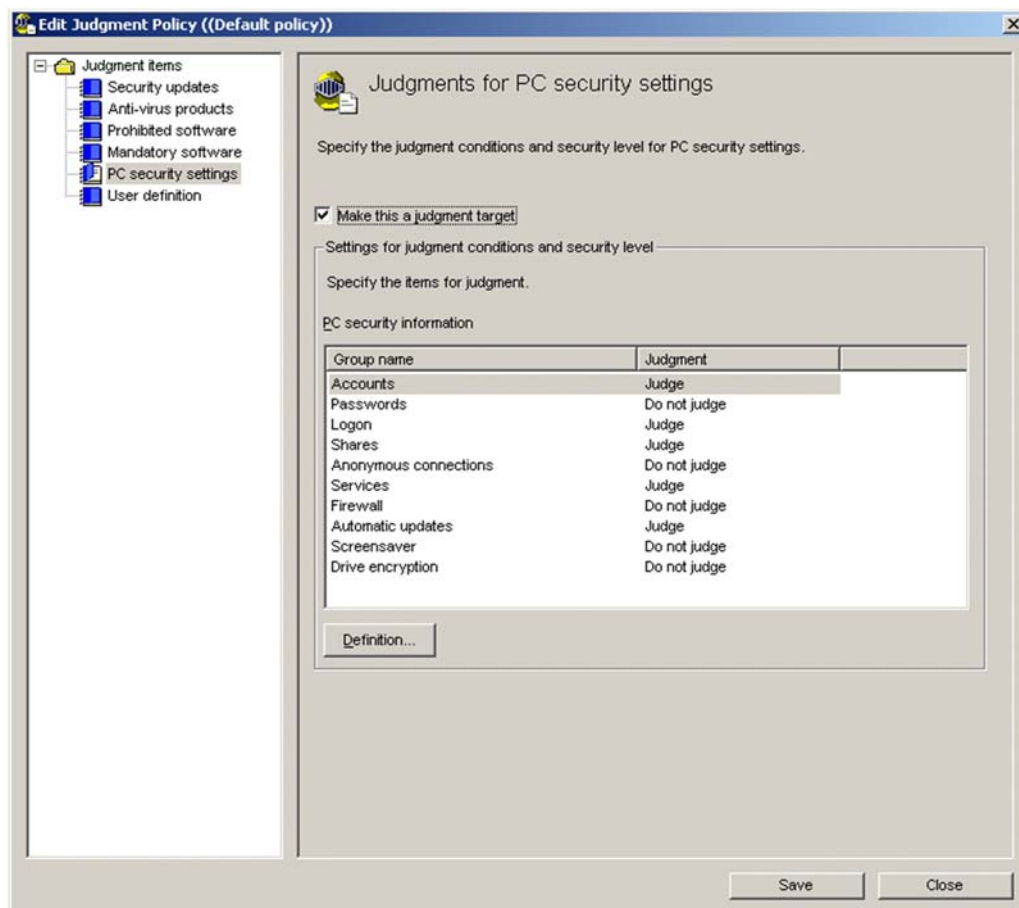
---

The Edit Judgment Policy (Judgments for PC security settings) window can be used to set judgment items concerning security-related settings on client PCs. These may include account and password settings, as well as the security level that applies when such settings are not implemented correctly on a client.

The Edit Judgment Policy (Judgments for PC security settings) window is displayed by selecting **PC security settings** from the judgment items tree view in the Edit Judgment Policy window.

The following figure shows the Edit Judgment Policy (Judgments for PC security settings) window.

Figure 6-14: Edit Judgment Policy (Judgments for PC security settings) window



The items set in the Edit Judgment Policy (Judgments for PC security settings) window are as follows.

#### **Make this a judgment target**

Select the check box to make PC security a judgment policy target. If the check box is selected, the window items are activated. This is cleared by default.

#### **PC security information**

Set the PC security information to be judged.

Use the Edit Judgment Policy (Judgments for PC security settings) window as follows:

1. In the Edit Judgment Policy (Judgments for PC security settings) window, select the **Make this a judgment target** check box.

All items in the Edit Judgment Policy (Judgments for PC security settings) window are activated.

2. Set the PC security information.

Either click the PC security judgment item that you want to edit and then click the **Definition** button, or double-click the item that you want to edit.

This displays a dialog box in which you can edit the PC security judgment item.

3. When you have finished editing judgment items, in the Edit Judgment Policy (Judgments for PC security settings) window, click the **Save** button.

The set contents are saved as a judgment policy.

The following table lists the PC security information that can form part of a judgment policy, and gives the section in the manual that describes how to set each item.

*Table 6-16:* PC security information able to be set in a judgment policy

No.	Judgment item name	Description	Section in manual
1	<b>Accounts</b>	Information relating to <b>Guest account settings</b> .	6.7.1
2	<b>Passwords</b>	Information relating to <b>Vulnerable password</b> , <b>Password that never expires</b> , and <b>Days since the password was updated</b> .	6.7.2
3	<b>Logon</b>	Information relating to <b>Automatic logon</b> and <b>Power-on password</b> .	6.7.3
4	<b>Shares</b>	Information relating to <b>Shared folder settings</b> .	6.7.4
5	<b>Anonymous connections</b>	Information relating to <b>Restriction of anonymous connections</b> .	6.7.5
6	<b>Services</b>	Information relating to <b>Status of unnecessary services</b> .	6.7.6
7	<b>Firewall</b>	Information relating to <b>Windows Firewall settings</b> .	6.7.7
8	<b>Automatic updates</b>	Information relating to <b>Settings for Windows automatic updates</b> .	6.7.8
9	<b>Screensaver</b>	Information relating to <b>Screensaver settings</b> and <b>Password protection</b> .	6.7.9
10	<b>Drive encryption</b>	Information relating to <b>Drive encryption by BitLocker</b> .	6.7.10

## 6.7.1 Defining account settings

To define account-related judgment items in the Edit Judgment Policy (Judgments for



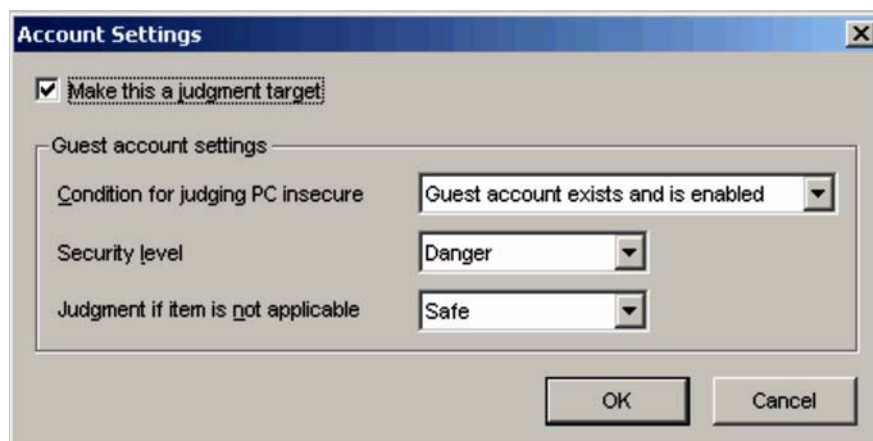
PC security settings) window:

1. In the Edit Judgment Policy (Judgments for PC security settings) window, select the **Make this a judgment target** check box.

The items in the Edit Judgment Policy (Judgments for PC security settings) window are activated.

2. In the Edit Judgment Policy (Judgments for PC security settings) window, select **Accounts** and then click the **Definition** button, or double-click **Accounts**.

The Account Settings dialog box appears.



3. Define the judgment conditions and security levels for accounts.

The following table describes the setting items.

*Table 6-17: Setting items in the Account Settings dialog box*

No.	Window item name		Judgment conditions and description	Default
1	<b>Make this a judgment target</b>		Select whether to make the information defined in <b>Guest account settings</b> a target for security level judgment.	Off
2	<b>Guest account settings</b>	<b>Condition for judging PC insecure</b>	From the pull-down menu, select the condition for judging a client PC insecure. The following options are available: <ul style="list-style-type: none"> <li>• <b>Guest account exists</b></li> <li>• <b>Guest account exists and is enabled</b></li> </ul>	<b>Guest account exists and is enabled</b>

No.	Window item name		Judgment conditions and description	Default
3		<b>Security level</b>	Select a security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	<b>Warning</b>
4		<b>Judgment if item is not applicable</b>	From the pull-down menu, select the desired behavior when the judgment item does not exist. The following options are available: <ul style="list-style-type: none"> <li>• <b>Set security level</b></li> <li>• <b>Safe</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Unknown</b></li> </ul>	<b>Not applicable</b>

- Click the **OK** button.

The Account Settings dialog box closes, and you are returned to the Edit Judgment Policy (Judgments for PC security settings) window.

### 6.7.2 Defining password settings

To define password-related judgment items in the Edit Judgment Policy (Judgments for PC security settings) window:

- In the Edit Judgment Policy (Judgments for PC security settings) window, select the **Make this a judgment target** check box.

The items in the Edit Judgment Policy (Judgments for PC security settings) window are activated.

- In the Edit Judgment Policy (Judgments for PC security settings) window, select **Passwords** and then click the **Definition** button, or double-click **Passwords**.

The Password Settings dialog box appears.

**Password Settings**

☒ **Make this a judgment target**

☒ **Vulnerable password**

Condition for judging PC insecure: An account with a vulnerable password exists.

Security level: Warning

Judgment if item is not applicable: Unknown

☒ **Password that never expires**

Condition for judging PC insecure: An account with a password that never expires exists.

Security level: Warning

Judgment if item is not applicable: Unknown

☒ **Days since the password was updated**

Condition for judging PC insecure: 3 days or more (1 - 1000)

Security level: Danger

Judgment if item is not applicable: Unknown

OK Cancel

3. Define the judgment conditions and security levels for passwords.

The following table describes the setting items.

*Table 6-18: Setting items in the Password Settings dialog box*

No.	Window item name		Judgment conditions and description	Default
1	<b>Make this a judgment target</b>		Select whether to make <b>Vulnerable password</b> , <b>Password that never expires</b> , and <b>Days since the password was updated</b> targets for security level judgment.	Off
2	<b>Vulnerable password<sup>#</sup></b>	--	Select whether or not to judge password vulnerability.	On

No.	Window item name		Judgment conditions and description	Default
3		<b>Condition for judging PC insecure</b>	An account with a vulnerable password exists.	--
4		<b>Security level</b>	Select a security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	<b>Warning</b>
5		<b>Judgment if item is not applicable</b>	From the pull-down menu, select the desired behavior when the judgment item does not exist. The following options are available: <ul style="list-style-type: none"> <li>• <b>Set security level</b></li> <li>• <b>Safe</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Unknown</b></li> </ul>	<b>Not applicable</b>
6	<b>Password that never expires<sup>#</sup></b>	--	Select whether or not to judge passwords that do not expire.	On
7		<b>Condition for judging PC insecure</b>	An account with a password that never expires exists.	--
8		<b>Security level</b>	Select a security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	<b>Warning</b>
9		<b>Judgment if item is not applicable</b>	From the pull-down menu, select the desired behavior when the judgment item does not exist. The following options are available: <ul style="list-style-type: none"> <li>• <b>Set security level</b></li> <li>• <b>Safe</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Unknown</b></li> </ul>	<b>Not applicable</b>

No.	Window item name		Judgment conditions and description	Default
10	<b>Days since the password was updated<sup>#</sup></b>	--	Select whether or not to judge the number of days since passwords are updated.	On
11		<b>Condition for judging PC insecure</b>	Specify the number of days that must have elapsed since a password was updated for the PC to be judged insecure. Either type a number between 1 and 1000, or select a number using the ▲ and ▼ buttons.	180
12		<b>Security level</b>	Select a security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	<b>Warning</b>
13		<b>Judgment if item is not applicable</b>	From the pull-down menu, select the desired behavior when the judgment item does not exist. The following options are available: <ul style="list-style-type: none"> <li>• <b>Set security level</b></li> <li>• <b>Safe</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Unknown</b></li> </ul>	<b>Not applicable</b>

Legend:

--: N/A

#

To exclude a specific user account from judgment, use an excluded user definition file. For details about how to create an excluded user definition file, see *16.19 Excluded user definition file*.

4. Click the **OK** button.

The Password Settings dialog box closes, and you are returned to the Edit Judgment Policy (Judgments for PC security settings) window.

### 6.7.3 Defining logon settings

To define logon-related judgment items in the Edit Judgment Policy (Judgments for PC security settings) window:

1. In the Edit Judgment Policy (Judgments for PC security settings) window, select the **Make this a judgment target** check box.

The items in the Edit Judgment Policy (Judgments for PC security settings) window are activated.

2. In the Edit Judgment Policy (Judgments for PC security settings) window, select **Logon** and then click the **Definition** button, or double-click **Logon**.

The Logon Settings dialog box appears.

3. Define the judgment conditions and security levels for logon settings.

The following table describes the setting items.

*Table 6-19: Setting items in the Logon Settings dialog box*

No.	Window item name	Judgment conditions and description	Default
1	<b>Make this a judgment target</b>	Select whether to make <b>Automatic logon</b> and <b>Power-on password</b> targets for security level judgment.	Off

No.	Window item name		Judgment conditions and description	Default
2	<b>Automatic logon</b>	--	Select whether or not to judge automatic logon settings.	On
3		<b>Condition for judging PC insecure</b>	Automatic logon is enabled.	--
4		<b>Security level</b>	Select a security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	<b>Warning</b>
5		<b>Judgment if item is not applicable</b>	From the pull-down menu, select the desired behavior when the judgment item does not exist. The following options are available: <ul style="list-style-type: none"> <li>• <b>Set security level</b></li> <li>• <b>Safe</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Unknown</b></li> </ul>	<b>Not applicable</b>
6	<b>Power-on password</b>	--	Select whether or not to judge power-on password settings.	On
7		<b>Condition for judging PC insecure</b>	From the pull-down menu, select the condition for judging the PC insecure. The following options are available: <ul style="list-style-type: none"> <li>• <b>Power-on password is not set</b></li> <li>• <b>Power-on password is not set or not installed</b></li> </ul>	<b>Power-on password is not set</b>
8		<b>Security level</b>	Select a security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	<b>Warning</b>

No.	Window item name		Judgment conditions and description	Default
9		<b>Judgment if item is not applicable</b>	From the pull-down menu, select the desired behavior when the judgment item does not exist. The following options are available: <ul style="list-style-type: none"> <li>• <b>Set security level</b></li> <li>• <b>Safe</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Unknown</b></li> </ul>	<b>Not applicable</b>

Legend:

--: N/A

4. Click the **OK** button.

The Logon Settings dialog box closes, and you are returned to the Edit Judgment Policy (Judgments for PC security settings) window.

#### 6.7.4 Defining share settings

To define shared folder-related judgment items in the Edit Judgment Policy (Judgments for PC security settings) window:

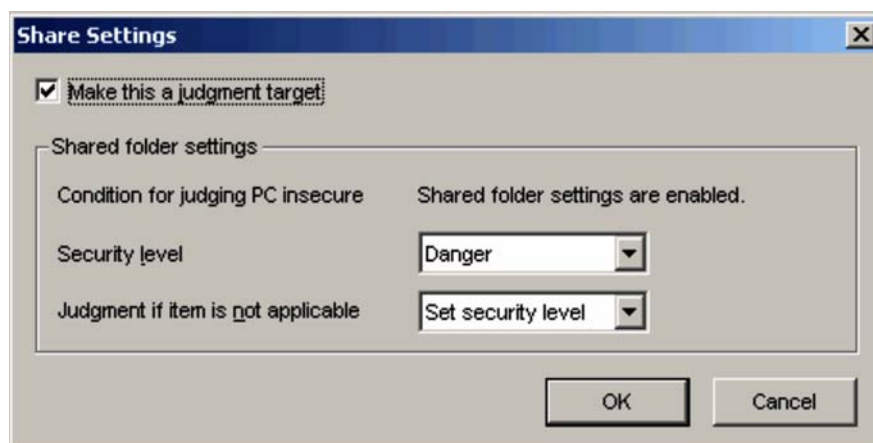
1. In the Edit Judgment Policy (Judgments for PC security settings) window, select the **Make this a judgment target** check box.

The items in the Edit Judgment Policy (Judgments for PC security settings) window are activated.

2. In the Edit Judgment Policy (Judgments for PC security settings) window, select **Shares** and then click the **Definition** button, or double-click **Shares**.

The Share Settings dialog box appears.





3. Define the judgment conditions and security levels for shared folder settings.  
The following table describes the setting items.

*Table 6-20:* Setting items in the Share Settings dialog box

No.	Window item name		Judgment conditions and description	Default
1	<b>Make this a judgment target</b>		Select whether to make <b>Shared folder settings</b> a target for security level judgment.	Off
2	<b>Shared folder settings</b>	<b>Condition for judging PC insecure</b>	Shared folder settings are enabled.	--
3		<b>Security level</b>	Select a security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	<b>Warning</b>

No.	Window item name		Judgment conditions and description	Default
4		<b>Judgment if item is not applicable</b>	From the pull-down menu, select the desired behavior when the judgment item does not exist. The following options are available: <ul style="list-style-type: none"> <li>• <b>Set security level</b></li> <li>• <b>Safe</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Unknown</b></li> </ul>	<b>Not applicable</b>

Legend:

--: N/A

4. Click the **OK** button.

The Share Settings dialog box closes, and you are returned to the Edit Judgment Policy (Judgments for PC security settings) window.

### 6.7.5 Defining anonymous connection settings

To define judgment items relating to anonymous connections in the Edit Judgment Policy (Judgments for PC security settings) window:

1. In the Edit Judgment Policy (Judgments for PC security settings) window, select the **Make this a judgment target** check box.

The items in the Edit Judgment Policy (Judgments for PC security settings) window are activated.

2. In the Edit Judgment Policy (Judgments for PC security settings) window, select **Anonymous connections** and then click the **Definition** button, or double-click **Anonymous connections**.

The Anonymous Connection Settings dialog box appears.



3. Define the judgment conditions and security levels for anonymous connection settings.

The following table describes the setting items.

*Table 6-21:* Setting items in the Anonymous Connection Settings dialog box

No.	Window item name		Judgment conditions and description	Default
1	<b>Make this a judgment target</b>		Select whether to make <b>Restriction of anonymous connections</b> a target for security level judgment.	Off
2	<b>Restriction of anonymous connections</b>	<b>Condition for judging PC insecure</b>	Anonymous connections are not restricted.	--
3		<b>Security level</b>	Select a security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	<b>Warning</b>

No.	Window item name		Judgment conditions and description	Default
4		<b>Judgment if item is not applicable</b>	From the pull-down menu, select the desired behavior when the judgment item does not exist. The following options are available: <ul style="list-style-type: none"> <li>• <b>Set security level</b></li> <li>• <b>Safe</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Unknown</b></li> </ul>	<b>Not applicable</b>

Legend:

--: N/A

4. Click the **OK** button.

The Anonymous Connection Settings dialog box closes, and you are returned to the Edit Judgment Policy (Judgments for PC security settings) window.

### 6.7.6 Defining service settings

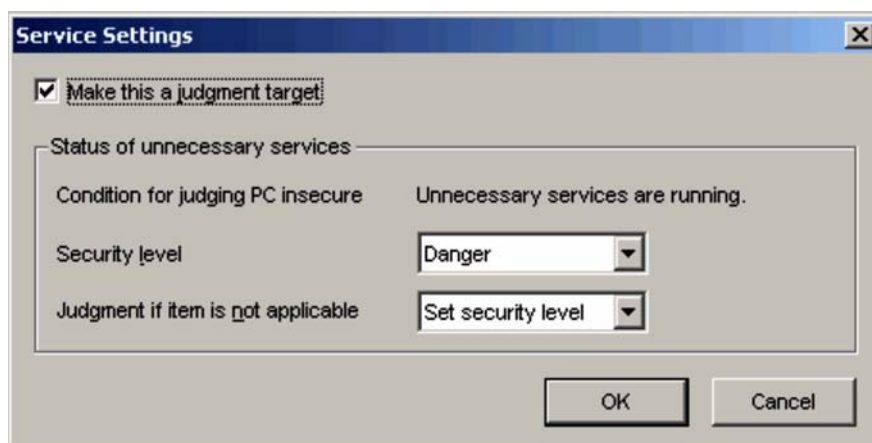
To define service-related judgment items in the Edit Judgment Policy (Judgments for PC security settings) window:

1. In the Edit Judgment Policy (Judgments for PC security settings) window, select the **Make this a judgment target** check box.

The items in the Edit Judgment Policy (Judgments for PC security settings) window are activated.

2. In the Edit Judgment Policy (Judgments for PC security settings) window, select **Services** and then click the **Definition** button, or double-click **Services**.

The Service Settings dialog box appears.



3. Define the judgment conditions and security levels for services.

The following table describes the setting items.

*Table 6-22: Setting items in the Service Settings dialog box*

No.	Window item name		Judgment conditions and description	Default
1	Make this a judgment target		Select whether to make <b>Status of unnecessary services</b> a target for security level judgment.	Off
2	Status of unnecessary services	Condition for judging PC insecure	Unnecessary services are running.	--
3		Security level	Select a security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	<b>Warning</b>

No.	Window item name		Judgment conditions and description	Default
4		<b>Judgment if item is not applicable</b>	From the pull-down menu, select the desired behavior when the judgment item does not exist. The following options are available: <ul style="list-style-type: none"> <li>• <b>Set security level</b></li> <li>• <b>Safe</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Unknown</b></li> </ul>	<b>Not applicable</b>

Legend:

--: N/A

4. Click the **OK** button.

The Service Settings dialog box closes, and you are returned to the Edit Judgment Policy (Judgments for PC security settings) window.

### 6.7.7 Defining firewall settings

To define firewall-related judgment items in the Edit Judgment Policy (Judgments for PC security settings) window:

1. In the Edit Judgment Policy (Judgments for PC security settings) window, select the **Make this a judgment target** check box.

The items in the Edit Judgment Policy (Judgments for PC security settings) window are activated.

2. In the Edit Judgment Policy (Judgments for PC security settings) window, select **Firewall** and then click the **Definition** button, or double-click **Firewall**.

The Firewall Settings dialog box appears.



3. Define the judgment conditions and security levels for firewall settings.

The following table describes the setting items.

*Table 6-23: Setting items in the Firewall Settings dialog box*

No.	Window item name		Judgment conditions and description	Default
1	<b>Make this a judgment target</b>		Select whether to make <b>Windows Firewall settings</b> a target for security level judgment.	Off
2	<b>Windows Firewall settings</b>	<b>Condition for judging PC insecure</b>	From the pull-down menu, select the condition for judging the PC insecure. The following options are available: <ul style="list-style-type: none"> <li><b>Windows Firewall is disabled</b></li> <li><b>Windows Firewall is disabled or allows exceptions</b></li> </ul>	<b>Windows Firewall is disabled</b>
3		<b>Security level</b>	Select a security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li><b>Caution</b></li> <li><b>Warning</b></li> <li><b>Danger</b></li> </ul>	<b>Warning</b>

No.	Window item name		Judgment conditions and description	Default
4		<b>Judgment if item is not applicable</b>	From the pull-down menu, select the desired behavior when the judgment item does not exist. The following options are available: <ul style="list-style-type: none"> <li>• <b>Set security level</b></li> <li>• <b>Safe</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Unknown</b></li> </ul>	<b>Not applicable</b>

- Click the **OK** button.

The Firewall Settings dialog box closes, and you are returned to the Edit Judgment Policy (Judgments for PC security settings) window.

### 6.7.8 Defining automatic update settings

To define judgment items relating to automatic updates in the Edit Judgment Policy (Judgments for PC security settings) window:

- In the Edit Judgment Policy (Judgments for PC security settings) window, select the **Make this a judgment target** check box.

The items in the Edit Judgment Policy (Judgments for PC security settings) window are activated.

- In the Edit Judgment Policy (Judgments for PC security settings) window, select **Automatic updates** and then click the **Definition** button, or double-click **Automatic updates**.

The Automatic Update Settings dialog box appears.





3. Define the judgment conditions and security levels for automatic updates.  
The following table describes the setting items.

*Table 6-24: Setting items in the Automatic Update Settings dialog box*

No.	Window item name		Judgment conditions and description	Default
1	<b>Make this a judgment target</b>		Select whether to make <b>Settings for Windows automatic updates</b> a target for security level judgment.	Off
2	<b>Settings for Windows automatic updates</b>	<b>Condition for judging PC insecure</b>	Automatic updating is disabled.	--
3		<b>Security level</b>	Select a security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	<b>Warning</b>

No.	Window item name		Judgment conditions and description	Default
4		<b>Judgment if item is not applicable</b>	From the pull-down menu, select the desired behavior when the judgment item does not exist. The following options are available: <ul style="list-style-type: none"> <li>• <b>Set security level</b></li> <li>• <b>Safe</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Unknown</b></li> </ul>	<b>Not applicable</b>

Legend:

--: N/A

4. Click the **OK** button.

The Automatic Update Settings dialog box closes, and you are returned to the Edit Judgment Policy (Judgments for PC security settings) window.

### 6.7.9 Defining screensaver settings

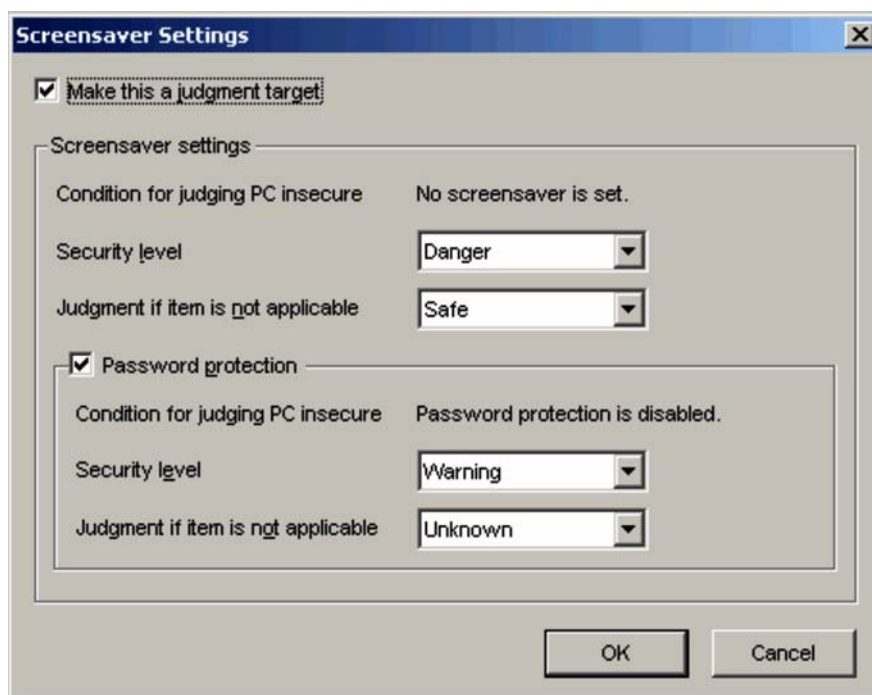
To define screensaver-related judgment items in the Edit Judgment Policy (Judgments for PC security settings) window:

1. In the Edit Judgment Policy (Judgments for PC security settings) window, select the **Make this a judgment target** check box.

The items in the Edit Judgment Policy (Judgments for PC security settings) window are activated.

2. In the Edit Judgment Policy (Judgments for PC security settings) window, select **Screensaver** and then click the **Definition** button, or double-click **Screensaver**.

The Screensaver Settings dialog box appears.



3. Define the judgment conditions and security levels for screensaver settings.  
The following table describes the setting items.

Table 6-25: Setting items in the Screensaver Settings dialog box

No.	Window item name		Judgment conditions and description	Default
1	Make this a judgment target		Select whether to make <b>Screensaver settings</b> and <b>Password protection</b> targets for security level judgment.	Off
2	Screensaver settings	Condition for judging PC insecure	No screensaver is set.	--
3		Security level	Select a security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	<b>Caution</b>

No.	Window item name		Judgment conditions and description	Default
4		<b>Judgment if item is not applicable</b>	From the pull-down menu, select the desired behavior when the judgment item does not exist. The following options are available: <ul style="list-style-type: none"> <li>• <b>Set security level</b></li> <li>• <b>Safe</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Unknown</b></li> </ul>	<b>Not applicable</b>
5	<b>Password protection<sup>#</sup></b>	--	Select this check box to judge whether the screensaver is password-protected.	On
6		<b>Condition for judging PC insecure</b>	Password protection is disabled.	--
7		<b>Security level</b>	Select a security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	<b>Caution</b>
8		<b>Judgment if item is not applicable</b>	From the pull-down menu, select the desired behavior when the judgment item does not exist. The following options are available: <ul style="list-style-type: none"> <li>• <b>Set security level</b></li> <li>• <b>Safe</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Unknown</b></li> </ul>	<b>Not applicable</b>

Legend:

--: N/A

#

The items under **Password protection** are activated when the **Make this a judgment target** check box is selected.

- Click the **OK** button.

The Screensaver Settings dialog box closes, and you are returned to the Edit Judgment Policy (Judgments for PC security settings) window.

### 6.7.10 Defining drive encryption

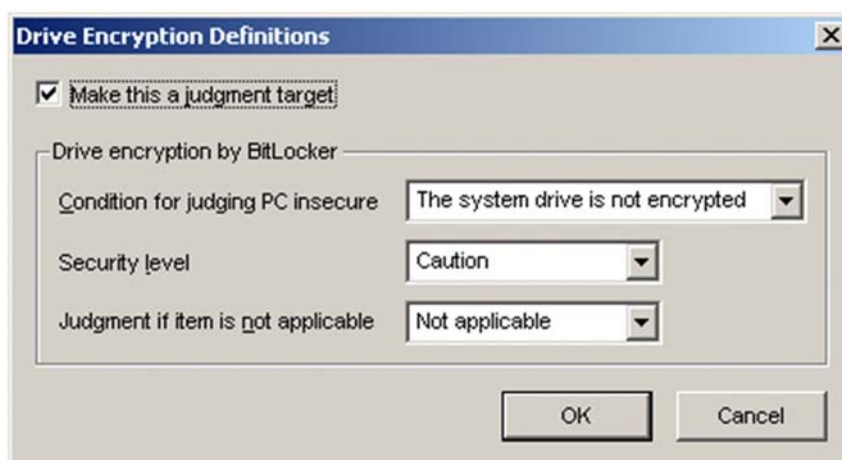
To define judgment items related to drive encryption in the Edit Judgment Policy (Judgments for PC security settings) window:

1. In the Edit Judgment Policy (Judgments for PC security settings) window, select the **Make this a judgment target** check box.

All items in the Edit Judgment Policy (Judgments for PC security settings) window are activated.

2. In the Edit Judgment Policy (Judgments for PC security settings) window, either click **Drive encryption** and then click the **Definition** button, or double-click **Drive encryption**.

The Drive Encryption Definitions dialog box appears.



3. Define the judgment conditions and security levels for the drive encryption definition.

The following table describes the setting items.

*Table 6-26: Setting items in the Drive Encryption Definitions dialog box*

No.	Window item name	Judgment conditions and description	Default
1	<b>Make this a judgment target</b>	Select whether to make the information defined in <b>Drive encryption settings</b> a target for security level judgment.	Off

No.	Window item name		Judgment conditions and description	Default
2	Drive encryption by BitLocker	Condition for judging PC insecure	From the pull-down menu, select the condition for judging that a client PC is insecure. The following options are available: <ul style="list-style-type: none"> <li>• The system drive is not encrypted</li> <li>• A drive is not encrypted</li> </ul>	The system drive is not encrypted
3		Security level	Select a security level from the pull-down menu. The following options are available: <ul style="list-style-type: none"> <li>• Caution</li> <li>• Warning</li> <li>• Danger</li> </ul>	Caution
4		Judgment if item is not applicable	From the pull-down menu, select the desired behavior if the judgment item does not exist. The following options are available: <ul style="list-style-type: none"> <li>• Set security level</li> <li>• Safe</li> <li>• Not applicable</li> <li>• Unknown</li> </ul>	Not applicable

4. Click the **OK** button.

The Drive Encryption Definitions dialog box closes, and you are returned to the Edit Judgment Policy (Judgments for PC security settings) window.

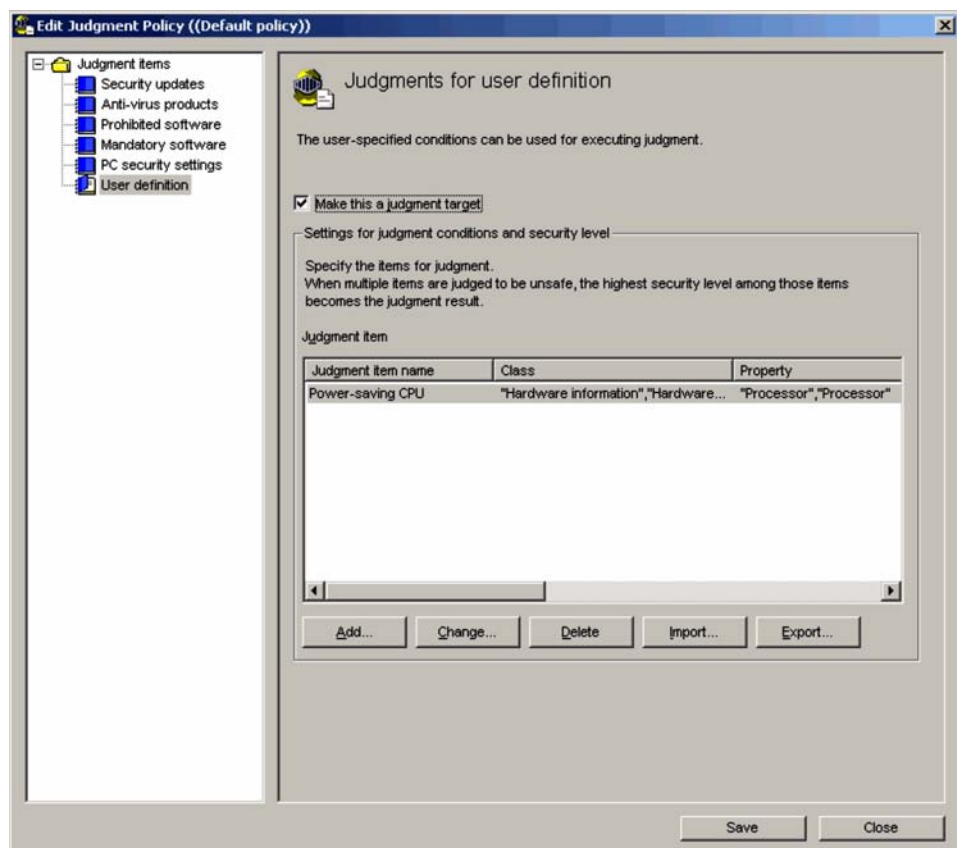
## 6.8 Editing a user-defined judgment policy

The Edit Judgment Policy (Judgments for user definition) window can be used to set user-specific judgment items about client asset information stored in the asset management database of AIM, as well as the client security level when such items are not implemented on the client. For example, you can judge whether the client is running a power-saving CPU or whether automatic logon is enabled.

To display the Edit Judgment Policy (Judgments for user definition) window, from the judgment items tree view in the Edit Judgment Policy window, select **User definition**.

The Edit Judgment Policy (Judgments for user definition) window is shown below.

*Figure 6-15: Edit Judgment Policy (Judgments for user definition) window*



The items to be set in the Edit Judgment Policy (Judgments for user definition) window are as follows:

### **Make this a judgment target**

Select the check box to make the user definition a judgment policy target. When the check box is selected, all window items are available. The check box is cleared by default.

### **Judgment item**

Set the judgment items.

Use the Edit Judgment Policy (Judgments for user definition) window as follows:

1. Select the **Make this a judgment target** check box.

All items in the Edit Judgment Policy (Judgments for user definition) window are available.

2. Set the judgment items.

You can add, change, and delete judgment items. You can also import and export judgment item information in a CSV file. Click the appropriate button, and then edit the information in the displayed dialog box.

3. When editing operations are complete, in the Edit Judgment Policy (Judgments for user definition) window, click the **Save** button.

The set contents are saved as a judgment policy.

#### *Reference note:*

A warning message may appear when you click the **Save** button. Read the message, and review your settings if necessary. Click the **OK** button to save the settings, or the **Cancel** button to discard them.

#### *Note:*

If you intend to count statistics for user-specific judgment items, note the following when editing a judgment policy:

- You can count statistics for no more than 10 judgment items. When a judgment policy includes 11 or more judgment items, statistics are counted only for the first 10 items, in order from the first to be defined.
- If you delete a judgment item after executing the statistics storage command, or change the order of the judgment items, the statistics for user-defined judgment items may not be counted correctly.
- If you specify multiple judgment policies, the user-defined judgment items must be arranged in the same order in each judgment policy.



The following table lists the names of the dialog boxes and message boxes displayed when the corresponding buttons are clicked in the Edit Judgment Policy (Judgments for user definition) window.

*Table 6-27:* Names of the dialog boxes and message boxes displayed from the Edit Judgment Policy (Judgments for user definition) window

No.	Button	Dialog box name or message box name
1	<b>Add</b>	Add (judgment item information) dialog box
2	<b>Change</b>	Update (judgment item information) dialog box
3	<b>Delete</b>	Delete (judgment item information) message box
4	<b>Import</b>	Import (judgment item information) dialog box
5	<b>Export</b>	Export (judgment item information) dialog box

The following explains the procedures for adding, changing, deleting, importing, and exporting information.

### 6.8.1 Adding a judgment item to a user definition

To add a judgment item to a user definition in the Edit Judgment Policy (Judgments for user definition) window:

1. In the Edit Judgment Policy (Judgments for user definition) window, click the **Add** button.

The Add (judgment item information) dialog box appears.

**Add (judgment item information)**

Judgment item information

Judgment item name: Power-saving CPU

Specify the judgment condition for this item.  
The security level will be set when all the judgment conditions exist.

Judgment condition

Class	Property	Comparison condition
Hardware information	Processor	Do not match
Hardware information	Processor	Do not match

Add... Change... Delete

Security level: Caution

OK Cancel

2. Enter the name of the judgment item.  
Type the judgment item name as a character string of no more than 255 bytes. This item is mandatory.
3. Define the user-defined judgment condition.  
Add, delete, or change the judgment condition. Click the appropriate button, and then edit the information in the displayed dialog box.
4. Select a security level.  
Select a security level from the pull-down menu. The default is **Caution**.
5. Click the **OK** button.  
The Add (judgment item information) dialog box closes, and you are returned to the Edit Judgment Policy (Judgments for user definition) window.

The following table lists the names of the dialog boxes and message boxes displayed when the corresponding buttons are clicked in the Add (judgment item information) dialog box.

*Table 6-28:* Names of the dialog boxes and message boxes displayed from the Add (judgment item information) dialog box

No.	Button	Dialog box name or message box name
1	<b>Add</b>	Add (judgment condition) dialog box
2	<b>Change</b>	Update (judgment condition) dialog box
3	<b>Delete</b>	Delete (judgment condition) message box

The following explains the procedures for adding, changing, or deleting a user-defined judgment condition, and describes how to set judgment conditions for these items.

### (1) Adding a user-defined judgment condition

To add a user-defined judgment condition:

1. In the Add (judgment item information) dialog box, click the **Add** button.

The Add (judgment condition) dialog box appears.

2. Enter the user-defined judgment condition.

The following table lists the items to set.

Table 6-29: Setting items for the Add (judgment condition) dialog box

No.	Window item name		Description	Default
1	<b>Class</b>		From the drop-down lists, select the class and property containing the information to be used in judging the user definition. For the available options, see Table 6-30 <i>List of classes and properties that can be used in user-defined judgments</i> . These items are mandatory.	<b>Asset information</b>
2	<b>Property</b>			<b>User property Area-1</b>
3	<b>Comparison condition</b>	Numeric property	Select a comparison condition from the pull-down menu. Four options are available: <ul style="list-style-type: none"> <li>• <b>Match</b></li> <li>• <b>Do not match</b></li> <li>• <b>Not greater than</b></li> <li>• <b>Not less than</b></li> </ul>	<b>Match</b>
		String property	Select a comparison condition from the pull-down menu. Seven options are available: <ul style="list-style-type: none"> <li>• <b>Match all the words</b></li> <li>• <b>Match part of the words</b></li> <li>• <b>Match beginning of the words</b></li> <li>• <b>Match end of the words</b></li> <li>• <b>Do not match</b></li> <li>• <b>Not greater than</b></li> <li>• <b>Not less than</b></li> </ul>	<b>Match all the words</b>
		Date/time property	Select a comparison condition from the pull-down menu. Four options are available: <ul style="list-style-type: none"> <li>• <b>Match</b></li> <li>• <b>Do not match</b></li> <li>• <b>Not greater than</b></li> <li>• <b>Not less than</b></li> </ul>	<b>Match</b>
4	<b>Comparison value</b>	Numeric property	Type a numeric value to compare with the property. You can enter a positive number of 1 to 19 digits, or a negative number of no more than 20 digits beginning with a hyphen (-). A value must be set.	--

No.	Window item name		Description	Default
		String property	Type a character string to compare with the property. Enter any string (other than a line feed code) no larger than the property size. For details about property sizes, see Table 6-30 <i>List of classes and properties that can be used in user-defined judgments</i> . A value must be set.	--
		Date/time property	Set one or more of the following items to compare with the property: Year: 1 to 9999 Month: 1 to 12 Day: 1 to 31 Hour: 0 to 23 Minute: 0 to 59 Second: 0 to 59	Time at which the Add (judgment condition) dialog box was opened.
5	<b>Treatment when value is not set for property</b>		Select <b>Treatment when value is not set for property</b> from the pull-down menu. Four options are available: <ul style="list-style-type: none"> <li>• <b>Treat the judgment condition as met</b></li> <li>• <b>Treat the judgment condition as not met</b></li> <li>• <b>Do not judge this condition</b></li> <li>• <b>Treat the security level as unknown</b></li> </ul>	<b>Treat the security level as unknown</b>

Legend:

--: No default provided.

*Note:*

- You cannot add a judgment condition that duplicates the class, property, comparison condition, and comparison value of another judgment condition.
- You cannot add a judgment condition that duplicates the class, property, and comparison condition (other than **Match part of the words**) of another judgment condition.
- You cannot add a judgment condition that duplicates the class, property, and comparison value (other than a value for **Match beginning of the words** or **Match end of the words** for a string property) of another judgment condition.

The display items in the Add (judgment condition) dialog box depend on the type of property. For property types, see Table 6-30 *List of classes and properties that can be used in user-defined judgments*.

Figure 6-16: Property of numeric type

The screenshot shows a dialog box titled "Add (judgment condition)". It contains the following fields and options:

- Judgment condition** (grouped label):
  - Class**: A dropdown menu with "Asset information" selected.
  - Property**: A dropdown menu with "User property Uint-1" selected.
  - Comparison condition**: A dropdown menu with "Match" selected.
  - Comparison value (number)**: A text input field containing "1234".
- Treatment when value is not set for property**: A dropdown menu with "Treat the security level as unknown" selected.
- Buttons**: "OK" and "Cancel" buttons at the bottom right.

Figure 6-17: Property of string type

The screenshot shows the 'Add (judgment condition)' dialog box. It has a title bar with a close button. The main area is titled 'Judgment condition' and contains four fields: 'Class' (Asset information), 'Property' (User property Area-2), 'Comparison condition' (Match all the words), and 'Comparison value (string)' (NG). Below these fields is a section titled 'Treatment when value is not set for property' with a dropdown menu set to 'Treat the security level as unknown'. At the bottom right are 'OK' and 'Cancel' buttons.

Figure 6-18: Property of date/time type

The screenshot shows the 'Add (judgment condition)' dialog box for a date/time type property. It has a title bar with a close button. The main area is titled 'Judgment condition' and contains four fields: 'Class' (Asset information), 'Property' (User property Date-1), 'Comparison condition' (Not greater than), and 'Comparison value (date)'. The date field is set to 2006 year 6 month 30 day 23 : 59 : 59. Below these fields is a section titled 'Treatment when value is not set for property' with a dropdown menu set to 'Treat the security level as unknown'. At the bottom right are 'OK' and 'Cancel' buttons.

The table below lists the classes and properties that can be used in the user-defined judgment.

*Table 6-30:* List of classes and properties that can be used in user-defined judgments

<b>Asset information name (Class)</b>	<b>Property name</b>	<b>Property display name<sup>#</sup></b>	<b>Type</b>	<b>Size (bytes)</b>
Asset information (AssetInfo)	AssetID	Asset ID	Numeric	10
	AssetKind	Asset type	String	3
	AssetNo	Asset No.	String	60
	AssetStatus	Status	String	3
	AssetWorkKind	Usage management	String	3
	DMLastUpdateTime	Inventory last update date/time	Date/time	8
	DMStatus	SD installed status	String	3
	EndDate	End date of use	Date/time	8
	GroupID	Group ID	String	64
	GroupName	Group name	String	512
	HrdInvUpdateDate	Update date of System information	Date/time	8
	InsPkgUpdateDate	Update date of installed package information	Date/time	8
	InventoryKey	Assignment key	String	128
	LocationID	Location ID	String	64
	LocationName	Location name	String	512
	ManagerialGroup	Managed group	String	512
	ManagerialGroupID	Managed group ID	String	64
	ManagerialUser	Administrator	String	255
	ManagerialUserID	User ID of administrator	String	64
	NNMUpdateDate	Update date of NNM	Date/time	8
	Note	Notes	String	255



Asset information name (Class)	Property name	Property display name <sup>#</sup>	Type	Size (bytes)
	PurchasePrice	Purchase price	String	15
	Purpose	Purpose	String	255
	RegistrationDate	Reg. date	Date/time	8
	SoftInvUpdateDate	Update date of Software inventory information	Date/time	8
	SoftwareStatus	Software status	String	3
	StartDate	Start date of use	Date/time	8
	StocktakingDate	Stocktaking date	Date/time	8
	UpdateUser	Update user name	String	255
	UserID	User ID	String	64
	UserName	User name	String	255
	UserPropertyArea_ <i>n</i> ( <i>n</i> is 1-2)	User property Area- <i>n</i> ( <i>n</i> is 1-2)	String	255
	UserPropertyCode_ <i>n</i> ( <i>n</i> is 1-6)	User property Code- <i>n</i> ( <i>n</i> is 1-6)	String	64
	UserPropertyDate_ <i>n</i> ( <i>n</i> is 1-6)	User property Date- <i>n</i> ( <i>n</i> is 1-6)	Date/time	8
	UserPropertyField128_ <i>n</i> ( <i>n</i> is 1-2)	User property Field 128- <i>n</i> ( <i>n</i> is 1-2)	String	128
	UserPropertyField255_ <i>n</i> ( <i>n</i> is 1-2)	User property Field 255- <i>n</i> ( <i>n</i> is 1-2)	String	255
	UserPropertyField32_ <i>n</i> ( <i>n</i> is 1-6)	User property Field 32- <i>n</i> ( <i>n</i> is 1-6)	String	32
	UserPropertyField64_ <i>n</i> ( <i>n</i> is 1-2)	User property Field 64- <i>n</i> ( <i>n</i> is 1-2)	String	64
	UserPropertyUint_ <i>n</i> ( <i>n</i> is 1-6)	User property Uint- <i>n</i> ( <i>n</i> is 1-6)	Numeric	10
	UsrInvUpdateDate	Update date of user inventory information	Date/time	8

<b>Asset information name (Class)</b>	<b>Property name</b>	<b>Property display name<sup>#</sup></b>	<b>Type</b>	<b>Size (bytes)</b>
Hardware information (HardwareInfo)	AssetID	Asset ID	Numeric	10
	CircuitSpeed	Line speed	Numeric	10
	ComputerID	Computer ID	String	200
	CPUClock	Processor speed	Numeric	10
	CPUNumber	Number of processors	Numeric	5
	CPUType	Processor	String	5
	Developer	Developer	String	60
	HostName	Host name	String	64
	IPAddress	IP address	String	15
	MACAddress	MAC address	String	17
	MachineKind	Device type	String	5
	MBSAVersion	MBSA version	String	200
	MemorySize	Memory	Numeric	19
	Model	Model	String	60
	ModelKind	Composition	String	3
	MonitorKind	Monitor type	String	3
	MonitorResolution	Monitor resolution	String	3
	MonitorSize	Monitor size	Numeric	5
	Name	Device name	String	255
	NNMSelectionName	NNM selection name	String	255
	NumberOfPort	Number of ports	Numeric	10
	OSInfo	OS	String	200
	OSVersion	OS version	String	200
	RemainHDSpace	Hard drive free space	Numeric	19
	SerialNo	Serial No.	String	30

Asset information name (Class)	Property name	Property display name <sup>#</sup>	Type	Size (bytes)
	Specification	Specification	String	255
	TotalHDSIZE	Hard drive sizes	Numeric	19
	UserPropertyArea_ <i>n</i> ( <i>n</i> is 1-4)	User property Area- <i>n</i> ( <i>n</i> is 1-4)	String	255
	UserPropertyCode_ <i>n</i> ( <i>n</i> is 1-12)	User property Code- <i>n</i> ( <i>n</i> is 1-12)	String	64
	UserPropertyDate_ <i>n</i> ( <i>n</i> is 1-6)	User property Date- <i>n</i> ( <i>n</i> is 1-6)	Date/time	8
	UserPropertyField128_ <i>n</i> ( <i>n</i> is 1-8)	User property Field 128- <i>n</i> ( <i>n</i> is 1-8)	String	128
	UserPropertyField255_ <i>n</i> ( <i>n</i> is 1-8)	User property Field 255- <i>n</i> ( <i>n</i> is 1-8)	String	255
	UserPropertyField32_ <i>n</i> ( <i>n</i> is 1-8)	User property Field 32- <i>n</i> ( <i>n</i> is 1-8)	String	32
	UserPropertyField64_ <i>n</i> ( <i>n</i> is 1-8)	User property Field 64- <i>n</i> ( <i>n</i> is 1-8)	String	64
	UserPropertyUint_ <i>n</i> ( <i>n</i> is 1-6)	User property Uint- <i>n</i> ( <i>n</i> is 1-6)	Numeric	10

#

The above property display names are the defaults. You can modify these display names in the Customize Managed Items window of AIM (by choosing **System Definition** and then **Customize Managed Items** in the job menu). For details about the Customize Managed Items window, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

*Note:*

Information about the properties that can be specified in user-defined judgment conditions must be set in advance. Use the Assign Inventory window of AIM (choose **System Definition** and then **Assign Inventory** in the job menu) or use the `jamimport` command (import command for reading asset information as a batch to the asset management database from a CSV file).

For details about assigning inventory information and about the `jamimport` command, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

3. Click the **OK** button.

The Add (judgment condition) dialog box closes and you are returned to the Add (judgment item information) dialog box. The entered judgment condition is added to the list.

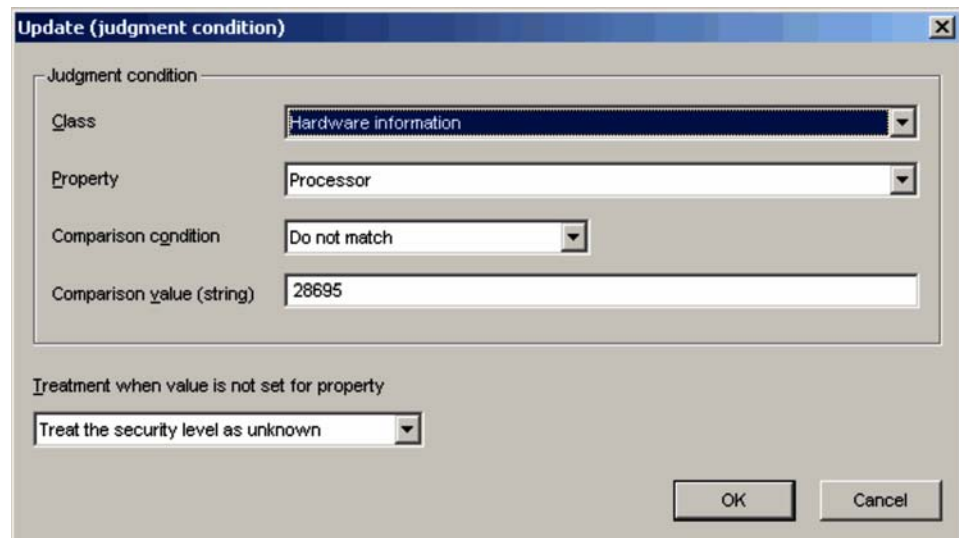
## **(2) Changing a user-defined judgment condition**

To change a user-defined judgment condition:

1. In the Add (judgment item information) dialog box, select a user-defined judgment condition you want to change, and then click the **Change** button. Alternatively, double-click the user-defined judgment condition you want to change.

The Update (judgment condition) dialog box appears.

Note that the **Change** button is disabled if you select multiple user-defined judgment conditions.



The dialog box titled "Update (judgment condition)" contains the following fields:

- Judgment condition:**
  - Class:** Hardware information (dropdown menu)
  - Property:** Processor (dropdown menu)
  - Comparison condition:** Do not match (dropdown menu)
  - Comparison value (string):** 28695 (text field)
- Treatment when value is not set for property:** Treat the security level as unknown (dropdown menu)

Buttons: OK, Cancel

2. Change the user-defined judgment condition.

*Note:*

- You cannot change a judgment condition to one that duplicates the class, property, comparison condition, and comparison value of another judgment condition.
- You cannot change a judgment condition to one that duplicates the class, property, and comparison condition (other than **Match part of the words** or **Do not match**) of another judgment condition.
- You cannot change a judgment condition to one that duplicates the class, property, and comparison value (other than a value for **Match beginning of the words** or **Match end of the words** for a string property) of another judgment condition.

3. Click the **OK** button.

The Update (judgment condition) dialog box closes and you are returned to the Add (judgment item information) dialog box. The entered judgment condition is changed.

**(3) Deleting a user-defined judgment condition**

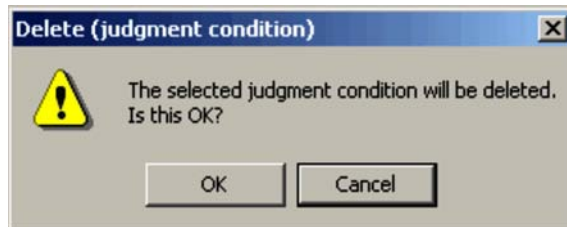
To delete a user-defined judgment condition:

1. In the Add (judgment item information) dialog box, click to select the user-defined judgment condition you want to delete.

You can select multiple user-defined judgment conditions.

2. Click the **Delete** button.

The Delete (judgment condition) message box appears.



3. Click the **OK** button if you are sure you want to delete the judgment condition.

The Delete (judgment condition) message box closes and you are returned to the Add (judgment item information) dialog box. The selected judgment condition is deleted.

**(4) Example of setting a judgment condition judging client compliance with power-saving initiatives**

By setting a user-defined judgment condition based on asset information of a client, you can judge whether the client is complying with power-saving initiatives.

**(a) Checking whether a power-saving CPU is present**

The following table shows an example of setting a judgment condition for checking whether the client has a power-saving CPU.

*Table 6-31:* Example of setting a judgment condition for checking whether a power-saving CPU is present

No.	Item	Setting value
1	Class	<b>Hardware information</b>
2	Property	<b>CPU</b>
3	Comparison condition	<b>Do not match</b>
4	Comparison value (string)	Type code for the power-saving CPU <sup>#</sup>

No.	Item	Setting value
5	Treatment when a value is not set for the property	<b>Treat the security level as unknown</b>

#

You can specify more than one CPU type by setting multiple judgment conditions.

For details about the type codes that identify different CPU types, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

#### (b) Checking whether automatic power-off is enabled for the monitor

The following table shows an example of setting a judgment condition for checking whether client monitor power is turned off after a certain length of time (10 minutes). Note that this judgment requires JP1/Software Distribution Client 08-51 or later.

*Table 6-32:* Example of setting a judgment condition for checking whether the monitor is turned off after the time of 10 minutes

No.	Item	Setting value
1	Class	Name of the class to which the following inventory information is to be assigned: If the monitor power is AC: • <b>Turn off monitor (AC)</b> If the monitor power is DC: • <b>Turn off monitor (DC)</b>
2	Property	Name of the property to which the following inventory information is to be assigned: If the monitor power is AC: • <b>Turn off monitor (AC)</b> If the monitor power is DC: • <b>Turn off monitor (DC)</b>
3	Comparison condition	<b>Not less than</b>
4	Comparison value (string)	0000000600 <sup>#</sup>
5	Treatment if a value is not set for the property	<b>Treat the security level as unknown</b>

#

Specify a 10-digit numeric value, in seconds, that indicates the time when the monitor is turned off.

*Reference note:*

As with monitor power judgment, the following items can also be used as judgment conditions for the client power-saving settings. Note, however, that the following items can be used as judgment conditions only if the JP1/Software Distribution Client version is 09-00 or later.

- Time after which the hard disks are turned off
- Time after which the system is placed in standby or sleep status
- Time after which the system hibernates

For details about setting the corresponding judgment conditions, see Table 6-31.

**(c) Checking whether power-saving settings are specified for the CPU (processor)**

The following table shows an example of setting a judgment condition for checking whether the processor power management settings specify power saving. Note that this judgment requires JP1/Software Distribution Client 08-51 or later.

*Table 6-33:* Example of setting a judgment condition for checking whether the processor power management settings specify power saving

No.	Item	Setting value
1	Class	Name of the class to which the following inventory information is to be assigned: If the processor power is AC: • <b>Processor Throttle (AC)</b> If the processor power is DC: • <b>Processor Throttle (DC)</b>
2	Property	Name of the property to which the following inventory information is to be assigned: If the processor power is AC: • <b>Processor Throttle (AC)</b> If the processor power is DC: • <b>Processor Throttle (DC)</b>
3	Comparison condition	<b>Do not match</b>
4	Comparison value (string)	Value to set the processor adjustment you allow <sup>#</sup>
5	Treatment if a value is not set for the property	<b>Treat the security level as unknown</b>

#

To specify more than one value, you must set more than one judgment condition.



The following explains the values you can set:

**NONE:** The processor always runs at its highest performance level.

**ADAPTIVE:** The performance level is selected based on the CPU status.

**DEGRADE:** The processor starts at its lowest performance level, after which its Linear Performance Reduction mechanism (stop clock throttling function) operates governed by the amount of battery discharge.

**CONSTANT:** The processor always runs at its lowest performance level.

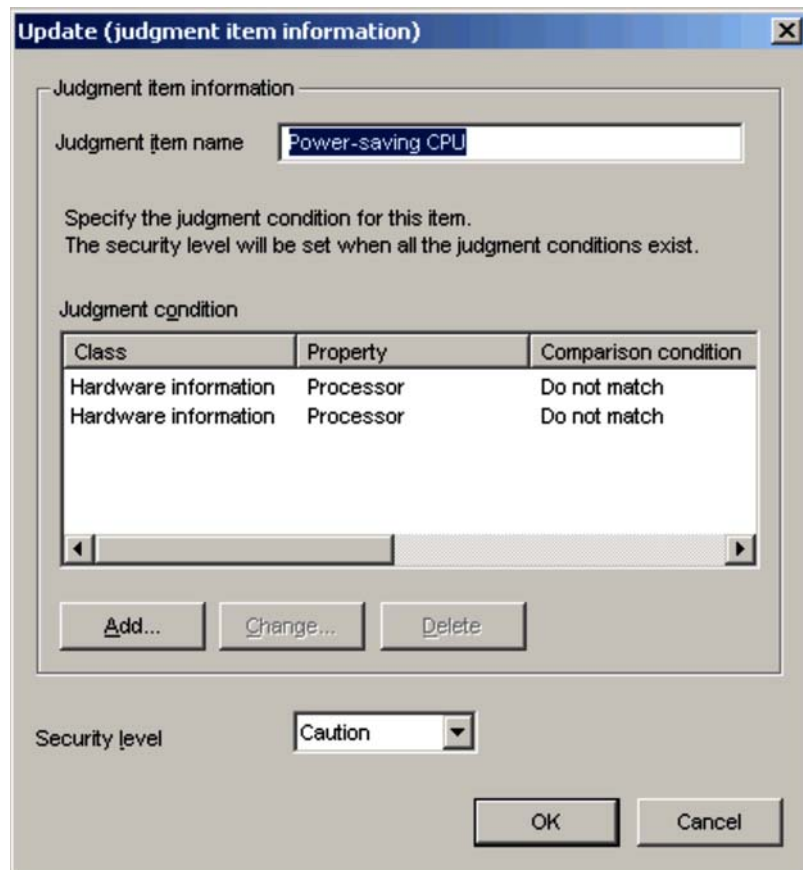
### 6.8.2 Changing a judgment item in a user definition

To change a judgment item in a user definition in the Edit Judgment Policy (Judgments for user definition) window:

1. In the Edit Judgment Policy (Judgments for user definition) window, click the judgment item you want to change and click the **Change** button. Alternatively, double-click the user-defined judgment item you want to change.

The Update (judgment item information) dialog box appears.

Note that the **Change** button is disabled if you select multiple user-defined judgment items.



**Update (judgment item information)**

Judgment item information

Judgment item name:

Specify the judgment condition for this item.  
The security level will be set when all the judgment conditions exist.

Judgment condition

Class	Property	Comparison condition
Hardware information	Processor	Do not match
Hardware information	Processor	Do not match

Security level:

2. Enter a new name for the judgment item.  
Type the judgment item name as a character string of no more than 255 bytes. This item is mandatory.
3. Define the user-defined judgment condition.  
Add, change, or delete the judgment condition. Click the appropriate button, and then edit the information in the displayed dialog box.
4. Select a security level.  
Select a security level from the pull-down menu.
5. Click the **OK** button.  
The Update (judgment item information) dialog box closes and you are returned to the Edit Judgment Policy (Judgments for user definition) window.

The following table lists the names of the dialog boxes and message boxes displayed when the corresponding buttons are clicked in the Update (judgment item information) dialog box.

*Table 6-34: Names of the dialog boxes and message boxes displayed from the Update (judgment item information) dialog box*

No.	Button	Dialog box name or message box name
1	<b>Add</b>	Add (judgment condition) dialog box
2	<b>Change</b>	Update (judgment condition) dialog box
3	<b>Delete</b>	Delete (judgment condition) message box

The procedures for adding, changing, or deleting a user-defined judgment condition in the Update (judgment item information) dialog box are the same as in the Add (judgment item information) dialog box. For details about adding, changing, and deleting judgment conditions, see *6.8.1 Adding a judgment item to a user definition*.

### 6.8.3 Deleting a judgment item in a user definition

To delete a judgment item in a user definition in the Edit Judgment Policy (Judgments for user definition) window:

1. In the Edit Judgment Policy (Judgments for user definition) window, click to select the judgment item you want to delete.

You can select multiple user-defined judgment items.

2. Click the **Delete** button.

The Delete (judgment item information) message box appears.



3. Click the **OK** button if you are sure you want to delete the judgment item.

The Delete (judgment item information) message box closes and you are returned to the Edit Judgment Policy (Judgments for user definition) window. Information about the judgment item you selected is deleted.

### 6.8.4 Importing user-defined judgment items

When setting a large number of user-defined judgment items, an administrator can create a user definition file in CSV format, and import the file.

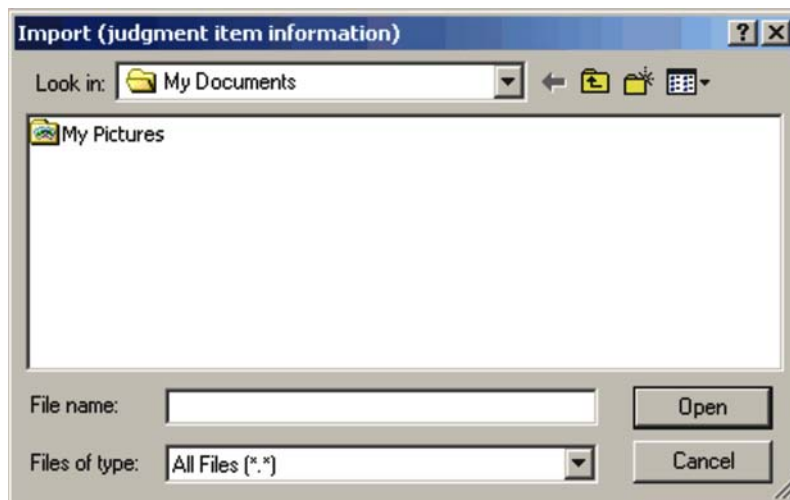
The client security control system provides a sample of a user definition file. The administrator can customize the sample file to create a definition file based on the security objectives and then import it. For details about a sample of this definition file, see *A.4(7) Sample of a user definition file*.

For details about the file format, see *16.2.9 User definition file*.

To import user-defined judgment items:

1. In the Edit Judgment Policy (Judgments for user definition) window, click the **Import** button.

The Import (judgment item information) dialog box appears.



2. Specify **Look in**.

Specify the location of the user definition file to be imported.

3. Specify the name of the user definition file, and then click the **Open** button.

The specified file is read, and the Edit Judgment Policy (Judgments for user definition) window is displayed again.

If the specified file does not contain user-defined information (the file is empty), an error message appears and the import is canceled.

### 6.8.5 Exporting user-defined judgment items

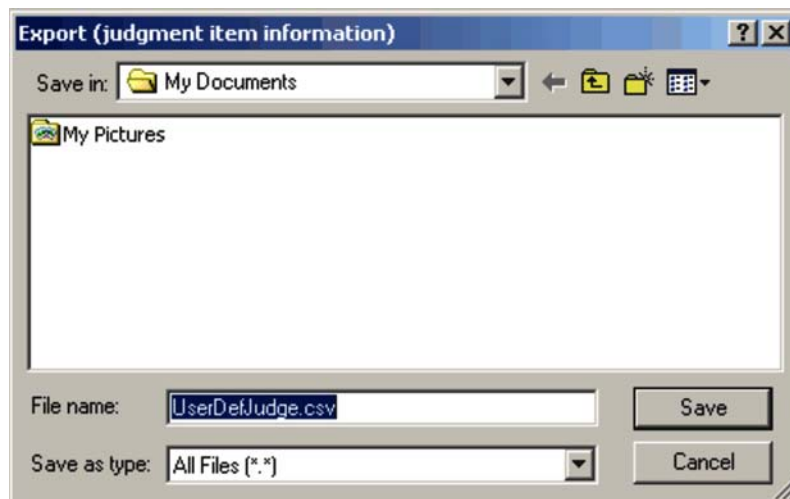
The judgment items in a user definition can be exported to a CSV file.

To export user-defined judgment items:

1. In the Edit Judgment Policy (Judgments for user definition) window, click the **Export** button.

The Export (judgment item information) dialog box appears.

Note that the **Export** button is disabled when no definition has been registered in the Edit Judgment Policy (Judgments for user definition) window.



2. Specify **Save in**.
3. Specify the name of the CSV file to be exported, and click the **Save** button.

The specified file is saved, and the Edit Judgment Policy (Judgments for user definition) window is displayed again.

## 6.9 Managing action policies

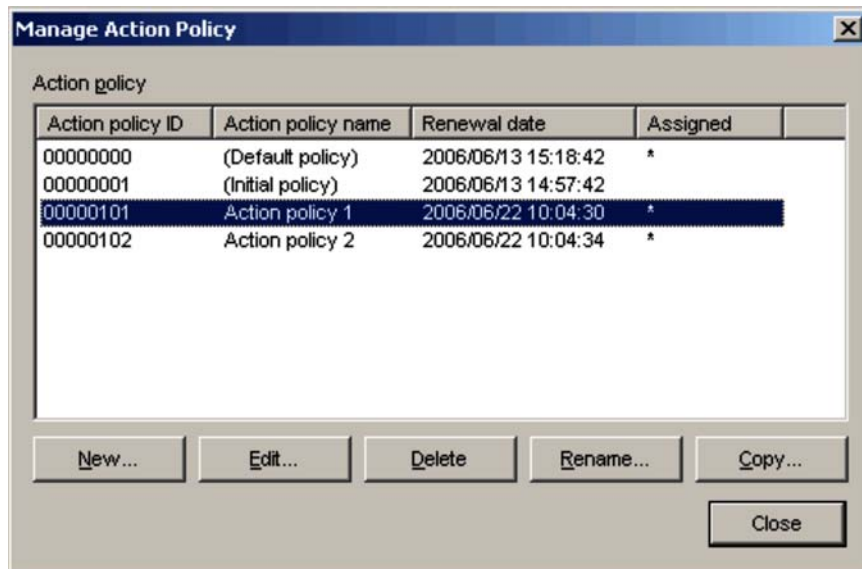
An action policy can be managed in the Manage Action Policy dialog box.

In this dialog box, you can create, edit, delete, rename, and copy action policies.

To open the Manage Action Policy dialog box, in the Policy Management main window choose **Policy** and then **Manage Action Policy**.

The following figure shows the Manage Action Policy dialog box.

Figure 6-19: Manage Action Policy dialog box



The display items and buttons in the Manage Action Policy dialog box are as follows.

### Action policy

Lists information about created action policies, including the ID and name of each policy, latest update time, and whether the policy has been assigned (indicated by an asterisk (\*)) if so. The following two action policies are preset by the system:

No.	Action policy name	Action policy ID	Description
1	Default policy	00000000	A policy initially assigned to every client. You can customize this policy.

No.	Action policy name	Action policy ID	Description
2	Initial policy	00000001	An action policy for saving the default settings. You cannot edit, delete, or rename this policy. By copying the contents of this policy, you can change a modified default policy back to its original contents.

Like clicking the **Edit** button, double-clicking an action policy in the list displays a window for editing the action policy. For details, see *6.9.2 Editing an action policy*.

#### **New** button

Opens the Create New Action Policy dialog box. Use this button to create a new action policy. For details, see *6.9.1 Creating an action policy*.

#### **Edit** button

Opens a window for editing an action policy selected in the list. You can have multiple Edit Action Policy windows open at the same time. Note that the **Edit** button is disabled when multiple action policies are selected in the list. For details, see *6.9.2 Editing an action policy*.

#### **Delete** button

Deletes an action policy selected in the list. You can select multiple action policies. When you delete an assigned action policy, the system assigns the default policy to that client. For details, see *6.9.3 Deleting an action policy*.

#### **Rename** button

Opens the Rename Action Policy dialog box. Use this button to rename an action policy selected in the list. Note that the **Rename** button is disabled when multiple action policies are selected in the list. For details, see *6.9.4 Renaming an action policy*.

#### **Copy** button

Opens the Copy Action Policy dialog box. Use this button to copy the contents of a particular action policy to another action policy.

For details, see *6.9.5 Copying an action policy*.

The operations you can perform depend on the type of policy you select, as shown in the table below.

Table 6-35: Operations that can be performed on each type of policy

No.	Action policy type	Edit	Delete	Rename	Copy
1	Default policy	Yes	No	No	Yes
2	Initial policy	No	No	No	Yes <sup>#</sup>
3	Created action policy	Yes	Yes	Yes	Yes

Legend:

Yes: The operation can be performed.

No: The operation cannot be performed.

#

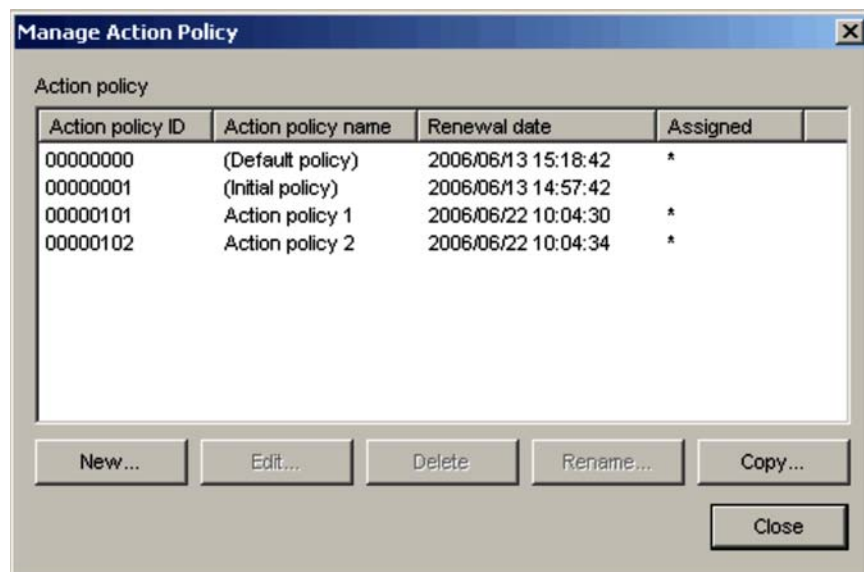
Can be performed only when the initial policy is selected as the copy source, not the copy destination.

### 6.9.1 Creating an action policy

To create a new action policy, follow the steps below. If you use the default policy, this operation is unnecessary.

1. In the Policy Management main window, choose **Policy** and then **Manage Action Policy**.

The Manage Action Policy dialog box appears.





2. Click the **New** button.

The Create New Action Policy dialog box appears.

*Figure 6-20: Create New Action Policy dialog box*

**Create New Action Policy**

Action policy name:

☒ Create a copy from an existing action policy

Action policy for the copy source

Action policy ID	Action policy name	Renewal date	Assigned
00000000	(Default policy)	2006/07/19 18:58:12	*
00000001	(Initial policy)	2006/07/19 18:58:12	
00000101	Action policy 1	2006/07/19 20:44:09	*
00000102	Action policy 2	2006/07/19 20:44:12	*

OK Cancel

The items to set in the Create New Action Policy dialog box are as follows.

#### **Action policy name**

Specify the name of the new action policy as a character string of no more than 128 bytes. You cannot duplicate the name of an existing action policy.

#### **Create a copy from an existing action policy**

Select this check box to create a new action policy based on the initial policy or other existing policy. This check box is selected by default.

#### **Action policy for the copy source**

If you selected the **Create a copy from an existing action policy** check box, select the source action policy from this list.

3. Click the **OK** button.

You are returned to the Manage Action Policy dialog box. The new policy is added to the listed action policies.

## 6.9.2 Editing an action policy

To edit an action policy, follow the steps below. You can set the following items in an action policy:

■ Action items

- Actions for the **Danger** security level
- Actions for the **Warning** security level
- Actions for the **Caution** security level
- Actions for the **Safe** security level

You can set any of the following actions for each security level:

- Notify the administrator by email
- Send a message to the client
- Control client connections to the network
- Implement a user-defined action

■ Customized items

- Customizations for emails sent to administrators
- Customizations for messages sent to client users

Set the type of action to implement for each security level. If you choose to notify the administrator by email or to send a message to the client, you can customize the email or message text as required.

To edit an action policy:

1. Perform either of the following operations.

To edit an action policy selected from the list:

In the Policy Management main window, choose **Policy** and then **Manage Action Policy**. The Manage Action Policy dialog box appears.

From the list of action policies in the dialog box, select the action policy you want to edit and then click the **Edit** button. Alternatively, from the list of action policies in the Manage Action Policy dialog box, double-click the action policy you want to edit.

Note that the **Edit** button is disabled if you select multiple action policies in the list in the Manage Action Policy dialog box.

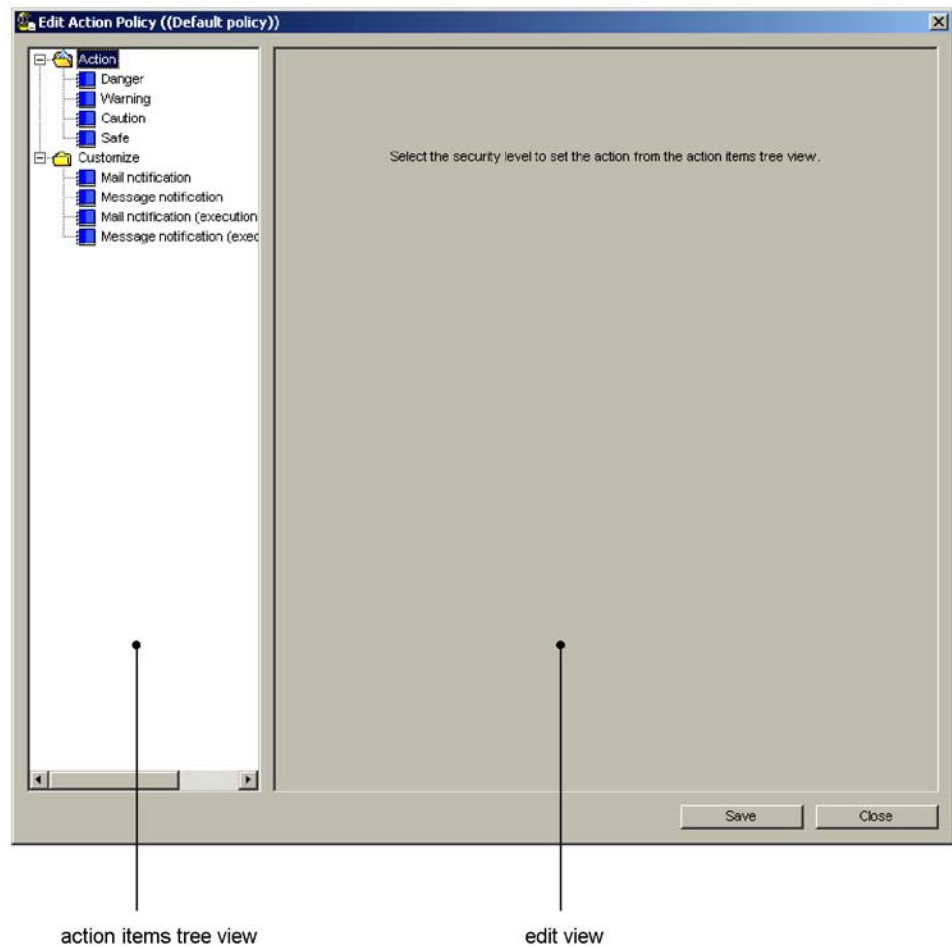
To edit an action policy assigned to a client:

In the Policy Management main window, select a client who has been

assigned the action policy you want to edit. Then choose **Policy** and **Edit Action Policy**.

The Edit Action Policy window appears.

Figure 6-21: Edit Action Policy window



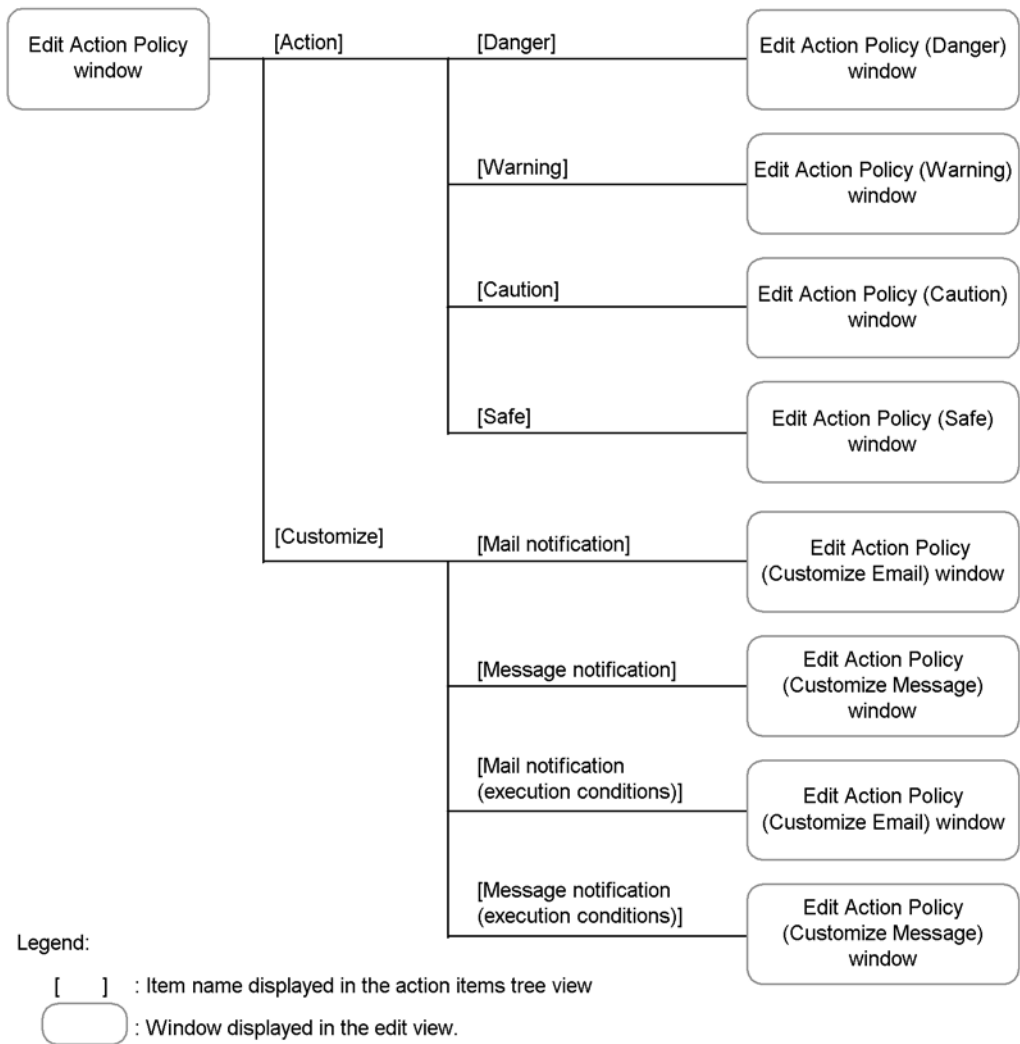
The Edit Action Policy window consists of the *action items tree view* and the *edit view*. When you select an item from the action items tree view, a window for editing the items appears in the edit view.

In the action items tree view, the action items are listed under **Action** and the customize options are listed under **Customize**.

The following figure shows the window transitions for the Edit Action Policy

window.

Figure 6-22: Windows transitions for the Edit Action Policy window



2. In the action items tree view, select an action item or customized item to edit.

An edit window for the selected item appears in the edit view.

For details about editing each action item and customized item, see the following sections:

- To edit an action item

See 6.10 *Setting an action for each security level*.

- To edit a customized item

See 6.11 *Editing an administrator notification email* and 6.12 *Editing a client user notification message*.

*Note:*

You cannot edit the initial policy settings.

### 6.9.3 Deleting an action policy

To delete an action policy:

1. In the Policy Management main window, choose **Policy** and then **Manage Action Policy**.

The Manage Action Policy dialog box appears.

2. In the list of policies in the Manage Action Policy dialog box, select the action policy you want to delete.

You can select multiple action policies.

3. Click the **Delete** button.

A message box asks if you are sure you want to delete the policy.

4. Click the **OK** button in the message box.

The action policy is deleted. If the action policy you selected at step 1 has been assigned to any clients, the default policy will be assigned to those clients.

*Note:*

You cannot delete a default policy or initial policy.

### 6.9.4 Renaming an action policy

To rename an action policy:

1. In the Policy Management main window, choose **Policy** and then **Manage Action Policy**.

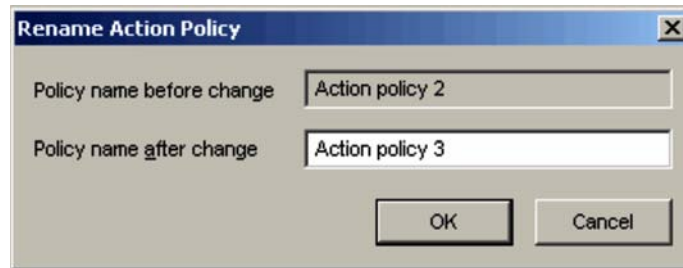
The Manage Action Policy dialog box appears.

2. In the policy list in the Manage Action Policy dialog box, select an action policy to rename and then click the **Rename** button.

The Rename Action Policy dialog box appears.

Note that the **Rename** button is disabled when multiple action policies are selected in the list in the Manage Action Policy dialog box.

Figure 6-23: Rename Action Policy dialog box



3. In the **Policy name after change** box, type the new name as a character string of no more than 128 bytes.
4. Click the **OK** button.

The new policy name is listed in the Manage Action Policy dialog box.

*Note:*

Note these points when renaming an action policy:

- You cannot rename a default policy or initial policy.
- You cannot duplicate the name of an existing action policy, but you can specify the same name as an existing judgment policy.

### 6.9.5 Copying an action policy

To copy an action policy, follow the steps below. This operation writes the contents of an existing policy to another action policy, replacing its contents.

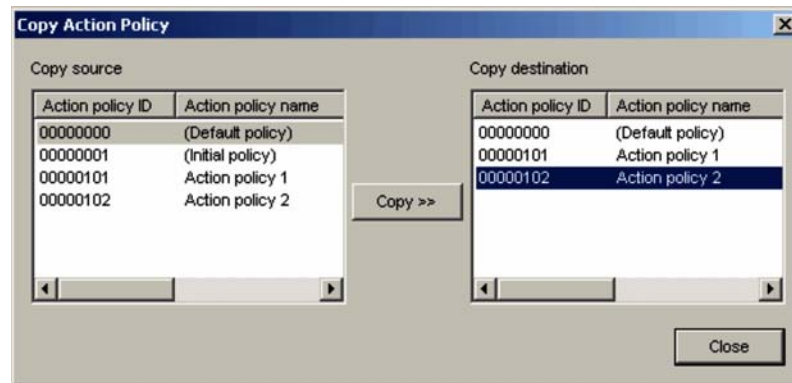
1. In the Policy Management main window, choose **Policy** and then **Manage Action Policy**.

The Manage Action Policy dialog box appears.

2. In the policy list in the Manage Action Policy dialog box, click the **Copy** button.

The Copy Action Policy dialog box appears.

Figure 6-24: Copy Action Policy dialog box



3. Select one action policy from the **Copy source** list and one from the **Copy destination** list, and then click the **Copy>>** button.

A message box asks if you are sure you want to copy the policy.

4. Click the **OK** button in the message box.

The contents of the action policy you selected in the **Copy source** list are copied to the action policy you selected in the **Copy destination** list.

*Note:*

You cannot specify the initial policy as the copy destination.

*Reference note:*

If you have modified the default policy and want to reset it to the defaults, select the initial policy as the copy source.

## 6.10 Setting an action for each security level

From **Action** in the action items tree view in the Edit Action Policy window, an administrator can select a security level for which to set an action.

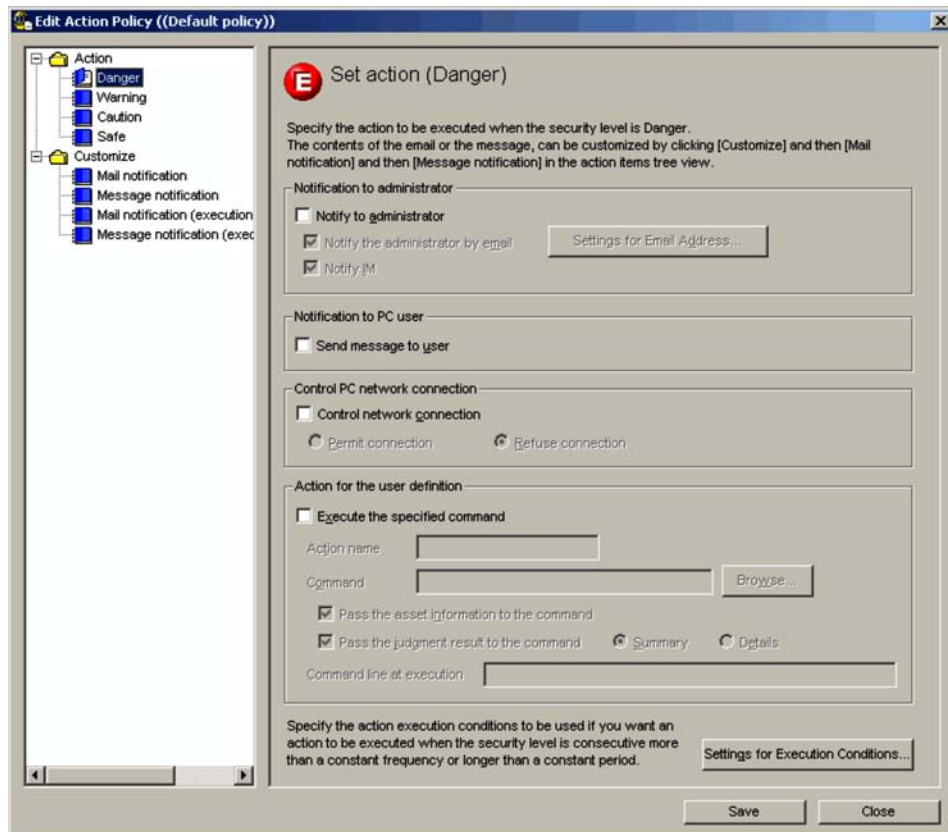
This section describes how to set an action for a security level and how commands are executed based on a user-defined action.

### 6.10.1 Setting an action for a security level in the Edit Action Policy window

Actions are set in the Edit Action Policy window.

The following figure shows the Edit Action Policy window.

Figure 6-25: Edit Action Policy window



There is an Edit Action Policy window for each security level, but the items for the



customized items view are shared across all windows.

The action items set in the Edit Action Policy window are as follows:

### **Notify to administrator**

Select this check box to notify administrators of the security level judgment results.

#### *Note:*

To enable administrator notification by email, you must configure the SMTP virtual server in Microsoft Internet Information Services and specify that incoming messages should be relayed to the remote domain. When setting up the SMTP virtual server, you must set a limit for the message size. To estimate the maximum message size, use the following expression (in megabytes):

$$(4,096 + 202 \times \text{number of assets}) / (1,024 \times 1,024)$$

For details about setup in Microsoft Internet Information Services, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

### **Notify the administrator by email**

Select this check box to notify administrators by email of the security level judgment results. Click the **Settings for Email Address** button, and set the administrator email address in the displayed Settings for Email Address dialog box.

*Figure 6-26: Settings for Email Address dialog box*

- **Email address to add**

To add a notification email address, enter the email address to be added, and then click the **Add** button. The email address is added to the list displayed for **Email address to be notified**.

- **Email address to be notified**

Displays no more than 100 email addresses already set.

If there are any unnecessary email addresses, select them and click the **Delete** button.

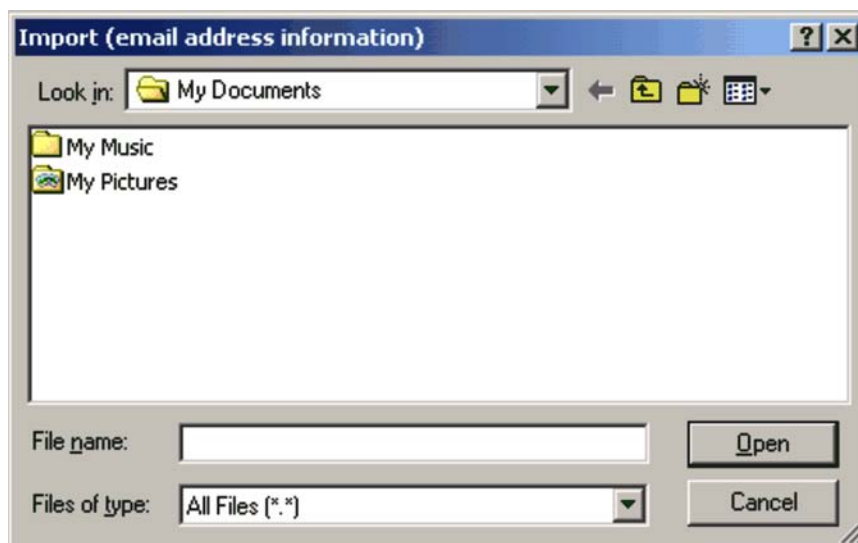
The selected addresses are deleted from the **Email address to be notified** list.

When **Email address to be notified** contains a large amount of information, you can create a mail address definition file in CSV format, and import the file.

In the Import (Email Address Information) dialog box displayed by clicking

the **Import** button, specify the location of the mail address definition file you want to import.

Figure 6-27: Import (Email Address Information) dialog box



In the **File name** text box, specify the name of the mail address definition file you want to import, and then click the **Open** button. The specified file is read, and the Settings for Email Address dialog box appears again.

The client security control system provides a sample of a mail address definition file. The administrator can customize the sample file to create a definition file and then import it. For details about a sample of this definition file, see *A.4(8) Sample of a mail address definition file*. For details about the mail address definition file, see *16.3 Mail address definition file*.

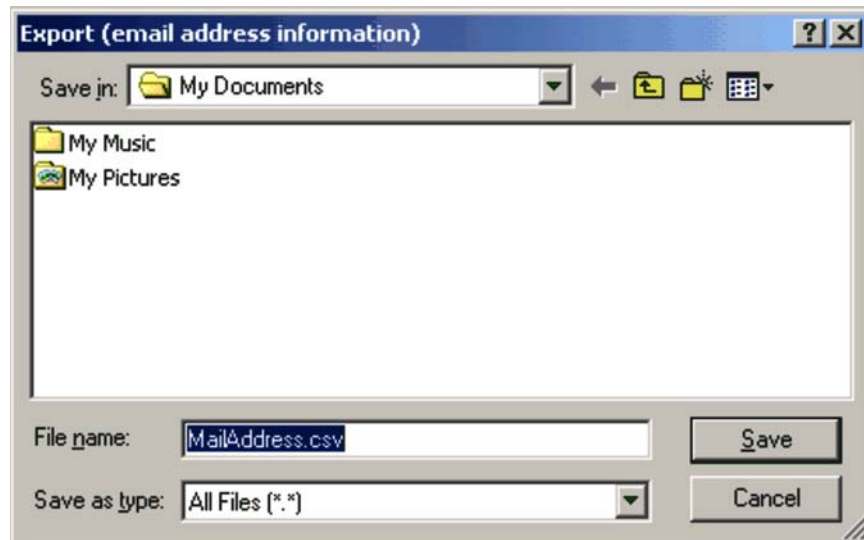
If the specified file does not contain the information indicated in the **Email address to be notified** list (the file is empty), an error message appears and the import is canceled.

The information in **Email address to be notified** can be exported to a CSV file. This file can then be used as a mail address definition file.

In the Export (Email Address Information) dialog box displayed by clicking the **Export** button, specify the location where you want to save the exported file.

Note that the **Export** button is disabled when no definitions have been registered in **Email address to be notified**.

Figure 6-28: Export (Email Address Information) dialog box



In the **File name** text box, specify the name of the CSV file to be exported, and then click the **Save** button. The specified file is saved, and the Settings for Email Address dialog box appears again.

The default file name is `MailAddress.csv`. For details about the mail address definition file, see *16.3 Mail address definition file*.

Note that the contents of email notifications can be edited by choosing **Customize** and then **Mail notification** in the action items tree view.

#### Notify IM

Select this check box to Notify IM of security level judgment results. For details about linkage to JP1/IM, see *11.1 Linking to JP1/IM*.

#### Note:

To notify JP1/IM of security level judgment results, during JP1/CSC - Manager setup, set **IM linkage** to **Notify**. For details about JP1/CSC - Manager setup, see *5.4.3 Setting up JP1/CSC - Manager*.

#### Send message to user

Select this check box to notify users of security level judgment results. Note that the contents of notification messages can be edited by choosing **Customize** and then **Message notification** in the action items tree view.

#### Control network connection

Select this check box to permit or deny client network connection.

Choose this action when using a quarantine system.

#### **Permit connection**

Select this radio button to permit client network connection.

#### **Refuse connection**

Select this radio button to deny client network connection.

#### **Execute the specified command**

Select this check box to implement a user-defined action (user-specific command set by the administrator). The check box is cleared by default.

Commands are executed automatically as set in the user-defined action. For details about command execution, see *Command used in a user-defined action in 15. Commands*.

#### **Action name**

Type the action name in no more than 255 bytes.

#### **Command**

Click the **Browse** button to display the Select File (Execution Command) window and select a command file. You can select any command file (\*.exe or \*.bat) stored on the management server.

The specified command is executed as described in *Command used in a user-defined action in 15. Commands*. For command details, see *Command used in a user-defined action in 15. Commands*.

Enter any parameters you want to specify after the command name. Type the command path as a character string of no more than 1,000 bytes. If you include any spaces, enclose the entire path with double quotation marks (").

#### **Pass the asset information to the command**

Select this check box to pass asset information judged *Danger*, *Warning*, or *Caution* to the command. The check box is selected by default.

For the file format of asset information passed to a command, see *16.8 Asset information file*.

#### **Pass the judgment result to the command**

Select this check box to pass information about unapplied Windows security updates (patches and service packs), and whether the required anti-virus products are installed, to the command. The check box is selected by default.

After selecting this check box, you must select either of the following types

of judgment results. The default is **Summary**.

- **Summary**

Select the **Summary** radio button to pass the judgment items and security level judgment results to the command.

- **Details**

Select the **Details** radio button to pass the summary results, and the judgment result for each item set in the judgment policy, to the command.

For the file format of judgment results passed to a command, see *16.9 Judgment result file for security level*.

### **Command line at execution**

This is the command line when the specified command is executed.

For details about this command line, see *Command used in a user-defined action* in *15. Commands*.

*Note:*

If both **Send message to user** and **Refuse connection** are selected, messages may not reach the user because client network connections will be denied.

### **Settings for Execution Conditions** button

Use this button to set a condition for implementing an action. When you click this button, the Settings for Action Execution Conditions dialog box appears.

*Note:*

When an action execution condition is set, the action is not implemented until the condition is satisfied.

The following figure shows the Settings for Action Execution Conditions dialog box.

Figure 6-29: Settings for Action Execution Conditions dialog box

**Settings for Action Execution Conditions**

**Notification to administrator**

☐ Specify number of consecutive days 10 days or more (1 - 1000)

☐ Specify number of consecutive times 3 times or more (1 - 1000)

☐ Execute the action when the security level changes

**Notification to PC user**

☐ Specify number of consecutive days 10 days or more (1 - 1000)

☐ Specify number of consecutive times 3 times or more (1 - 1000)

☐ Execute the action when the security level changes

**Control PC network connection**

☐ Specify number of consecutive days 10 days or more (1 - 1000)

☐ Specify number of consecutive times 3 times or more (1 - 1000)

☐ Execute the action when the security level changes

**Action for the user definition**

☐ Specify number of consecutive days 10 days or more (1 - 1000)

☐ Specify number of consecutive times 3 times or more (1 - 1000)

☐ Execute the action when the security level changes

To customize the contents of the mail and message used to notify when the action execution conditions exist, in the action items tree view click [Customize], [Mail notification (execution conditions)] and then [Message notification (execution conditions)].

OK Cancel

For each type of action (**Notification to administrator**, **Notification to PC user**, **Control PC network connection**, and **Action for the user definition**), you can select the following three execution conditions:

#### **Specify number of consecutive days**

Select this check box to specify a consecutive number of days. The check box is cleared by default. After you select this check box, you can enter the number of days. Either type a number between 1 and 1000, or select a

number using the ▲ and ▼ buttons.

You can set this option for the *Danger*, *Warning*, and *Caution* security levels.

#### **Specify number of consecutive times**

Select this check box to specify a consecutive number of times. The check box is cleared by default. After you select this check box, you can enter the number of times. Either type a number between 1 and 1000, or select a number using the ▲ and ▼ buttons.

You can set this option for the *Danger*, *Warning*, and *Caution* security levels.

#### **Execute the action when the security level changes**

Select this check box to implement an action when the security level changes. The check box is cleared by default.

You can set this option for the *Safe* security level.

The number of consecutive days and times can be counted in either of the following ways:

- Increase the count when the security level is the same

The count is increased when the security level is the same as the previous judgment. When the security level differs from the previous result, the consecutive days and times are cleared.

- Increase the count when the security level is the same as or higher

The count is increased when the security level is the same as or higher than the previous judgment. When the security level is lower than the previous result, or is not *Danger*, *Warning*, or *Caution*, the consecutive days and times are cleared.

Set the count method for the number of consecutive days and times in the **Basic Settings** page of the Client Security Control - Manager Setup dialog box. Set either of the above methods in **Method for counting the number of consecutive days and times** under **Security level judgment information**.

#### *Note:*

If you choose to increase the count when the security level is the same as or higher than last time, you must set the same number of consecutive days and times as the action execution condition for each security level.

The following table lists the default for each setting item in the Edit Action Policy



window, by security level.

*Table 6-36: Default security levels for the Edit Action Policy window*

No.	Edit Action Policy window item name	Default security level			
		Danger	Warning	Caution	Safe
1	Notify to administrator	Do not notify	Do not notify	Do not notify	Do not notify
2	Notify the administrator by email	Notify	Notify	Notify	Do not notify
3	Notify IM	Notify	Notify	Notify	Do not notify
4	Send message to user	Do not notify	Do not notify	Do not notify	Do not notify
5	Control network connection	Do not control	Do not control	Do not control	Do not control
6	Permit connection or Refuse connection	Refuse connection	Refuse connection	Refuse connection	Permit connection
7	Execute the specified command	Do not execute	Do not execute	Do not execute	Do not execute

To save the settings in the Edit Action Policy window:

1. Set the action item.
2. Click the **Save** button.

The set contents are saved as an action policy.

*Reference note:*

An error message or warning message may appear when you click the **Save** button. Read the message, and review your settings if necessary. Click the **OK** button to save the settings, or the **Cancel** button to discard them.

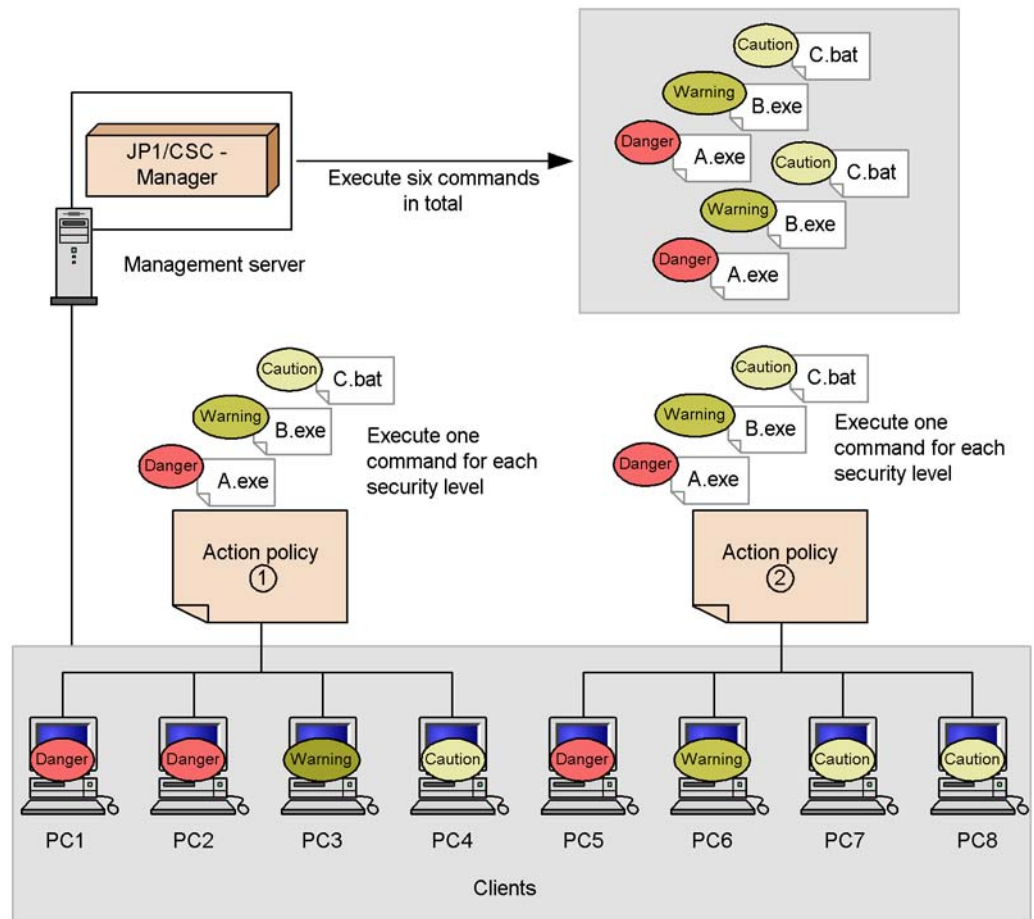
## 6.10.2 Command execution for user-defined actions

The following describes how commands are executed based on user-defined actions set by the administrator.

At each judgment, commands are executed as user-defined actions according to the number of action policies defined and the number of security levels set in each policy. For example, if you set two action policies and three security levels for each policy, six commands will be executed as user-defined actions.

The following figure shows an example of command execution in this situation.

Figure 6-30: Example of command execution



---

## 6.11 Editing an administrator notification email

---

If the **Notify the administrator by email** check box is selected in the Edit Action Policy window, the administrator is notified of security level judgment results by email. In the Edit Action Policy (Customize Email) window, you can edit the contents of the email sent for each security level.

The following explains how to edit these contents.

### 6.11.1 Editing email in the Edit Action Policy (Customize Email) window

The Edit Action Policy (Customize Email) window differs depending on whether any action execution conditions have been set.

No action execution conditions set:

    Edit the email contents in the window displayed when you select **Mail notification** in the action items tree view.

Action execution conditions set:

    Edit the email contents in the window displayed when you select **Mail notification (execution conditions)** in the action items tree view.

The following figures show the Edit Action Policy (Customize Email) window in each case.

Figure 6-31: Edit Action Policy (Customize Email) window (no action execution conditions set)

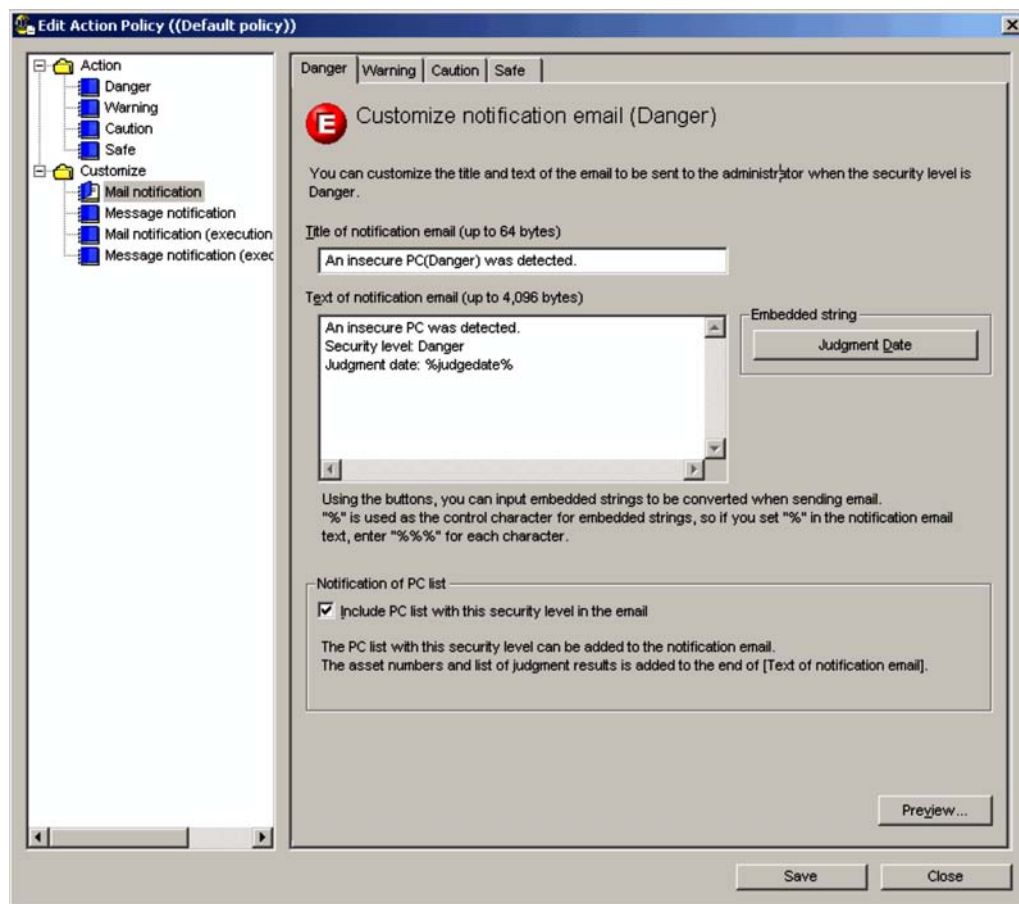
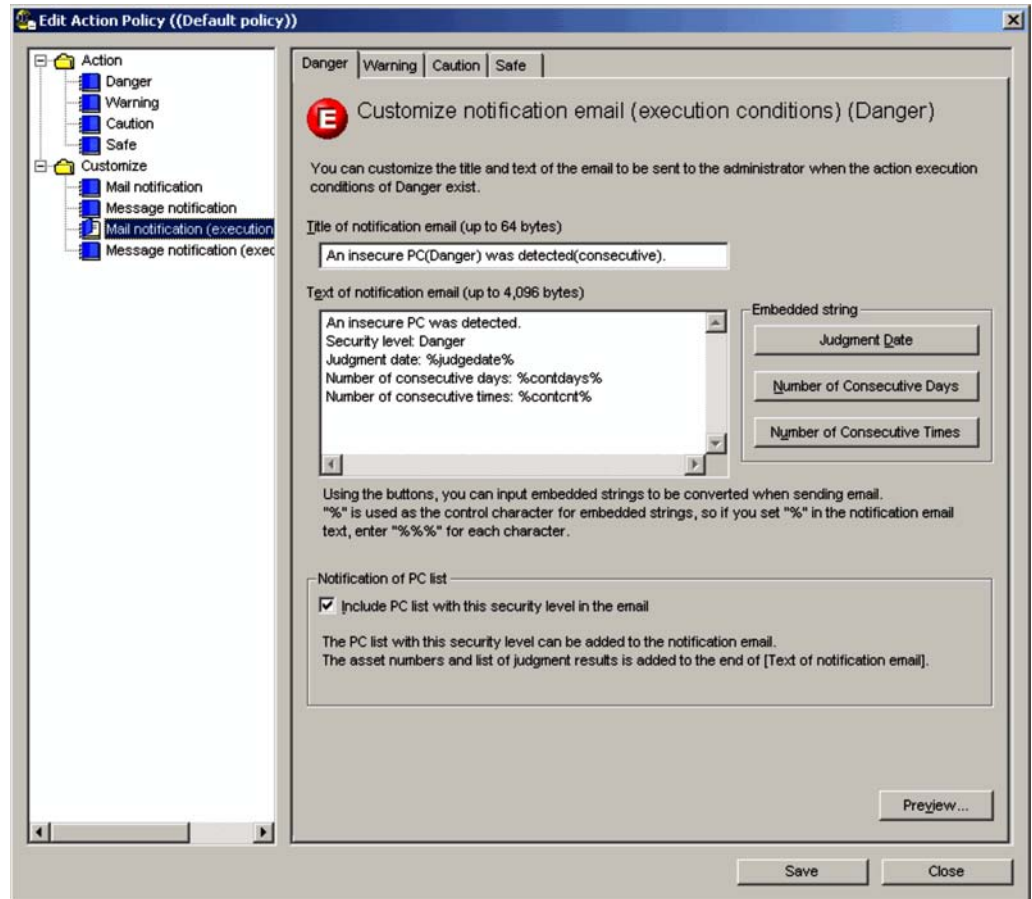


Figure 6-32: Edit Action Policy (Customize Email) window (action execution conditions set)



The Edit Action Policy (Customize Email) window contains a tab for each security level, but the items for the customized items view are shared across all windows.

The items set in the Edit Action Policy (Customize Email) window are as follows:

#### **Title of notification email**

Enter the title of the email to the administrator, in 64 or fewer bytes.

#### **Text of notification email**

Enter the body of the message to the administrator, in 4,096 or fewer bytes.

#### **Judgment Date button**

Use this to include the date of the security level judgment in the email body.

Click the **Judgment Date** button to insert %judgedate% into **Text of notification email 1** at the position of the cursor.

You cannot insert a judgment date if the email text will thereby exceed 4,096 bytes.

#### **Number of Consecutive Days** button

Use this to include the number of consecutive days set as an action execution condition in the email body. This button appears only when you select **Mail notification (execution conditions)** in the action items tree view.

Click this button to insert %contdays% into **Text of notification email** at the position of the cursor.

You cannot insert the number of consecutive days if the email text will thereby exceed 4,096 bytes.

#### **Number of Consecutive Times** button

Use this to include the number of consecutive times set as an action execution condition in the email body. This button appears only when you select **Mail notification (execution conditions)** in the action items tree view.

Click this button to insert %content% into **Text of notification email** at the position of the cursor.

You cannot insert the number of consecutive times if the email text will thereby exceed 4,096 bytes.

#### **Include PC list with this security level in the email**

Select this check box to include a list of PCs with the corresponding security level, in the text in the notification email. If this is selected, a list of judgment results is appended to the end of the notification email.

When there are more than 3,000 assets with the corresponding security level, the list of judgment results is split over multiple emails, each containing a maximum of 3,000 items. When this occurs, the sequence number of the email and the total number of emails are appended to the end of the email title (in the format *sequence-number/total-number-of-split-emails*). For example, suppose that there are 4,000 assets with the corresponding security level. In this case, two emails will be sent, with (1/2) and (2/2) appended to the titles of the respective emails. For this reason, if you expect the number of assets with the corresponding security level to exceed 3,000, give the email a title that will not exceed 64 bytes in length once the sequence number and total number of emails have been appended.

#### **Preview** button

Click this button to preview a sample of the notification email sent to the

administrator.

The following tables describe the default for each setting item in the Edit Action Policy (Customize Email) window, by security level.

*Table 6-37:* Default settings in the Edit Action Policy (Customize Email) window (no action execution conditions set)

No.	Window item name	Default settings for each security level			
		Danger	Warning	Caution	Safe
1	<b>Title of notification email</b>	An insecure PC (Danger) was detected.	An insecure PC (Warning) was detected.	An insecure PC (Caution) was detected.	None
2	<b>Text of notification email</b>	An insecure PC was detected. Security level: Danger Judgment date: %judgedate%	An insecure PC was detected. Security level: Warning Judgment date: %judgedate%	An insecure PC was detected. Security level: Caution Judgment date: %judgedate%	None
3	<b>Include PC list with this security level in the email</b>	Include	Include	Include	Do not

*Table 6-38:* Default settings in the Edit Action Policy (Customize Email) window (action execution conditions set)

No.	Window item name	Default settings for each security level			
		Danger	Warning	Caution	Safe
1	<b>Title of notification email</b>	An insecure PC (Danger) was detected (consecutive).	An insecure PC (Warning) was detected (consecutive).	An insecure PC (Caution) was detected (consecutive).	The security measure of the insecure PC has been completed.

No.	Window item name	Default settings for each security level			
		Danger	Warning	Caution	Safe
2	<b>Text of notification email</b>	An insecure PC was detected. Security level: Danger Judgment date: %judgedate% Number of consecutive days: %contdays% Number of consecutive times: %content%	An insecure PC was detected. Security level: Warning Judgment date: %judgedate% Number of consecutive days: %contdays% Number of consecutive times: %content%	An insecure PC was detected. Security level: Caution Judgment date: %judgedate% Number of consecutive days: %contdays% Number of consecutive times: %content%	The security measure of the insecure PC has been completed. Security level: Safe Judgment date: %judgedate%
3	<b>Include PC list with this security level in the email</b>	Include	Include	Include	Include

To edit, preview, and save email in the Edit Action Policy (Customize Email) window:

1. Edit the contents of the email.

Edit the title and body of the notification email.

2. Click the **Preview** button.

Check the contents set for **Text of notification email**, as displayed. If the **Include PC list with this security level in the email** check box is selected, a sample list of PCs is appended to the end of the email.

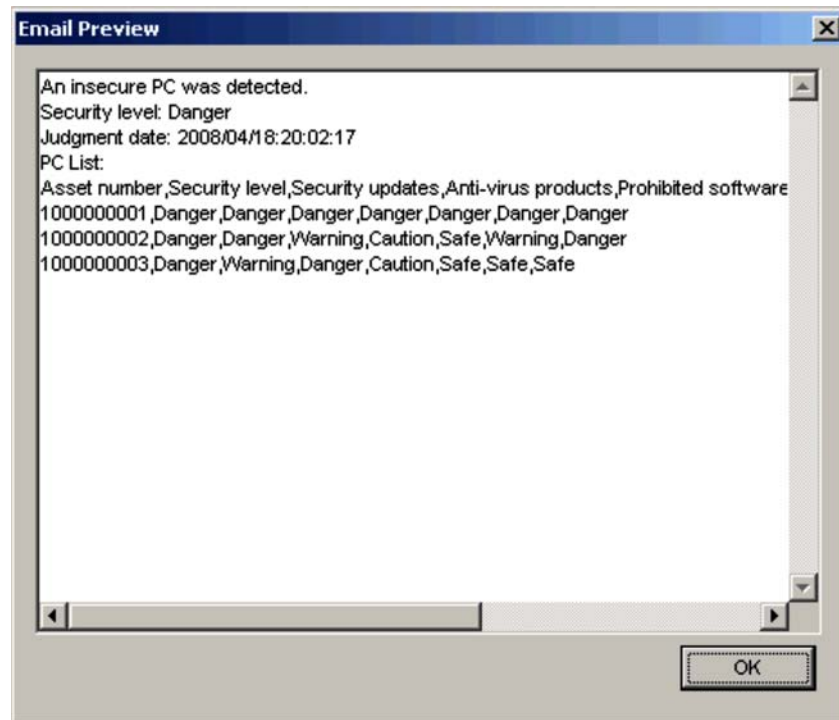
3. Click the **Save** button.

The edited email contents are saved.

The following figure shows a sample of the Email Preview window displayed when the **Preview** button is clicked.



Figure 6-33: Email Preview window (sample)



Of the contents displayed in the preview window, following items differ from the contents set for **Text of notification email**.

- **Judgment date**

The previewed date is displayed. The date of judgment is displayed for actual notification emails.

- **PC List**

If the **Include PC list with this security level in the email** check box is selected, samples of the list of PCs and judgment results are displayed. A list of judgment target PCs and judgment results are displayed for actual notification emails.

- **URL and email address**

If **Text of notification email** contains any URLs or email addresses, they are displayed in the preview window, underlined in blue.

### 6.11.2 Email sender address and transmission unit

The following explains the sender email address and email transmission unit for email sent to the administrator.

**(1) Email sender address**

By default, the sender address of emails sent to the administrator is set as follows:

Sender address

`manager@csc.message`

Emails originating from this sender address are security level judgment results from JP1/CSC - Manager. Note that emails are sent to administrators by BCC.

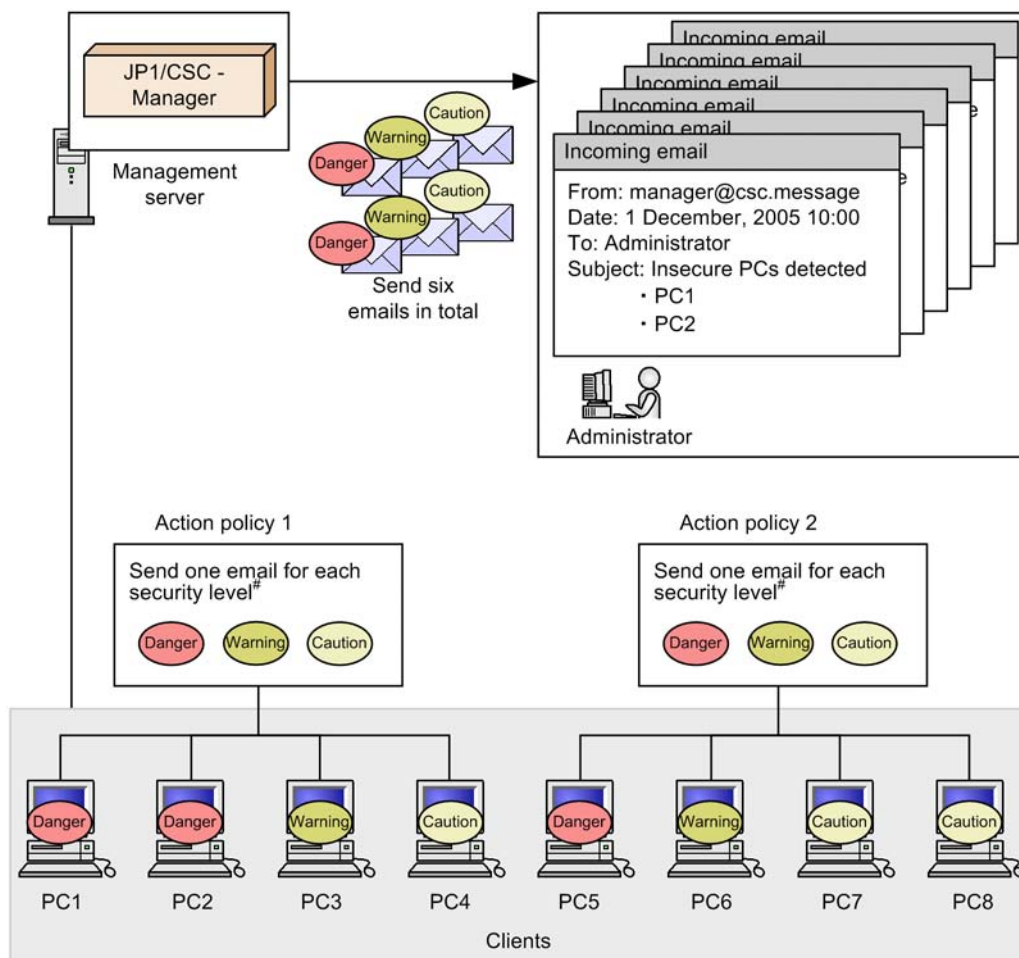
You can change the sender address in the **Basic Settings** page of the Client Security Control - Manager Setup dialog box. Enter an email address for **Mail notification information**.

**(2) Email transmission unit**

At each judgment, emails are sent to the administrator according to the number of action policies defined and the number of security levels set in each policy. For example, if you set two action policies and three security levels for each policy, six emails will be sent to the administrator.

The following figure shows an example of email notification in this situation.

Figure 6-34: Example of email notification



<sup>#</sup>: If you configure email notification to include a list of PCs with the corresponding security level in the body of the notification email, transmission may involve multiple emails containing a maximum of 3,000 items each.

---

## 6.12 Editing a client user notification message

---

If the **Send message to user** check box is selected in the Edit Action Policy window, the client user is notified of security level judgment results via a message. In the Edit Action Policy (Customize Message) window, you can edit the contents of the message sent for each security level. The following explains how to edit these contents.

### 6.12.1 Editing messages in the Edit Action Policy (Customize Message) window

The Edit Action Policy (Customize Message) window differs depending on whether any action execution conditions have been set.

No action execution conditions set:

    Edit the message contents in the window displayed when you select **Message notification** in the action items tree view.

Action execution conditions set:

    Edit the message contents in the window displayed when you select **Message notification (execution conditions)** in the action items tree view.

The following figures show the Edit Action Policy (Customize Message) window in each case.

Figure 6-35: Edit Action Policy (Customize Message) window (no action execution conditions set)

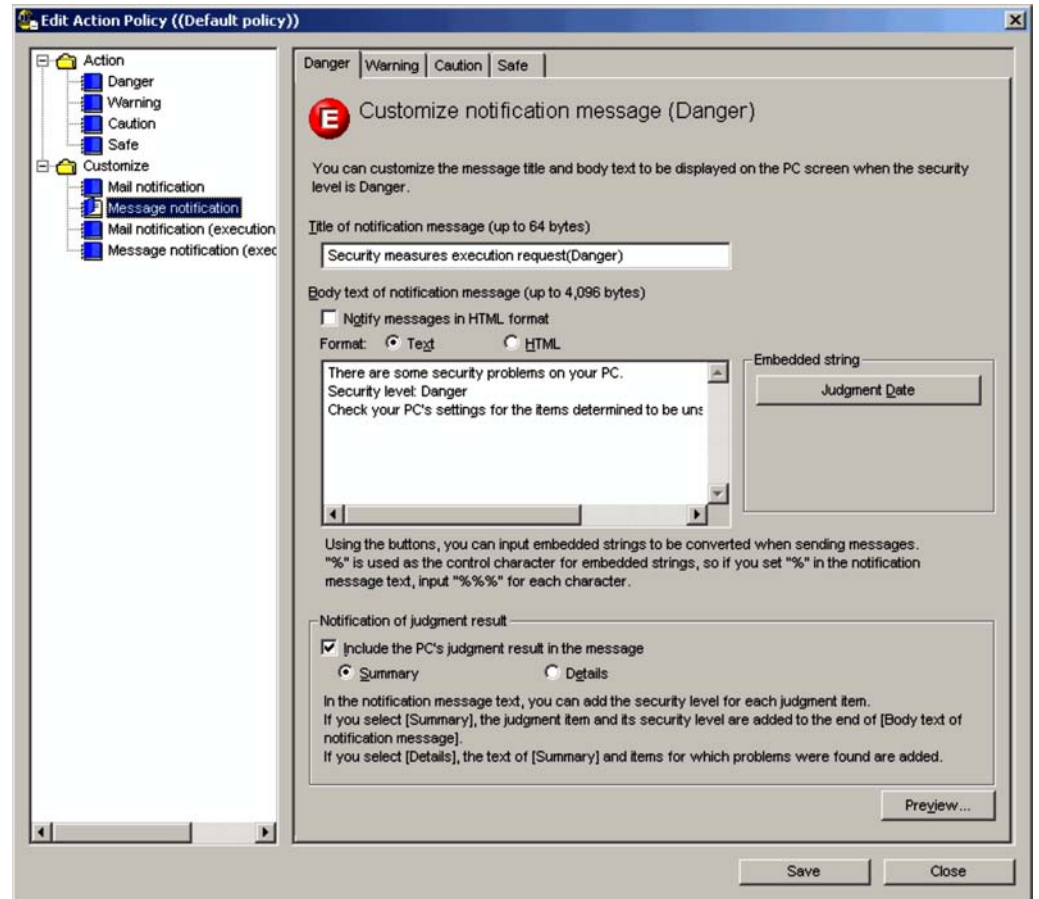
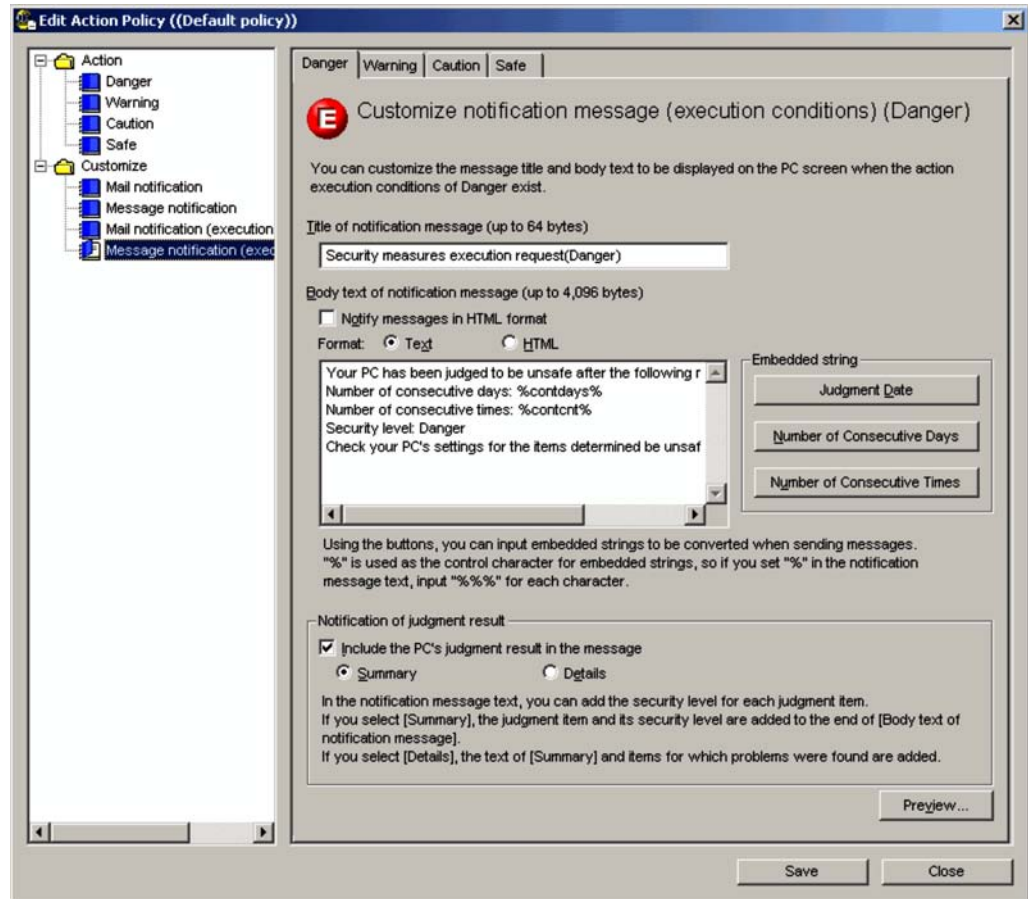


Figure 6-36: Edit Action Policy (Customize Message) window (action execution conditions set)



The Edit Action Policy (Customize Message) window contains a tab for each security level, but the items in the edit view are shared across all windows.

The following explains the items to be set in the Edit Action Policy (Customize Message) window.

#### Title of notification message

Enter the title of the user notification message, in 64 or fewer bytes.

#### Body text of notification message

Enter the body text of the notification message that is to be sent to the user. How the body text is set depends on the format of the displayed message.

- When the body text of a notification message is to be displayed in HTML

### format

You must enter the body text of the message for both **Text** and **HTML**. First, select the **Notify messages in HTML format** check box. For **Format**, select the **Text** or **HTML** radio button, and then enter the body text of the message. Use a character string of no more than 4,096 bytes for text format, and no more than 32,768 bytes for HTML format.

In this case, an HTML message is sent to the client whose JP1/Software Distribution Client version is 08-10 or later, and a plain-text message is sent to the client whose JP1/Software Distribution Client version is 08-00 or earlier.

- When the body text of a notification message is displayed in text format  
Clear the **Notify messages in HTML format** check box. Select the **Text** radio button for **Format**, and then enter the body text of the message, using a character string of no more than 4,096 bytes. Even if you select the **HTML** radio button and enter the body text of the message, an HTML message will not be sent.

In this case, a plain-text message is sent regardless of the JP1/Software Distribution Client version.

### Judgment Date button

Use this to include the date of the security level judgment in the message body. Click the **Judgment Date** button to insert %judgedate% into **Body text of notification message** at the position of the cursor.

You cannot insert a judgment date if the message text will exceed 4,096 bytes in text format or 32,768 bytes in HTML format as a result.

### Number of Consecutive Days button

Use this to include the number of consecutive days set as an action execution condition in the message body. This button appears only when you select **Message notification (execution conditions)** in the action items tree view.

Click this button to insert %contdays% into **Body text of notification message** at the position of the cursor.

You cannot insert the number of consecutive days if the message text will exceed 4,096 bytes in text format or 32,768 bytes in HTML format as a result.

### Number of Consecutive Times button

Use this to include the number of consecutive times set as an action execution condition in the message body. This button appears only when you select **Message notification (execution conditions)** in the action items tree

view.

Click this button to insert %content% into **Body text of notification message** at the position of the cursor.

You cannot insert the number of consecutive times if the message text will exceed 4,096 bytes in text format or 32,768 bytes in HTML format as a result.

#### **Include the PC's judgment result in the message**

Select this check box to include the security level for each judgment item, in the body of the notification message.

##### **Summary**

Select the **Summary** radio button to include the judgment item and security level in the body of the message.

##### **Details**

Select the **Details** radio button to include items for which problems occurred, in addition to summary information. The items included in the message include information about unapplied security updates, the application status of anti-virus products, and the software installation status.

The following shows examples of a message sent when the **Include the PC's judgment result in the message** check box is selected.



- If you select the Summary radio button, the following is displayed.

Message	There are some security problems on your PC. Security level: Danger Check your PC's settings for the items determined to be unsafe, as soon as possible.
PC judgment results (summary)	*****Security updates*****: Danger *****Anti-virus products*****: Warning *****Prohibited software*****: Safe *****Mandatory software*****: Danger *****PC security settings*****: Warning *****User definition*****: Caution

- If you select the Details radio button, the following is displayed.

Message	There are some security problems on your PC. Security level: Danger Check your PC's settings for the items determined to be unsafe, as soon as possible.
PC judgment results (details)	*****Security updates*****: Danger [unapplied security updates] 04-003(832483) 04-030(824151)  *****Anti-virus products*****: Warning Product version: Passed Engine version: Failed Virus definition file version: Passed Resident settings: Failed  *****Prohibited software*****: Safe  *****Mandatory software*****: Warning [Uninstalled mandatory software] Microsoft Office Microsoft Office 2000  *****PC security settings*****: Warning [Insecure PC security settings] Vulnerable password user01;user03  *****User definition*****: Caution [Noncompliant items] Power-saving CPU

- Display position of the judgment results

The judgment results for the PC are displayed at the beginning of the message in the following case: **Display at the beginning of the message** is set for **Display position of the judgment results** under **Message**

**notification information** on the **Basic Settings** page of the Client Security Control - Manager Setup dialog box.

- Effect of the **"Safe" or "Not applicable" results** setting

The **"Safe" or "Not applicable" results** setting is under **Message notification information** on the **Basic Settings** page of the Client Security Control - Manager Setup dialog box. The items that will be reported change depending on whether **Include** or **Do not include** is selected for the **"Safe" or "Not applicable" results** setting. If **Include** is selected, the items judged *Danger*, *Warning*, *Caution*, *Safe*, *Unknown*, or *Not applicable* are displayed. If **Do not include** is selected, only the items judged *Danger*, *Warning*, *Caution*, or *Unknown* are displayed.

The following shows examples of judgment result (details) displayed in a message

When Judgment results for safety items is set to include	When Judgment results for safety items is set to Do not include
<p>*****Security updates*****: Caution [unapplied security updates] Security updates A</p> <p>*****Anti-virus products*****: Caution Product version: Failed Engine version: Passed Virus definition file version: Passed Resident setting: Not applicable</p> <p>*****Prohibited software*****: Safe</p> <p>*****Mandatory software*****: Safe</p> <p>*****PC security settings*****: Caution [Insecure PC-security settings] Password that never expires: Account3; Account4</p> <p>*****User definition*****: Not applicable</p>	<p>*****Security updates*****: Caution [unapplied security updates] Security updates A</p> <p>*****Anti-virus products*****: Caution Product version: Failed</p> <p>*****PC security settings*****: Caution [Insecure PC-security settings] Password that never expires: Account3; Account4</p>

*Reference note:*

You can specify whether to display PC judgment results at the beginning or end of the message in the **Basic settings** page of the setup window of JP1/CSC - Manager. For details about how to specify this setting, see 5.4.3(1) *Using the Basic Settings page*.

*Note:*

When a message is sent to a client user, the execution history is saved to JP1/ Software Distribution Manager's CSCSendMessage folder, which logs the status of executed jobs. The number of jobs logged depends on whether you select the **Include the PC's judgment result in the message** check box.

- Check box selected

The result of the notification job executed for each client is logged in the CSCSendMessage folder.

- Check box cleared

The result of the notification job executed for each security level in each action policy is logged in the CSCSendMessage folder.

**Preview button**

Click this button to preview a sample of the notification message sent to the user.

The following tables describe the default for each setting item in the Edit Action Policy (Customize Message) window, by security level.

*Table 6-39: Default settings in the Edit Action Policy (Customize Message) window (no action execution conditions set)*

No.	Window item name	Default setting for each security level			
		Danger	Warning	Caution	Safe
1	<b>Title of notification message</b>	Security measure execution request (Danger)	Security measure execution request (Warning)	Security measure execution request (Caution)	None
2	<b>Body text of notification message</b>	There are some security problems on your PC. Security level: Danger Check your PC's settings for the items determined to be unsafe, as soon as possible.	There are some security problems on your PC. Security level: Warning Check your PC's settings for the items determined to be unsafe, as soon as possible.	There are some security problems on your PC. Security level: Caution Check your PC's settings for the items determined to be unsafe, as soon as possible.	None

No.	Window item name	Default setting for each security level			
		Danger	Warning	Caution	Safe
3	Include the PC's judgment result in the message	Include	Include	Include	Do not include
4	Summary or Details	Summary	Summary	Summary	Summary

## Note

The default settings are the same for text format and HTML format, with the exception that a linefeed tag (<BR>) is inserted in HTML format.

*Table 6-40:* Default settings in the Edit Action Policy (Customize Message) window (action execution conditions set)

No.	Window item name	Default setting for each security level			
		Danger	Warning	Caution	Safe
1	Title of notification message	Security measure execution request (Danger)	Security measure execution request (Warning)	Security measure execution request (Caution)	Security measures completion notification
2	Body text of notification message	Your PC has been judged to be unsafe after the following number of days or times: Number of consecutive days: %contdays% Number of consecutive times: %content% Security level: Danger Please check the PC settings for the items judged to be unsafe, as soon as possible.	Your PC has been judged to be unsafe after the following number of days or times: Number of consecutive days: %contdays% Number of consecutive times: %content% Security level: Warning Please check the PC settings for the items judged to be unsafe, as soon as possible.	Your PC has been judged to be unsafe after the following number of days or times: Number of consecutive days: %contdays% Number of consecutive times: %content% Security level: Caution Please check the PC settings for the items judged to be unsafe, as soon as possible.	The security measures for the unsafe PC have been executed.

No.	Window item name	Default setting for each security level			
		Danger	Warning	Caution	Safe
3	<b>Include the PC's judgment result in the message</b>	Include	Include	Include	<b>Not include</b>
4	<b>Summary or Details</b>	<b>Summary</b>	<b>Summary</b>	<b>Summary</b>	<b>Summary</b>

#### Note

The defaults settings are the same for text format and HTML format, with the exception that a linefeed tag (<BR>) is inserted in HTML format.

To edit a message in the Edit Action Policy (Customize Message) window:

1. Edit the contents of the message.

Edit the title and body of the notification message.

2. Click the **Preview** button.

Check the contents set for **Body text of notification message**, as displayed. If **Include the PC's judgment result in the message** is selected, the judgment items and security levels are also displayed.

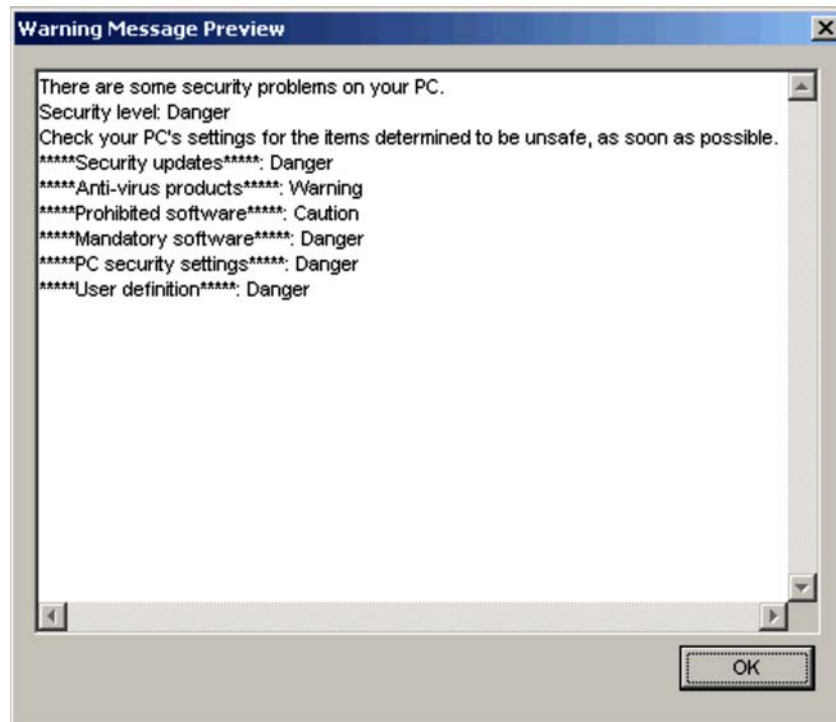
3. Click the **Save** button.

The edited message contents are saved.

The following figure shows a sample of the Warning Message Preview window displayed when the **Preview** button is clicked.

Note that the Warning Message Preview window displayed by clicking the **Preview** button might differ slightly from the warning message displayed in JP1/Software Distribution Client.

Figure 6-37: Warning Message Preview window (Summary)



Of the contents displayed in the Warning Message Preview window, the following items differ from the contents set for **Body text of notification message**.

- Judgment date  
The previewed date is displayed. The date of the judgment is displayed for actual notification messages.
- Judgment results  
If the **Include the PC's judgment result in the message** check box is selected, sample judgment results are displayed. The security level for each judgment item is displayed for actual notification messages.
- URL and email address  
Any URLs or email addresses contained in **Body text of notification message** are underlined in blue in the Preview window when the message is displayed in text format. When the message is displayed in HTML format, URLs and email addresses are underlined by link anchors when HTML anchor tags are set.

### 6.12.2 Checking the execution results of message notification jobs

When a message is sent to a client user, the job execution result is saved to the job status information of JP1/Software Distribution Manager. The results of message notification jobs executed by JP1/CSC are logged to the `CSCSendMessage` folder, which is created in the Manager's job status information. From the results saved in this folder, the administrator can check the result of a message notification job and the recipient to which the message was sent.

However, when the `CSCSendMessage` folder contains a large amount of job execution results, processing time in JP1/Software Distribution Manager may be adversely affected.

If job execution results do not need to be kept, you can set up JP1/Software Distribution Manager to delete them automatically. Only successful jobs are deleted automatically.

For details on how to automatically delete the execution results of message notification jobs, see 5.2.2(3) *Setting up for automatic deletion of message notification job results*.

---

## 6.13 Assigning security policies to clients

---

After setting judgment policies and action policies, the administrator assigns them to the clients.

This section describes how to assign judgment and action policies to clients.

### (1) *Assigning a judgment policy*

To assign a judgment policy to a client:

1. In the Policy Management main window, select one or more clients.

To assign the judgment policy to all clients:

In the group tree view, select **Overall system**.

To assign the judgment policy to all clients in a particular department or section:

In the group tree view, select the required group.

To assign the judgment policy to a particular client:

In the PC list tree view, select the required client. You may select multiple clients.

*Note:*

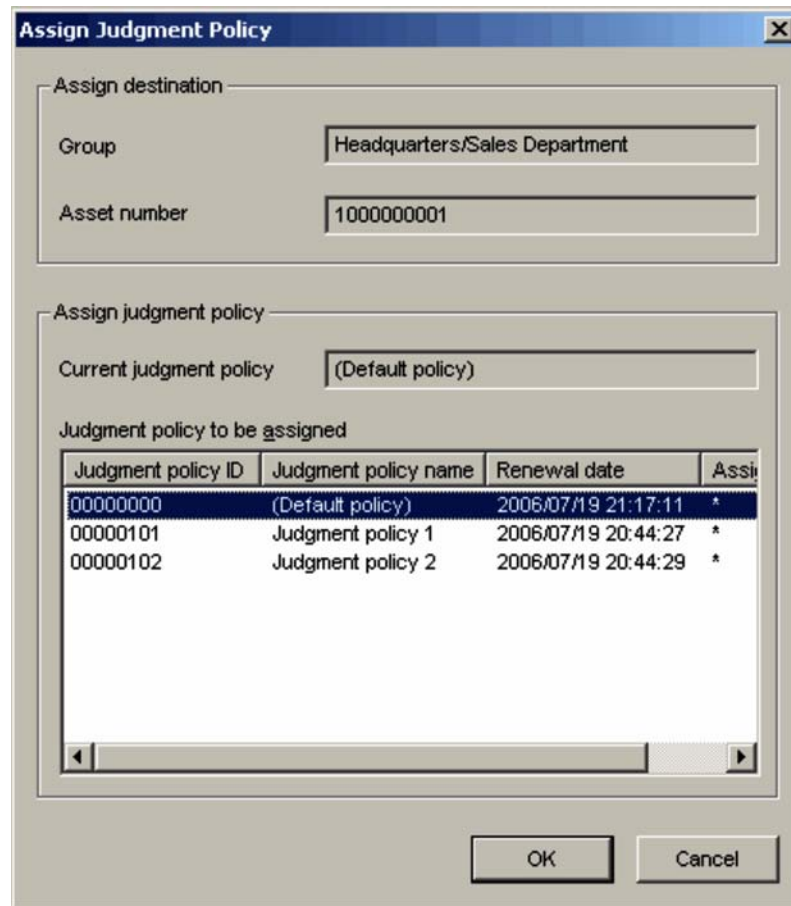
When you assign a judgment policy by selecting **Overall system** or a particular group, make sure no display conditions are set. If display conditions are set, clients that do not appear in the PC list tree view will not be assigned the policy.

2. Choose **Policy** and then **Assign Judgment Policy**.

The Assign Judgment Policy dialog box appears.



Figure 6-38: Assign Judgment Policy dialog box



The dialog box is titled "Assign Judgment Policy". It contains two main sections: "Assign destination" and "Assign judgment policy".

**Assign destination:**

- Group:** Headquarters/Sales Department
- Asset number:** 1000000001

**Assign judgment policy:**

- Current judgment policy:** (Default policy)
- Judgment policy to be assigned:** A table with the following data:
 

Judgment policy ID	Judgment policy name	Renewal date	Assi
00000000	(Default policy)	2006/07/19 21:17:11	*
00000101	Judgment policy 1	2006/07/19 20:44:27	*
00000102	Judgment policy 2	2006/07/19 20:44:29	*

At the bottom right, there are "OK" and "Cancel" buttons.

If you selected one client at step 1, the path of the group to which the client belongs and the client's asset number appear under **Assign destination**. If you selected a group, only the group path is displayed. If you selected multiple clients or **Overall system**, information about the first client you selected is displayed, followed by an ellipsis (. . .).

The box labeled **Current judgment policy** shows the name of the policy assigned to the selected client or to the clients in the selected group. If you selected multiple clients or **Overall system**, information about the first client you selected is displayed, followed by an ellipsis (. . .).

- From the list, select a policy to assign.

From the created judgment policies listed under **Judgment policy to be assigned**, select a judgment policy to assign to the selected clients.

4. Click the **OK** button.

A message asks if you are sure you want to assign the policy.

5. Click the **OK** button in the message box.

You are returned to the Policy Management main window. The assigned judgment policy appears under **Judgment policy name** in the PC list tree view.

## **(2) Assigning an action policy**

To assign an action policy to a client:

1. In the Policy Management main window, select one or more clients.

To assign the action policy to all clients:

In the group tree view, select **Overall system**.

To assign the action policy to all clients in a particular department or section:

In the group tree view, select the required group.

To assign the action policy to a particular client:

In the PC list tree view, select the required client. You may select multiple clients.

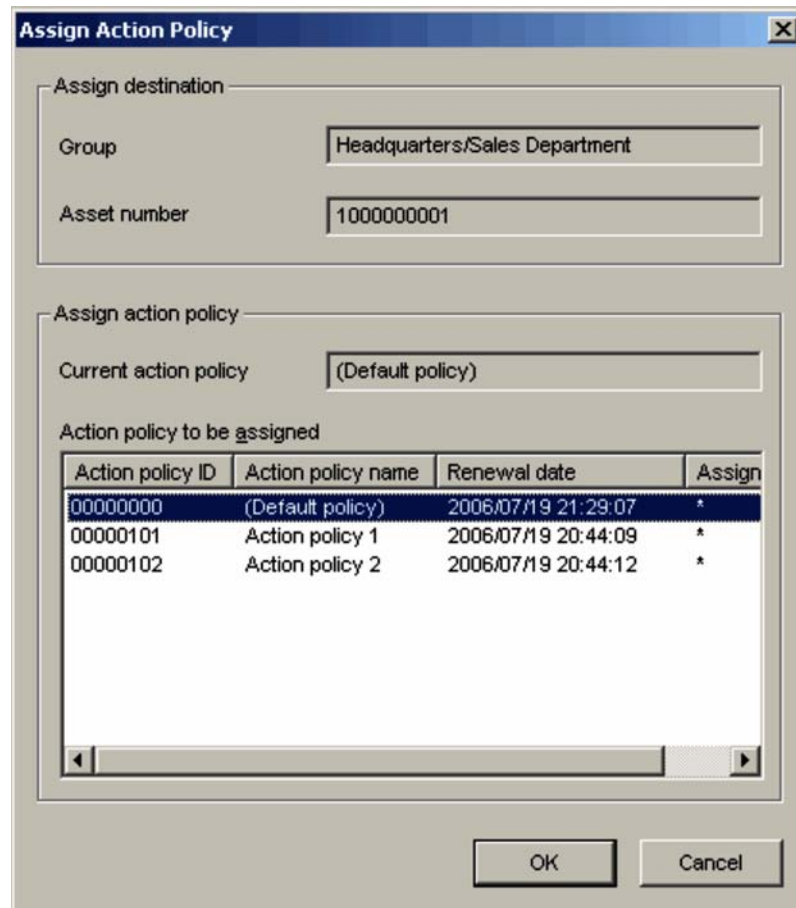
*Note:*

When you assign an action policy by selecting **Overall system** or a particular group, make sure no display conditions are set. If display conditions are set, clients that do not appear in the PC list tree view will not be assigned the policy.

2. Choose **Policy** and then **Assign Action Policy**.

The Assign Action Policy dialog box appears.

Figure 6-39: Assign Action Policy dialog box



The dialog box is titled "Assign Action Policy". It contains two main sections: "Assign destination" and "Assign action policy".

**Assign destination:**

- Group:** Headquarters/Sales Department
- Asset number:** 1000000001

**Assign action policy:**

- Current action policy:** (Default policy)
- Action policy to be assigned:** A table with the following data:
 

Action policy ID	Action policy name	Renewal date	Assign
00000000	(Default policy)	2006/07/19 21:29:07	*
00000101	Action policy 1	2006/07/19 20:44:09	*
00000102	Action policy 2	2006/07/19 20:44:12	*

At the bottom right, there are "OK" and "Cancel" buttons.

If you selected one client at step 1, the path of the group to which the client belongs and the client's asset number appear under **Assign destination**. If you selected a group, only the group path is displayed. If you selected multiple clients or **Overall system**, information about the first client you selected is displayed, followed by an ellipsis (. . .).

The box labeled **Current action policy** shows the name of the policy assigned to the selected client or to the clients in the selected group. If you selected multiple clients or **Overall system**, information about the first client you selected is displayed, followed by an ellipsis (. . .).

- From the list, select a policy to assign.

From the created action policies listed under **Action policy to be assigned**, select an action policy to assign to the selected clients.

4. Click the **OK** button.

A message asks if you are sure you want to assign the policy.

5. Click the **OK** button in the message box.

You are returned to the Policy Management main window. The assigned action policy appears under **Action policy name** in the PC list tree view.

## 6.14 Displaying clients that meet specified conditions

Display conditions can be set for the clients that appear in the PC list tree view in the Policy Management main window. Set the display conditions in the Set Display Conditions dialog box.

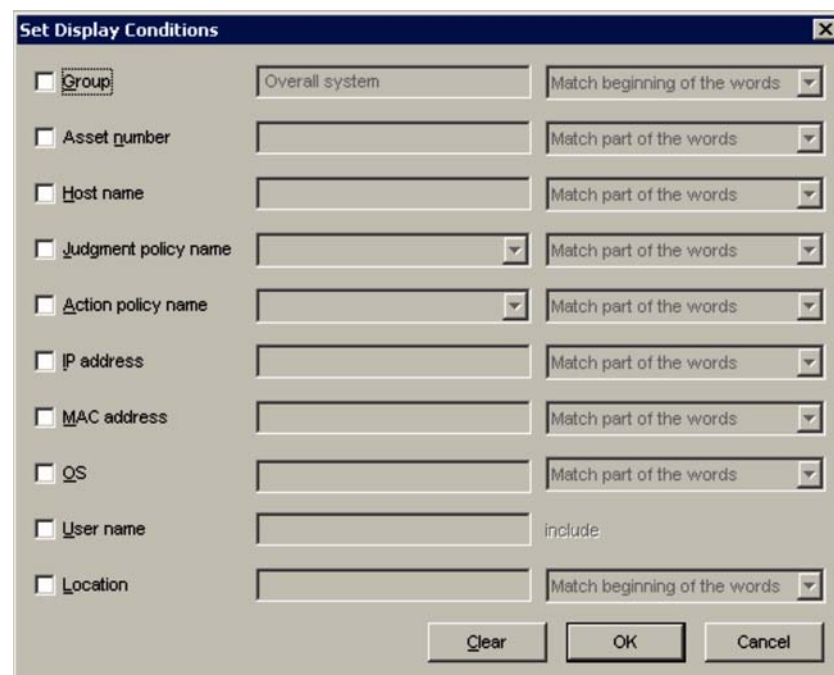
Before you set any display conditions, **Policy Management Window (display conditions: No setting)** appears in the title bar of the Policy Management main window.

To specify display conditions for the PCs listed in the Policy Management main window:

1. In the group tree view of the Policy Management main window, select a group and then choose **View** and **Set Display Conditions**.

The Set Display Conditions dialog box appears.

*Figure 6-40: Set Display Conditions dialog box*



The dialog box titled "Set Display Conditions" contains a list of items with checkboxes and associated input fields or dropdown menus. The items are:

- ☐ **Group**: Overall system (text field), Match beginning of the words (dropdown)
- ☐ **Asset number**: (text field), Match part of the words (dropdown)
- ☐ **Host name**: (text field), Match part of the words (dropdown)
- ☐ **Judgment policy name**: (dropdown), Match part of the words (dropdown)
- ☐ **Action policy name**: (dropdown), Match part of the words (dropdown)
- ☐ **IP address**: (text field), Match part of the words (dropdown)
- ☐ **MAC address**: (text field), Match part of the words (dropdown)
- ☐ **OS**: (text field), Match part of the words (dropdown)
- ☐ **User name**: (text field), include (text field)
- ☐ **Location**: (text field), Match beginning of the words (dropdown)

At the bottom right are three buttons: Clear, OK, and Cancel.

2. Set each item in the dialog box.

Each item in the Set Display Conditions dialog box has a check box.

To set an item as a display condition, select its check box.

All the check boxes are cleared by default.

The following table shows the items that can be specified as display conditions.

*Table 6-41: Items specifiable as display conditions*

No.	Item	Specification	Search options	Default search option
1	<b>Group</b>	Shows the group name selected in the group tree view in the Policy Management main window. Not specifiable.	Select either of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Match all the words</b></li> <li>• <b>Match beginning of the words</b></li> </ul>	<b>Match beginning of the words</b>
2	<b>Asset number</b>	Specify the asset number in no more than 60 alphanumeric characters.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Match all the words</b></li> <li>• <b>Match part of the words</b></li> <li>• <b>Match beginning of the words</b></li> <li>• <b>Match end of the words</b></li> </ul>	<b>Match part of the words</b>
3	<b>Host name</b>	Specify the PC host name as a string of no more than 255 characters.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Match all the words</b></li> <li>• <b>Match part of the words</b></li> <li>• <b>Match beginning of the words</b></li> <li>• <b>Match end of the words</b></li> </ul>	<b>Match part of the words</b>

No.	Item	Specification	Search options	Default search option
4	<b>Judgment policy name</b>	Select the appropriate judgment policy from the combo box, or type the judgment policy name in no more than 128 bytes.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Match all the words</b></li> <li>• <b>Match part of the words</b></li> <li>• <b>Match beginning of the words</b></li> <li>• <b>Match end of the words</b></li> </ul>	<b>Match part of the words</b>
5	<b>Action policy name</b>	Select the appropriate action policy from the combo box, or type the action policy name in no more than 128 bytes.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Match all the words</b></li> <li>• <b>Match part of the words</b></li> <li>• <b>Match beginning of the words</b></li> <li>• <b>Match end of the words</b></li> </ul>	<b>Match part of the words</b>
6	<b>IP address</b>	Specify the PC's IP address in no more than 70 alphanumeric characters.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Match all the words</b></li> <li>• <b>Match part of the words</b></li> <li>• <b>Match beginning of the words</b></li> <li>• <b>Match end of the words</b></li> </ul>	<b>Match part of the words</b>

No.	Item	Specification	Search options	Default search option
7	<b>MAC address</b>	Specify the PC's MAC address in no more than 70 alphanumeric characters.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Match all the words</b></li> <li>• <b>Match part of the words</b></li> <li>• <b>Match beginning of the words</b></li> <li>• <b>Match end of the words</b></li> </ul>	<b>Match part of the words</b>
8	<b>OS</b>	Specify the OS name as a string of no more than 200 characters.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Match all the words</b></li> <li>• <b>Match part of the words</b></li> <li>• <b>Match beginning of the words</b></li> <li>• <b>Match end of the words</b></li> </ul>	<b>Match part of the words</b>
9	<b>User name<sup>#</sup></b>	Specify the PC user name as a string of no more than 255 characters.	--	--
10	<b>Location</b>	Specify the PC location as a string of no more than 512 characters.	Select either of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Match all the words</b></li> <li>• <b>Match beginning of the words</b></li> </ul>	<b>Match beginning of the words</b>

Legend:

--: No search options

#

The condition is regarded as satisfied when the specified character string matches part of a user name.

**Clear** button



Clears all settings in the text boxes.

This button does not clear the check boxes and search options.

3. Click the **OK** button.

The Set Display Conditions dialog box closes and the clients matching the specified condition are listed in the Policy Management main window.

After you set the display conditions, **Policy Management Window (display conditions: Setting)** appears in the title bar of the Policy Management main window.

*Note:*

Note the following when using the Set Display Conditions dialog box:

- The set display conditions apply until you exit the Policy Management main window. The next time you open the window, no display conditions apply.
- The set display conditions still apply when you select a different group in the group tree view. Thus, information about the clients in the selected group appears in the PC list tree view.



## **Chapter**

---

# **7. Managing Inventory Information**

---

This chapter explains how to manage inventory information.

- 7.1 Managing inventory information
- 7.2 Detecting non-Software Distribution clients
- 7.3 Automatically obtaining client inventory information
- 7.4 Detecting security updates not applied to a client

---

## 7.1 Managing inventory information

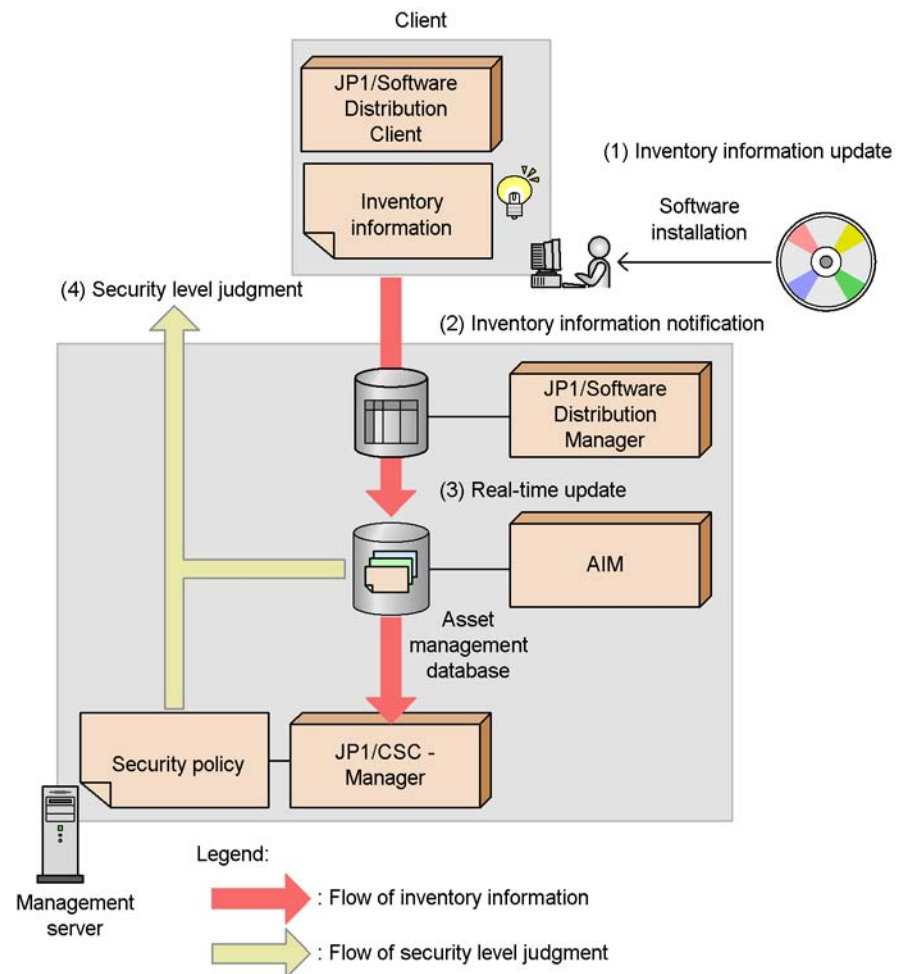
---

When inventory information such as software information and security update information is updated on a client, the client notifies JP1/Software Distribution Manager of the information. This inventory information is then reflected in the asset management database of AIM.

The security level of a client is judged according to the security policy, based on the latest inventory information reflected in the asset management database.

The following figure shows the flow of inventory information collection, and the flow in which a client security level is judged based on this inventory information.

Figure 7-1: Inventory information collection and client security level judgment



- (1) Client inventory information is updated due to software installation.
- (2) Inventory information is sent from JP1/Software Distribution Client to JP1/Software Distribution Manager.
- (3) Inventory information in the asset management database is updated in real-time.
- (4) The client security level is judged according to the security policy and inventory information.

This section explains the inventory information used on a client security control system, as well as the JP1/Software Distribution functionality used to manage inventory information.

### 7.1.1 Inventory information used on a client security control system

Of the inventory information collected by JP1/Software Distribution, a client security control system uses the following software information to judge a client security level:

- Version information for JP1/Software Distribution Client

This information is necessary for judging the security levels of clients. If this information does not exist, the judgment result of each judgment item will be **Unknown**.

- Information about applied security updates (patches and service packs)

This is used to check whether or not the latest Windows security update has been applied to a client. For details about the items you can set, see *6.3 Editing a security update judgment policy*.

To check information about unapplied security updates, MBSA or WUA must be set up on the client. For details about setting up MBSA or WUA, see *7.4 Detecting security updates not applied to a client*.

- Information about anti-virus products

This is used to check information about the presence of anti-virus product installations, as well as engine versions, and resident statuses. For details about the items you can set, see *6.4 Editing an anti-virus product judgment policy*.

- Information about installed prohibited software

This is used to check whether or not software not needed for operations, or software that could cause security holes is installed on a client. For details about the items you can set, see *6.5 Editing a prohibited software judgment policy*.

- Information about installed mandatory software

This is used to check whether or not the software used for operations, as well as JP1/Software Distribution, is installed on a client. For details about the items you can set, see *6.6 Editing a mandatory software judgment policy*.

- Information about PC security settings

This is used to check whether security-related settings, for example account and password settings, are implemented correctly on a client PC. For details about the items you can set, see *6.7 Editing a PC security setting judgment policy*.

- Information about user-specific judgment items (judgment items in user definitions)

This is used to check security information defined by an administrator using the asset information stored in the asset management database, such as whether the client is running a power-saving CPU or whether automatic login is enabled. For details about the judgment items you can set, see *6.8 Editing a user-defined*

*judgment policy.*

### 7.1.2 Detecting non-Software Distribution clients

To collect the inventory information needed for security management, JP1/Software Distribution must be installed on a client. If a client exists for which JP1/Software Distribution is not installed, the status of security measures cannot be measured properly, because not all client inventory information can be collected.

The following JP1/Software Distribution functionality is used to check whether or not JP1/Software Distribution is installed on all clients.

- Detecting non-Software Distribution clients

This functionality detects clients for which JP1/Software Distribution is not installed, by comparing the clients registered in JP1/Software Distribution Manager with those on the network.

To detect non-Software Distribution clients, see *7.2 Detecting non-Software Distribution clients*.

### 7.1.3 Automatically collecting inventory information

To judge a client security level according to a security policy when client inventory information is updated, client inventory information must be collected in real time.

Use the following JP1/Software Distribution functionality to automatically collect client inventory information:

- Automatically collecting client inventory information

This functionality automatically notifies the higher system of inventory information updated on a client.

For details about automatic collection of inventory information, see *7.3 Automatically obtaining client inventory information*.

### 7.1.4 Detecting unapplied security updates

Use the following JP1/Software Distribution functionality to check whether or not the latest security update has been applied to a client.

- Detecting security updates not applied to a client

This functionality links to MBSA or WUA to detect information about patches and service packs not applied to a client.

For details about how to detect security updates not applied to a client, see *7.4 Detecting security updates not applied to a client*.

---

## 7.2 Detecting non-Software Distribution clients

---

An action is implemented when a client security level is judged according to a security policy, based on inventory information collected from a client on which JP1/Software Distribution is installed. To accurately assess the status of client security measures, JP1/Software Distribution must be installed on the client.

When **search host** is performed on JP1/Software Distribution Manager, the non-Software Distribution clients are detected from those on the network, and the installation status of JP1/Software Distribution can be checked.

With JP1/Software Distribution, a non-Software Distribution client is called a *non-Software Distribution host*. These hosts include servers and UNIX machines other than clients. Note that the client security control system supports only Windows machines. Therefore, machines other than Windows machines must be excluded from non-Software Distribution host detection.

This section describes how to detect non-Software Distribution clients and how to exclude non-Windows machines from detection.

### 7.2.1 Using the JP1/Software Distribution host search to detect non-Software Distribution clients

To detect non-Software Distribution clients, from the Detection of Hosts Not Containing Software Distribution dialog box, display and use the search host dialog box.

For details about how to perform a JP1/Software Distribution host search to detect non-Software Distribution clients, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems.

### 7.2.2 Excluding non-Windows machines from detection

The client security control system manages only network machines whose OS is Windows. It does not manage machines that run HP-UX, Solaris, and other non-Windows OSs.

If a non-Windows machine is detected as a non-Software Distribution host, an incorrect action might be performed on that machine. To prevent incorrect actions, specify the following settings during JP1/Software Distribution Manager setup so that those machines whose node type is *Computer* and whose OS is not Windows are not detected as non-Software Distribution hosts:

- Before non-Windows hosts can be excluded from non-Software Distribution detection, specify settings that will display the detection results under the **Hold** icon.

For details about setting the non-Software Distribution host detection results to



display below the **Hold** icon, see *5.2.2(1) Setting up to detect non-Software Distribution clients*.

To exclude non-Windows machines from detection, perform the following operation:

- From the devices listed under the **Hold** icon displayed in the Detection of Hosts Not Containing Software Distribution dialog box, move all HP-UX, Solaris, and other non-Windows machines to the list of devices under the **Non-detection** icon.

For details about how to exclude HP-UX, Solaris, and other non-Windows machines from non-Software Distribution detection, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems.

Note that machines set to be excluded from detection as non-Software Distribution hosts are not displayed in the Client Security Management window.

*Reference note:*

Network devices with a node type other than **Computer**, such as routers and printers, are automatically detected as **Non-detection**.

*Note:*

For Windows machines, such as a server machine or an offline machine, that must be excluded from client security management, use the Client Security Management window to set the security management to **Invalid**. For details about how to disable security management, see *8.5.1 Disabling security management*.

---

## 7.3 Automatically obtaining client inventory information

---

When software is first installed on a client or a patch is applied thereafter, the corresponding inventory information is updated. The updated inventory information can then be reported automatically to JP1/Software Distribution Manager. Inventory information about any new client added to the network is also sent to JP1/Software Distribution Manager. JP1/Software Distribution Manager notifies AIM in real time whenever inventory information is updated. AIM receives the notification, and stores the inventory information in the asset management database.

JP1/CSC automatically judges a client security level according to the security policy, based on the latest inventory information stored in the asset management database.

This section explains how to set client inventory information to be obtained automatically, as well as timing and precautions regarding inventory information.

### 7.3.1 Setup methods

To enable automatic judgment of security levels according to the security policy whenever a client connects to the server and its updated inventory information is notified to JP1/Software Distribution Manager, you must complete the following setup.

- Setting up JP1/Software Distribution

- Setting up JP1/Software Distribution Manager

During JP1/Software Distribution Manager setup, set inventory information to be automatically reported to AIM. For details on how to do this, see *5.2.2(2) Setting up for automatic notification of inventory information to AIM*.

When you are using Asset Information Manager Subset Component of JP1/Software Distribution Manager, during setup of the server for Asset Information Manager Subset, specify the setting for automatically obtaining inventory information from JP1/Software Distribution Manager. For details about the setting, see *5.2.2(5)(b) Setting up to automatically obtain inventory information from JP1/Software Distribution Manager*.

- Setting up JP1/Software Distribution Client

During JP1/Software Distribution Client setup, specify that updated inventory information is to be reported to the higher-level system.

For details on how to do this, see *5.6 Installing and setting up JP1/Software Distribution Client*.

For details about the function that automatically reports updated inventory

information, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

#### ■ Setting up AIM

To automatically obtain inventory information, start the Asset Information Synchronous Service. For details about starting the service, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

#### *Note:*

When starting Asset Information Synchronous Service, use the following service start order:

- Client Security Control - Manager
- Asset Information Synchronous Service

During setup of Asset Information Manager, specify the setting for automatically obtaining inventory information from JP1/Software Distribution Manager. For details about the setting, see 5.3.2(2) *Setting up to automatically obtain inventory information from JP1/Software Distribution Manager*.

#### ■ Setting up JP1/CSC - Manager

To automatically judge a client security level according to the security policy when inventory information is updated, in the **Basic settings** tab of the setup window of JP1/CSC - Manager, specify the following settings:

- In **Security level judgment information**, set **At addition of asset information** to **Judge**.
- In **Security level judgment information**, set **At update of asset information** to **Judge**.

For details about setting up JP1/CSC - Manager, see 5.4.3 *Setting up JP1/CSC - Manager*.

### 7.3.2 Notification timing for inventory information

JP1/Software Distribution Manager is notified of changes to the following inventory items when the client connects to the server at polling or job execution:

- System information (system information and registry information)
- Software information (software registered in **Add/Remove Programs**, Hitachi program products, security update information <sup>#1</sup>, and software specified as management targets in the software inventory dictionary of JP1/Software Distribution <sup>#2</sup>)
- Microsoft Office products <sup>#3</sup>

- Anti-virus products<sup>#3</sup>

For details about the inventory information sent, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

#1

To automatically notify JP1/Software Distribution Manager of updated software information, MBSA or WUA must be set up on the client. For details about setting up MBSA and WUA, see 7.4 *Detecting security updates not applied to a client*.

#2

This software information is obtained when a target product for patch information has not been registered in the asset management database of AIM. In JP1/Software Distribution, execute the *Get software information from client* job with **Software search list** or **Search for a file** specified to obtain the software information.

For details about the software inventory dictionary of JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

#3

If the client OS is Windows NT 4.0 or Windows 98, the *Windows scripting host* must be installed on the client. For details about installing the Windows scripting host, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

### 7.3.3 Precautions

Keep the following in mind when performing automatic notification for updated inventory information:

- Automatic notification is not performed for information about prohibited software and mandatory software installed without using the installer. As such, inventory information is not automatically collected. To prevent leaks from occurring for collected inventory information, in JP1/Software Distribution, perform regular execution of **Search all software** and **Search for a file** for the *Get software information from the client* job to obtain the software information.
- When automatic notification is enabled, JP1/Software Distribution Manager is notified of changes to inventory information whenever a client connects to the server at polling or job execution. As a result, the servers and network environment may occasionally encounter heavy loads. For environments where such a load is unacceptable, turn off automatic notification for inventory information, and execute a job to obtain inventory information.

- To perform relay for the UNIX version of JP1/Software Distribution SubManager, and to perform automatic notification for inventory information, make sure that the version of the UNIX JP1/Software Distribution SubManager is 07-00 or later. When relay is performed with a version of UNIX JP1/Software Distribution SubManager earlier than 07-00, and JP1/Software Distribution Manager is notified of inventory information, unnecessary files reported to the UNIX version of JP1/Software Distribution SubManager may accumulate on disk, affecting disk capacity.

---

## 7.4 Detecting security updates not applied to a client

---

JP1/Software Distribution links to MBSA or WUA to detect security updates that have not been applied to a client. This section describes the procedures for each product:

For details and precautions on detecting information about unapplied security updates, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

### (1) When JP1/Software Distribution links to MBSA

To detect security updates that have not been applied to a client, distribute to the client the MBSA command line interface (`mbsaccli.exe` file) and MBSA database files, and then specify **Search all software** in JP1/Software Distribution, and execute the *Get software information from the client* job.

With JP1/Software Distribution, of the **Security Updates** scan results for which `mbsaccli.exe` can be executed, information for which the latest security update was not found (displayed as **Not Found** in the scan results) is detected as security update information (unapplied patch information) not applied to the client. Note that Microsoft Office security updates are not covered by `mbsaccli.exe` scans, and therefore such unapplied security update information cannot be detected.

To use MBSA to detect information about unapplied security updates, the client must satisfy all of the following conditions:

- The OS is Windows NT 4.0, Windows 2000, Windows XP, or Windows Server 2003.
- JP1/Software Distribution SubManager (version 07-50 or later) or JP1/Software Distribution Client (version 07-50 or later) is installed.
- Version 6.0 or later of Microsoft Internet Explorer is installed.
- The client has the MBSA 1.2.1 `mbsaccli.exe` file, and the MBSA database files.

If the above conditions are not satisfied, an error will occur during execution of the *Get software information from the client* job.

Note that there are no OS or version limitations for systems relaying the *Get software information from the client* job.

### (2) When JP1/Software Distribution links to WUA

To detect security updates that have not been applied to a client, perform a remote installation of WUA 2.0 and Windows Installer 3.0 on the client and distribute the WUA 2.0 database files to the client. Then, specify **Search all software** in JP1/Software Distribution and execute the *Get software information from client* job.

Information about security updates provided by Windows Update that have not been

applied to a client is detected in JP1/Software Distribution as unapplied security update information (unapplied patch information). By linking to WUA you can detect unapplied patch information for software such as Microsoft Office as well as for the OS.

The client must satisfy all of the following conditions:

- The OS is Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP, or Windows 2000.
- Version 6.0 or later of Microsoft Internet Explorer is installed.
- JP1/Software Distribution Client (version 08-00 or later) is installed.
- Version 3.0 or later of Windows Installer is installed.
- Version 2.0 or later of WUA is installed.
- The client has the WUA 2.0 database files.

If the above conditions are not satisfied, an error will occur during execution of the *Get software information from the client* job.

Note that there are no OS or version limitations for systems relaying the *Get software information from the client* job.





## Chapter

---

# 8. Monitoring Clients

---

This chapter explains how to monitor clients using the Client Security Management window of AIM.

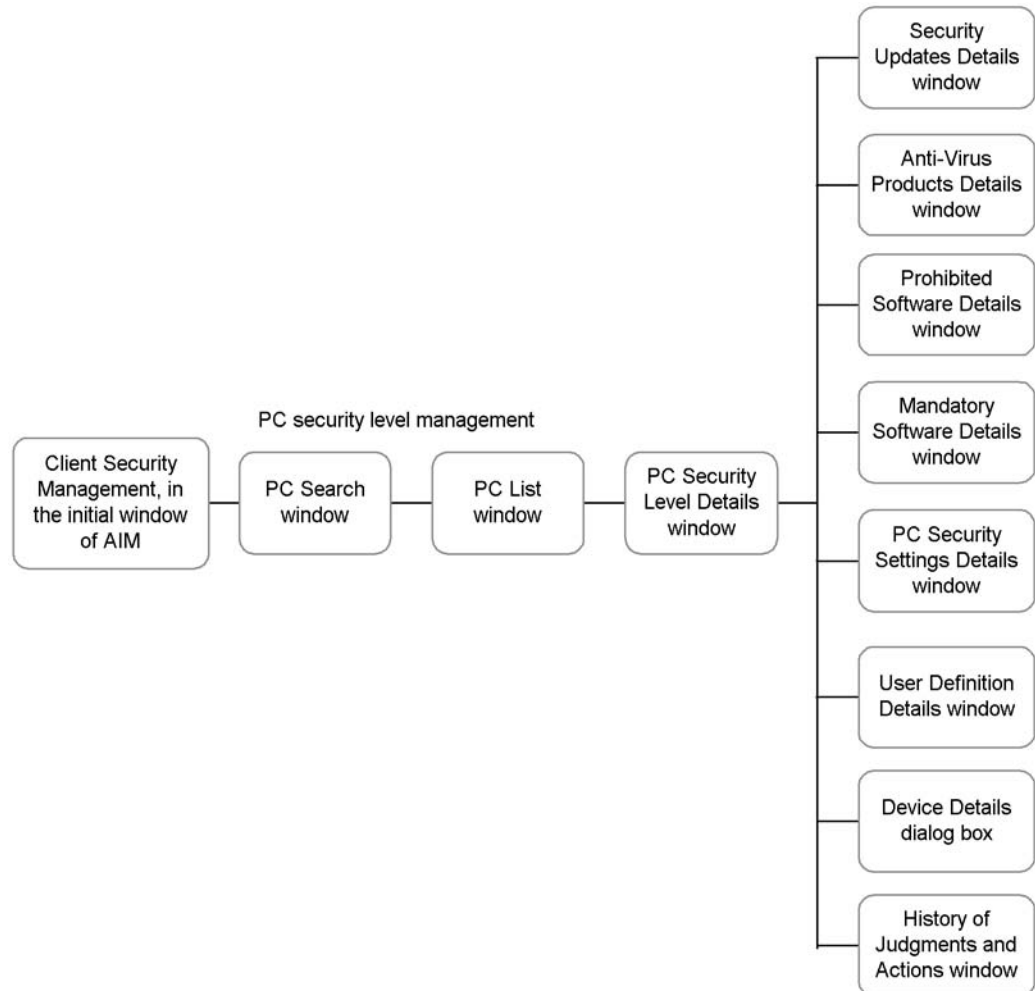
- 8.1 Transitions of windows used for client monitoring
- 8.2 Searching for clients
- 8.3 Checking detailed information for a client
- 8.4 Judging a client security level
- 8.5 Enabling and disabling security management for a client
- 8.6 Outputting history of judgments and actions as a CSV file

## 8.1 Transitions of windows used for client monitoring

An administrator can use the Client Security Management window in AIM to monitor client security levels.

The following figure shows the transitions of windows used for client monitoring.

*Figure 8-1:* Transitions of windows used for client monitoring



To open the initial window of AIM, log in to AIM as a user with the CSC administrator or CSC user role.

To log in to AIM:

1. Open a Web browser, and go to the Login window.

The Login window can be accessed by entering a URL from a Web browser. The URL of the Login window is `http://host-name/jplasset/login.htm`.

2. Set each item.

The items to set are as follows:

**User ID** text box

Enter the user ID of a CSC administrator or CSC user.

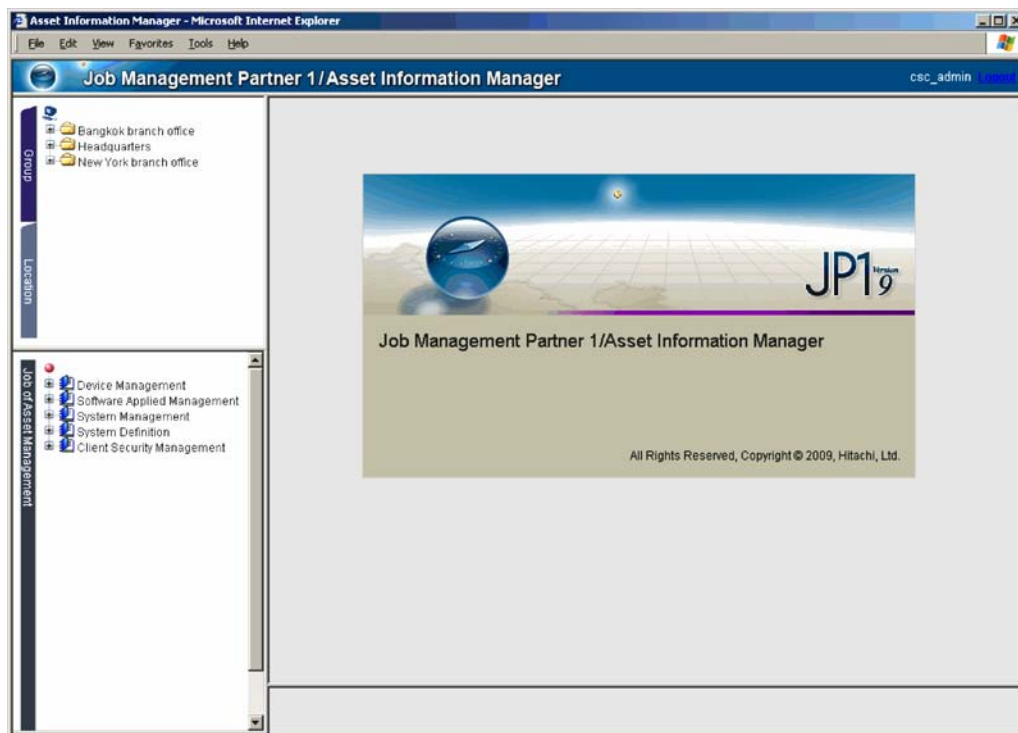
**Password** text box

Enter the password of the CSC administrator or CSC user.

3. Click the **Login** button.

If user authentication is successful, the initial window of AIM is displayed as shown in the following figure.

*Figure 8-2: Initial window of AIM*



## 8.2 Searching for clients

An administrator can specify search conditions to search for clients to be managed, and check the security status of clients that meet the search conditions.

Use the PC Search window to search for clients.

To search for clients by specifying search conditions:

1. From the job menu in the initial window of AIM, choose **Client Security Management**, and then **PC Security Level Management**.

The PC Search window is displayed.

Figure 8-3: PC Search window

The screenshot shows the 'Job Management Partner 1/Asset Information Manager' window. The left sidebar contains a tree view with 'Client Security Management' selected. The main area displays a search form with the following fields and options:

- Search:** CSV button
- Display:** 200 results per page
- Asset No.:** [Text input] match part of the words
- Host name:** [Text input] match part of the words
- IP address:** [Text input] match part of the words
- User name:** [Text input] including
- Group name:** [Text input] Browse
- PC security level:** [Dropdown] not less than
- PC security level judgment date:** [Text input] (YYYYMMDD)
- Number of consecutive times for the same security level:** [Text input] times not less than
- Number of consecutive days for the same security level:** [Text input] days not less than
- MAC address:** [Text input]
- Warning date:** [Text input] (YYYYMMDD)
- Network connection status:** [Dropdown]
- Update date of network connection status:** [Text input] (YYYYMMDD)
- Execution date of user definition:** [Text input] (YYYYMMDD)
- Security level of security updates:** [Dropdown] not less than
- Security level of anti-virus products:** [Dropdown] not less than

2. In the PC Search window, specify the search conditions.

Specify the search conditions in the PC Search window. Search is performed using an AND condition for the specified items.

The specified contents for each item are as follows.

Table 8-1: Specified contents for each item in the PC Search window

No.	Search condition item	Specification method	Specifiable search options	Default search option
1	<b>Asset No.</b>	Enter a unique number for user management, in 60 or fewer bytes of alphanumeric characters.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>match all the words</b></li> <li>• <b>match part of the words</b></li> <li>• <b>match beginning of the words</b></li> <li>• <b>match end of the words</b></li> </ul>	<b>match part of the words</b>
2	<b>Host name</b>	Enter the host name of the PC, in 64 or fewer bytes of characters.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>match all the words</b></li> <li>• <b>match part of the words</b></li> <li>• <b>match beginning of the words</b></li> <li>• <b>match end of the words</b></li> </ul>	<b>match part of the words</b>
3	<b>IP address</b>	Enter the IP address of the PC, in 15 or fewer bytes of alphanumeric characters.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>match all the words</b></li> <li>• <b>match part of the words</b></li> <li>• <b>match beginning of the words</b></li> <li>• <b>match end of the words</b></li> </ul>	<b>match part of the words</b>
4	<b>User name</b>	Enter the name of the PC user, in 255 or fewer bytes of characters.	None	None
5	<b>Group name</b> <sup>#1</sup>	Click the <b>Browse</b> button and specify the group.	None	None

## 8. Monitoring Clients

No.	Search condition item	Specification method	Specifiable search options	Default search option
6	<b>PC security level</b> <sup>#2</sup>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Not yet judged</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Safe</b></li> <li>• <b>Unknown</b></li> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>not greater than</b></li> <li>• <b>not less than</b></li> <li>• <b>equal</b></li> </ul>	<b>not less than</b>
7	<b>PC security level judgment date</b> (from the start date to the end date) <sup>#3</sup>	Enter a number in characters, in the <i>YYYYMMDD</i> format.	None	None
8	<b>Number of consecutive times for the same security level</b>	Enter a number in characters, from 0 to 999.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>not greater than</b></li> <li>• <b>not less than</b></li> <li>• <b>equal</b></li> </ul>	<b>not less than</b>
9	<b>Number of consecutive days for the same security level</b>	Enter a number in characters, from 0 to 999.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>not greater than</b></li> <li>• <b>not less than</b></li> <li>• <b>equal</b></li> </ul>	<b>not less than</b>
10	<b>MAC address</b>	Enter the MAC address of the PC, in 17 or fewer bytes of alphanumeric characters.	None	None
11	<b>Warning date</b> (from the start date to the end date) <sup>#3</sup>	Enter a number in characters, in the <i>YYYYMMDD</i> format.	None	None

No.	Search condition item	Specification method	Specifiable search options	Default search option
12	<b>Network connection status</b>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Permit</b></li> <li>• <b>Refuse</b></li> <li>• <b>Refuse in the emergency</b></li> <li>• -</li> </ul> - indicates that network control is not implemented.	None	None
13	<b>Update date of network connection status</b> (from the start date to the end date) <sup>#3</sup>	Enter a number in characters, in the <i>YYYYMMDD</i> format.	None	None
14	<b>Execution date of user definition</b> (from the start date to the end date) <sup>#3</sup>	Enter a number in characters, in the <i>YYYYMMDD</i> format.	None	None
15	<b>Security level of security updates</b> <sup>#2</sup>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Not yet judged</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Safe</b></li> <li>• <b>Unknown</b></li> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>not greater than</b></li> <li>• <b>not less than</b></li> <li>• <b>equal</b></li> </ul>	<b>not less than</b>
16	<b>Security level of anti-virus products</b> <sup>#2</sup>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Not yet judged</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Safe</b></li> <li>• <b>Unknown</b></li> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>not greater than</b></li> <li>• <b>not less than</b></li> <li>• <b>equal</b></li> </ul>	<b>not less than</b>

No.	Search condition item	Specification method	Specifiable search options	Default search option
17	<b>Security level of prohibited software<sup>#2</sup></b>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Not yet judged</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Safe</b></li> <li>• <b>Unknown</b></li> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>not greater than</b></li> <li>• <b>not less than</b></li> <li>• <b>equal</b></li> </ul>	<b>not less than</b>
18	<b>Security level of mandatory software<sup>#2</sup></b>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Not yet judged</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Safe</b></li> <li>• <b>Unknown</b></li> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>not greater than</b></li> <li>• <b>not less than</b></li> <li>• <b>equal</b></li> </ul>	<b>not less than</b>
19	<b>Security level of PC security settings</b>	<ul style="list-style-type: none"> <li>• Select one of the following from the pull-down menu:</li> <li>• <b>Not yet judged</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Safe</b></li> <li>• <b>Unknown</b></li> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	<ul style="list-style-type: none"> <li>• Select one of the following from the pull-down menu:</li> <li>• <b>not greater than</b></li> <li>• <b>not less than</b></li> <li>• <b>equal</b></li> </ul>	<b>not less than</b>
20	<b>Security level of user definition</b>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Not yet judged</b></li> <li>• <b>Not applicable</b></li> <li>• <b>Safe</b></li> <li>• <b>Unknown</b></li> <li>• <b>Caution</b></li> <li>• <b>Warning</b></li> <li>• <b>Danger</b></li> </ul>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>not greater than</b></li> <li>• <b>not less than</b></li> <li>• <b>equal</b></li> </ul>	<b>not less than</b>



No.	Search condition item	Specification method	Specifiable search options	Default search option
21	OS	Enter the name of the OS, in 200 or fewer bytes of characters.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>match all the words</b></li> <li>• <b>match part of the words</b></li> <li>• <b>match beginning of the words</b></li> <li>• <b>match end of the words</b></li> </ul>	<b>match part of the words</b>
22	<b>Location</b> <sup>#4</sup>	Click the <b>Browse</b> button and specify the location name.	None	None
23	<b>Security management</b>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>Valid</b></li> <li>• <b>Invalid</b></li> </ul>	None	None
24	<b>Evaluation point</b>	Enter a number in the range 0-100, or a hyphen (-). Specify - to search for a PC for which no evaluation points were awarded. <sup>#5</sup>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>not greater than</b></li> <li>• <b>not less than</b></li> <li>• <b>equal</b></li> </ul>	<b>not greater than</b>
25	<b>Judgment policy</b>	Enter the name of the judgment policy assigned to the PC, in 128 or fewer bytes of characters.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>match all the words</b></li> <li>• <b>match part of the words</b></li> <li>• <b>match beginning of the words</b></li> <li>• <b>match end of the words</b></li> </ul>	<b>match part of the words</b>
26	<b>Renewal date of judgment policy</b>	Enter a number in characters, in the <i>YYYYMMDD</i> format.	None	None
27	<b>Assigned date of judgment policy</b>	Enter a number in characters, in the <i>YYYYMMDD</i> format.	None	None

No.	Search condition item	Specification method	Specifiable search options	Default search option
28	<b>Action policy</b>	Enter the name of the action policy assigned to the PC, in 128 or fewer bytes of characters.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>match all the words</b></li> <li>• <b>match part of the words</b></li> <li>• <b>match beginning of the words</b></li> <li>• <b>match end of the words</b></li> </ul>	<b>match part of the words</b>
29	<b>Renewal date of action policy</b>	Enter a number in characters, in the <i>YYYYMMDD</i> format.	None	None
30	<b>Assigned date of action policy</b>	Enter a number in characters, in the <i>YYYYMMDD</i> format.	None	None

None: No search option is specified.

#1

Click the group **Browse** button to display the Browse Groups dialog box. Select the group you would like to specify, and click the **OK** button to specify the group.

#2

If **Unknown** and **not less than** are selected, the search is performed for **Unknown**, **Caution**, **Warning**, and **Danger**.

#3

Search is performed from 00:00:00 on the start day until 23:59:59 on the end day.

#4

Click the location **Browse** button to display the Browse Locations dialog box. Select the location you would like to specify, and click the **OK** button to specify the location.

#5

No evaluation points are awarded when any of the following is satisfied:

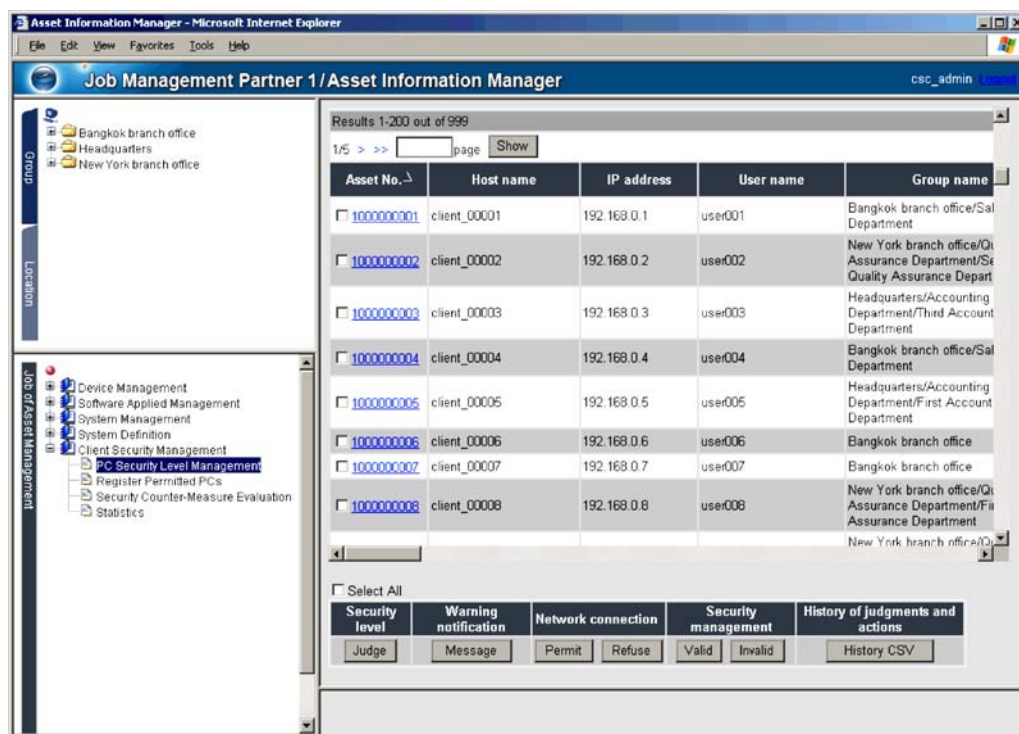
- **Not yet judged** is displayed for the security level of all the judgment items.
- **Not applicable** or **Unknown** is displayed for the security level of all the judgment items.

- No judgments have been executed since JP1/CSC - Manager was upgraded.

1. Specify **Display**, and then click the **Search** button.

Specify the number of results to display in the window, and perform the search. The PC List window is displayed, in which search results can be checked.

Figure 8-4: PC List window



The following table describes the items displayed in the PC List window.

Table 8-2: Items displayed in the PC List window

No.	Item	Description
1	<b>Asset No.</b>	PC asset number. An anchor (underlined link) is displayed below the asset number.
2	<b>Host name</b>	Name for identification
3	<b>IP address</b>	IP address
4	<b>User name</b>	Name of the user
5	<b>Group name</b>	Group to which the user belongs

No.	Item	Description
6	PC security level	PC security level. <b>Safe</b> , <b>Unknown</b> , <b>Caution</b> , <b>Warning</b> , <b>Danger</b> , <b>Not applicable</b> , or <b>Not yet judged</b> is displayed.
7	PC security level judgment date	Date on which the PC security level was judged
8	Number of consecutive times for the same security level	Number of times the same security level other than <b>Safe</b> existed during security level judgment
9	Number of consecutive days for the same security level	Number of days for which the same security level other than <b>Safe</b> existed during security level judgment
10	MAC address	MAC address
11	Warning date	Date of the latest user warning
12	Network connection status	PC network connection status. <b>Permit</b> , <b>Refuse</b> , <b>Refuse in the emergency</b> , or <b>-#1</b> is displayed.
13	Update date of network connection status	Date on which permission, denial, or refuse in the emergency of the PC network connection was implemented
14	Execution date of user definition	Date on which the user-defined action was executed
15	Security level of security updates	Security level for security updates
16	Security level of anti-virus products	Security level for anti-virus products
17	Security level of prohibited software	Security level for prohibited software
18	Security level of mandatory software	Security level for mandatory software
19	Security level of PC security settings	Security level for PC security settings
20	Security level of user definition	Security level for the user definition
21	OS	Name of the OS currently used
22	Location	Location
23	Security management	Whether PC security management is performed. <b>Valid</b> or <b>Invalid</b> is displayed.

No.	Item	Description
24	<b>Evaluation point</b>	Point indicating the status of PC security measures taken. A point or -#2 is displayed.
25	<b>Judgment policy</b>	Name of the judgment policy assigned to the PC
26	<b>Renewal date of judgment policy</b>	Date on which the judgment policy was updated
27	<b>Assigned date of judgment policy</b>	Date on which the judgment policy was assigned
28	<b>Action policy</b>	Name of the action policy assigned to the PC
29	<b>Renewal date of action policy</b>	Date on which the action policy was updated
30	<b>Assigned date of action policy</b>	Date on which the action policy was assigned

#1

For **Network connection status**, - indicates that network connection control is not implemented for the client, but that connection to the network is permitted.

#2

For **Evaluation point**, - is displayed if one of the following conditions is satisfied:

- **Not yet judged** is displayed for the security level of all the judgment items.
- **Not applicable** or **Unknown** is displayed for the security level of all the judgment items.
- No judgments have been executed since JP1/CSC - Manager was upgraded.

*Reference note:*

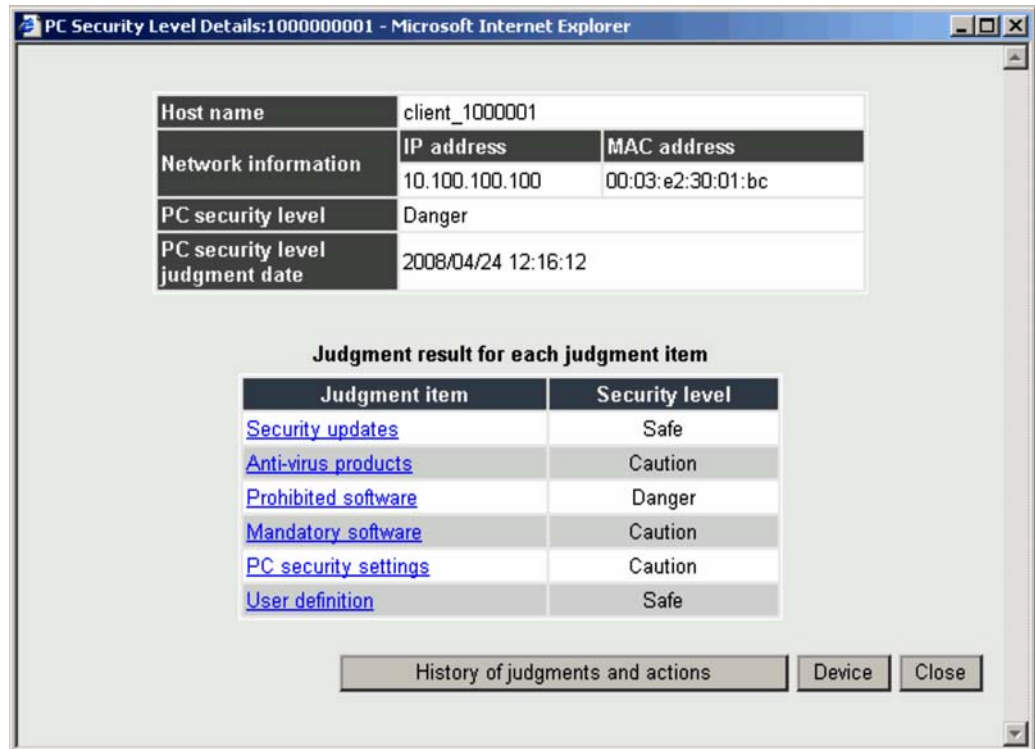
The Customize Job Windows window of AIM can be used to customize the contents displayed for the PC Search window and PC List window. The search condition items in the PC Search window and the search results in the PC List window can be set to be shown or hidden, and the display order of each item can be changed. For details about the Customize Job Windows window, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

### 8.3 Checking detailed information for a client

An administrator can use the PC List window to check detailed information about the security level for a selected client.

In the PC List window, click the **Asset No.** anchor to display detailed information about the client security level, in the PC Security Level Details window.

Figure 8-5: PC Security Level Details window



The following table describes the items displayed in the PC Security Level Details window.

Table 8-3: Items displayed in the PC Security Level Details window

No.	Item		Description
1	Host name		Name for identification
2	Network information <sup>#1</sup>	IP address	IP address
3		MAC address	MAC address

No.	Item		Description
4	<b>PC security level</b> <sup>#2</sup>		PC security level. <b>Safe, Unknown, Caution, Warning, Danger, Not applicable</b> , or <b>Not yet judged</b> is displayed.
5	<b>PC security level judgment date</b>		Date on which the PC security level was judged. This is displayed in <i>YYYY/MM/DD hh:mm:ss</i> format.
6	<b>Judgment item</b>	<b>Security updates</b>	Security level judgment items. Click the anchor for each judgment item to display the corresponding Details window.
7		<b>Anti-virus products</b>	
8		<b>Prohibited software</b>	
9		<b>Mandatory software</b>	
10		<b>PC security settings</b>	
11		<b>User definition</b>	
12	<b>Security level</b>		Security level for each judgment item. <b>Safe, Unknown, Caution, Warning, Danger, Not applicable</b> , or <b>Not yet judged</b> is displayed.

#1

Multiple lines can be displayed for PCs with multiple IP addresses and MAC addresses.

#2

The highest security level for the judgment items becomes the PC security level.

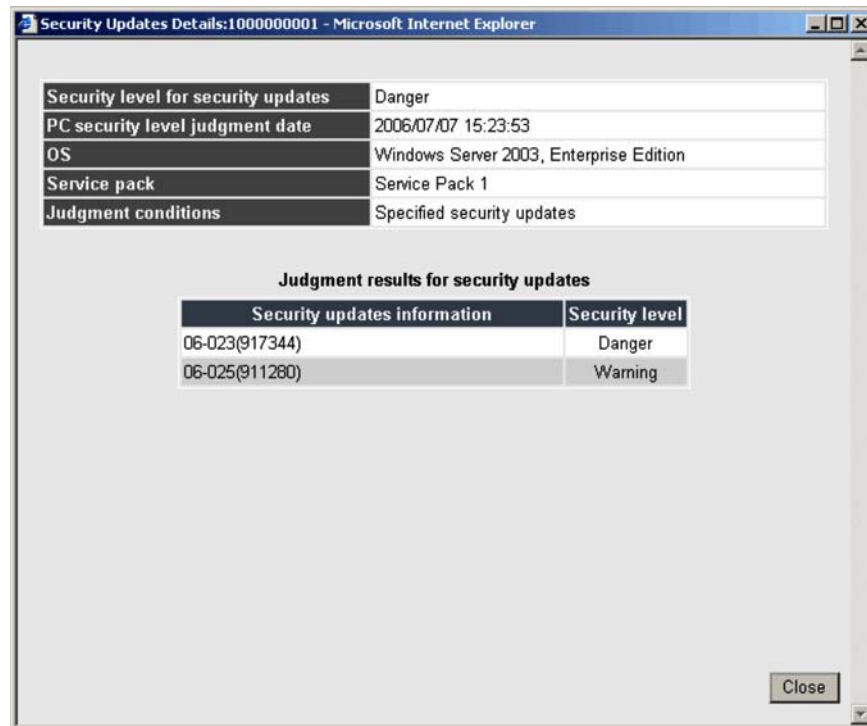
The following explains the Details window for each judgment item.

### 8.3.1 Checking detailed information for a security update

An administrator can use the Security Updates Details window to check detailed information about security updates for a selected client.

The Security Updates Details window is displayed by clicking the **Security updates** anchor for the judgment item, in the PC Security Level Details window.

Figure 8-6: Security Updates Details window



The following table describes the items displayed in the Security Updates Details window.

Table 8-4: Items displayed in the Security Updates Details window

No.	Item	Description
1	Security level for security updates	Security level for the security update. Of the security levels of all the security updates, that with the highest risk level becomes the security level of the security updates. <b>Safe, Unknown, Caution, Warning, Danger, or Not applicable<sup>#1</sup></b> is displayed.
2	PC security level judgment date	Date on which the PC security level was judged. This is displayed in <i>YYYY/MM/DD hh:mm:ss</i> format.
3	OS	Name of the OS currently used
4	Service pack	Type of service packs applied to the OS



No.	Item	Description
5	<b>Judgment conditions</b> <sup>#2</sup>	Judgment conditions set in the Edit Judgment Policy (Security Update) window. <b>Latest security updates</b> or <b>Specified security updates</b> is displayed.
6	<b>Security updates information</b>	<ul style="list-style-type: none"> <li>When the judgment condition is <b>Latest security updates</b>: The update number and article ID number are displayed.</li> <li>When the judgment condition is <b>Specified security updates</b>: The update number and article ID number are displayed. Note that if the service pack and IE version set on the client are older than the judgment policy definition, the service pack and IE version defined in the judgment policy are displayed.<sup>#3</sup></li> </ul>
7	<b>Security level</b>	Security level judgment results for each piece of security update information. <b>Safe</b> , <b>Unknown</b> , <b>Caution</b> , <b>Warning</b> , or <b>Danger</b> is displayed.

#1

**Not applicable** is displayed when any of the following conditions applies:

- JP1/Software Distribution Client is not installed on the client.
- The version of JP1/Software Distribution Client installed on the client is 07-00 or earlier.
- The **Make this a judgment target** check box in the Edit Judgment Policy (Security Update) window is cleared.
- The **Make this a judgment target** check box in the Edit Judgment Policy (Security Update) window is selected, and the judgment condition is one of the following:

**Latest security updates**: If MBSA is being used, the MBSA command line interface and MBSA database files have not been distributed to the client. If WUA is being used, WUA 2.0 and Windows Installer 3.0 have not been installed on the client, and the WUA 2.0 database files have not been distributed to the client.

**Specified security updates**: no security update is defined in the judgment policy.

#2

The contents displayed for **Security updates information** are different depending on **Judgment conditions**. The contents displayed for each judgment condition are as follows:

- For **Latest security updates**:

When an administrator selects **Latest security updates** for the judgment policy settings and sets a security update, **Latest security updates** is displayed for **Judgment conditions** in the Security Updates Details window. Information about the latest security update not installed on the client is displayed for **Security updates information** in the Security Updates Details window. Note that if **Exclude specified security update** is selected in the Edit Judgment Policy (Security Update) window, the excluded security update is not displayed here.

- For **Specified security updates**:

When an administrator selects **Specify security updates** for the judgment policy settings and sets a security update, **Specified security updates** is displayed for **Judgment conditions** in the Security Updates Details window. Information about mandatory security updates not installed on the client is displayed in **Security updates information**, in the Security Updates Details window.

#3

The service pack and IE version are displayed on a separate line from the update number and article ID number.

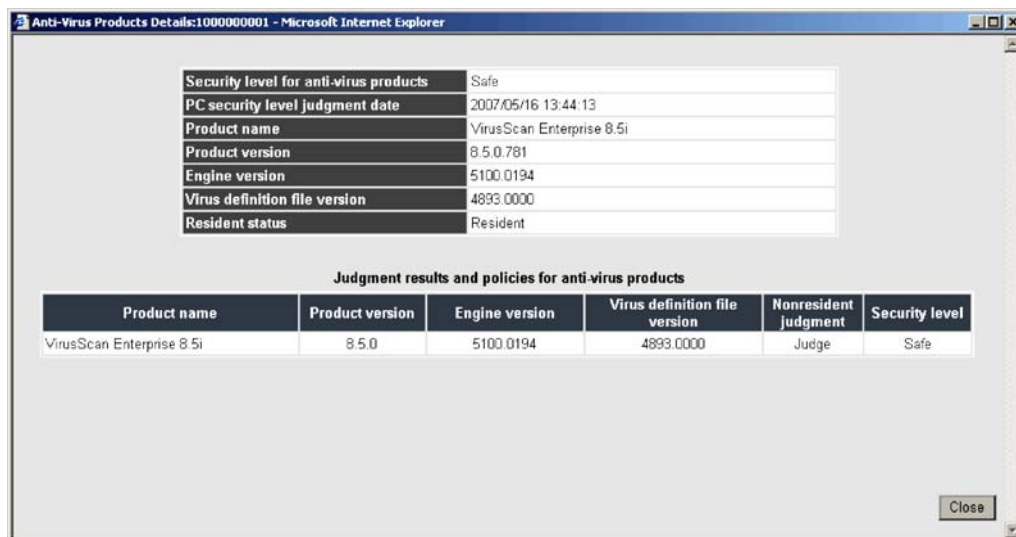
For details about the settings for the security update judgment policy, see *6.3 Editing a security update judgment policy*.

### 8.3.2 Checking detailed information for an anti-virus product

An administrator can use the Anti-Virus Products Details window to check detailed information about anti-virus products for a selected client.

The Anti-Virus Products Details window is displayed by clicking the **Anti-virus products** anchor for the judgment item, in the PC Security Level Details window.

Figure 8-7: Anti-Virus Products Details window



The following table describes the items displayed in the Anti-Virus Products Details window.

Table 8-5: Items displayed in the Anti-Virus Products Details window

No.	Item	Description
1	Security level of anti-virus products	Security level for the PC anti-virus product. <b>Safe, Unknown, Caution, Warning, Danger</b> , or <b>Not applicable</b> <sup>#</sup> is displayed.
2	PC security level judgment date	Date when the PC security level was judged. This is displayed in <i>YYYY/MM/DD hh:mm:ss</i> format.
3	Product name	Name of the anti-virus product currently used on the PC
4	Product version	Version information for the anti-virus product currently used on the PC
5	Engine version	Version information for the virus search engine of the anti-virus product
6	Virus definition file version	Version information for the virus definition file defined as mandatory by the administrator
7	Resident status	Status of whether or not an anti-virus product is resident on the PC. <b>Resident, Nonresident</b> , or nothing (when search cannot be performed) is displayed.
8	Product name	Name of the anti-virus product set in the judgment policy

No.	Item	Description
9	<b>Product version</b>	Version information of the anti-virus product set in the judgment policy
10	<b>Engine version</b>	Version information of the virus search engine for the anti-virus product set in the judgment policy
11	<b>Virus definition file version</b>	Version information for the virus definition file defined as mandatory in the judgment policy
12	<b>Nonresident judgment</b>	Whether or not anti-virus product residency is to be judged under the judgment policy. <b>Judge</b> or <b>Do not judge</b> is displayed.
13	<b>Security level</b>	Security level judgment results for the anti-virus product. <b>Safe</b> , <b>Unknown</b> , <b>Caution</b> , <b>Warning</b> , or <b>Danger</b> is displayed.

#

**Not applicable** is displayed when any of the following conditions applies:

- JP1/Software Distribution Client is not installed on the client.
- The version of JP1/Software Distribution Client installed on the client is Version 6 or earlier.
- The **Make this a judgment target** check box in the Edit Judgment Policy (Anti-Virus Product) window is cleared.
- The **Make this a judgment target** check box in the Edit Judgment Policy (Anti-Virus Product) window is selected, and no anti-virus product is defined in the judgment policy.
- The **Make this a judgment target** check box in the Edit Judgment Policy (Anti-Virus Product) window is selected, and the anti-virus product installed on the client does not exist in the judgment policy.

### 8.3.3 Checking detailed information for prohibited software

An administrator can use the Prohibited Software Details window to check detailed information about prohibited software for a selected client.

The Prohibited Software Details window is displayed by clicking the **Prohibited software** anchor for the judgment item, in the PC Security Level Details window.

Figure 8-8: Prohibited Software Details window

Security level for prohibited software	Safe
PC security level judgment date	2005/07/21 14:57:56

**Judgment results for prohibited software**

Prohibited software name	Install status	Installed version	Prohibited version	Security level
cardgame	Not installed			Safe
baseballgame	Not installed			Safe

Close

The following table describes the items displayed in the Prohibited Software Details window.

Table 8-6: Items displayed in the Prohibited Software Details window

No.	Item	Description
1	<b>Security level for prohibited software</b>	Security level for prohibited software on the PC. Of the security levels of all the security updates, that with the highest risk level becomes the security level of the prohibited software. <b>Safe, Unknown, Caution, Warning, Danger, or Not applicable<sup>#</sup></b> is displayed.
2	<b>PC security level judgment date</b>	Date when the PC security level was judged. This is displayed in <i>YYYY/MM/DD hh:mm:ss</i> format.
3	<b>Prohibited software name</b>	The following information is displayed: <ul style="list-style-type: none"> <li>Name of the prohibited software set in the judgment policy</li> <li>Name of the prohibited software installed on the selected client</li> </ul>
4	<b>Install status</b>	Installation status of prohibited software on the PC. <b>Installed</b> or <b>Not installed</b> is displayed.

No.	Item	Description
5	<b>Installed version</b>	Version information for the prohibited software installed on the PC
6	<b>Prohibited version</b>	Version information for the prohibited software defined in the judgment policy
7	<b>Security level</b>	Judgment results for each security level of the prohibited software. <b>Safe</b> , <b>Unknown</b> , <b>Caution</b> , <b>Warning</b> , or <b>Danger</b> is displayed.

#

**Not applicable** is displayed when any of the following conditions applies:

- JP1/Software Distribution Client is not installed on the client.
- The **Make this a judgment target** check box in the Edit Judgment Policy (Prohibited Software) window is cleared.
- The **Make this a judgment target** check box in the Edit Judgment Policy (Prohibited Software) window is selected, and no prohibited software is defined in the judgment policy.

### 8.3.4 Checking detailed information for mandatory software

An administrator can use the Mandatory Software Details window to check detailed information about mandatory software for a selected client.

The Mandatory Software Details window is displayed by clicking the **Mandatory software** anchor for the judgment item, in the PC Security Level Details window.

Figure 8-9: Mandatory Software Details window



The following table describes the items displayed in the Mandatory Software Details window.

Table 8-7: Items displayed in the Mandatory Software Details window

No.	Item	Description
1	<b>Security level for mandatory software</b>	Security level for mandatory software on the PC. <b>Safe, Unknown, Caution, Warning, Danger, or Not applicable<sup>#1</sup></b> is displayed.
2	<b>PC security level judgment date</b>	Date when the PC security level was judged. This is displayed in <i>YYYY/MM/DD hh:mm:ss</i> format.
3	<b>Software group name</b>	Group name set in the judgment policy
4	<b>Mandatory software name</b>	The following information is displayed: <ul style="list-style-type: none"> <li>Name of the mandatory software set in the judgment policy</li> <li>Name of the mandatory software installed on the selected client</li> </ul>
5	<b>Install status</b>	Installation status of mandatory software on the PC. <b>Installed</b> or <b>Not installed</b> is displayed.
6	<b>Installed version</b>	Version information for the mandatory software installed on the PC
7	<b>Mandatory version</b>	Version information for the mandatory software defined in the judgment policy

No.	Item	Description
8	<b>Security level of software</b>	Judgment results for each security level of the mandatory software. <b>Safe</b> , <b>Unknown</b> , <b>Caution</b> , <b>Warning</b> , <b>Danger</b> , or <b>Not applicable</b> <sup>#1</sup> is displayed.
9	<b>Security level of group</b>	Security level for each group <sup>#2</sup>

#1

**Not applicable** is displayed when any of the following conditions applies:

- The **Make this a judgment target** check box in the Edit Judgment Policy (Mandatory Software) window is cleared.
- In the Edit Judgment Policy (Mandatory Software) window, the **Make this a judgment target** check box is selected and the **Judge Client** check box is cleared.

#2

If any of the mandatory software items registered in the group is judged to be *Safe*, **Safe** is displayed for the security level of that group.

### 8.3.5 Checking detailed information for PC security settings

An administrator can use the PC Security Settings Details window to check detailed information about the PC security settings for a selected client.

The PC Security Settings Details window is displayed by clicking the **PC security settings** anchor for the judgment item, in the PC Security Level Details window.



Figure 8-10: PC Security Settings Details window

Group	Judgment item	PC settings	Judgment condition	Security level
Accounts	Guest account settings	Invalid Guest account	Valid Guest account	Safe
	Vulnerable password	Does not exist	-	Safe
Passwords	Password that never expires	Administrator,IUSR_VM-2003_ENG,IWAM_VM-2003_ENG,SQLDebugger	-	Warning
	Days since the password was updated	Administrator,IUSR_VM-2003_ENG,IWAM_VM-2003_ENG,SQLDebugger	180days or more	Warning
Logon	Automatic logon settings	Not specified	-	Safe
	Power-on password settings	Not specified	Not specified	Warning
Shares	Shared folder settings	Specified	-	Warning
Anonymous connections	Anonymous connections are restricted	Invalid (not restrict)	-	Warning
Services	Unnecessary services are running	An unnecessary service exists	-	Warning
Firewall	Windows Firewall Settings	Invalid	Invalid	Warning
Automatic updates	Settings for Windows automatic updates	Invalid	-	Warning
	Screensaver settings	Valid	-	Safe
Screensaver	Password protection of screensaver	Valid	-	Safe
Drive encryption	Drive encryption by BitLocker		The system drive is not encrypted	Caution

The following table describes the items displayed in the PC Security Settings Details window.

Table 8-8: Items displayed in the PC Security Settings Details window

No.	Item	Description
1	<b>Security level for PC security settings</b>	Security level for the PC security settings. This is the highest security risk level for the judgment items among the security level results in item 7. <b>Safe, Unknown, Caution, Warning, Danger, or Not applicable<sup>#</sup></b> is displayed.
2	<b>PC security level judgment date</b>	Date when the PC security level was judged. This is displayed in <i>YYYY/MM/DD hh:mm:ss</i> format.
3	<b>Group</b>	Group name assigned to the judgment item.
4	<b>Judgment item</b>	Name of the item that was judged.
5	<b>PC settings</b>	Information about the setting on the client PC for the judgment item.
6	<b>Judgment condition</b>	Judgment condition set for the judgment item.

No.	Item	Description
7	Security level	Judgment result for the judgment item. <b>Safe, Unknown, Caution, Warning, Danger</b> , or <b>Not applicable</b> <sup>#</sup> is displayed.

#

**Not applicable** is displayed when none of the judgment items is applicable. This situation arises when either of the following conditions applies:

- JP1/Software Distribution Client is not installed on the client.
- The version of JP1/Software Distribution Client is 08-10 or earlier.

### 8.3.6 Checking detailed information for a user definition

An administrator can use the User Definition Details window to check detailed results relating to a user definition for a selected client.

The User Definition Details window is displayed by clicking the **User definition** anchor for the judgment item, in the PC Security Level Details window.

Figure 8-11: User Definition Details window



The following table describes the items displayed in the User Definition Details window.

Table 8-9: Items displayed in the User Definition Details window

No.	Item	Description
1	<b>Security level for user definition</b>	PC security level in respect of the user definition. This is the highest security risk level for the judgment item among the security level results in item 10. <b>Safe, Unknown, Caution, Warning, Danger, or Not applicable</b> <sup>#</sup> is displayed.
2	<b>PC security level judgment date</b>	Date when the PC security level was judged. This is displayed in <i>YYYY/MM/DD hh:mm:ss</i> format.
3	<b>Judgment item</b>	Name of a user-defined judgment item in the judgment policy.
4	<b>Class</b>	Class set for the user-defined judgment condition in the judgment policy. For details about classes that can be set, see Table 6-30 <i>List of classes and properties that can be used in user-defined judgments</i> .
5	<b>Property</b>	Property set for the user-defined judgment condition in the judgment policy. For details about properties that can be set, see Table 6-30 <i>List of classes and properties that can be used in user-defined judgments</i> .
6	<b>Value</b>	Value of the property when the user definition was judged.
7	<b>Comparison condition</b>	Comparison condition set for the user-defined judgment condition in the judgment policy. <b>Match all the words, Match part of the words, Match beginning of the words, Match end of the words, Match, Do not match, Not greater than, or Not less than</b> is displayed.
8	<b>Comparison value</b>	Comparison value set for the user-defined judgment condition in the judgment policy.
9	<b>Result</b>	Judgment result for the judgment condition. <b>Failed</b> (Match), <b>Passed</b> (Do not match), <b>Skip, Unknown, or -</b> (Not yet judged) is displayed.
10	<b>Security level</b>	Judgment result for the judgment item. <b>Safe, Unknown, Caution, Warning, Danger, or Not applicable</b> <sup>#</sup> is displayed.

#

**Not applicable** is displayed in the following circumstances:

- If **Not applicable** appears for **Security level for user definition**  
The judgment result for all items was **Not applicable**.
- If **Not applicable** appears for **Security level**

The result of all judgment conditions was **Skip**.

### 8.3.7 Checking device details for a client

An administrator can use the PC List window to check detailed device information for a selected client. Detailed device information is displayed in the Device Details dialog box by clicking the **Device** button in the PC Security Level Details window.

A variety of device information is displayed in the Device Details dialog box. The information and pages displayed in this dialog box are as follows:

- Asset information and hardware asset information (**Device** page)
- Network information (**Network** page)
- Information about installed software (**Software** page)
- Patch information (**Patch** page)
- Information about anti-virus products (**Anti-Virus** page)
- License information (**License** page)<sup>#</sup>
- Inventory information (**Inventory** page)
- Contract information (**Contract** page)<sup>#</sup>
- Maintenance history (**Maintenance** page)<sup>#</sup>
- Transfer log, device change log and software update records log (**Update Records** page)<sup>#</sup>

For details about the Device Details dialog box, see the manual *Job Management Partner 1/Asset Information Manager Administrator's Guide*.

#

Not displayed if the management server is set up using Asset Information Manager Subset Component of JP1/Software Distribution Manager.

*Note:*

For details about how to prevent CSC administrators and CSC users from updating detailed device information, see *5.8.3 Preventing update processing for detailed device information*.

### 8.3.8 Checking history of judgments and actions for a client

An administrator can use the PC List window to check by GUI the history of judgments and actions for a selected client, and output the history as a CSV file.

### (1) Checking the client's history of judgments and actions in the GUI

Judgment and action history is displayed in the History of Judgments and Actions window by clicking the **History of judgments and actions** button in the PC Security Level Details window.

Figure 8-12: History of Judgments and Actions window

Trigger for judgment or action	PC security level	PC security level judgment date	Administrator Email notification	User Message notification	Network Permit connection	Refuse connection	Action
Inventory information collection	Safe	2007/08/21 14:58:14					
Administrator indication	Caution	2007/08/19 01:46:17	Passed	Passed			Ac
Network connection control command	Warning					Passed	
Judgment command execution	Warning	2007/08/14 17:43:34		Passed			Ac
Inventory information collection	Safe	2007/08/11 07:12:54			Passed		
Inventory information collection	Danger	2007/08/05 04:18:14				Passed	Ac
Inventory information collection	Caution		Passed				Ac

The following table describes the items displayed in the History of Judgments and Actions window.

Table 8-10: Items displayed in the History of Judgments and Actions window

No.	Item	Description
1	Trigger for judgment and action <sup>#1</sup>	The timing at which a client security level is judged and an action is implemented. <b>Inventory information collection, Administrator indication, Judgment command execution, Action command, or Network control command</b> is displayed.
2	PC security level	PC security level. <b>Safe, Unknown, Caution, Warning, Danger, Not applicable, or Not yet judged</b> is displayed. In the PC List window, when an administrator clicks the <b>Message, Permit, or Refuse</b> button to implement an action, the PC security level of the previous history is inherited and displayed.
3	PC security level judgment date	Date when the PC security level was judged. This is displayed in <b>YYYY/MM/DD hh:mm:ss</b> format. In the PC List window, when an administrator clicks the <b>Message, Permit, or Refuse</b> button to implement an action, nothing is displayed.

No.	Item	Description
4	<b>Email notification</b> <sup>#2</sup>	Displays the results of actions implemented to perform administrator email notification. If nothing is displayed, no action was implemented to notify the administrator by email.
5	<b>Message notification</b> <sup>#3</sup>	Displays the results of actions implemented to perform message notification to the client user. If nothing is displayed, no action was implemented to notify the user by message.
6	<b>Permit connection</b> <sup>#4</sup>	Displays the results of permitting a client network connection. If nothing is displayed, no action was implemented to permit the client network connection.
7	<b>Refuse connection</b> <sup>#4</sup>	Displays the results of refusing a client network connection. If nothing is displayed, no action was implemented to refuse the client network connection.
8	<b>Action name</b>	The user-defined action name set for the action policy.
9	<b>Action result</b> <sup>#5</sup>	The result of implementing the user-defined action. If nothing is displayed, no user-defined action was implemented.
10	<b>Action date</b>	Date when the action was implemented. This is displayed in <i>YYYY/MM/DD hh:mm:ss</i> format.
11	<b>Judgment policy</b>	Name of the judgment policy used to judge the PC security level.
12	<b>Action policy</b>	Name of the action policy used to implement actions according to the security level judgment results.

#1

Judgment of the security level and implementation of an action are triggered by one of the following:

- **Inventory information collection**

When the client inventory information collected by JP1/Software Distribution is updated, the security level is automatically judged, and an action is implemented according to the security level judgment results.

- **Administrator indication**

In the PC list window of the Client Security Management window, an administrator specifies a client, and then judges the security level or implements an action.

- **Judgment command execution**

When an administrator executes the security level judgment command

(`cscjudge`), the security level is judged and an action is implemented according to the security level judgment results.

- **Action command**

When an administrator executes the action command (`cscaction`), an action is implemented according to the security level judgment results.

- **Network connection control command**

When an administrator executes the network control command (`cscnetctrl`), client network connections are permitted or an emergency denial is enforced.

#2

If **Notify the administrator by email** is selected for an action policy setting and processing is successful, **Passed** is displayed. If processing fails, **Failed** is displayed.

#3

If **Send message to user** is selected for an action policy setting, or an administrator uses the PC List window to perform Message notification, and processing is successful, **Passed** is displayed. If processing fails, **Failed** is displayed.

#4

- If **Control network connection** is selected for an action policy setting or an administrator uses the PC List window to perform network control, and the network permission or denial is successful, **Passed** is displayed. If permission or denial fails, **Failed** is displayed.

Note that if a client has more than one MAC address, **Failed** is displayed if network control fails for even one of those MAC addresses.

- If **Network connection control command** is displayed for **Trigger for judgment and action**, and **Passed** is displayed for **Refuse connection**, this means that the status of the network connection is *Refuse in the emergency*.
- If **Network connection control command** or **Administrator indication** is displayed for **Trigger for judgment and action**, and **Passed** is displayed for **Permit connection**, this means that the network connection is no longer in *Refuse in the emergency* status.
- If **Inventory information collection** is displayed for **Trigger for judgment and action**, and **Permit connection** is blank, this means one of the following:
  - There is no setting in the action policy for permitting network connections.

- Because the status of the network connection is *Refuse in the emergency*, network connection permission based on the security level judgment result was ignored.

#5

When **Action for the user definition** is selected for an action policy setting, or when an administrator uses the PC List window to perform a user-defined action, **Passed** is displayed if the action is successful. If the action fails, **Failed** is displayed.

Note that the default number of results displayed in the History of Judgments and Actions window is 20. To change this number, in the JP1/CSC - Manager setup window, change **Number of history preservation generations**. For details about the JP1 /CSC - Manager setup window, see *5.4.3 Setting up JP1/CSC - Manager*.

## ***(2) Outputting the client's history of judgments and actions as a CSV file***

Judgment and action history for a client is displayed in the History CSV Output window by clicking the **CSV** button in the History of Judgments and Actions window.

Figure 8-13: History CSV Output window

```
"Asset No.", "Trigger for judgment or action", "PC security level", "PC security level I", "PC s
"1000000001", "Inventory information collection", "Safe", "2007/08/21 14:58:14", "", "", "", ""
"1000000001", "Administrator indication", "Caution", "", "Passed", "", "", "", "2007/08/20 17
"1000000001", "Administrator indication", "Caution", "2007/08/19 01:46:17", "Passed", "", "", ""
"1000000001", "Network connection control command", "Warning", "", "", "", "Passed", "", ""
"1000000001", "Judgment command execution", "Warning", "2007/08/14 07:43:34", "", "Pas
"1000000001", "Inventory information collection", "Safe", "2007/08/11 07:12:54", "", "Pass
"1000000001", "Inventory information collection", "Danger", "2007/08/05 04:18:14", "", ""
"1000000001", "Inventory information collection", "Caution", "Passed", "", "", "Action1", "P
```



---

## 8.4 Judging a client security level

---

An administrator can judge the security level for a selected client.

To judge the security level for a selected client:

1. In the PC Search window, search for the client for which the security level is to be judged.

The PC List window is displayed.

2. In the PC List window, select the **Asset No.** check box for the client for which the security level is to be judged.

The client to be judged is selected. To perform judgment for all found clients, select the **Select All** check box. When the **Select All** check box is selected, each **Asset No.** check box will not be selected.

3. Click the **Judge** button.

A confirmation message box is displayed.

4. Click the **OK** button.

Judgment processing is performed and the Action Message dialog box is displayed. If an error message is displayed, see *17.4.1 Action messages in the PC List window*, and act accordingly.

5. Click the **Close** button.

The Action Message dialog box closes.

To check the judgment results, perform a search again, and check the contents displayed for **PC security level** in the PC List window.

Note that judgment is only performed for clients for which **Security management** is set to **Valid**. For details about how to enable and disable security management, see 8.5 *Enabling and disabling security management for a client*.

If you have selected **Skip** for the **Perform judgment if asset information is not updated** setting in JP1/CSC - Manager, security level judgment is skipped for clients whose asset information has not changed since the last time their security level was judged. For details about this setting, see 5.4.3 *Setting up JP1/CSC - Manager*.

---

## 8.5 Enabling and disabling security management for a client

---

Although the client security control system manages security for all Windows machines on which JP1/Software Distribution Client is installed, not all Windows machines require security management. For example, Windows server machines managed by the administrator do not need to receive messages and are not subject to network control. For such machines, disable security management. Judgment is not performed by security policy or administrator for machines for which **Security management** is set to **Invalid**. Note that if an administrator uses the PC List window to manually implement an action, Message notification and network connection control can be performed even for clients for which **Security management** is set to **Invalid**.

### 8.5.1 Disabling security management

An administrator can use the PC List window to select a machine for which security management is performed, and disable security management.

To disable security management for a specified client:

1. In the PC Search window, search for the machine for which to disable security management.

The PC List window is displayed.

2. In the PC List window, select the **Asset No.** check box for the client for which security management is to be disabled.

Select the machine to be disabled.

3. For **Security management**, click the **Invalid** button.

A confirmation message box is displayed.

4. Click the **OK** button.

Processing to disable security management is performed, and the Action Message dialog box is displayed. If an error message is displayed, see *17.4.1 Action messages in the PC List window*, and act accordingly.

5. Click the **Close** button.

The Action Message dialog box closes.

To check the results of disabling security management, perform a search again, and check the contents displayed for **Security management** in the PC List window.

*Note:*

Exclude non-Windows machines, such as HP-UX and Solaris machines, from non-Software Distribution host detection. Because they are excluded, these machines are not subject to security management, and therefore are not displayed in the Client Security Management window. For details about how to exclude these machines from non-Software Distribution host detection, see *7.2.2 Excluding non-Windows machines from detection*.

## 8.5.2 Enabling security management

An administrator can use the PC List window to select a machine for which security management is not being performed, and enable security management.

To enable security management for a specified client:

1. In the PC Search window, search for the machine for which security management is to be enabled.

The PC List window is displayed.

2. In the PC List window, select the **Asset No.** check box for the client for which security management is to be enabled.

Select the machine to be enabled.

3. For **Security management**, click the **Valid** button.

A confirmation message box is displayed.

4. Click the **OK** button.

Processing to enable security management is performed, and the Action Message dialog box is displayed. If an error message is displayed, see *17.4.1 Action messages in the PC List window*, and act accordingly.

5. Click the **Close** button.

The Action Message dialog box closes.

To check the results of enabling security management, perform a search again, and check the contents displayed for **Security management** in the PC List window.

---

## 8.6 Outputting history of judgments and actions as a CSV file

---

The history of judgments and actions of a client selected in the PC List window can be output to a CSV file.

To output the history of judgments and actions of a selected client to a CSV file:

1. In the PC Search window, search for the machine from which the history of judgments and actions are to be output to a CSV file.

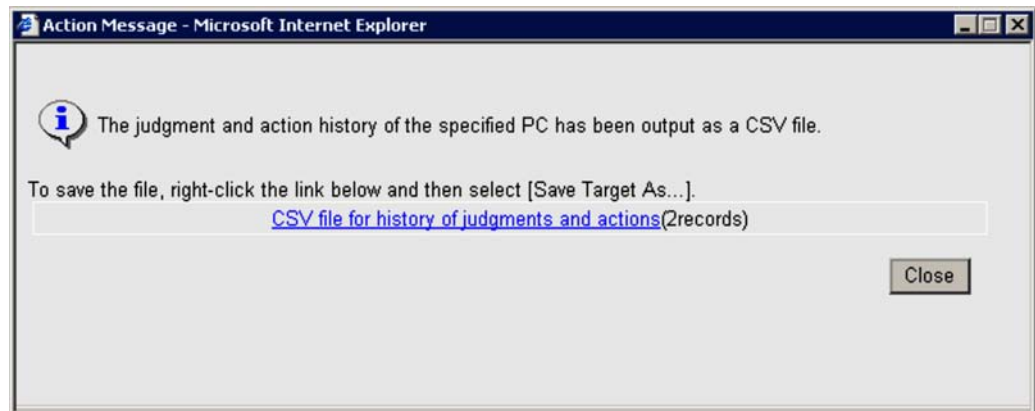
The PC List window is displayed.

2. In the PC List window, select the **Asset No.** check box for the client for which the history of judgments and actions are to be output to a CSV file.

The client for which a CSV file is to be output is selected.

3. For **History of judgments and actions**, click the **History CSV** button.

Processing to output a CSV file is performed, and the Action Message dialog box is displayed.



If an error message is displayed, see *17.4.1 Action messages in the PC List window*, and act accordingly.

4. In the Action Message dialog box, right-click the **CSV file for history of judgments and actions** link, and select **Save Target As...**

The Save As dialog box is displayed.

5. For **File name** in the Save As dialog box, enter a file name and click the **Save** button.

Change the file name, as a string (consisting of alphanumeric characters and

symbols) to identify the file set by default for **File name** in the Save As dialog box.

The history of judgments and actions is saved to a file in CSV format.

To view the CSV file, in the Action Message dialog box, right-click the **CSV file for history of judgments and actions** link, and select **Open in new window**. The CSV file of the history of judgments and actions is displayed in a separate window.



## Chapter

---

# 9. Dealing with Security Risks

---

This chapter explains the actions implemented for clients with a high security level. Actions consist of those implemented by an action policy based on security level judgment results, and those performed by an administrator.

- 9.1 Action implementation methods and action types
- 9.2 Sending messages to client users
- 9.3 Controlling client network connections
- 9.4 Sending email to administrators
- 9.5 Executing user-defined actions

---

## 9.1 Action implementation methods and action types

---

This section explains how to implement actions, as well as the types of actions.

### 9.1.1 Action implementation methods

Actions for clients with a high security level are implemented in the following two ways:

- By security level judgment results

Actions are implemented by action policy when the following security level judgments are performed:

- Automatic judgment when inventory information is updated
- Judgment by periodic task execution

- By an administrator

An administrator can perform the following three types of actions:

- Implementing an action from the Client Security Management window

An administrator can use the PC Search window to search for clients, and perform actions for those judged to be at risk. For example, if warning messages have been sent based on an action policy but still there are clients for which no measures have been taken, an administrator can implement an action manually. In this case, warning messages can be sent and the clients forced to disconnect from the network, irrespective of the result of the security level judgment.

- Implementing an action by using the action command (`cscaction`)

By issuing the action command (`cscaction`) from a management server, an administrator can implement an action according to the result of the latest security level judgment.

For example, the administrator can use the functionality that allows the judgment of security levels and implementation of actions to be done separately to implement actions based on the result of security level judgment. The administrator can also implement actions again for specific clients.

For details about the action command (`cscaction`), see *cscaction (implements actions for a specified client)* in 15. Commands.

- Implementing an action by using the network control command

By issuing the network control command (`cscnetctrl`) from a remote



management server, an administrator can permit or immediately deny client connections to the network. For example, if the remote management server detects that the client is infected with a virus, the administrator can, from the remote system, immediately stop the client from accessing the network. Immediate denial by using the network control command (*cscnetctrl*) takes precedence over any other action.

For details about the network control command, see *cscnetctrl (controls network connections)* in 15. *Commands*.

### 9.1.2 Action types

Implemented actions consist of the following types:

- Sending messages to client users

Client users can be notified of security level judgment results via messages. The messages sent are displayed as pop-up windows on the client's screen. For details about how to send messages to client users, see 9.2 *Sending messages to client users*.

- Controlling client network connections

Clients can be granted or denied network connection, and can be immediately prevented from accessing the network in an emergency. This action is available only with a quarantine system. For details about controlling client network connections, see 9.3 *Controlling client network connections*.

- Sending emails to administrators

Administrators can be notified of security level judgment results via email. For details about how to send email to administrators, see 9.4 *Sending email to administrators*. JP1/IM can also be notified of security level judgment results. To notify JP1/IM of security level judgment results, select the **Notify IM** check box in the Edit Action Policy window. For details on setting up the Edit Action Policy window, see 6.10 *Setting an action for each security level*.

- Executing user-defined actions

Administrators can execute user-specific commands (\*.exe or \*.bat). For details about user-defined actions, see 9.5 *Executing user-defined actions*.

Note that the four kinds of actions can be combined and implemented at the same time. However, note that if client user message notification and client network connection control are selected at the same time, messages may not reach users due to transmission disconnection.

## 9.2 Sending messages to client users

Client user can be notified of security level judgment results via messages. When a message is sent, it is displayed as a pop-up window on the client's screen.

This section explains notification by action policy and notification by administrator.

### 9.2.1 Message notification by action policy

Select the **Send message to user** check box in the Edit Action Policy window to notify client users of judgment results when a security level is judged. The contents of the notification message can be edited in the Edit Action Policy (Customize Message) window. For details about the Edit Action Policy window, see *6.10 Setting an action for each security level*. For details about the Edit Action Policy (Customize Message) window, see *6.12 Editing a client user notification message*.

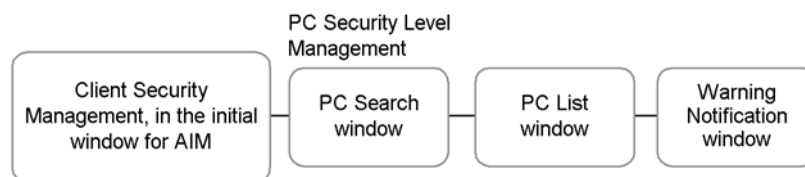
### 9.2.2 Message notification by administrator

Administrators can send messages to clients using the Client Security Management window of AIM. Note that JP1/Software Distribution Client 07-50 or later must be installed on any client that receives messages.

#### (1) Transitions of windows used to send messages

The following figure shows the transitions of windows used to send messages.

Figure 9-1: Transitions of windows used to send messages



To open the initial window of AIM, log in to AIM with CSC administrator permissions. For the procedure to open the initial window, see *8.1 Transitions of windows used for client monitoring*.

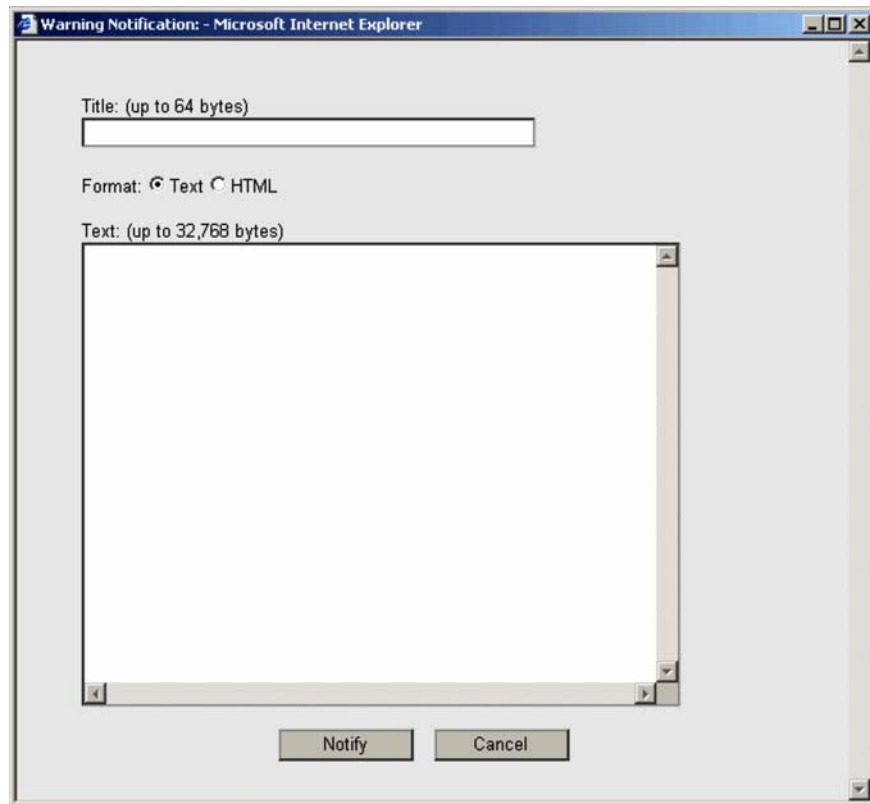
#### (2) Sending messages

You need to specify a client to which a message is to be sent, and also write the message. Messages can be edited in the Warning Notification window.

To edit and send a message to a specified client:

1. In the PC Search window, search for the client to which to send the message.  
The PC List window is displayed.

2. Select the **Asset No.** check box of the client to which the message is to be sent.  
The client to which the message is to be sent is selected.
3. In **Warning notification**, click the **Message** button.  
The Warning Notification window is displayed.



The image shows a web browser window titled "Warning Notification: - Microsoft Internet Explorer". Inside the window is a form for sending a message. The form has a "Title: (up to 64 bytes)" label above a single-line text input field. Below this is a "Format:" section with two radio buttons: "Text" (which is selected) and "HTML". Underneath is a "Text: (up to 32,768 bytes)" label above a large multi-line text area. At the bottom of the form are two buttons: "Notify" and "Cancel".

4. Enter the title.  
Enter the title of the message as a string of 64 or fewer bytes
5. Select either **Text** or **HTML** as the format of the displayed message.

Note

HTML messages can be sent only if the version of JP1/Software Distribution Client is 08-10 or later. If the version is 08-00 or earlier, plain-text messages are sent even if **HTML** is selected.

6. Enter the text.  
Enter the body of the message as a string of 32,768 or fewer bytes.

7. Click the **Notify** button.

A message box is displayed to confirm client notification.

8. Click the **OK** button.

The message is sent to the client, and the Action Message dialog box is displayed. If an error message is displayed, see *17.4.1 Action messages in the PC List window*, and act accordingly.

9. Click the **Close** button.

The Action Message dialog box closes.

Note that messages can be sent even when client security management is disabled for the client.

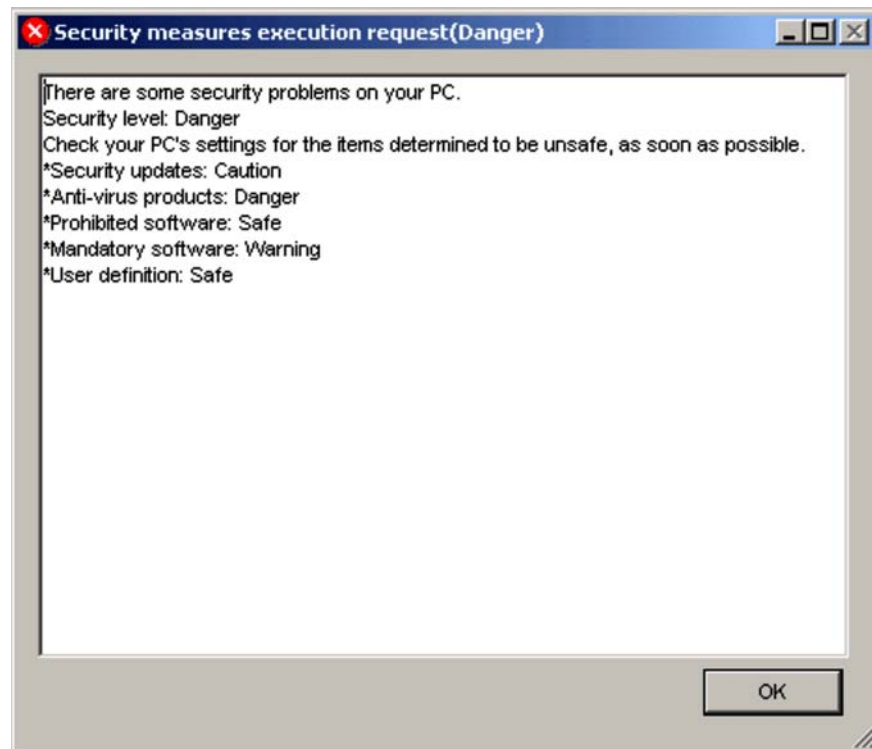
*Note:*

When a message is sent to a client user, the job execution result is saved as a processing job to the execution log of JP1/Software Distribution Manager. For details about saving the results of message notification jobs, see *6.12.2 Checking the execution results of message notification jobs*.

### 9.2.3 Example of a notification message to a client user

When a user is notified of security level judgment results, a pop-up message is displayed on the user's client.

The following figure shows an example of a message displayed on the client.



*Reference note:*

Messages are displayed either in text format or HTML format. Which format is used depends on the settings in the Edit Action Policy (Customize Message) window or the Warning Message Notification window displayed from the PC List window.

Note that HTML messages are displayed only if the version of JP1/Software Distribution Client is 08-10 or later.

Selecting HTML format for a message sent to a client whose JP1/Software Distribution Client version is 08-00 or earlier results in the following:

- When a message is sent according to an action policy  
The text message specified in the Edit Action Policy (Customize Message) window is displayed.
- When a message is sent from the PC List window  
The contents of the HTML message specified in the Warning Message Notification window, which is displayed from the PC List window, are displayed as text that includes HTML tags.

## 9.3 Controlling client network connections

Clients can be disconnected from the network, or their connections can be permitted. This action is available only with a quarantine system.

This section explains network connection control by action policy, and network connection control by administrator.

### 9.3.1 Network connection control by action policy

In the Edit Action Policy window, select the **Control network connection** check box, and then select either the **Permit connection** radio button or **Refuse connection** radio button. When a security level is judged, the selected network control is implemented.

For details about the Edit Action Policy window, see *6.10 Setting an action for each security level*.

### 9.3.2 Network connection control by administrator

An administrator can control network connections by specifying the particular client in the Client Security Management window of AIM or by using the network control command (`cscnetctrl`).

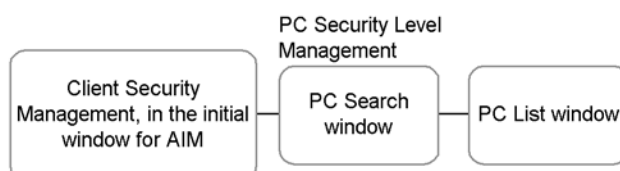
#### (1) Controlling network connections from the Client Security Management window of AIM

Using the Client Security Management window of AIM, an administrator can control client access to the network. The administrator can cut network connections for clients with a high security level, or reconnect clients confirmed as safe.

##### (a) Transition of windows used to control network connections

The following figure shows the transition of windows used to control network connections.

Figure 9-2: Transition of windows used to control network connections



To open the initial window of AIM, log in to AIM with CSC administrator permissions. For the procedure to open the initial window, see *8.1 Transitions of windows used for client monitoring*.

### (b) Controlling network connections

An administrator can specify a client, and permit or deny the network connection.

To control the network connection for a specified client:

1. In the PC Search window, search for the client for which the network connection is to be controlled.

The PC List window is displayed.

2. Select the **Asset No.** check box of the client for which the network connection is to be controlled.

The client for which the network connection is to be controlled is selected.

3. For **Network connection**, click either the **Refuse** button or the **Permit** button.

A message box is displayed to confirm client network control.

4. Click the **OK** button.

The specified processing is performed, and the Action Message dialog box is displayed. If an error message is displayed, see *17.4.1 Action messages in the PC List window*, and act accordingly.

5. Click the **Close** button.

The Action Message dialog box closes.

Note that network connections can be controlled even when client security management is disabled for the client.

*Note:*

Do not attempt to control client network connections by directly accessing a linked network control product. Always use the Client Security Management window of AIM.

### (2) Controlling network connections by command

The JP1/CSC administrator or an administrator of a remote system can control client connections to the network by executing the network control command (`cscnetctrl`) from a remote management server linked to the remote system. This enables the administrator to disconnect any client judged a high security risk when a virus is detected by the remote system, and to reconnect the client when certain that it is secure.

When a client is disconnected by execution of the network control command (`cscnetctrl`), the network connection status becomes *immediate denial*. Network connection permission as the result of a subsequent security level judgment does not clear an immediate denial already in force. To clear an immediate denial, permit



network connection using the `cscnetctrl` command or the Client Security Management window.

In the following example, the command disconnects the client with IP address `100.20.150.40` from the network as an immediate denial:

```
cscnetctrl -r -i 100.20.150.40
```

For details about the network control command, see *cscnetctrl (controls network connections)* in *15. Commands*.

---

## 9.4 Sending email to administrators

---

Administrators can be notified of client security level judgment results via email.

Administrator email notification can be set by action policy. Emails cannot be sent from the Client Security Management window of AIM.

In the Edit Action Policy window, select the **Notify to administrator** check box and the **Notify the administrator by email** check box to notify the administrator of judgment results when a security level is judged. The contents of notification emails can be edited in the Edit Action Policy (Customize Email) window.

For details about the Edit Action Policy window, see *6.10 Setting an action for each security level*. For details about the Edit Action Policy (Customize Email) window, see *6.11.1 Editing email in the Edit Action Policy (Customize Email) window*.

By default, the sender address of emails sent to the administrator is set to `manager@csc.message`. For details about the email sender address and email transmission unit, see *6.11.2 Email sender address and transmission unit*.

---

## 9.5 Executing user-defined actions

---

In the **Action for the user definition** area of the Edit Action Policy window, select the **Execute the specified command** check box and specify the **Action** and **Command** names and other details. The specified command will be executed when the security level is judged.

You can specify any command file (\*.exe or \*.bat) stored on the management server.

For details about the Edit Action Policy window, see *6.10 Setting an action for each security level*.



## Chapter

---

# 10. Auditing Security

---

This chapter describes how to output client search results and information about the status of security measures to a file from the Client Security Management window of AIM. It also explains how to display trends in the status of security measures using graphs or other means.

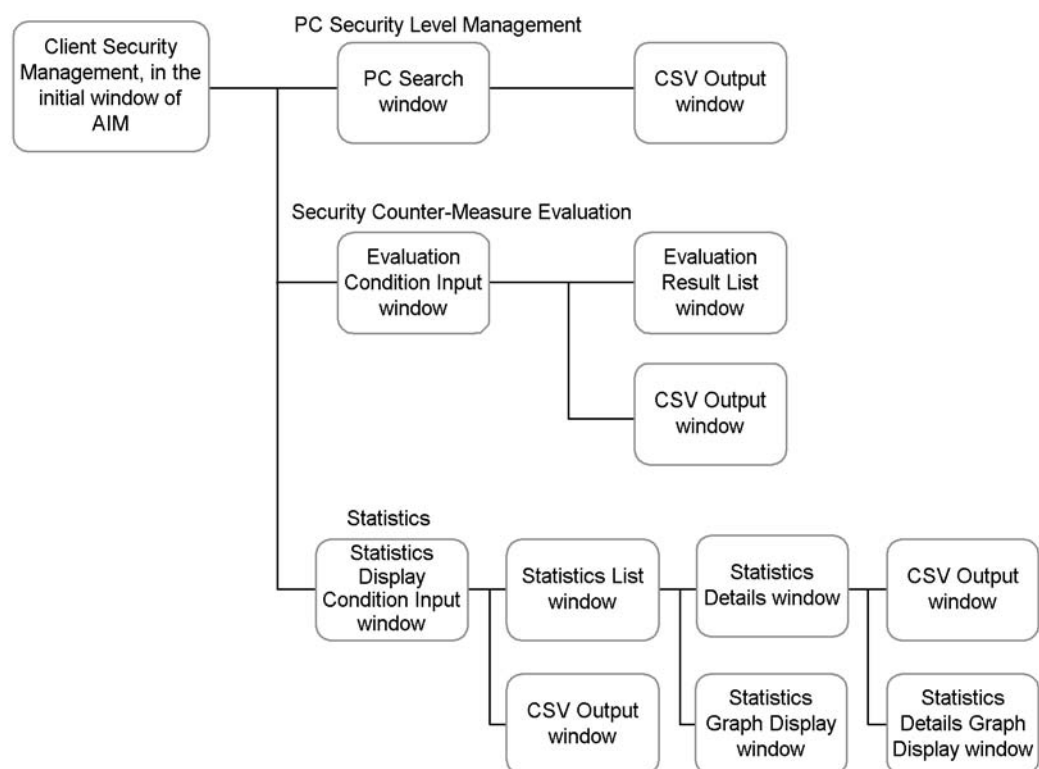
- 10.1 Transitions of windows used for auditing security
- 10.2 Outputting search results of clients to a file
- 10.3 Evaluating the status of security measures on clients
- 10.4 Gauging trends in security measure evaluation

## 10.1 Transitions of windows used for auditing security

Client information retrieved from the PC Search window can be output to a CSV file. Also, the status of security measures taken on clients can be evaluated for each user and group on the basis of points awarded. This allows administrators to audit security for clients.

The following figure shows the transitions of windows used for auditing security.

Figure 10-1: Transitions of windows used for auditing security



To open the initial window of AIM, log in to AIM with CSC administrator or CSC user permissions. For the procedure to open the initial window, see *8.1 Transitions of windows used for client monitoring*.

## 10.2 Outputting search results of clients to a file

Client information searched from the PC Search window can be output to a CSV file.

### 10.2.1 Outputting search results as a CSV

Search conditions can be used to specify clients to be managed, and the search results can be viewed and saved as a CSV file. CSV files are output from the PC Search window.

To specify a search condition and output the search results as a CSV file:

1. From the job menu of the AIM initial window, choose **Client Security Management** and then **PC Security Level Management**.

The PC Search window is displayed.

Figure 10-2: PC Search window

Output to CSV file

Asset Information Manager - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Job Management Partner 1/Asset Information Manager csc\_admin Logout

Search CSV

Display 200 results per page

Asset No. match part of the words

Host name match part of the words

IP address match part of the words

User name including

Group name Browse

PC security level not less than

PC security level judgment date (YYYYMMDD)

Number of consecutive times for the same security level times not less than

Number of consecutive days for the same security level days not less than

MAC address

Warning date (YYYYMMDD)

Network connection status

Update date of network connection status (YYYYMMDD)

Execution date of user definition (YYYYMMDD)

Security level of security updates not less than

Security level of anti-virus products not less than

## 2. Specify a search condition.

Specify a search condition for each item. For details about the item specifications, see 8.2 *Searching for clients*.

3. Click the **CSV** button.

The File Download dialog box is displayed.

Skip to step 5 if you are saving the file. Note that for IE version 5.5 or earlier, the **Open** button and **Save** button are displayed as radio buttons.

4. Click the **Open** button.

The search results are displayed in the CSV Output window.

Asset No.	Host name	IP address	User name	Group name	PC security level	PC security level judgment date	Num
10000001	client_10001	10.100.100.1	user001	Head Office	Safe	2005/07/22 10:29:14	4
10000002	client_10002	10.100.100.2	user002	Head Office	Caution	2005/07/27 05:16:03	2
10000003	client_10003	10.100.100.3	user003	Head Office/Head Office/Sales Dept	Danger	2005/07/07 00:23:54	3
10000004	client_10004	10.100.100.4	user004	Head Office	Safe	2005/07/26 15:44:03	3
10000005	client_10005	10.100.100.5	user005	Head Office/Head Office/Accounting Dept	Caution	2005/07/03 06:06	3
10000006	client_10006	10.100.100.6	user006	Head Office/Head Office/Sales Dept	Safe	2005/07/19 03:00:30	0
10000007	client_10007	10.100.100.7	user007	Head Office/Head Office/Accounting Dept	Warning	2005/07/23 11:22	5
10000008	client_10008	10.100.100.8	user008	Head Office	Warning	2005/07/17 02:32:16	1
10000009	client_10009	10.100.100.9	user009	Head Office	Danger	2005/07/11 01:58:16	2
10000010	client_10010	10.100.100.10	user010	Head Office/Head Office/Accounting Dept	Safe	2005/07/23 05:29:48	3
10000011	client_10011	10.100.100.11	user011	Head Office/Head Office/Sales Dept	Danger	2005/07/16 03:51:05	3
10000012	client_10012	10.100.100.12	user012	Head Office	Safe	2005/07/13 22:40:45	0
10000013	client_10013	10.100.100.13	user013	Head Office/Head Office/Sales Dept	Safe	2005/07/14 12:36:54	0
10000014	client_10014	10.100.100.14	user014	Head Office/Head Office/Sales Dept	Danger	2005/07/22 21:03:01	1
10000015	client_10015	10.100.100.15	user015	Head Office	Safe	2005/07/06 20:33:15	2
10000016	client_10016	10.100.100.16	user016	Head Office/Head Office/Accounting Dept	Safe	2005/07/28 19:40:27	2
10000017	client_10017	10.100.100.17	user017	Head Office	Safe	2005/07/19 02:10:25	1
10000018	client_10018	10.100.100.18	user018	Head Office/Head Office/Sales Dept	Safe	2005/07/28 20:57:46	0
10000019	client_10019	10.100.100.19	user019	Head Office/Head Office/Sales Dept	Caution	2005/07/10 01:47:49	3
10000020	client_10020	10.100.100.20	user020	Head Office/Head Office/Accounting Dept	Safe	2005/07/19 20:48:30	3
10000021	client_10021	10.100.100.21	user021	Head Office/Head Office/Accounting Dept	Safe	2005/07/16 04:33:48	3
10000022	client_10022	10.100.100.22	user022	Head Office	Danger	2005/07/08 16:30:17	2
10000023	client_10023	10.100.100.23	user023	Head Office	Safe	2005/07/03 12:19:11	2
10000024	client_10024	10.100.100.24	user024	Head Office/Head Office/Accounting Dept	Safe	2005/07/28 11:52:48	3
10000025	client_10025	10.100.100.25	user025	Head Office	Safe	2005/07/15 18:19:05	3
10000026	client_10026	10.100.100.26	user026	Head Office	Safe	2005/07/16 04:07:57	0
10000027	client_10027	10.100.100.27	user027	Head Office/Head Office/Sales Dept	Danger	2005/07/12 04:09:48	3
10000028	client_10028	10.100.100.28	user028	Head Office	Safe	2005/07/22 03:44:42	1
10000029	client_10029	10.100.100.29	user029	Head Office	Safe	2005/07/20 19:41:13	3
10000030	client_10030	10.100.100.30	user030	Head Office	Safe	2005/07/26 09:33:37	2
10000031	client_10031	10.100.100.31	user031	Head Office/Head Office/Accounting Dept	Safe	2005/07/13 10:40:23	3
10000032	client_10032	10.100.100.32	user032	Head Office	Safe	2005/07/18 15:36:10	3
10000033	client_10033	10.100.100.33	user033	Head Office	Safe	2005/07/08 21:27:14	5
10000034	client_10034	10.100.100.34	user034	Head Office/Head Office/Accounting Dept	Safe	2005/07/22 11:56:49	3
10000035	client_10035	10.100.100.35	user035	Head Office/Head Office/Sales Dept	Safe	2005/07/19 08:17:44	0
10000036	client_10036	10.100.100.36	user036	Head Office/Head Office/Accounting Dept	Safe	2005/07/01 13:28:13	3
10000038	client_10038	10.100.100.38	user038	Head Office/Head Office/Sales Dept	Safe	2005/07/25 03:53:16	0
10000039	client_10039	10.100.100.39	user039	Head Office	Safe	2005/07/26 16:39:28	1
10000040	client_10040	10.100.100.40	user040	Head Office	Safe	2005/07/23 23:54:35	1

The following table describes the contents of the search results displayed in the CSV Output window.

Table 10-1: Contents of the search results displayed in the CSV Output window

No.	Item	Contents
1	Asset No.	PC asset number
2	Host name	Name for identification
3	IP address	IP address
4	User name	Name of the user



No.	Item	Contents
5	<b>Group name</b>	Group to which the user belongs
6	<b>PC security level</b>	Latest PC security level judged by the judgment policy. <b>Safe, Unknown, Caution, Warning, Danger, Not applicable</b> , or <b>Not yet judged</b> is displayed.
7	<b>PC security level judgment date</b>	Date on which the PC security level was judged Displayed in <i>YYYY/MM/DD hh:mm:ss</i> format.
8	<b>Number of consecutive times for the same security level</b>	Number of times the same security level other than <b>Safe</b> existed during security level judgment
9	<b>Number of consecutive days for the same security level</b>	Number of days the same security level other than <b>Safe</b> existed during security level judgment
10	<b>MAC address</b>	MAC address
11	<b>Warning date</b>	Date of the latest user warning
12	<b>Network connection status</b>	PC network connection status. Displayed as <b>Refuse, Permit, Refuse in the emergency</b> , or <b>--</b> . <b>--</b> indicates that no network control is in effect.
13	<b>Update data of network connection status</b>	Date and time at which the client's network access was permitted, denied, or immediately blocked
14	<b>Execution date of user definition</b>	Date and time at which the user-defined action was implemented
15	<b>Security level of security updates</b>	Security level for security updates
16	<b>Security level of anti-virus products</b>	Security level for anti-virus products
17	<b>Security level of prohibited software</b>	Security level for prohibited software
18	<b>Security level of mandatory software</b>	Security level for mandatory software
19	<b>Security level of PC security settings</b>	Security level for PC security settings
20	<b>Security level of user definition</b>	Security level for a user definition
21	<b>OS</b>	Name of the OS currently used
22	<b>Location</b>	Location
23	<b>Security management</b>	Whether PC security management is performed. <b>Valid</b> or <b>Invalid</b> is displayed.

No.	Item	Contents
24	<b>Evaluation point</b>	Points indicating the status of PC security measures
25	<b>Judgment policy</b>	Name of the judgment policy assigned to the PC
26	<b>Renewal date of judgment policy</b>	Date and time at which the judgment policy was updated
27	<b>Assigned date of judgment policy</b>	Date and time at which the judgment policy was assigned
28	<b>Action policy</b>	Name of the action policy assigned to the PC
29	<b>Renewal date of action policy</b>	Date and time at which the action policy was updated
30	<b>Assigned date of action policy</b>	Date and time at which the action policy was assigned

5. To save the search results, click the **Save** button in the File Download dialog box. The Save As dialog box is displayed.
6. For **File name** in the Save As dialog box, enter a file name and click the **Save** button.

Change the file name. Note that a string (consisting of alphanumeric characters and symbols) to identify the file is set by default for **File name** in the Save As dialog box.

The search results are saved to a file in CSV format.

*Reference note:*

When the PC list information output command (`cscexportpclist`) is executed, the asset information and judgment results of all PCs whose security levels were judged on the specified date are output as PC list information to a CSV file. The administrator can use this PC list information file to manage the PC security levels.

For details about the PC list information output command (`cscexportpclist`), see *cscexportpclist (outputs PC list information)* in 15. *Commands*. For details about the PC list information file, see 16.10 *PC list information file*.

## 10.3 Evaluating the status of security measures on clients

The status of security measures taken on clients can be evaluated on the basis of points awarded. The points used for evaluation are called *evaluation points*.

The results of evaluation can be retrieved for each group or user using a window, and can be output to a CSV file. By using points to represent the status of security measures on clients, groups or users without security measures taken can be determined at a glance. This feature can be used by an Asset Information Manager administrator, CSC administrator, or CSC user.

The evaluation point score of a client is obtained by multiplying the security level factor for each judgment item.

The following shows the formula for the evaluation point score.

$$\begin{aligned} \text{Evaluation points} = & 100 \text{ (points)} \times (\text{security level factor of security updates}) \\ & \times (\text{security level factor of anti-virus products}) \\ & \times (\text{security level factor of prohibited software}) \\ & \times (\text{security level factor of mandatory software}) \\ & \times (\text{security level factor of PC security settings}) \\ & \times (\text{security level factor of user definition}) \end{aligned}$$

*Note:*

The fractional part is rounded.

Security level factors are used for all judgment items. The following table lists the security level factors for the judgment items.

*Table 10-2:* Security level factors for judgment items

No.	Security level for a judgment item	Security level factor
1	Safe	1
2	Caution	0.75
3	Warning	0.5
4	Danger	0.25
5	Unknown	1
6	Not applicable	1

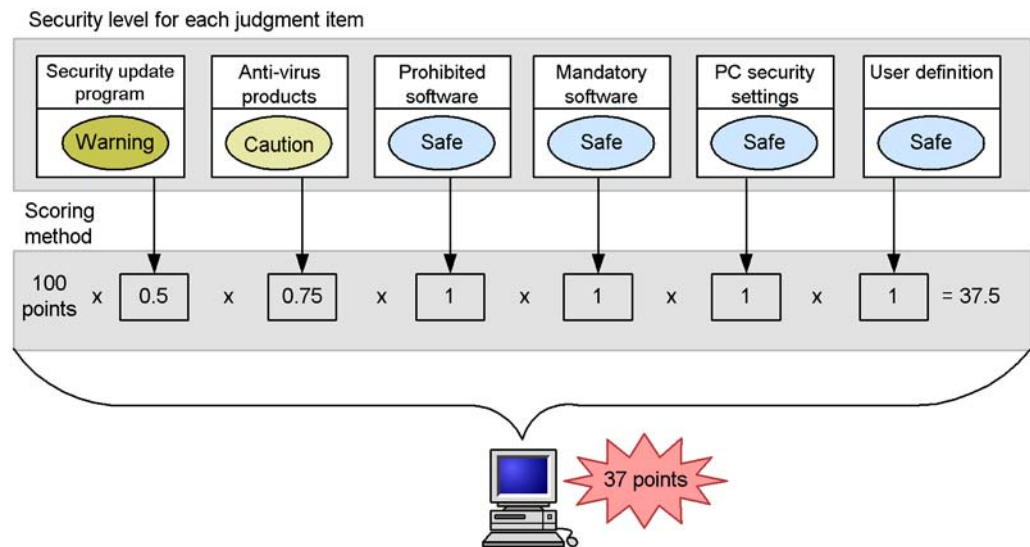
*Note:*

No evaluation points are awarded if one of the following conditions is satisfied:

- **Not yet judged** is displayed for the security level of all the judgment items.
- **Not applicable** or **Unknown** is displayed for the security level of all the judgment items.
- No judgment has been performed since JP1/CSC - Manager was upgraded.

The following gives an example of rating of the security measures on a client.

Figure 10-3: Example of rating of the security measures on a client



### 10.3.1 Searching for the evaluation results of the status of security measures

Evaluation conditions can be specified to search for the results of the evaluation of security measures taken on clients. The search results display the score of the client that has the lowest evaluation point score, the average score for each group or user, and the number of clients evaluated.

Use the Evaluation Condition Input window to search for evaluation results.

To specify evaluation conditions to be used to search for evaluation results:

1. From the job menu of the AIM initial window, choose **Client Security**

## Management and then Security Counter-Measure Evaluation.

The Evaluation Condition Input window appears.

Figure 10-4: Evaluation Condition Input window

2. In the Evaluation Condition Input window, specify the search conditions.

Specify the search conditions in the Evaluation Condition Input window. A search is performed using an AND condition for the specified items.

The following table describes the specifications for each item.

Table 10-3: Specified contents for each item in the Evaluation Condition Input window

No.	Search condition item	Specification method	Specifiable search options	Default search option
1	Group name <sup>#1</sup>	Click the <b>Browse</b> button and specify the group.	None	None

No.	Search condition item	Specification method	Specifiable search options	Default search option
2	<b>Asset No.</b>	Enter a unique number for user management, using 60 or fewer bytes of alphanumeric characters.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>match all the words</b></li> <li>• <b>match part of the words</b></li> <li>• <b>match beginning of the words</b></li> <li>• <b>match end of the words</b></li> </ul>	<b>match part of the words</b>
3	<b>User name</b>	Enter the name of the PC user, using 255 or fewer bytes.	None	None
4	<b>IP address</b>	Enter the IP address of the PC, using 15 or fewer bytes of alphanumeric characters.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>match all the words</b></li> <li>• <b>match part of the words</b></li> <li>• <b>match beginning of the words</b></li> <li>• <b>match end of the words</b></li> </ul>	<b>match part of the words</b>
5	<b>OS</b>	Enter the name of the OS, using a string of 200 or fewer bytes.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>match all the words</b></li> <li>• <b>match part of the words</b></li> <li>• <b>match beginning of the words</b></li> <li>• <b>match end of the words</b></li> </ul>	<b>match part of the words</b>
6	<b>Location</b> <sup>#2</sup>	Click the <b>Browse</b> button and specify the location.	None	None
7	<b>Lowest score</b>	Enter a number from 0 to 100	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>not greater than, not less than, or equal</b></li> </ul>	<b>not greater than</b>

No.	Search condition item	Specification method	Specifiable search options	Default search option
8	<b>Average score</b>	Enter a number from 0 to 100.	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>not greater than</b></li> <li>• <b>not less than,</b></li> <li>• <b>equal</b></li> </ul>	<b>not greater than</b>
9	<b>Totals by</b>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>• <b>User</b></li> <li>• <b>Group</b></li> </ul>	None	None
10	<b>Group level</b> <sup>#3</sup>	Specify the level of the groups to be displayed in the search result. Enter a number from 0 to 256. This item is disabled when <b>User</b> is specified for <b>Totals by</b> .	None	None

Legend:

None: No search option is specified.

#1

Click the **Browse** button for the group to display the Browse Groups dialog box. From the tree view, select the group you would like to specify, and click the **OK** button. The selected group is specified.

#2

Click the **Browse** button for the location to display the Browse Locations dialog box. From the tree view, select the location you would like to specify, and click the **OK** button. The selected location is specified.

#3

Specify the level of groups under the group specified for **Group name** in item 1 (level 0). For example, if **Sales Dept.** and **Accounting Dept.** exist under **Head Office** and you want to display **Head Office/Sales Dept.** and **Head Office/Accounting Dept.** as the search results, specify **Head Office** for **Group name** and specify 1 for **Group level**.

3. Specify **Display**, and then click the **Search** button.

Specify the number of results to display in the window, and perform the search. The Evaluation Result List window appears, in which you can check the search results. The displayed items vary depending on whether **Group** or **User** is

specified for **Totals by**. If an error message appears, take action according to *17.4.4 Error message in the Evaluation Result List window*.

*Reference note:*

Using the Customize Jobs window of AIM, you can customize the contents displayed in the Evaluation Result List window. The items in the Evaluation Result List window can be set to be shown or hidden, and the display order of each item can be changed. For details about the Customize Jobs window, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

Note that **User name** will not be displayed in the Evaluation Result List window if **Group** is specified for **Totals by**.

**(1) Evaluation results for each group**

If **Group** is specified for **Totals by** in the Evaluation Condition Input window, the evaluation results for the status of security measures are displayed for each group, in the Evaluation Result List window.

The following shows the Evaluation Result List window when **Group** is specified.



Figure 10-5: Evaluation Result List window when **Group** is specified

The screenshot shows the 'Asset Information Manager' web application. The main window is titled 'Job Management Partner 1/Asset Information Manager'. It features a search bar with 'Search' and 'CSV' buttons. Below the search bar, there are several filter fields: 'Group name' (with a 'Browse' button), 'Asset No.' (with a 'match part of the words' dropdown), 'User name' (with an 'including' dropdown), 'IP address' (with a 'match part of the words' dropdown), 'OS' (with a 'match part of the words' dropdown), 'Location' (with a 'Browse' button), 'Lowest score' (with a 'points' dropdown and a 'not greater than' dropdown), 'Average score' (with a 'points' dropdown and a 'not greater than' dropdown), 'Totals by' (set to 'Group'), and 'Group level' (set to '2 levels').

On the left side, there is a sidebar with a tree view showing the following structure:

- Group
  - Bangkok branch office
  - Headquarters
  - New York branch office
- Location
- Job of Asset Management
  - Device Management
  - Software Applied Management
  - System Management
  - System Definition
  - Client Security Management
  - PC Security Level Management
  - Register Permitted PCs
  - Security Counter-Measure Evaluation
  - Statistics

The main content area displays a table of results. The table has the following columns: 'Group name', 'Lowest score', 'Average score', 'Number of total units', and 'Number of management units'. The results are as follows:

Group name	Lowest score	Average score	Number of total units	Number of management units
Bangkok branch office/Development Department	1	48	127	137
Bangkok branch office/Sales Department	1	55	109	124
Headquarters/Accounting Department	1	52	186	207
Headquarters/Sales Department	1	51	146	160
New York branch office/Personnel Department	6	52	153	170
New York branch office/Quality Assurance Department	3	60	86	97

The following table lists the items displayed in the Evaluation Result List window when **Group** is specified.

Table 10-4: Items displayed in the Evaluation Result List window when **Group** is specified

No.	Item	Contents
1	<b>Group name</b>	The group names for the group levels specified for <b>Group level</b> in the Evaluation Condition Input window are displayed.
2	<b>Lowest score</b>	The lowest evaluation point score of a PC for the status of security measures among PCs in the group
3	<b>Average score</b>	The average score for the status of security measures taken for the group
4	<b>Number of total units</b>	The number of PCs subject to calculation of the lowest and average scores. This is the number of management units, excluding PCs for which the evaluation points are displayed as -#.
5	<b>Number of management units</b>	The number of PCs to be managed, that is, the PCs for which <b>Valid</b> is displayed for <b>Security management</b> . This also includes PCs for which evaluation points are displayed as -#.

#

The evaluation points are displayed as – if one of the following conditions is satisfied:

- **Not yet judged** is displayed for the security level of all the judgment items.
- **Not applicable** or **Unknown** is displayed for the security level of all the judgment items.
- No judgment has been performed since JP1/CSC - Manager was upgraded.

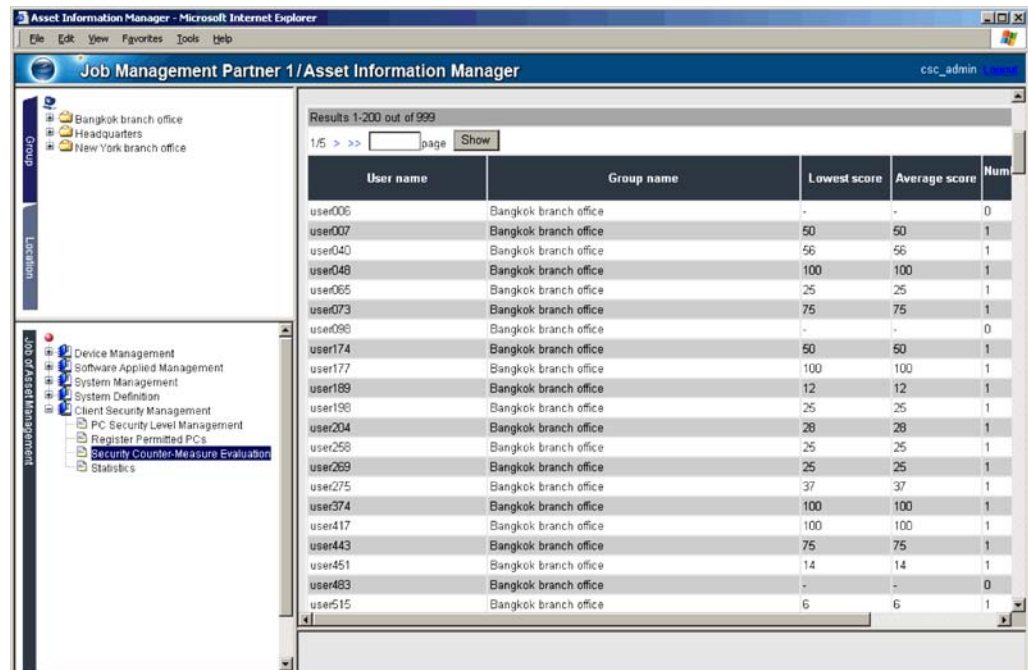
If – is displayed for the evaluation points for all the clients, both the lowest and average scores are displayed as –.

## (2) Evaluation results for each user

If **User** is specified for **Totals by** in the Evaluation Condition Input window, the evaluation results for the status of security measures are displayed for each user, in the Evaluation Result List window.

The following shows the Evaluation Result List window when **User** is specified.

Figure 10-6: Evaluation Result List window when **User** is specified



User name	Group name	Lowest score	Average score	Num
user006	Bangkok branch office	-	-	0
user007	Bangkok branch office	50	50	1
user040	Bangkok branch office	56	56	1
user048	Bangkok branch office	100	100	1
user065	Bangkok branch office	25	25	1
user073	Bangkok branch office	75	75	1
user098	Bangkok branch office	-	-	0
user174	Bangkok branch office	50	50	1
user177	Bangkok branch office	100	100	1
user189	Bangkok branch office	12	12	1
user198	Bangkok branch office	25	25	1
user204	Bangkok branch office	28	28	1
user258	Bangkok branch office	25	25	1
user269	Bangkok branch office	25	25	1
user275	Bangkok branch office	37	37	1
user374	Bangkok branch office	100	100	1
user417	Bangkok branch office	100	100	1
user443	Bangkok branch office	75	75	1
user451	Bangkok branch office	14	14	1
user483	Bangkok branch office	-	-	0
user515	Bangkok branch office	6	6	1

The following table lists the items displayed in the Evaluation Result List window when **User** is specified.

*Table 10-5:* Items displayed in the Evaluation Result List window when **User** is specified

No.	Item	Contents
1	<b>User name</b>	User name
2	<b>Group name</b>	The group to which the user belongs
3	<b>Lowest score</b>	The lowest evaluation point score of a PC for the status of security measures among the PCs used by the user
4	<b>Average score</b>	The average score for the status of security measures taken for the user
5	<b>Number of total units</b>	The number of PCs subject to calculation of the lowest and average scores. This is the number of management units, excluding PCs for which the evaluation points are displayed as -#.
6	<b>Number of management units</b>	The number of PCs to be managed, that is, the PCs for which <b>Valid</b> is displayed for <b>Security management</b> . This also includes PCs for which evaluation points are displayed as -#.

#

The evaluation points are displayed as - if one of the following conditions is satisfied:

- **Not yet judged** is displayed for the security level of all the judgment items.
- **Not applicable** or **Unknown** is displayed for the security level of all the judgment items.
- No judgments have been performed after upgrading JP1/CSC - Manager.

If - is displayed for the evaluation points of a client, both the lowest and average scores are displayed as -.

### 10.3.2 Outputting results of estimation to a CSV file

Retrieved evaluation results for the status of security measures taken on clients can be saved and viewed as a CSV file.

Use the Evaluation Condition Input window to output CSV files.

To specify search conditions and output the evaluation results to a CSV file:

1. From the job menu of the AIM initial window, choose **Client Security Management** and then **Security Counter-Measure Evaluation**.

The Evaluation Condition Input window appears.

Figure 10-7: Evaluation Condition Input window

Output to CSV file

The screenshot shows a web application window titled 'Asset Information Manager - Microsoft Internet Explorer'. The main content area is titled 'Job Management Partner 1/Asset Information Manager'. On the left, there is a sidebar with a tree view showing a hierarchy of locations and tools. The 'Tools of Asset Management' section is expanded, showing 'Security Counter Measure Evaluation' selected. The main area contains a search form with the following fields and options:

- Search:** A button labeled 'CSV' is highlighted, with an arrow pointing to it from the text 'Output to CSV file' above.
- Display:** A dropdown menu set to '200 results per page'.
- Group name:** A text input field with a 'Browse' button.
- Asset No.:** A text input field with a dropdown menu set to 'match part of the words'.
- User name:** A text input field with a dropdown menu set to 'including'.
- IP address:** A text input field with a dropdown menu set to 'match part of the words'.
- OS:** A text input field with a dropdown menu set to 'match part of the words'.
- Location:** A text input field with a 'Browse' button.
- Lowest score:** A text input field with a dropdown menu set to 'points not greater than'.
- Average score:** A text input field with a dropdown menu set to 'points not greater than'.
- Totals by:** A dropdown menu set to 'Group'.
- Group level:** A text input field set to '1 levels'.

2. Specify the search conditions.

Specify a search condition for each item. For details on specifying items, see *10.3.1 Searching for the evaluation results of the status of security measures*.

3. Click the **CSV** button.

The File Download dialog box appears.

Skip to step 5 if you are saving the file. Note that for IE version 5.5 or earlier, the **Open** button and **Save** button are displayed as radio buttons.

4. Click the **Open** button.

The search results are displayed in the CSV Output window. The items displayed vary depending on what is specified for **Totals by** during the search.

Figure 10-8: CSV Output window when **Group** is specified for Totals by

```

"Group name","Lowest score","Average score","Number of total units","Number of management units"
"Head office/Accounting Dept./The first Accounting Dept.",18,12,2,2
"Head office/Accounting Dept./The fourth Accounting Dept.",4,11,2,2
"Head office/Accounting Dept./The second Accounting Dept.",2,10,4,4
"Head office/Accounting Dept./The third Accounting Dept.",12,12,2,2
"Head office/Development Dept./The first Development Dept.",6,12,3,3
"Head office/Development Dept./The second Development Dept.",0,10,3,3
"Head office/Development Dept./The third Development Dept.",6,6,2,2
"Head office/Quality assurance Dept./The first Quality assurance Dept.",3,3,1,1
"Head office/Quality assurance Dept./The fourth Quality assurance Dept.",1,3,2,2
"Head office/Quality assurance Dept./The second Quality assurance Dept.",1,7,2,2
"Head office/Quality assurance Dept./The third Quality assurance Dept.",3,22,2,2
"Head office/Sales Dept./The first Sales Dept.",3,3,2,2
"Head office/Sales Dept./The fourth Sales Dept.",37,37,1,1
"Head office/Sales Dept./The second Sales Dept.",1,21,4,4
"Head office/Sales Dept./The third Sales Dept.",3,3,1,1

```

Figure 10-9: CSV Output window when **User** is specified for Totals by

```

"user004","Head office/Accounting Dept.",4,4,1,1
"user007","Head office/Accounting Dept.",18,18,1,1
"user015","Head office/Accounting Dept.",4,4,1,1
"user073","Head office/Accounting Dept.",3,3,1,1
"user077","Head office/Accounting Dept.",37,37,1,1
"user095","Head office/Accounting Dept.",4,4,1,1
"user096","Head office/Accounting Dept.",9,9,1,1
"user051","Head office/Accounting Dept./The fourth Accounting Dept.",4,4,1,1
"user079","Head office/Accounting Dept./The fourth Accounting Dept.",18,18,1,1
"user038","Head office/Accounting Dept./The second Accounting Dept.",2,2,1,1
"user082","Head office/Accounting Dept./The second Accounting Dept.",9,9,1,1
"user099","Head office/Accounting Dept./The second Accounting Dept.",3,3,1,1
"user041","Head office/Accounting Dept./The third Accounting Dept.",12,12,1,1
"user067","Head office/Accounting Dept./The third Accounting Dept.",12,12,1,1
"user023","Head office/Development Dept.",9,9,1,1
"user092","Head office/Development Dept.",14,14,1,1
"user094","Head office/Development Dept.",18,18,1,1

```

The following table describes the contents of the search results displayed in the CSV Output window.

Table 10-6: Contents of the search results displayed in the CSV Output window

No.	Item	Contents
1	<b>User name</b>	The name of the user. This item is output only when <b>User</b> is specified for <b>Totals by</b> .
2	<b>Group name</b>	The group to which the user belongs
3	<b>Lowest score</b>	The lowest evaluation point score of a PC for the status of security measures among PCs used in the group or by the user
4	<b>Average score</b>	The average score for the status of security measures taken for the group or user
5	<b>Number of total units</b>	The number of PCs subject to calculation of the lowest and average scores. This is the number of management units, excluding PCs for which the evaluation points are displayed as -#.

No.	Item	Contents
6	<b>Number of management units</b>	The number of PCs to be managed, that is, PCs for which <b>Valid</b> is displayed for <b>Security management</b> . This also includes PCs for which evaluation points are displayed as -#.

5. To save the search results, click the **Save** button in the File Download dialog box.  
The Save As dialog box is displayed.
6. For **File name** in the Save As dialog box, enter a file name and click the **Save** button.  
Change the file name. Note that a string (consisting of alphanumeric characters and symbols) to identify the file is set by default for **File name** in the Save As dialog box. The search results are saved to a file in CSV format.

## 10.4 Gauging trends in security measure evaluation

Statistics representing trends in the status of security measures can be checked on a group-by-group basis. From the Client Security Management window, you can search for the following three types of statistics:

- Evaluation points

Trends in the evaluation points indicating the results of evaluation of security measures.

- Countermeasure usage

Trends in the proportion of clients whose safety level was judged to be safe for the judgment items specified in a judgment policy. These judgment items may relate to security updates, anti-virus programs, or other information.

- User definition countermeasure usage

Trends in the proportion of clients whose safety level was judged to be safe for the judgment items specified in a user definition.

The results of your search for evaluation points, countermeasure usage, or user definition countermeasure usage can be displayed as a graph or output to a CSV file. For countermeasure usage, trends can be checked for a particular judgment item. By displaying a graph that shows trends in security measures over time, you can judge whether a problem with security measures is a short-term or long-term problem.

This feature can be used by an Asset Information Manager administrator, CSC administrator, or CSC user.

Countermeasure usage and user definition countermeasure usage are statistics representing the proportion of clients whose security level was judged to be safe. User definition countermeasure usage calculates countermeasure usage for each of the judgment items in a user-defined judgment policy.

The formula used to calculate countermeasure usage and user definition countermeasure usage is as follows:

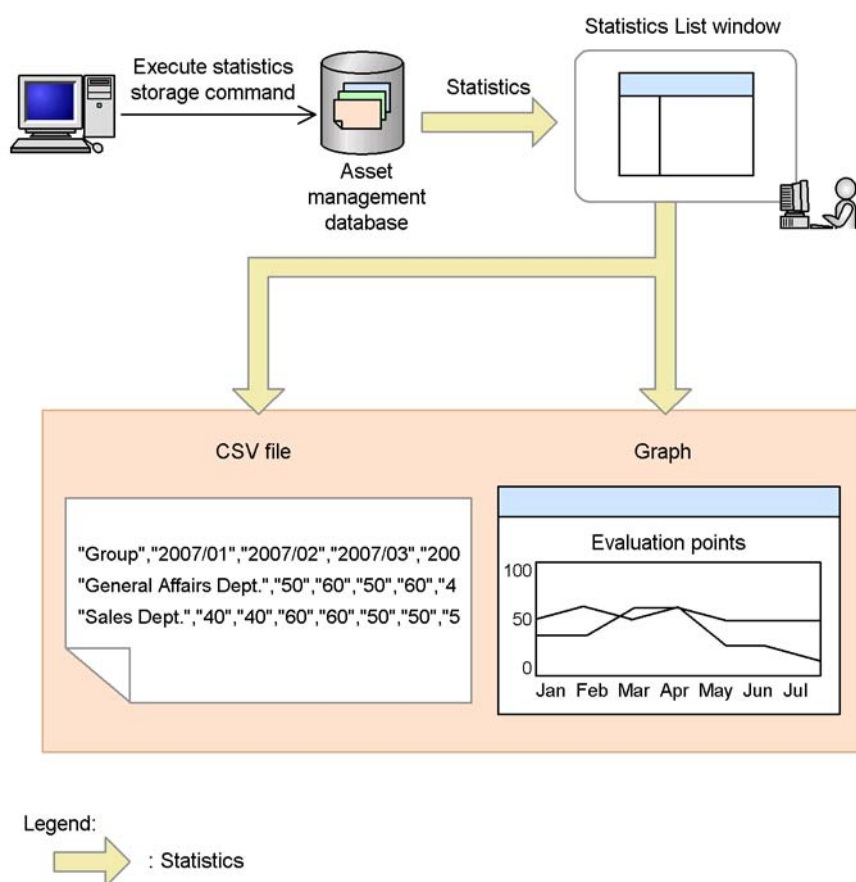
$$\begin{aligned} &\text{Countermeasure usage (overall and for user definition) (\%)} \\ &= \text{Number of clients judged as safe} \\ &\div \text{Number of clients judged as safe, caution, warning, or danger} \\ &\times 100 \end{aligned}$$

*Note:*

The decimal part is truncated to two decimal places.

The following figure gives an overview of statistics.

Figure 10-10: Overview of statistics



#### 10.4.1 Storing statistics

To use the statistics function in the Client Security Management window, information about security measures, such as security level judgment results and evaluation points, must be stored periodically in the asset management database as statistics.

To output the status of user-defined judgment items as statistics, in the JP1/CSC - Manager Setup dialog box, specify **Include in the "Type of total" pulldown menu** for **User definition judgment**. For details about setting up JP1/ CSC - Manager, see *5.4.3 Setting up JP1/CSC - Manager*.

Execute the following command periodically to store statistics in the asset management database:



- Statistics storage command (*cscstorecount*)

For details about the statistics storage command, see *cscstorecount* (*stores statistics about the status of security measures*) in 15. *Commands*.

As a guide, Hitachi recommends that you execute the statistics storage command once a day. Doing so provides a database of statistics that is highly accurate. To reduce the administrator's workload and guarantee that the command is executed regularly, Hitachi recommends that you register this command in Windows Scheduled Tasks. For details about how to register commands in Scheduled Tasks, see 5.9 *Procedures for setting a task in Scheduled Tasks*.

### 10.4.2 Searching statistics

You can search statistics on the status of security measures by specifying display conditions. By doing so, you can view the evaluation points, countermeasure usage, and user definition countermeasure usage for a particular group over time.

#### (1) *Searching statistics for specific groups*

You can search statistics from the Statistics Display Condition Input window.

To search statistics by entering display conditions:

1. From the job menu of the AIM initial window, choose **Client Security Management**, and then **Statistics**.

The Statistics Display Condition Input window appears.

Figure 10-11: Statistics Display Condition Input window

The screenshot shows a web application window titled "Asset Information Manager - Microsoft Internet Explorer". The main content area is titled "Job Management Partner 1/Asset Information Manager". On the left, there is a sidebar with a tree view. The "Job of Asset Management" section is expanded, and "Statistics" is selected. The main area contains a search form with the following fields:

- Group name:** A text input field with a "Browse" button.
- Group level:** A dropdown menu showing "1" and "levels".
- Type of totals:** A dropdown menu showing "Countermeasure usage".
- Period to total:** A date range selector showing "YYYYMMDD".
- Interval to total:** A dropdown menu showing "Month".
- Start of week:** A dropdown menu showing "Sun".

- In the Statistics Display Condition Input window, specify the search conditions.

Specify the search conditions in the Statistics Display Condition Input window. The search takes place using an AND condition for the specified items.

The following table shows the content that can be specified for each item.

Table 10-7: Contents specifiable for each item in the Statistics Display Condition Input window

No.	Search condition item	Specification method	Default value
1	Group name <sup>#1</sup>	Click the <b>Browse</b> button and specify the group.	--
2	Group level <sup>#2</sup>	Specify the level of groups to include in the search result. Enter a number from 0 to 256.	1

No.	Search condition item	Specification method	Default value
3	Type of totals	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>Countermeasure usage</li> <li>Evaluation point</li> <li><i>user-defined-judgment-item-name</i><sup>#3</sup></li> </ul>	Countermeasure usage
4	Period to total (start-date - end-date) <sup>#4</sup>	Enter a number in the format <i>YYYYMMDD</i> .	--
5	Interval to total <sup>#5, #6</sup>	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>Month</li> <li>Week</li> <li>Day</li> </ul>	Month
6	Start of week	Select one of the following from the pull-down menu: <ul style="list-style-type: none"> <li>Sun</li> <li>Mon</li> <li>Tue</li> <li>Wed</li> <li>Thu</li> <li>Fri</li> <li>Sat</li> </ul> This item is activated when <b>Week</b> is specified for <b>Interval to total</b> .	Sun

Legend:

--: N/A

#1

When you click the **Browse** button, the Browse Groups dialog box appears. To specify a group, select the group from the tree and then click the **OK** button.

#2

Specify the group level below the group specified for **Group name** in item 1 (level 0). For example, if *Sales Dept.* and *Accounting Dept.* exist under *Head Office* and you want to display **Head Office/Sales Dept.** and **Head Office/Accounting Dept.** as the search results, specify *Head Office* for **Group name** and specify 1 for **Group level**.

#3

The names of the judgment items defined in the user-defined judgment policy are displayed.

This item only appears if **Include in the "Type of total" pulldown menu** is specified for **User definition judgment** in the JP1/CSC - Manager Setup dialog box. For details about setting up JP1/CSC - Manager, see *5.4.3 Setting up JP1/CSC - Manager*.

A maximum of 10 user-defined judgment items are displayed, in the order in which they were added to the judgment policy.

#4

You can use the date entry assistance feature to enter dates.

#5

When **Interval to total** is set to **Month**, the period over which data is collected may be limited according to the setting for **Period to total**.

The following shows an example of such a situation:

■ Totals compiled when 2007/10/20 to 2008/2/15 is specified as the period to total				
October	2007	10/20 to 10/31 (11 days)		
November	2007	11/1 to 11/30		
December	2007	12/1 to 12/31		
January	2008	1/1 to 1/31		
February	2008	2/1 to 2/15 (15 days)		

#6

When **Interval to total** is set to **Week**, the period over which data is collected may be limited according to the settings for **Period to total** and **Start of week**.

The following shows an example of such a situation:

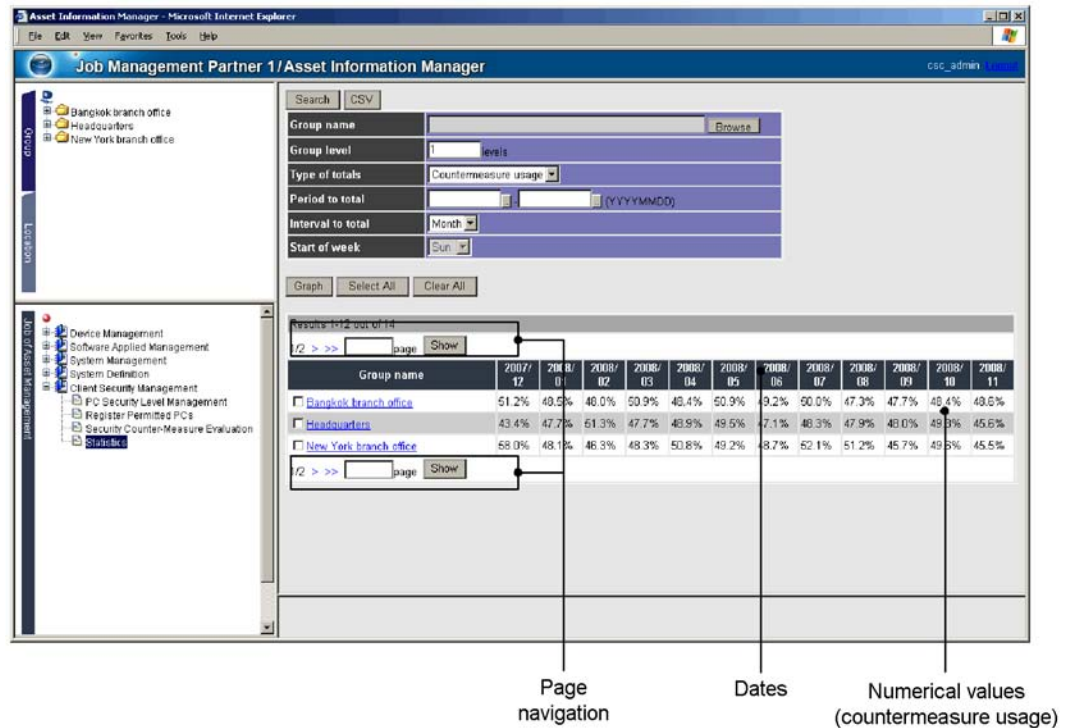
■ Totals compiled when 2007/10/1 (Mon) to 2007/11/15 (Thu) is specified as the period to total, and weeks start on Wednesday.				
Week 1: 10/1 (Mon) to 10/2 (Tue) (2 days)				
Week 2: 10/3 (Wed) to 10/9 (Tue)				
Week 3: 10/10 (Wed) to 10/16 (Tue)				
Week 4: 10/17 (Wed) to 10/23 (Tue)				
Week 5: 10/24 (Wed) to 10/30 (Tue)				
Week 6: 10/31 (Wed) to 11/6 (Tue)				
Week 7: 11/7 (Wed) to 11/13 (Tue)				
Week 8: 11/14 (Wed) to 11/15 (Thu) (2 days)				

3. Click the **Search** button.

The Statistics List window appears. The items displayed in this window depend on whether **Countermeasure usage**, **Evaluation point**, or a user-defined judgment item was specified for **Type of totals**.

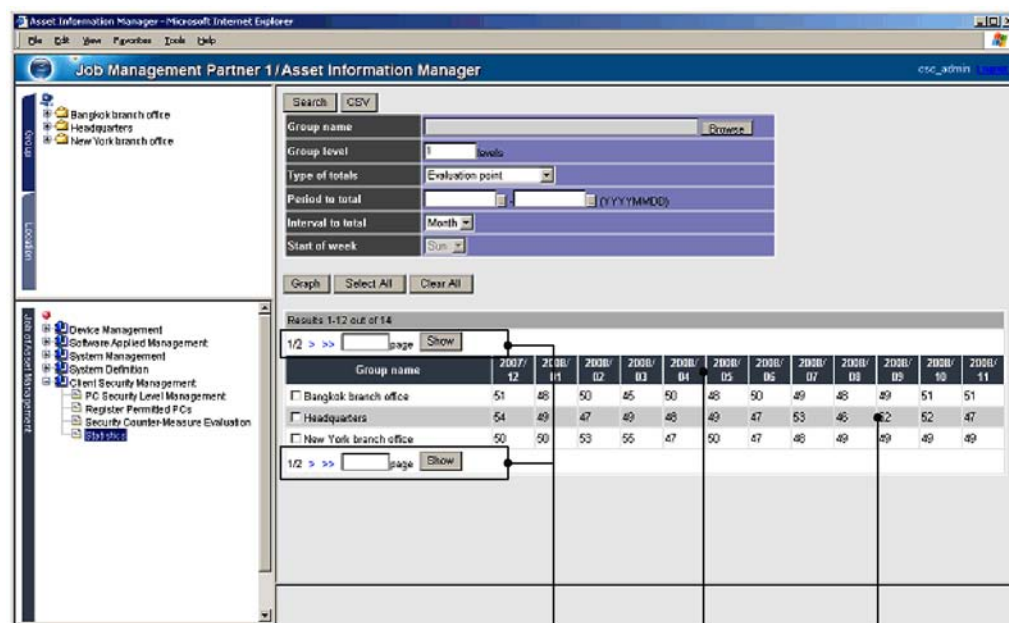
The following shows an example of the Statistics List window when **Countermeasure usage** is specified for **Type of totals**.

Figure 10-12: Statistics List window when Countermeasure usage is specified



The following shows an example of the Statistics List window when **Evaluation point** is specified for **Type of totals**.

Figure 10-13: Statistics List window when Evaluation point is specified

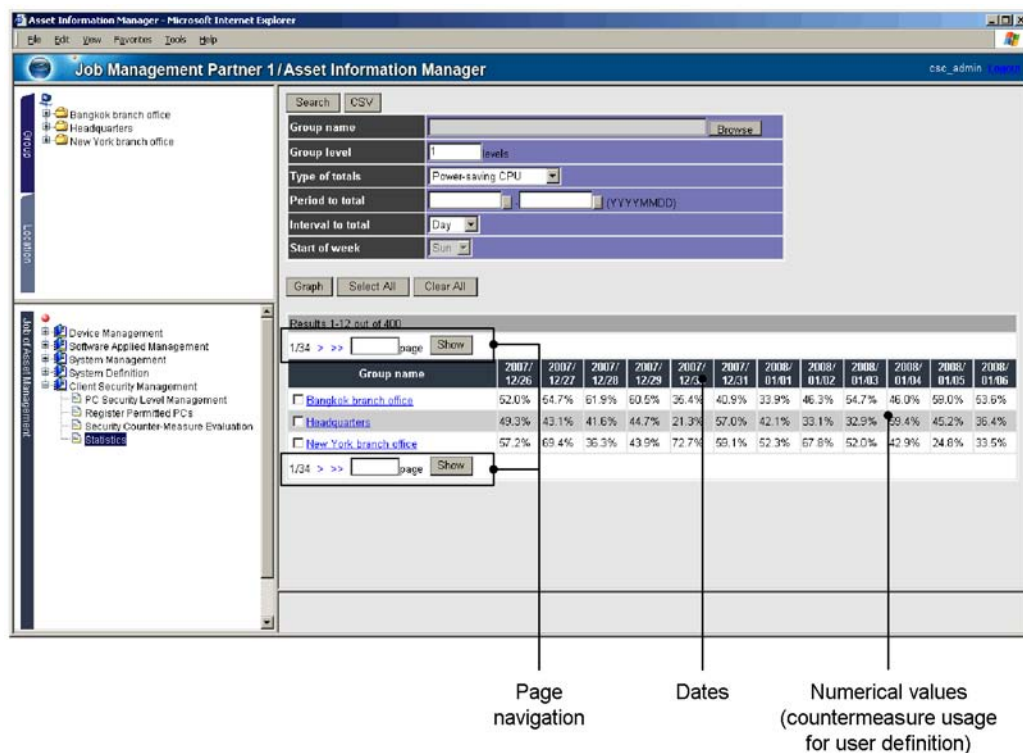
Page  
navigation

Dates

Numerical values  
(evaluation points)

The following shows an example of the Statistics List window when a user-defined judgment item is specified for **Type of totals**.

Figure 10-14: Statistics List window when user-defined judgment item is specified



The following table describes the items displayed in the Statistics List window.

Table 10-8: Items displayed in the Statistics List window

No.	Item	Contents
1	Group names	<p>The group names for the group levels specified for <b>Group level</b> in the Statistics Display Condition Input window.</p> <p>If you specified <b>Countermeasure usage</b> for <b>Type of totals</b>, you can display the Statistics Detail window by clicking the anchor for the group name.</p>

No.	Item	Contents
2	Dates <sup>#</sup>	<p>The date of the statistics.</p> <ul style="list-style-type: none"> <li>When <b>Month</b> is specified for <b>Interval to total</b> A maximum of 12 dates per page are displayed in the format <i>YYYY/MM</i>. Each date represents one month.</li> <li>When <b>Week</b> is specified for <b>Interval to total</b> A maximum of 12 dates per page are displayed in the format <i>YYYY/MM/DD</i>. Each date represents one week, starting on the day of the week specified for <b>Start of week</b>.</li> <li>When <b>Day</b> is specified for <b>Interval to total</b> A maximum of 12 dates per page are displayed in the format <i>YYYY/MM/DD</i>. Each date represents one day.</li> </ul>
3	Numerical values	<p>Numerical values representing countermeasure usage, evaluation points, or user-defined countermeasure usage, depending on the option specified for <b>Type of totals</b>.</p> <p>The evaluation points when <b>Month</b> or <b>Week</b> is specified for <b>Interval to total</b> are the average score over the stated period.</p> <p>If there are no applicable statistics, - is displayed.</p>

#

If there are more dates than can fit on one page, you can display the other pages by clicking the anchors in the page navigation area. The following describes the behavior of each anchor:

> : Displays the next page.

< : Displays the previous page.

>> : Displays the last page.

<< : Displays the first page.

You can also go directly to a specific page by entering the page number in the box in the page navigation area and clicking **Show**.

*Note:*

The search may fail if you attempt to display too much data. In this case, try using more specific search criteria.

## (2) Checking countermeasure usage for each judgment item

When you specify **Countermeasure usage** as the **Type of totals**, you can select a group in the Statistics List window and check the status of countermeasure usage over time for each judgment item.

To display countermeasure usage for each judgment item:



1. From the job menu of the AIM initial window, choose **Client Security Management** and then **Statistics**.

The Statistics Display Condition Input window appears.

2. In the Statistics Display Condition Input window, specify the search conditions.

Specify the search conditions in the Statistics Display Condition Input window. Make sure that you specify **Countermeasure usage** for **Type of totals**. For details about the content that can be specified for each item, see Table 10-7 *Contents specifiable for each item in the Statistics Display Condition Input window*.

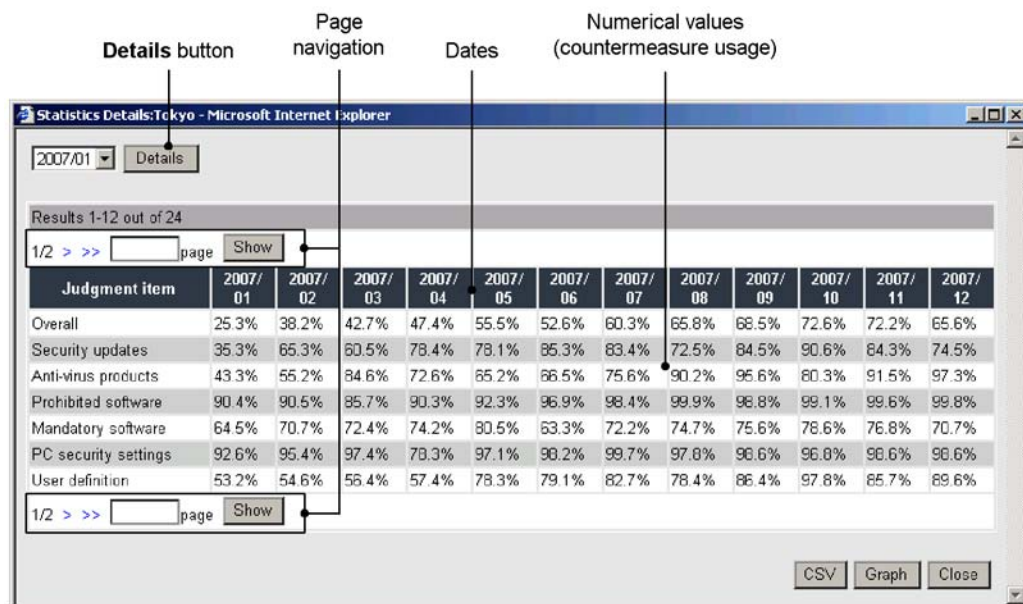
3. Click the **Search** button.

The Statistics List window appears.

4. Click a group name anchor.

The Statistics Details window appears, displaying the countermeasure usage over time for each judgment item for the group you selected.

Figure 10-15: Statistics Details window



The following table describes the items displayed in the Statistics Details window.

Table 10-9: Items displayed in the Statistics Details window

No.	Item	Contents
1	Items	Displays <b>Overall</b> and the name of each judgment item.
2	Dates <sup>#</sup>	<p>The date of the statistics.</p> <ul style="list-style-type: none"> <li>When <b>Month</b> is specified for <b>Interval to total</b> A maximum of 12 dates per page are displayed in the format <i>YYYY/MM</i>. Each date represents one month.</li> <li>When <b>Week</b> is specified for <b>Interval to total</b> A maximum of 12 dates per page are displayed in the format <i>YYYY/MM/DD</i>. Each date represents one week, starting on the day of the week specified for <b>Start of week</b>.</li> <li>When <b>Day</b> is specified for <b>Interval to total</b> A maximum of 12 dates per page are displayed in the format <i>YYYY/MM/DD</i>. Each date represents one day.</li> </ul>
3	Numerical values	Displays the countermeasure usage for each judgment item. If there are no applicable statistics, – is displayed.

#

If there are more dates than can fit on one page, you can display the other pages by clicking the anchors in the page navigation area. The navigation area works in the same way as that of the Statistics List window.

#### Details button

This button appears when **Month** or **Week** is specified for **Interval to total**. When the **Details** button is clicked, the countermeasure usage is displayed for each judgment item on a daily basis for the period selected from the pull-down menu.

### 10.4.3 Outputting statistics to a CSV file

Search results for statistics indicating the status of security measures can be displayed or saved as a file in CSV format.

#### (1) Outputting statistics for specific groups to a CSV file

You can output the statistics for specific groups to a CSV file from the Statistics Display Condition Input window.

To output statistics for specific groups to a CSV file based on search conditions:

- From the job menu of the AIM initial window, choose **Client Security Management** and then **Statistics**.

The Statistics Display Condition Input window appears.

Figure 10-16: Statistics Display Condition Input window

Output to CSV file

2. In the Statistics Display Condition Input window, specify the search conditions.

Specify the search conditions in the Statistics Display Condition Input window. For details about the content that can be specified for each item, see Table 10-7 *Contents specifiable for each item in the Statistics Display Condition Input window*.

3. Click the **CSV** button.

The File Download dialog box appears.

Skip to step 5 if you are saving the file. Note that in Internet Explorer 5.5 and earlier, the options to save or open the file are displayed as radio buttons.

4. Click the **Open** button.

The search results are displayed in the CSV Output window. The displayed contents vary depending on the options specified for **Type of totals** and **Interval to total** when the search was performed.

*Figure 10-17:* CSV output when Type of totals is Countermeasure usage and Interval to total is Month

```
"Group name","2007/01","2007/02","2007/03","2007/04","2007/05","2007/06","2007/07","
"Tokyo","25.8","38.2","42.7","47.4","55.5","52.6","60.8","65.8","68.5","72.6","72.2","65.6","
"Shanghai","54.4","54.6","57.1","57.6","58.8","60.1","60.2","60.3","61.7","61.4","62.4","63.
"Singapore","41.6","41.0","45.5","46.3","47.5","47.8","48.7","50.2","51.2","50.8","53.4","52
```

*Figure 10-18:* CSV output when Type of totals is Evaluation point and Interval to total is Week

```
"Group name","2007/01/01","2007/01/07","2007/01/14","2007/01/21","2007/01/28","2007/
"Tokyo","30","24","26","19","32","36","42","45","45","41"
"Shanghai","34","40","36","39","51","41","41","38","44","47"
"Singapore","84","67","72","65","58","62","67","65","60","57"
```

*Figure 10-19:* CSV output when Type of totals is user-defined and Interval to total is Day

```
"Group name","2008/05/12","2008/05/13","2008/05/14","2008/05/15","2008/05/16","2008/
"Tokyo","35.2","41.1","42.1","47.6","49.8","54.2","56.9","57.4","55.1","58.6","60.3","65.4","
"Shanghai","54.4","54.6","57.1","57.6","58.8","60.1","60.2","60.3","61.7","61.4","62.4","63.
"Singapore","41.6","41.0","45.5","46.3","47.5","47.8","48.7","50.2","51.2","50.8","53.4","52
```

The following table describes the contents of the search results displayed in the CSV Output window.

*Table 10-10:* Contents of the search results displayed in the CSV Output window

No.	Item	Contents
1	<b>Group name</b>	The name of the group.
2	Dates	The date of the statistics. Data is displayed as monthly, weekly, or daily data depending on the option specified for <b>Interval to total</b> .
3	Numerical values	Numerical values representing countermeasure usage, evaluation points, or user-defined countermeasure usage, depending on the option specified for <b>Type of totals</b> . The evaluation points when <b>Month</b> or <b>Week</b> is specified for <b>Interval to total</b> are the average score over the stated period. If there are no applicable statistics, a blank character is displayed.

5. To save the search results, click the **Save** button in the File Download dialog box.  
The Save As dialog box appears.
6. Enter a file name in the Save As dialog box and click the **Save** button.  
A string (consisting of alphanumeric characters and symbols) to identify the file is set by default for **File name** in the Save As dialog box. Change this to a file name of your choice. The search results are saved to a file in CSV format.

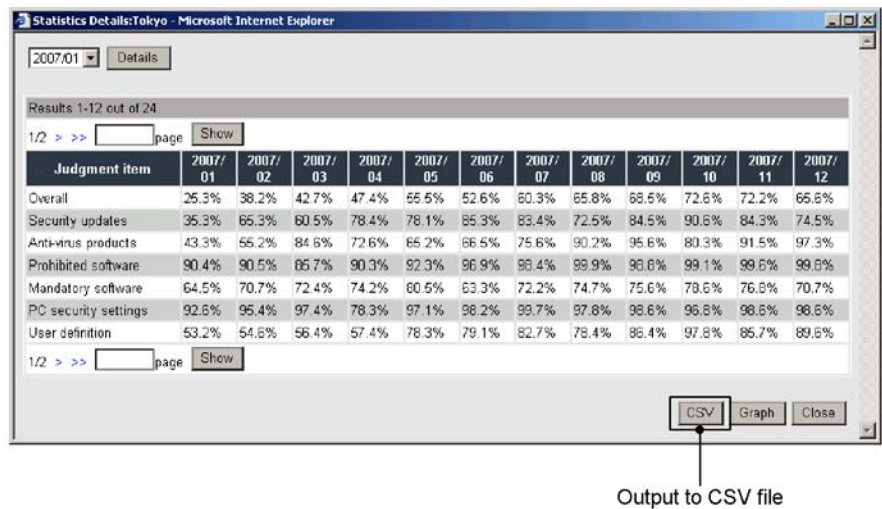
## **(2) Outputting statistics for specific judgment items as a CSV file**

You can output the statistics for specific judgment items to a CSV file from the Statistics Details window.

To output statistics for specific judgment items to a CSV file:

1. From the job menu of the AIM initial window, choose **Client Security Management** and then **Statistics**.  
The Statistics Display Condition Input window appears.
2. In the Statistics Display Condition Input window, specify the search conditions.  
Specify the search conditions in the Statistics Display Condition Input window. Make sure that you specify **Countermeasure usage** for **Type of totals**. For details about the content that can be specified for each item, see Table 10-7 *Contents specifiable for each item in the Statistics Display Condition Input window*.
3. Click the **Search** button.  
The Statistics List window appears.
4. Click a group name anchor.  
The Statistics Details window appears.

Figure 10-20: Statistics Details window



5. Click the **CSV** button.

The File Download dialog box appears.

Skip to step 7 if you are saving the file. Note that in Internet Explorer 5.5 and earlier, the options to save or open the file are displayed as radio buttons.

6. Click the **Open** button.

The countermeasure usage for each judgment item is displayed in the CSV Output window.

Figure 10-21: CSV output of countermeasure usage by judgment item

```
"Judgment item","2007/01","2007/02","2007/03","2007/04","2007/05","2007/06","2007/07"
"Overall","25.3","38.2","42.7","47.4","55.5","52.6","60.3","65.8","68.5","72.6","72.2","65.6",
"Security updates","35.3","65.3","60.5","78.4","78.1","85.3","83.4","72.5","84.5","90.6","84
"Anti-virus products","43.3","55.2","84.6","72.6","65.2","66.5","75.6","90.2","95.6","80.3","
"Prohibited software","90.4","90.5","85.7","90.3","92.3","96.9","98.4","99.9","98.8","99.1","
"Mandatory software","64.5","70.7","72.4","74.2","80.5","63.3","72.2","74.7","75.6","78.6","
"PC security settings","92.6","95.4","97.4","78.3","97.1","98.2","99.7","97.8","98.6","98.6",
"User definition","53.2","54.6","56.4","57.4","78.3","79.1","82.7","78.4","86.4","97.8","85.7"
```

The following table describes the contents displayed in the CSV Output window.

Table 10-11: Contents displayed in the CSV Output window

No.	Item	Contents
1	Judgment items	Displays <b>Overall</b> and the name of each judgment item.

No.	Item	Contents
2	Dates	The date of the statistics. Data is displayed as monthly, weekly, or daily data depending on the option specified for <b>Interval to total</b> .
3	Numerical values	Numerical values representing countermeasure usage. If there are no applicable statistics, a blank character is displayed.

7. To save the output results, click the **Save** button in the File Download dialog box.  
The Save As dialog box appears.
8. Enter a file name in the Save As dialog box and click the **Save** button.  
A string (consisting of alphanumeric characters and symbols) to identify the file is set by default for **File name** in the Save As dialog box. Change this to a file name of your choice. The output results are saved to a file in CSV format.

#### 10.4.4 Displaying statistics as a graph

Search results for statistics indicating the status of security measures can be displayed as a graph.

To use this feature, Office Web Components 10.0 or Office Web Components 11.0 must be installed on the management terminal.

##### (1) *Displaying statistics for specific groups as a graph*

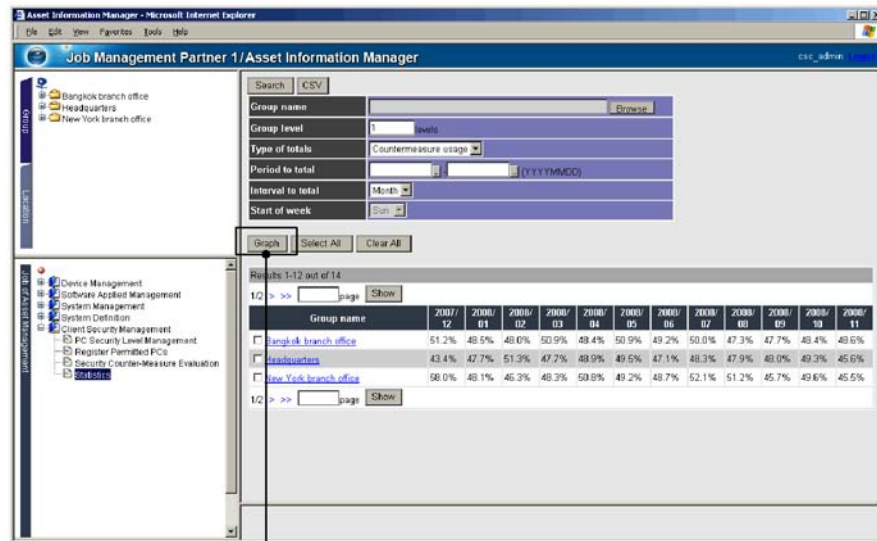
You can display the statistics for specific groups as a graph from the Statistics List window.

To display statistics for specific groups as a graph:

1. From the job menu of the AIM initial window, choose **Client Security Management** and then **Statistics**.  
The Statistics Display Condition Input window appears.
2. In the Statistics Display Condition Input window, specify the search conditions.  
Specify the search conditions in the Statistics Display Condition Input window. For details about the content that can be specified for each item, see Table 10-7 *Contents specifiable for each item in the Statistics Display Condition Input window*.
3. Click the **Search** button.  
The Statistics List window appears. The items displayed in this window depend on whether **Countermeasure usage**, **Evaluation point**, or a user-defined judgment item was specified for **Type of totals**.

The following shows an example of the Statistics List window when **Countermeasure usage** is specified for **Type of totals**.

Figure 10-22: Statistics List window (countermeasure usage)



Show as graph

4. Select the groups whose statistics you want to display as a graph.

Select the check boxes for the groups whose data you want to display as a graph. To select all the groups on the page, click the **Select All** button. To clear all the check boxes on the page, click the **Clear All** button.

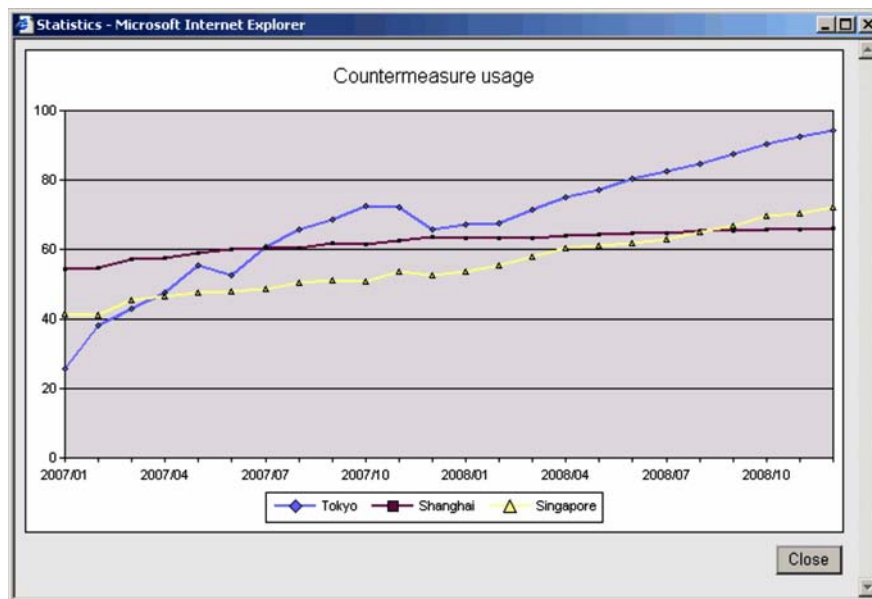
5. Click the **Graph** button.

The Statistics Graph Display window appears. The items displayed in this window depend on whether **Countermeasure usage**, **Evaluation point**, or a user-defined judgment item was specified for **Type of totals**.

The following shows an example of the Statistics Graph Display window when **Countermeasure usage** is specified for **Type of totals**.

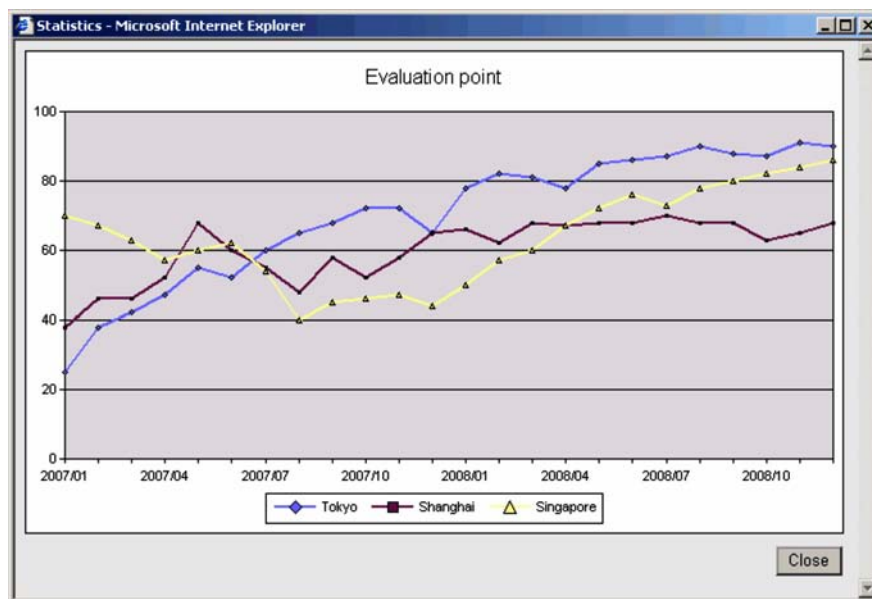


Figure 10-23: Statistics Graph Display window (countermeasure usage)



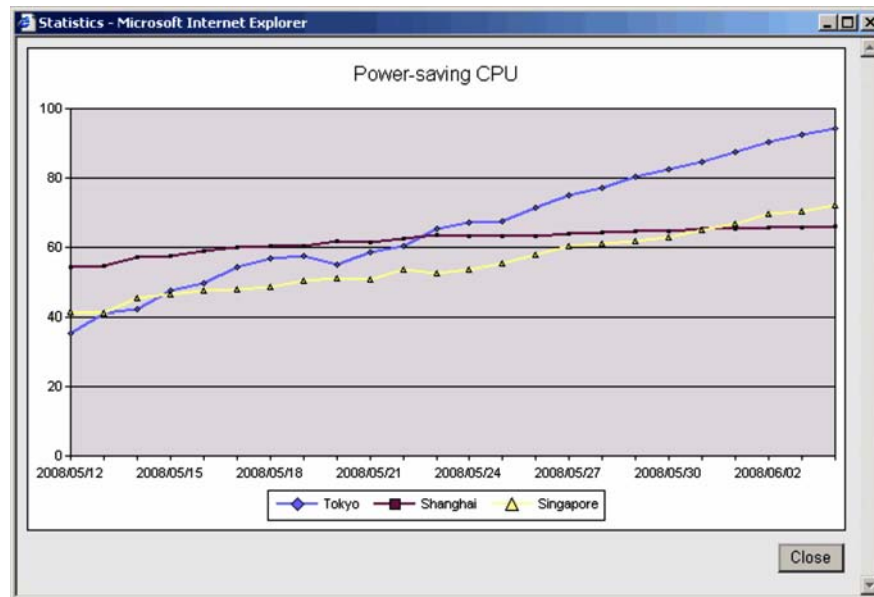
The following shows an example of the Statistics Graph Display window when **Evaluation point** is specified for **Type of totals**.

Figure 10-24: Statistics Graph Display window (evaluation points)



The following figure shows an example of the Statistics Graph Display window when a user-defined judgment item name is specified for **Type of totals**.

*Figure 10-25:* Statistics Graph Display window (user-defined countermeasure usage)



The following table describes the items displayed in the Statistics Graph Display window.

*Table 10-12:* Items displayed in the Statistics Graph Display window

No.	Item	Contents
1	Title	Displays <b>Countermeasure usage</b> , <b>Evaluation point</b> , or the name of the user-defined judgment item.
2	Numerical values (vertical axis)	Displays countermeasure usage (%), evaluation points (point value) or countermeasure usage for the user definition (%), according to the option selected for <b>Type of totals</b> .
3	Dates (horizontal axis)	Monthly, weekly, or daily dates according to the option selected for <b>Interval to total</b> .
4	Legend	The group names that correspond to the data plotted on the graph.

## (2) Displaying statistics for specific judgment items as a graph

You can display countermeasure usage for specific judgment items as a graph from the Statistics Details window.

To display countermeasure usage for specific judgment items as a graph:

1. From the job menu of the AIM initial window, choose **Client Security Management** and then **Statistics**.

The Statistics Display Condition Input window appears.

2. In the Statistics Display Condition Input window, specify the search conditions.

Specify the search conditions in the Statistics Display Condition Input window. Make sure that you specify **Countermeasure usage** for **Type of totals**. For details about the content that can be specified for each item, see Table 10-7 *Contents specifiable for each item in the Statistics Display Condition Input window*.

3. Click the **Search** button.

The Statistics List window appears.

4. Click a group name anchor.

The Statistics Details window appears.

Figure 10-26: Statistics Details window

Statistics Details: Tokyo - Microsoft Internet Explorer

2007/01 Details

Results 1-12 out of 24

1/2 > >> page Show

Judgment item	2007/01	2007/02	2007/03	2007/04	2007/05	2007/06	2007/07	2007/08	2007/09	2007/10	2007/11	2007/12
Overall	25.3%	38.2%	42.7%	47.4%	55.5%	52.6%	60.3%	65.8%	68.5%	72.6%	72.2%	65.6%
Security updates	35.3%	65.3%	60.5%	78.4%	78.1%	85.3%	83.4%	72.5%	84.5%	90.6%	84.3%	74.5%
Anti-virus products	43.3%	55.2%	84.6%	72.6%	65.2%	66.5%	75.6%	90.2%	95.6%	80.3%	91.5%	97.3%
Prohibited software	90.4%	90.5%	65.7%	90.3%	92.3%	96.9%	98.4%	99.9%	98.8%	99.1%	99.6%	99.8%
Mandatory software	64.5%	70.7%	72.4%	74.2%	60.5%	63.3%	72.2%	74.7%	75.6%	79.6%	76.8%	70.7%
PC security settings	92.6%	95.4%	97.4%	78.3%	97.1%	98.2%	99.7%	97.8%	98.6%	96.8%	98.6%	98.6%
User definition	53.2%	54.6%	56.4%	57.4%	78.3%	79.1%	82.7%	78.4%	85.4%	97.8%	85.7%	89.6%

1/2 > >> page Show

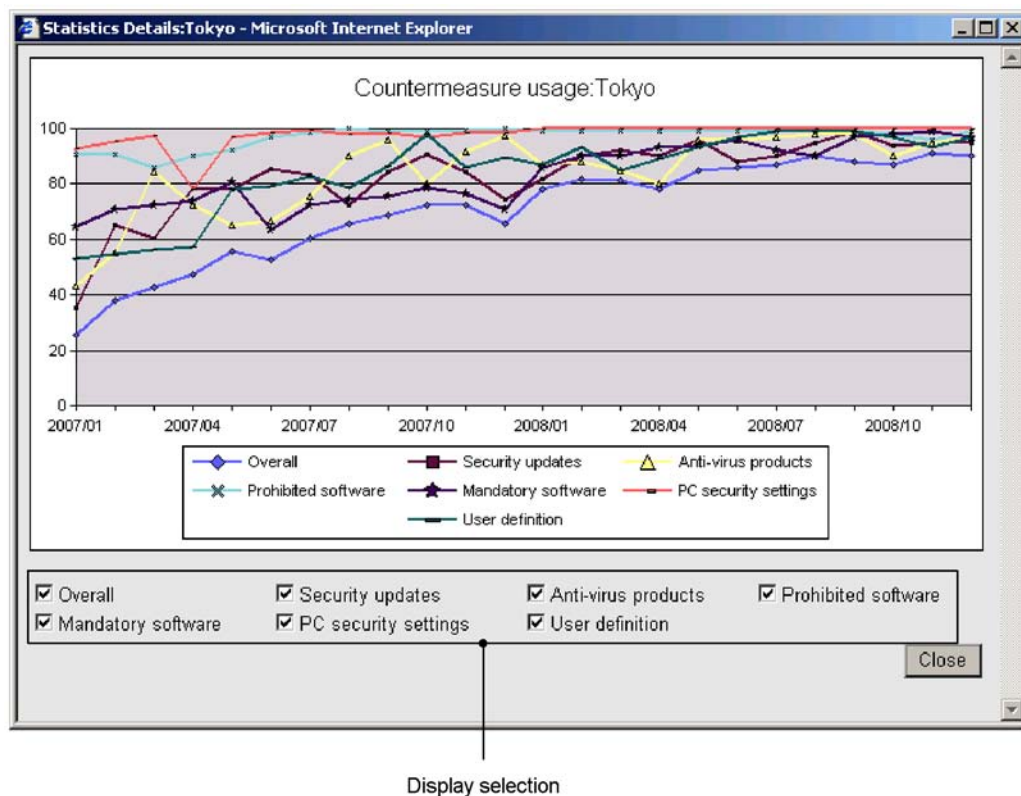
CSV Graph Close

Show as graph

5. Click the **Graph** button.

Statistics Details Graph Display window appears.

Figure 10-27: Statistics Details Graph Display window



The following table describes the items displayed in the Statistics Details Graph Display window.

Table 10-13: Items displayed in the Statistics Details Graph Display window

No.	Item	Contents
1	Title	Displays <b>Countermeasure usage:</b> followed by the group name.
2	Numerical values (vertical axis)	Countermeasure usage (%).
3	Dates (horizontal axis)	Monthly, weekly, or daily dates according to the option selected for <b>Interval to total</b> .
4	Legend	The judgment items that correspond to the data plotted on the graph.

No.	Item	Contents
5	Display selection	Use this area to select which judgment items to display in the graph.



## Chapter

---

# 11. Linking to JP1/IM

---

This chapter explains the configuration and setup for linking to JP1/IM.

### 11.1 Linking to JP1/IM

## 11.1 Linking to JP1/IM

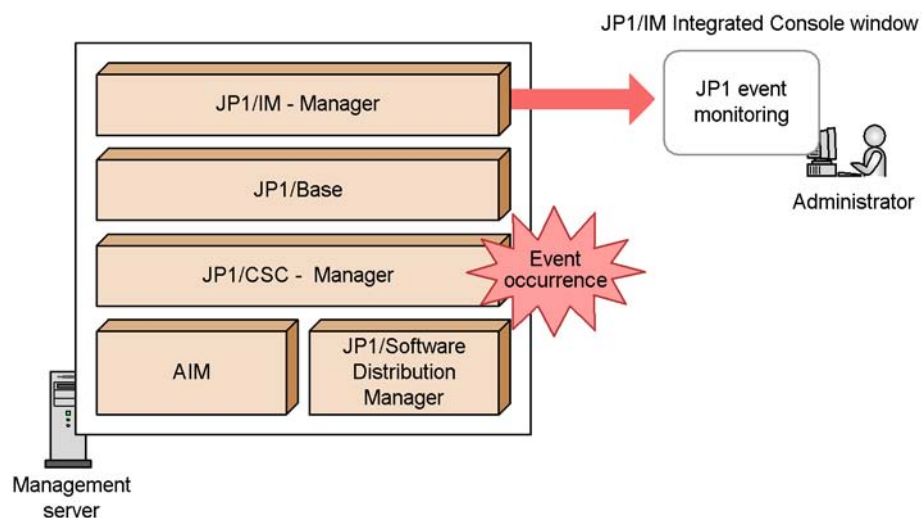
JP1/CSC can link to JP1/IM, allowing client security levels and network connection statuses to be monitored from the JP1/IM integrated console, and clients for which security measures are insufficient to be detected.

JP1/CSC can send messages to JP1/IM as JP1 events when a client security level changes. JP1/IM outputs these messages to the JP1/IM integrated console. This allows an administrator to perform centralized management from the JP1/IM integrated console.

### 11.1.1 Example system configuration

The following figure shows an example configuration of a system linked to JP1/IM.

*Figure 11-1: Example configuration of a system linked to JP1/IM*



Note that JP1/IM can be installed on a machine other than the one on which JP1/CSC - Manager is installed.

### 11.1.2 Setting up JP1/IM linkage

To send a JP1 event to JP1/IM, in the JP1/CSC - Manager setup window, set **IM linkage** to **Notify**.

For details about how to set up JP1/CSC - Manager, see *5.4.3 Setting up JP1/CSC - Manager*.

For details about the JP1 events and included messages sent by JP1/CSC, see *17*.



*Messages.*

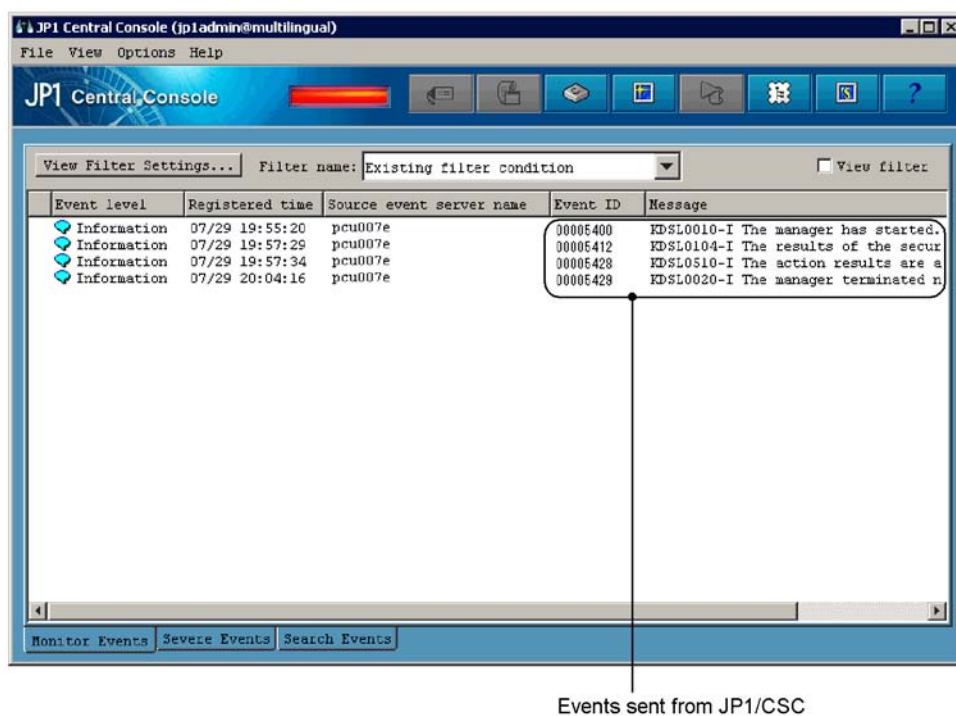
For details about installing and setting up JP1/IM, see the manuals *Job Management Partner 1/Integrated Management - Manager System Configuration and User's Guide* and *Job Management Partner 1/Integrated Management - Manager Reference*.

### 11.1.3 Displaying JP1/IM integrated console windows

With JP1/IM linkage, JP1 events from JP1/CSC can be checked from the JP1/IM integrated console.

The following figure shows a JP1/IM window with a JP1 event sent from JP1/CSC.

*Figure 11-2: JP1/IM window*



Events sent from JP1/CSC



## **Chapter**

---

# **12. Overview of Quarantine Systems**

---

This chapter provides an overview of quarantine systems on JP1/CSC.

- 12.1 About quarantine systems
- 12.2 Quarantine system linked to JP1/NM
- 12.3 Quarantine system linked to an authentication server
- 12.4 Quarantine system linked to JP1/Software Distribution (AMT Linkage facility)

---

## 12.1 About quarantine systems

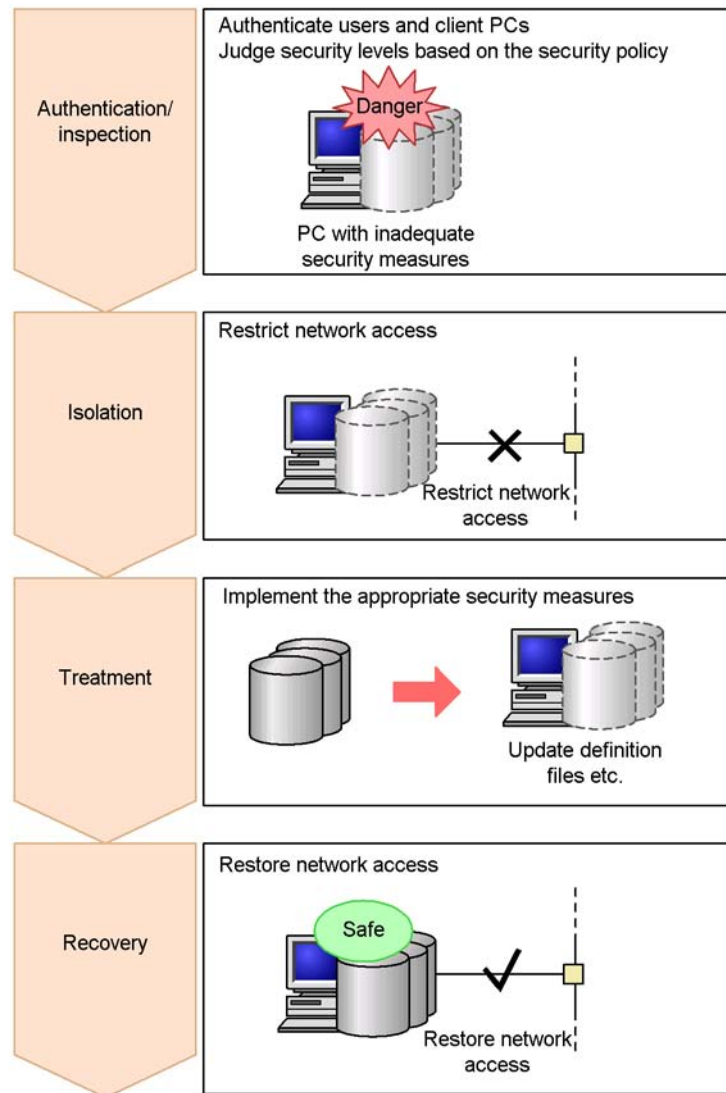
---

A quarantine system provides overall process management, including detecting clients that pose a security risk, network connection control, implementation of security measures, and reconnection to the network.

Quarantine system operation consists of four processes: *authentication/inspection*, *isolation*, *treatment*, and *recovery*. In JP1/CSC, these processes are referred to collectively as the *quarantine process*.

The following figure shows an overview of the quarantine process.

Figure 12-1: Overview of the quarantine process



In the *authentication/inspection* process, users and client PCs are authenticated, and their security levels are judged based on the security policy.

In the *isolation* process, access controls are placed on any client judged to be a security risk and the client is disconnected from the corporate network.

In the *treatment* process, security measures are implemented on the client via an isolated network or in an offline environment.

In the *recovery* process, the client for which security measures were implemented is authenticated and inspected again, and reconnected to the network if found to be *Safe*.

The functionality of a quarantine system can be realized under JP1/CSC by linking with a network control product or device.

### 12.1.1 Network control products that can link to JP1/CSC

A quarantine system can be set up by linking JP1/CSC to either of the following products:

- JP1/NM

JP1/NM is software that controls network connections. It consists of two programs, JP1/NM and JP1/NM - Manager. JP1/NM and JP1/NM - Manager contain NetMonitor and NetMonitor/Manager. JP1/NM and JP1/NM - Manager contains NX NetMonitor and NX NetMonitor/Manager.

JP1/NM - Manager monitors the overall system. JP1/NM is placed in each subnetwork and is used to control client network connections.

- Authentication server

An authentication server, also called a *RADIUS server*, is required to authenticate clients. To link to JP1/CSC, install either Microsoft Internet Authentication Service or Network Policy Server on a RADIUS server.

The available authentication methods are IEEE 802.1X authentication and MAC authentication.

#### IEEE 802.1X authentication

A user ID and password are used to authenticate a user. Authentication requires a switch and a RADIUS server that comply with IEEE 802.1X. The Windows standard supplicant is required on the client that is to be authenticated.

#### MAC authentication

A MAC address is used to authenticate a client. Authentication requires a switch and a RADIUS server that support MAC authentication. No supplicant is required on a client that is to be authenticated.

Two VLAN environments are available: dynamic and static.

#### Dynamic VLAN environment

A switch determines the destination for the client connection based on the authentication result.

#### Static VLAN environment

A switch restricts connection to specific networks based on the authentication result.

The following table shows the possible combinations of authentication method and VLAN environment that can be used when a quarantine system linked to an authentication server is created.

*Table 12-1:* Authentication method and VLAN environment available when a quarantine system linked to an authentication server is created

Authentication method	VLAN environment	
	Dynamic VLAN	Static VLAN
IEEE802.1X authentication	Y	Y
MAC authentication	--	Y

Legend:

Y: Applicable

--: Not applicable

■ JP1/Software Distribution (AMT Linkage facility)

When a computer compatible with AMT is used as a client, AMT Linkage facility Component of JP1/Software Distribution uses the AMT packet control functionality to control client connections to the network.

## 12.1.2 Quarantine system overview by linked product

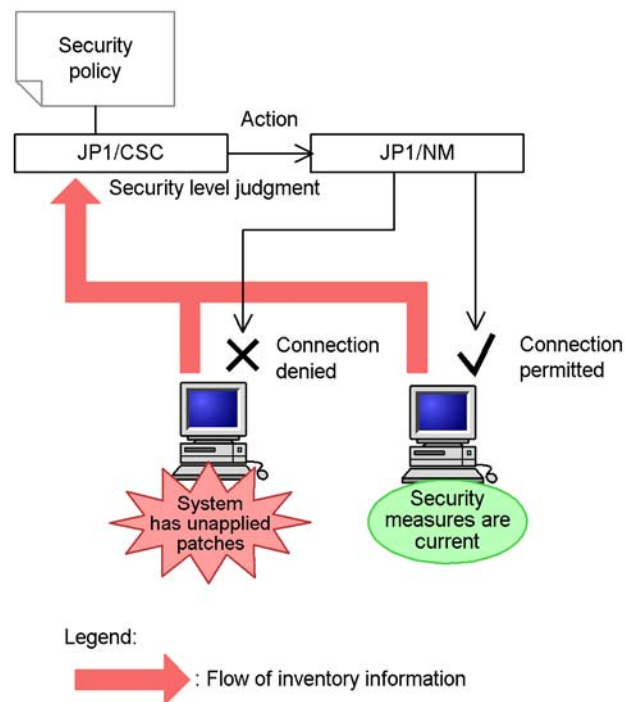
This subsection gives an overview of the quarantine system for each linked product.

### (1) Quarantine system linked to JP1/NM

In a quarantine system linked to JP1/NM, clients judged to be a security risk according to the security policy can be disconnected from the network.

The following figure shows a quarantine system linked to JP1/NM.



Figure 12-2: Quarantine system linked to JP1/NM





When a client is denied connection to the network, security measures can be implemented for the client in an offline environment, or in an online environment when using the JP1/NM *quarantine support facility*.

The following table shows the quarantine processes in a quarantine system linked to JP1/NM.

Table 12-2: Quarantine process (JP1/NM)

No.	Quarantine process	Description
1		Client security levels are judged, and clients that are a security risk are identified.
2		The network connections of clients judged to be a security risk are denied by JP1/NM.



No.	Quarantine process	Description
3		<p>Security measures are implemented for clients whose network connections were denied.</p> <ul style="list-style-type: none"> <li>• When using the quarantine support facility: Security measures are implemented in an online environment.</li> <li>• When not using the quarantine support facility: Security measures are implemented in an offline environment.</li> </ul>
4		<p>Client security levels are judged, and those found to be safe are reconnected to the network by JP1/NM.</p>

## (2) Overview of a quarantine system linked to an authentication server

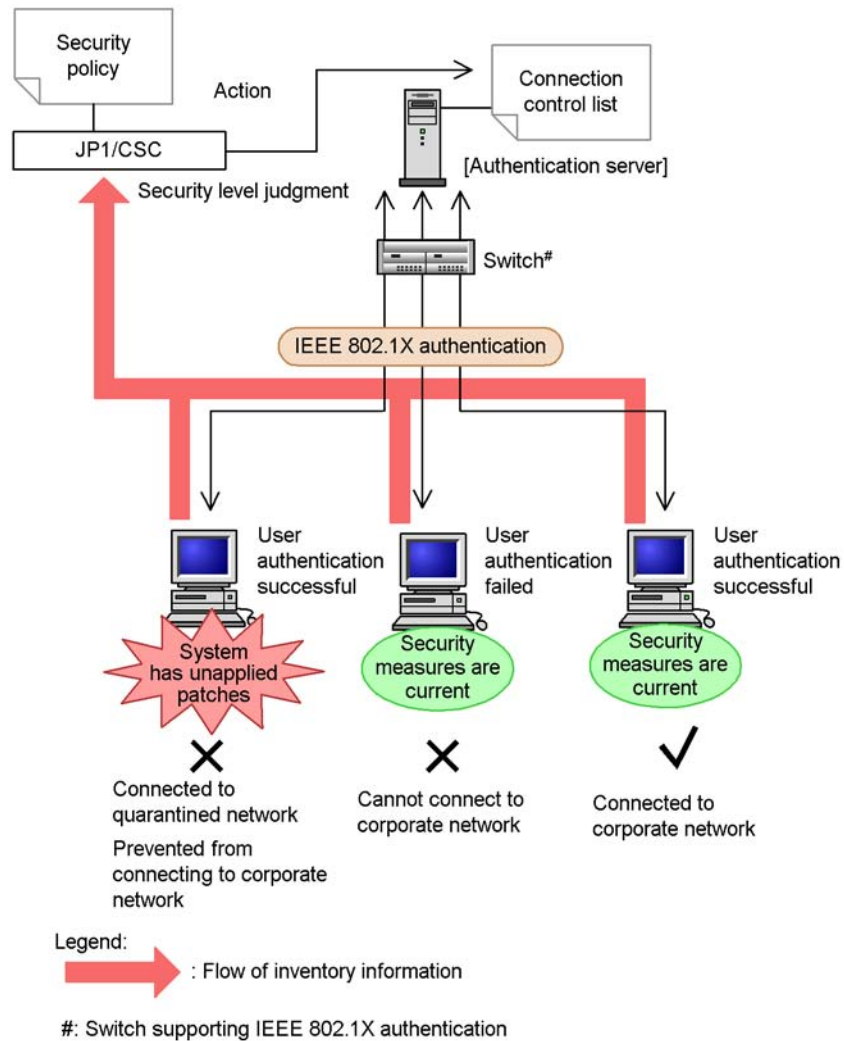
In a quarantine system linked to an authentication server, a client's safety is judged based on the security policy, and clients are authenticated by using either IEEE 802.1X or MAC authentication.

If the security level judgment determines that the client is safe, the client is connected to the corporate network. If a client is judged to be unsafe, the client is connected to a special network for unsafe clients. In addition, the client's request to connect to the network can also be rejected.

In this manual, the term for the special network for unsafe clients differs according to whether the VLAN environment is dynamic or static. In a dynamic VLAN environment, *quarantine network* is used, and in a static VLAN environment, *unauthenticated network* is used.

The following figure provides an overview of the quarantine system linked to an authentication server in a dynamic VLAN environment.

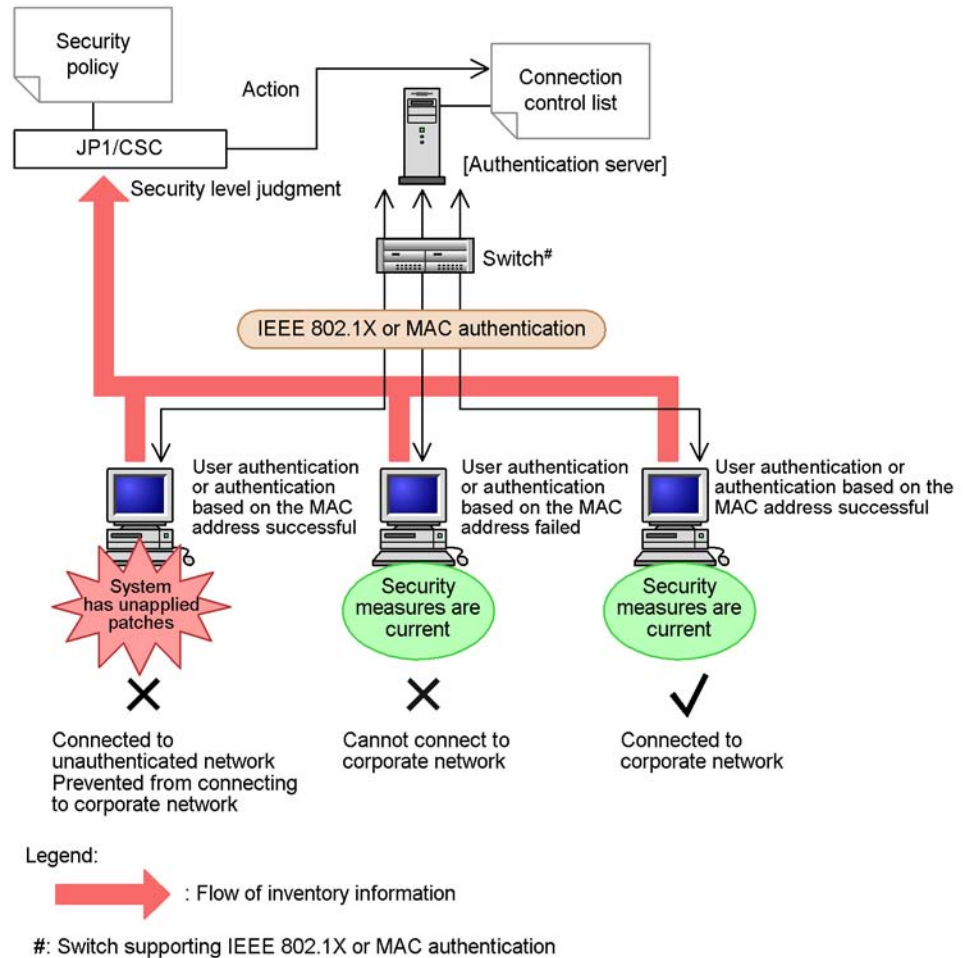
Figure 12-3: Overview of the quarantine system linked to an authentication server (in a dynamic VLAN environment)



In a dynamic VLAN environment, a client that is a high security risk is connected to the quarantine network, where security measures can be implemented. In this environment, a VLAN is created with a switch.

The following figure provides an overview of the quarantine system linked to an authentication server in a static VLAN environment.

Figure 12-4: Overview of the quarantine system linked to an authentication server (in a static VLAN environment)







In a static VLAN environment, a client that is a high security risk is connected to the unauthorized network, where security measures can be implemented.

In a quarantine system linked to an authentication server, the clients that are permitted to connect to the network according to the action policy are registered in the connection control list of JP1/CSC - Agent, which is used to control client network connection.

The following table shows the quarantine processes in a quarantine system linked to an authentication server.

*Table 12-3: Quarantine process (authentication server)*

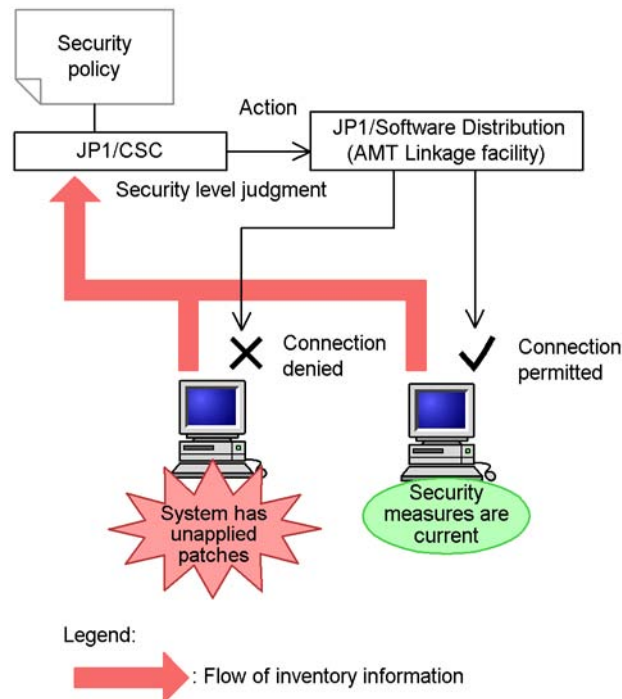
No.	Quarantine process	Description
1		Client security levels are judged, and clients that are a security risk are identified. Clients are authenticated by either IEEE 802.1X or MAC authentication.
2		The switch selects the destination for the client connection based on the connection control list as follows: <ul style="list-style-type: none"> <li>• In a dynamic VLAN environment, unsafe clients are connected to the quarantine network.</li> <li>• In a static VLAN environment, unsafe clients are connected to the unauthenticated network.</li> </ul>
3		Security measures are implemented for the clients connected to the quarantine or unauthorized network.
4		The clients are re-authenticated and their security levels are judged again. If the clients are judged to be safe, the switch connects them to the corporate network.

**(3) Quarantine system linked to JP1/Software Distribution (AMT Linkage facility)**

In a quarantine system linked to JP1/Software Distribution (AMT Linkage facility), clients judged to be a security risk according to the security policy can be disconnected from the network.

The following figure shows an overview of a quarantine system linked to JP1/Software Distribution (AMT Linkage facility).

Figure 12-5: Quarantine system linked to JP1/Software Distribution (AMT Linkage facility)





When a client is denied connection to the network, security measures can be implemented for the client in an online environment.

The following table shows the quarantine processes in a quarantine system linked to JP1/Software Distribution (AMT Linkage facility).

Table 12-4: Quarantine process (JP1/Software Distribution (AMT Linkage facility))

No.	Quarantine process	Description
1	<div style="border: 1px solid black; padding: 5px; text-align: center;">Inspection</div>	Client security levels are judged, and clients that are a security risk are identified.
2	<div style="border: 1px solid black; padding: 5px; text-align: center;">Isolation</div>	Connection to the network of clients judged to be a security risk is denied by the AMT Linkage facility of JP1/Software Distribution.

No.	Quarantine process	Description
3	 Treatment	Security measures are implemented in an online environment for clients for which connection to the network has been denied.
4	 Recovery	Client security levels are judged, and those found to be safe are reconnected to the network by the AMT Linkage facility of JP1/ Software Distribution.

---

## 12.2 Quarantine system linked to JP1/NM

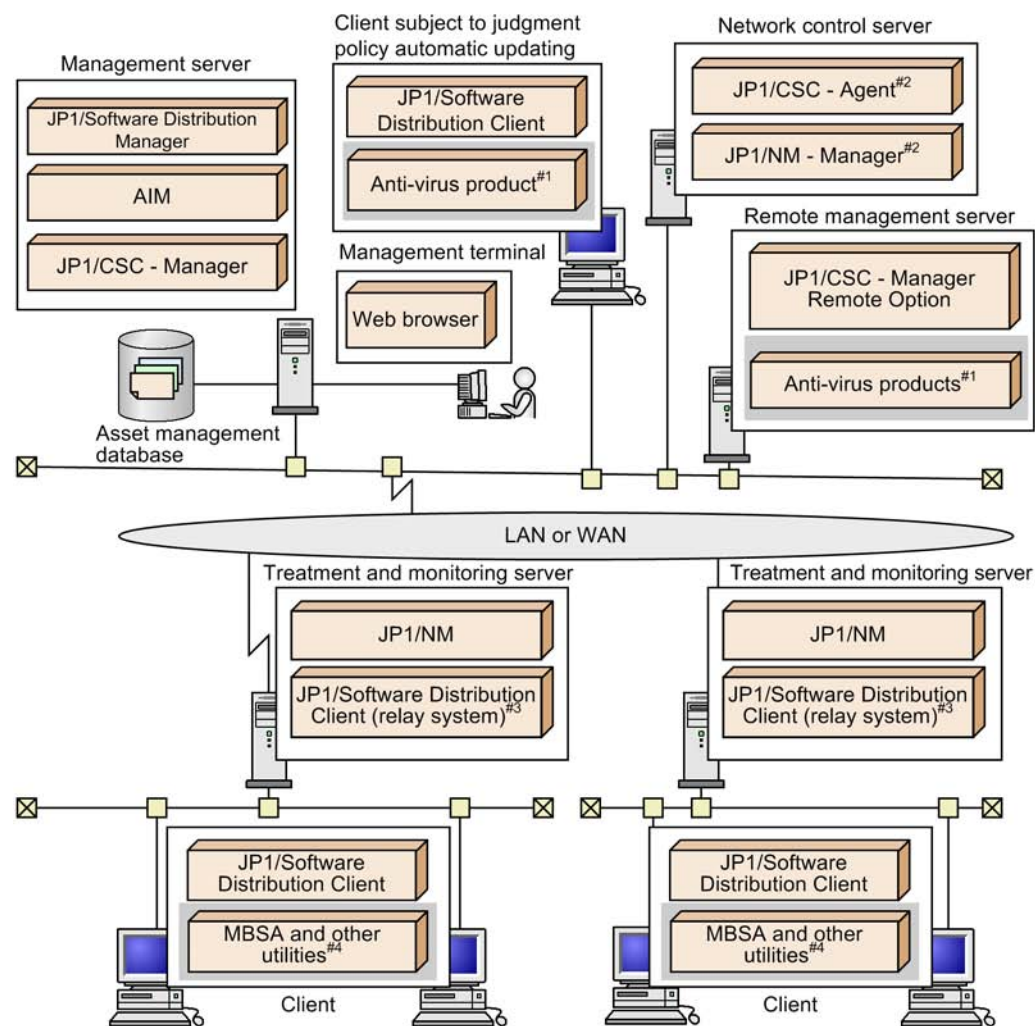
---

This subsection describes the basic configuration of a quarantine system linked to JP1/NM, and the programs and OS required to run it.

### 12.2.1 Basic configuration of quarantine system linked to JP1/NM

The following figure shows the basic configuration of a quarantine system linked to JP1/NM.

Figure 12-6: Basic configuration of quarantine system linked to JP1/NM



Legend:

■ : Optional product (install if needed)

#1: Anti-virus product linked with automatic judgment policy updating for anti-virus products.

#2: JP1/CSC - Agent and JP1/NM - Manager can be installed on the management server. These products can run on the same machine as JP1/CSC - Manager, AIM, and JP1/Software Distribution Manager.

#3: Required if you use the JP1/NM quarantine support facility. JP1/Software Distribution SubManager 07-50 or later may be used instead.

JP1/NM can also be installed on another machine, depending on the version. In Windows, JP1/NM 09-00 or later can be installed on another machine. In Linux, JP1/NM 08-11 or later can be installed on another machine.

#4: Optional in a basic configuration of a client security control system.

### Management terminal



A management terminal is used by an administrator to reference the asset management database, manage client asset information, monitor the status of client security measures, and implement actions. It uses the GUI for AIM.

#### Management server

A management server manages inventory information in an asset management database, judges client security levels according to the security policy, and implements actions appropriate to these security levels.

It also packages files used to implement the security measures, such as software patches.

#### Network control server

A network control server receives instructions from actions (permit or deny network connections) implemented on the management server, and from the network control command (`cscnetctrl`) executed on the remote management server. It then instructs the monitoring server to control client network connections based on these instructions.

#### Remote management server

A system configuration with a remote management server is set up to automatically update judgment policies by linkage with the anti-virus product installed on the remote management server, or to control client network connections from another system.

Install JP1/CSC - Manager Remote Option on the remote management server.

#### Client subject to judgment policy automatic updating

This client contains an anti-virus product linked with automatic judgment policy updating for anti-virus products. This client is required to automatically update judgment policy definitions for anti-virus products based on the update information for the anti-virus product installed on the client.

#### Treatment and monitoring servers

Set up a treatment server when using the JP1/NM quarantine support facility, or a monitoring server when not using this function.

- Treatment server

When using the JP1/NM quarantine support facility, set up a treatment server.

A treatment server controls client network connections. It also maintains communication with clients that have been disconnected from the network, in order to implement security measures on the client.

Clients disconnected from the network are shut off from communication

with other devices. These clients are allowed to communicate with the treatment server only through the quarantine support facility. This allows security measures to be implemented in an online environment.

- **Monitoring server**

When not using the JP1/NM quarantine support facility, set up a monitoring server. A monitoring server controls client network connections.

Only JP1/NM should be installed on the monitoring server if the quarantine support facility is not used. You do not need to install JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager.

#### Client

A client is the entity that is managed in a quarantine system. A client sends inventory information to the management server, which judges the security level of the client for the inventory information based on the security policy.

### 12.2.2 Required products and prerequisite OSs

This subsection describes the product and OS requirements for each system component when linking to JP1/NM.

#### (1) When using the JP1/NM quarantine support facility

The required products and prerequisite OSs when using the JP1/NM quarantine support facility are as follows.

*Table 12-5: Required products and prerequisite OSs for a quarantine system linked to JP1/NM (using the quarantine support facility)*

No.	System component	Required products	Prerequisite OS
1	Management server	<ul style="list-style-type: none"> <li>• JP1/CSC - Manager</li> <li>• Asset Information Manager or Asset Information Manager Subset Component of JP1/Software Distribution Manager</li> <li>• JP1/Software Distribution Manager</li> </ul>	<ul style="list-style-type: none"> <li>• Windows Server 2003</li> <li>• Windows Server 2008</li> <li>• Windows Server 2008 R2</li> </ul>
2	Network control server	<ul style="list-style-type: none"> <li>• JP1/NM - Manager</li> <li>• JP1/CSC - Agent</li> </ul>	<ul style="list-style-type: none"> <li>• Windows Server 2003</li> <li>• Windows Server 2008</li> <li>• Windows Server 2008 R2</li> </ul>

No.	System component	Required products	Prerequisite OS
3	Treatment server	<ul style="list-style-type: none"> <li>JP1/NM</li> <li>JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager<sup>#</sup></li> </ul>	See the manuals <i>Job Management Partner 1/Network Monitor Description, User's Guide and Operator's Guide</i> and <i>Job Management Partner 1/Software Distribution Setup Guide</i> , for Windows systems.
4	Client	JP1/Software Distribution Client	See the manual <i>Job Management Partner 1/Software Distribution Setup Guide</i> , for Windows systems.

#

Version 07-50 or later of JP1/Software Distribution SubManager is required.

## (2) When not using the JP1/NM quarantine support facility

The required programs and prerequisite OSs when running a quarantine system without the JP1/NM quarantine support facility are as follows.

*Table 12-6:* Required programs and prerequisite OSs for a quarantine system linked to JP1/NM (without the quarantine support facility)

No.	System component	Required products	Prerequisite OS
1	Management server	<ul style="list-style-type: none"> <li>JP1/CSC - Manager</li> <li>Asset Information Manager or Asset Information Manager Subset Component of JP1/Software Distribution Manager</li> <li>JP1/Software Distribution Manager</li> </ul>	<ul style="list-style-type: none"> <li>Windows Server 2003</li> <li>Windows Server 2008</li> <li>Windows Server 2008 R2</li> </ul>
2	Network control server	<ul style="list-style-type: none"> <li>JP1/NM - Manager</li> <li>JP1/CSC - Agent</li> </ul>	<ul style="list-style-type: none"> <li>Windows Server 2003</li> <li>Windows Server 2008</li> <li>Windows Server 2008 R2</li> </ul>
3	Monitoring server	JP1/NM	See the manual <i>Job Management Partner 1/Network Monitor Description, User's Guide and Operator's Guide</i> .
4	Client	JP1/Software Distribution Client <sup>#</sup>	See the manual <i>Job Management Partner 1/Software Distribution Setup Guide</i> , for Windows systems.

#

When running a quarantine system without the JP1/NM quarantine support facility, security measures are implemented on the client in an offline environment.

If you use the JP1/Software Distribution offline machine management facility (functionality for installing software offline and obtaining inventory information from offline machines) to take security measures for clients, the JP1/Software Distribution Client version must be 08-00 or later.

---

## 12.3 Quarantine system linked to an authentication server

---

This subsection describes the basic configuration of a quarantine system linked to an authentication server, and the programs and OS required to run it.

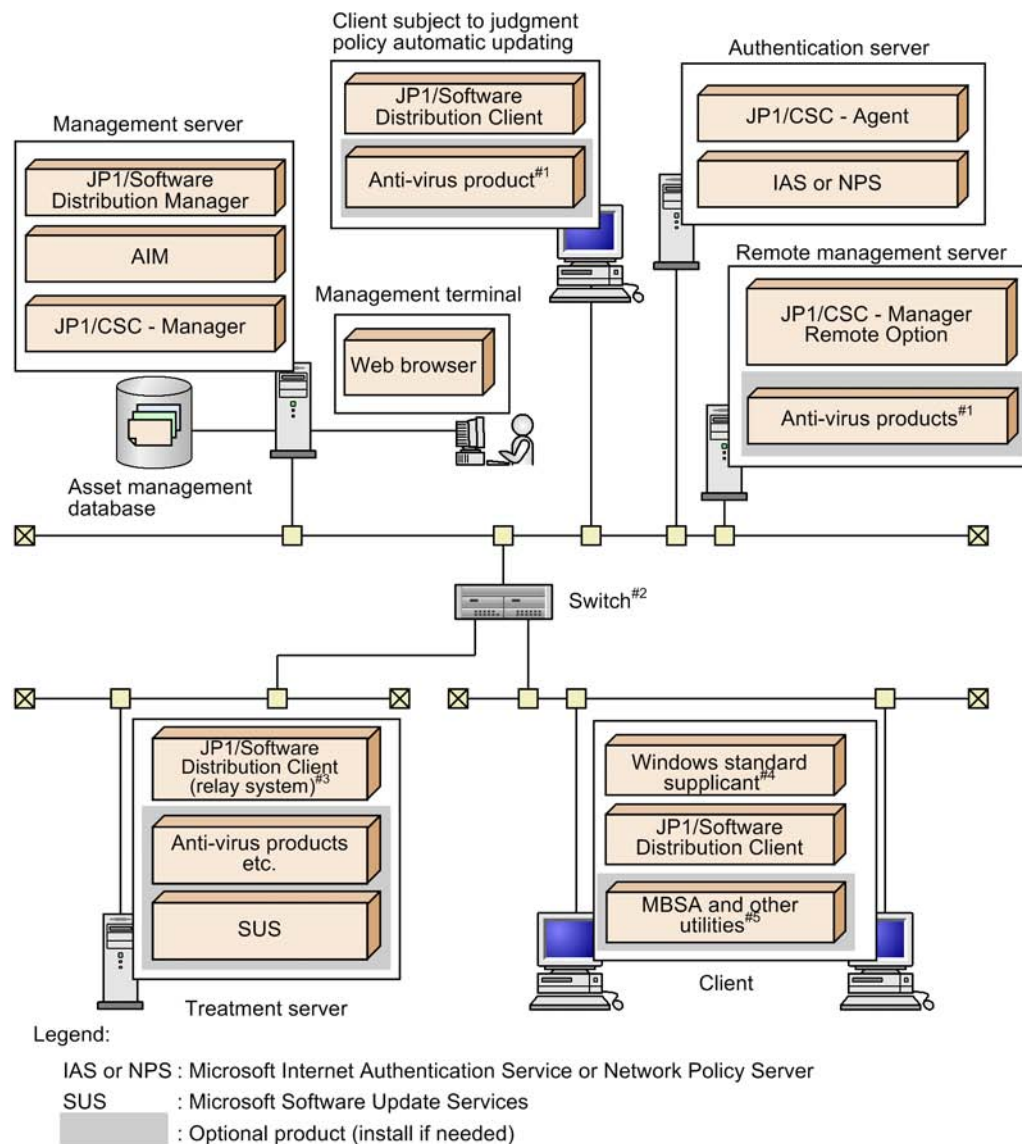
### 12.3.1 Configuration of a quarantine system linked to an authentication server

This subsection explains the basic configuration and network configuration of a quarantine system linked to an IEEE 802.1X authentication server, and the configuration of the network. It also explains the configuration of a system containing multiple authentication servers.

#### **(1) *Basic configuration of a quarantine system linked to an authentication server***

The following figure shows the basic configuration of a quarantine system linked to an authentication server.

Figure 12-7: Basic configuration of quarantine system linked to an authentication server



- #1: Anti-virus product linked with automatic judgment policy updating for anti-virus products.  
 #2: Switch supporting IEEE 802.1X or MAC authentication  
 #3: JP1/Software Distribution SubManager 07-50 or later may be used instead.  
 #4: This product is not necessary when MAC authentication is used.  
 #5: Optional in a basic configuration of a client security control system.

#### Management terminal

A management terminal is used by an administrator to reference the asset management database, manage client asset information, monitor the status of client security measures, and implement actions. It uses the GUI for AIM.

#### Management server

A management server manages inventory information in an asset management database, judges client security levels according to the security policy, and implements actions appropriate to these security levels.

It also packages files used to implement the security measures, such as software patches.

#### Authentication server

The authentication server uses either IEEE 802.1X or MAC authentication to authenticate clients.

The server also updates the connection control list based on a management server action (whether to permit network connection) and the network control command (`cscnetctrl`) received from a remote management server. In addition, the server instructs the switch to select the destination for client connection based on the connection control list.

#### Remote management server

A system configuration with a remote management server is set up to automatically update judgment policies for anti-virus products by linkage with the anti-virus product installed on the remote management server, or to control client network connections from another system.

Install JP1/CSC - Manager Remote Option on the remote management server.

#### Client subject to judgment policy automatic updating

This client contains an anti-virus product linked with automatic judgment policy updating for anti-virus products. This client is required to automatically update judgment policy definitions for anti-virus products based on the update information for the anti-virus product installed on the client.

#### Treatment server

A treatment server communicates with clients connected to the quarantined network, in order to implement security measures on those clients.

By installing Microsoft Software Update Services and an anti-virus product on the treatment server, security measures that use these products can be implemented.

Note that Microsoft Software Update Services and the anti-virus product can be installed on separate machines.

### Client

A client is the entity that is managed in a quarantine system. A client sends inventory information to the management server, which judges the security level of the client for the inventory information based on the security policy.

Note that if IEEE 802.1X authentication is used, the Windows standard supplicant supporting this type of authentication is required.

### Switch

A switch supporting either IEEE 802.1X or MAC authentication.

In a dynamic VLAN environment, the switch selects the destination for client connection in the VLAN based on the network connection control instruction from the authentication server. In a static VLAN environment, the switch controls connection of the client to the corporate network according to the authentication result on the authentication server.

## ***(2) Network configuration of a quarantine system linked to an authentication server***

The following explains the network configuration of a quarantine system linked to an authentication server.

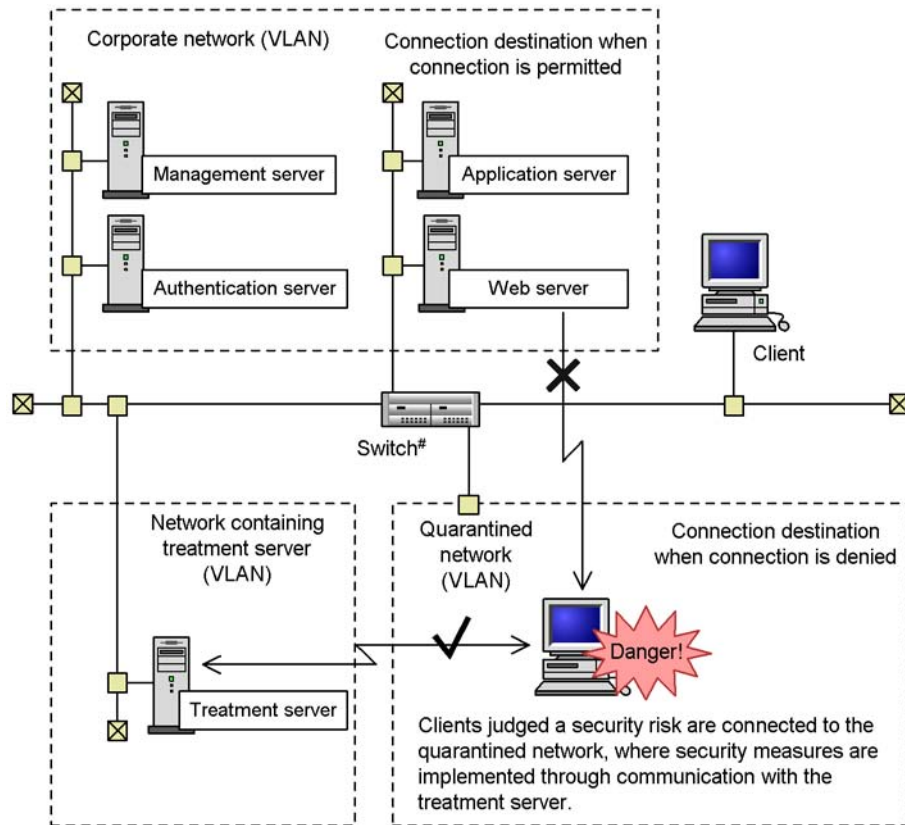
### **(a) In a dynamic VLAN environment**

In a quarantine system linked to an authentication server in a dynamic VLAN environment, a VLAN containing a switch that supports IEEE 802.1X authentication is used to set up the networks, such as the corporate and quarantine networks.

The following figure shows an example of the network configuration of a quarantine system linked to an authentication server in a dynamic VLAN environment.



Figure 12-8: Example of the network configuration of a quarantine system linked to an authentication server (dynamic VLAN environment)



#: Switch supporting IEEE 802.1X authentication

VLANs are used to isolate the quarantined network where client security measures are implemented, the network where the treatment server resides, and the corporate network. The quarantined network will be allowed to communicate with the network where the treatment server resides.

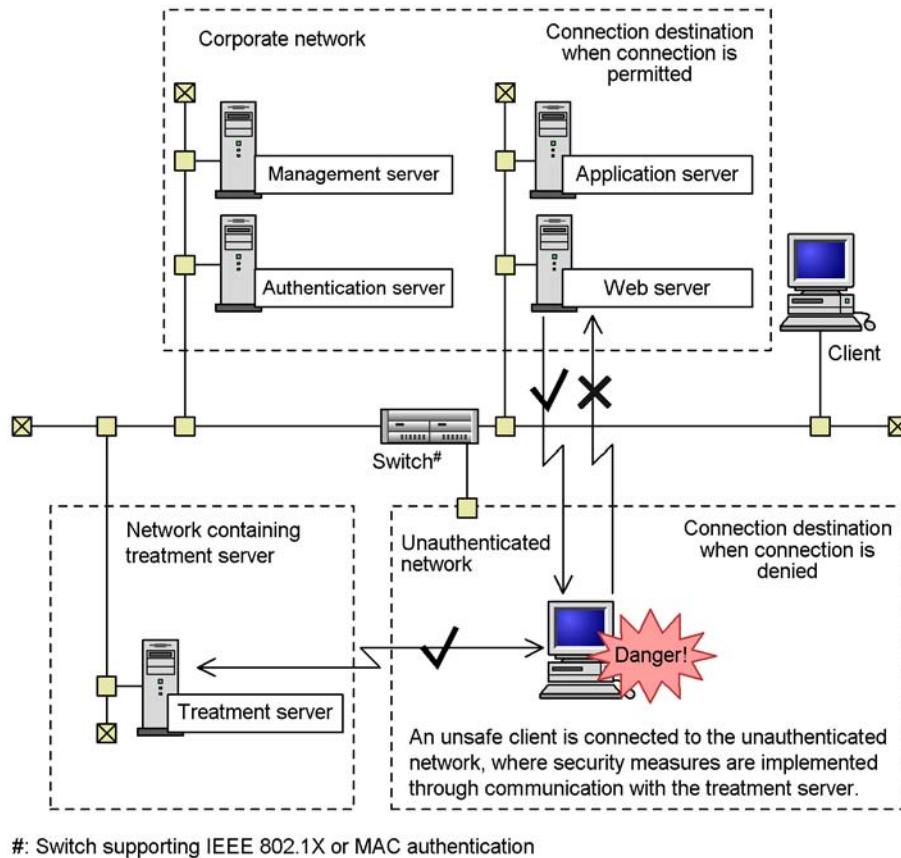
For details about the recommended network configuration and communication between networks, see *13.2.3 Setting up the network control device (dynamic VLAN environment)*.

#### (b) In a static VLAN environment

In a quarantine system linked to an authentication server in a static VLAN environment, a switch supporting IEEE 802.1X or MAC authentication is used to isolate the corporate and unauthenticated networks from each other.

The following figure shows an example of the network configuration of a quarantine system linked to an authentication server in a static VLAN environment.

*Figure 12-9: Example of the network configuration of a quarantine system linked to an authentication server (static VLAN environment)*



Connection of unsafe clients to the corporate network is controlled so that these clients are connected to the unauthenticated network, which is set to allow communication only with a network that contains a treatment server.

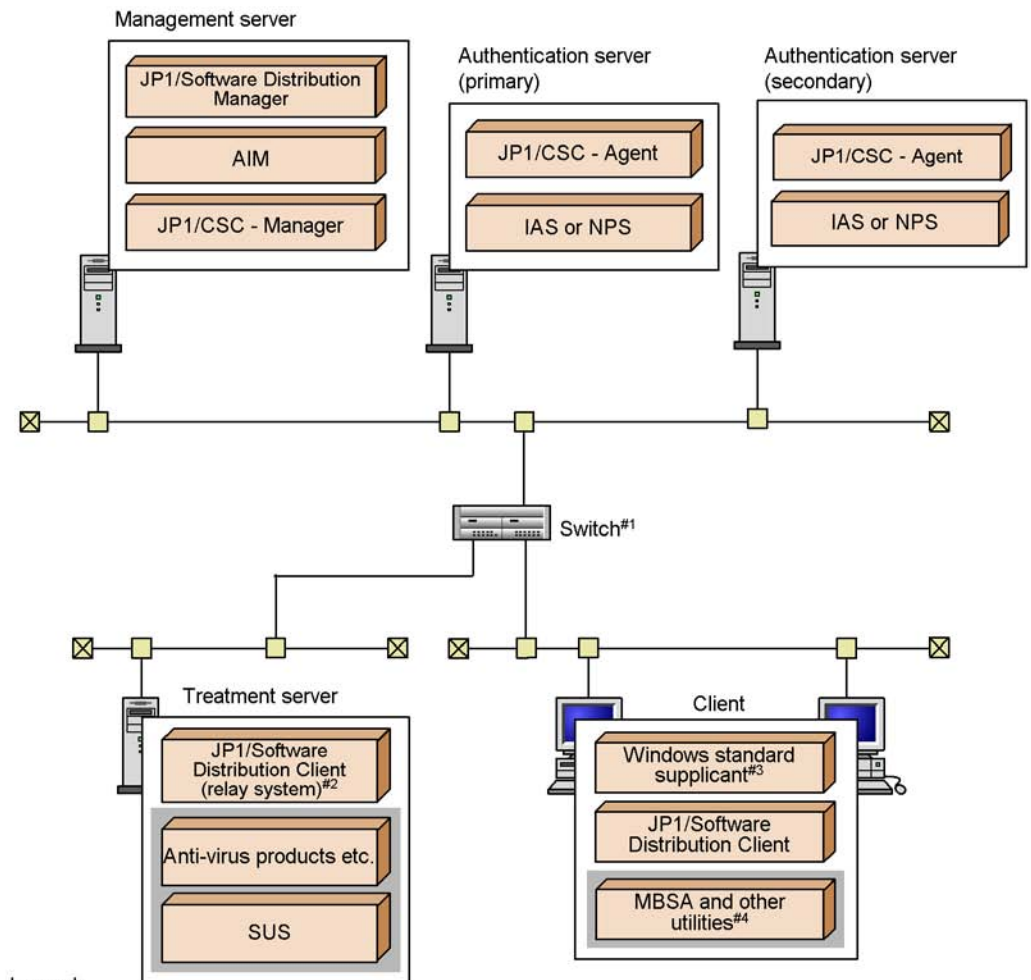
For details about the recommended network configuration, see *13.2.4 Setting up the network control device (static VLAN environment)*.

### **(3) System configuration containing multiple authentication servers**

If there are too many clients to be managed smoothly with a quarantine system linked to only one authentication server, you can add authentication servers to distribute the authentication processing.

The following figure shows a system configuration that contains more than one authentication server.

Figure 12-10: System configuration containing multiple authentication servers



Legend:

IAS or NPS : Microsoft Internet Authentication Service or Network Policy Server

SUS : Microsoft Software Update Services

Optional product (install if needed)

#1: Switch supporting IEEE 802.1X or MAC authentication

#2: JP1/Software Distribution SubManager 07-50 or later may be used instead.

#3: This product is not necessary when MAC authentication is used.

#4: Optional in a basic configuration of a client security control system.

### 12.3.2 Required products and prerequisite OSs

This subsection describes the product and OS requirements for each system component for linkage to an authentication server.

*Table 12-7: Required products and prerequisite OSs for a quarantine system linked to an authentication server*

No.	System component	Required products	Prerequisite OS
1	Management server	<ul style="list-style-type: none"> <li>JP1/CSC - Manager</li> <li>Asset Information Manager or Asset Information Manager Subset Component of JP1/Software Distribution Manager</li> <li>JP1/Software Distribution Manager</li> </ul>	<ul style="list-style-type: none"> <li>Windows Server 2003</li> <li>Windows Server 2008</li> </ul>
2	Authentication server	<ul style="list-style-type: none"> <li>JP1/CSC - Agent</li> <li>Microsoft Internet Authentication Service<sup>#1</sup> or Network Policy Server<sup>#2</sup></li> </ul>	<ul style="list-style-type: none"> <li>Windows Server 2003<sup>#3</sup></li> <li>Windows Server 2008<sup>#3</sup></li> </ul>
3	Treatment server	<ul style="list-style-type: none"> <li>JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager<sup>#4</sup></li> </ul>	See the manual <i>Job Management Partner 1/Software Distribution Setup Guide</i> , for Windows systems.
4	Client (IEEE 802.1X authentication)	<ul style="list-style-type: none"> <li>JP1/Software Distribution Client 08-00 or later</li> <li>Windows standard supplicant<sup>#5</sup></li> </ul>	<ul style="list-style-type: none"> <li>Windows 2000</li> <li>Windows XP</li> <li>Windows Server 2003</li> <li>Windows Vista</li> <li>Windows Server 2008</li> <li>Windows 7</li> </ul>
5	Client (MAC authentication)	<ul style="list-style-type: none"> <li>JP1/Software Distribution Client 08-00 or later</li> </ul>	See the manual <i>Job Management Partner 1/Software Distribution Setup Guide</i> , for Windows systems.

Legend:

--: None

#1

Provided as standard on the installation media for Windows Server 2003.

#2

Provided as standard on the installation media for Windows Server 2008.

#3

The 64-bit edition of Windows Server 2003, the 64-bit edition of Windows Server 2008 and the 64-bit edition of Windows Server 2008 R2 are not supported.

#4

If JP1/Software Distribution SubManager is used, the version must be 07-50 or later.

#5

The supplicant is a standard component of the prerequisite Windows OS. Note that, in Windows 2000, the supplicant is installed only if Service Pack 4 is installed.

---

## **12.4 Quarantine system linked to JP1/Software Distribution (AMT Linkage facility)**

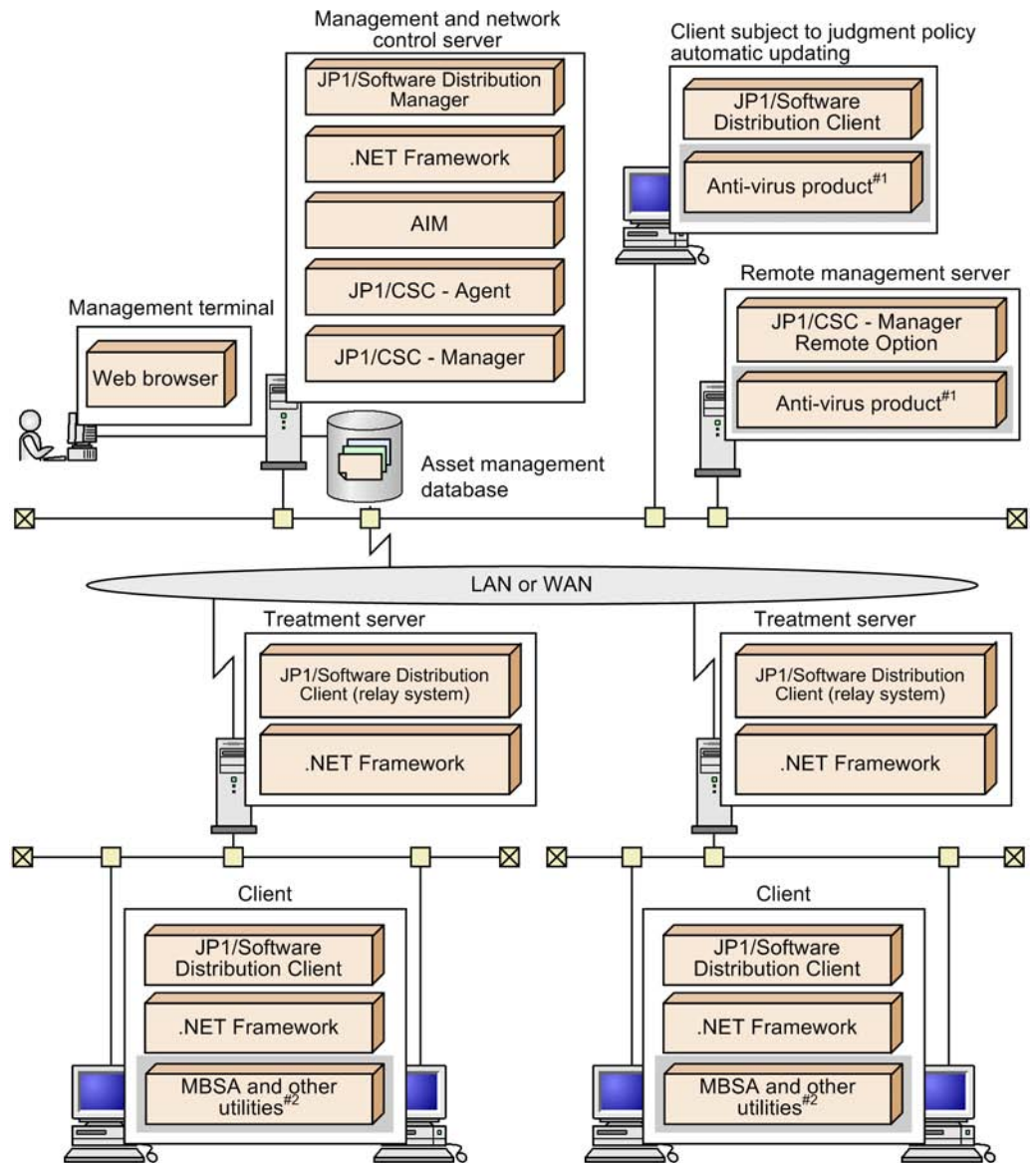
---

This subsection describes the basic configuration of a quarantine system linked to JP1/Software Distribution (AMT Linkage facility), and the programs and OS required to run it.

### **12.4.1 Basic configuration of quarantine system linked to JP1/Software Distribution (AMT Linkage facility)**

The following figure shows the basic configuration of a quarantine system linked to JP1/Software Distribution (AMT Linkage facility).

Figure 12-11: Basic configuration of quarantine system linked to JP1/Software Distribution (AMT Linkage facility)



Legend:

■ : Optional product (install if needed)

#1: Anti-virus product linked with automatic judgment policy updating for anti-virus products.

#2: Optional in the basic configuration of a client security control system.

### Management terminal

A management terminal is used by an administrator to reference the asset management database, manage client asset information, monitor the status of client security measures, and implement actions. It uses the GUI for AIM.

### Management and network control server

A management and network control server manages inventory information in an asset management database, judges client security levels according to the security policy, and exercises control appropriate for the security level over the connection of clients to the network.

It also packages files used to implement the security measures, such as software patches.

### Remote management server

A system configuration with a remote management server is set up to automatically update judgment policies for anti-virus products by linkage with the anti-virus product installed on the remote management server, or to control client network connections from another system.

Install JP1/CSC - Manager Remote Option on the remote management server.

### Client subject to judgment policy automatic updating

This client contains an anti-virus product linked with automatic judgment policy updating for anti-virus products. This client is required to automatically update judgment policy definitions for anti-virus products based on the update information for the anti-virus product installed on the client.

### Treatment server

A treatment server implements security measures on clients.

Clients disconnected from the network are shut off from communication with other devices, except through specific ports such as one for JP1/Software Distribution. The JP1/Software Distribution port allows JP1/Software Distribution on the treatment server to be used to implement security measures in an online environment.

### Client

A client is the entity that is managed in a quarantine system. A client sends inventory information to the management server, which judges the security level of the client for the inventory information based on the security policy.

## 12.4.2 Required products and prerequisite OS

This subsection describes the product and OS requirements for each system component for linking to JP1/Software Distribution (AMT Linkage facility).



*Table 12-8: Required programs and prerequisite OS for a quarantine system linked to JP1/Software Distribution (AMT Linkage facility)*

No.	System component	Required products	Prerequisite OS
1	Management and network control server	<ul style="list-style-type: none"> <li>JP1/CSC - Manager</li> <li>JP1/CSC - Agent</li> <li>Asset Information Manager Subset Component of JP1/Software Distribution or Asset Information Manager</li> <li>JP1/Software Distribution Manager<sup>#</sup></li> <li>.NET Framework 1.1 or 2.0</li> </ul>	<ul style="list-style-type: none"> <li>Windows Server 2003</li> <li>Windows Server 2008</li> </ul>
2	Treatment server	<ul style="list-style-type: none"> <li>JP1/Software Distribution Client (relay system)<sup>#</sup></li> <li>.NET Framework 1.1 or 2.0</li> </ul>	See the manual <i>Job Management Partner 1/ Software Distribution Setup Guide</i> , for Windows systems.
3	Client	<ul style="list-style-type: none"> <li>JP1/Software Distribution <sup>#</sup></li> <li>.NET Framework 1.1 or 2.0</li> </ul>	See the manual <i>Job Management Partner 1/ Software Distribution Setup Guide</i> , for Windows systems.

<sup>#</sup>

The AMT Linkage facility component of JP1/Software Distribution must be installed.



## Chapter

---

# 13. Setting Up a Quarantine System

---

This chapter describes how to set up a quarantine system on JP1/CSC with each linked product.

- 13.1 Setting up a quarantine system linked to JP1/NM
- 13.2 Setting up a quarantine system linked to an authentication server
- 13.3 Setting up a quarantine system linked to JP1/Software Distribution (AMT Linkage facility)

---

## 13.1 Setting up a quarantine system linked to JP1/NM

---

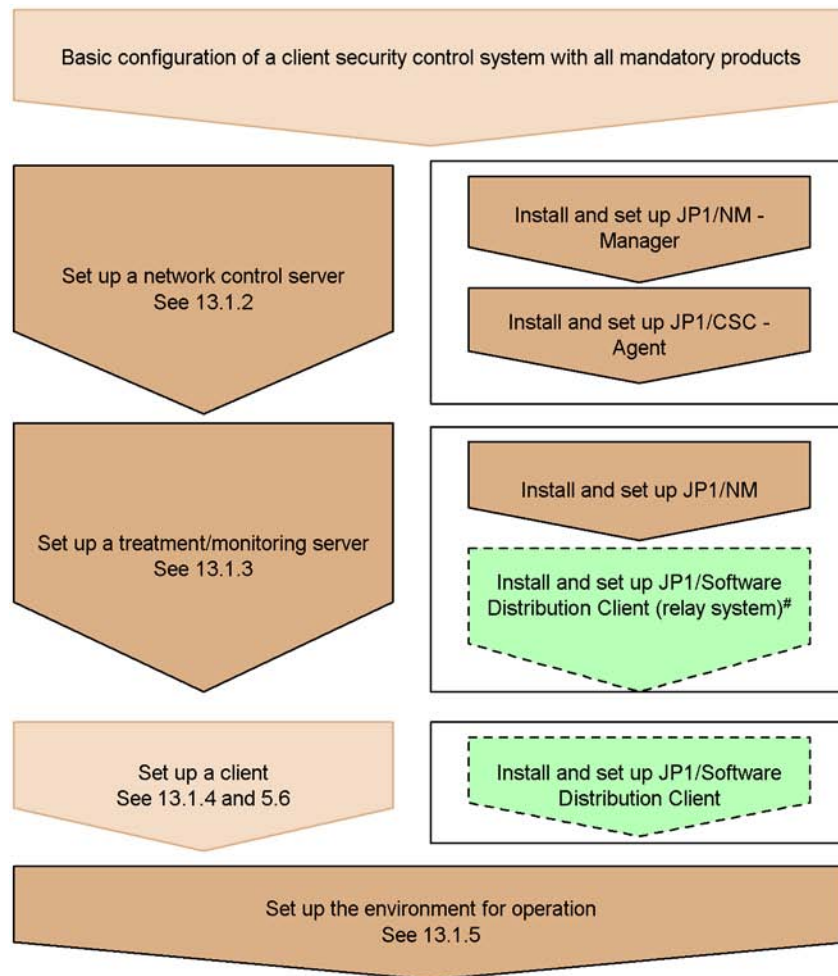
This section describes the procedure for setting up a quarantine system linked to JP1/NM.

### 13.1.1 Flow of system setup

The following figure shows the procedures for setting up a quarantine system linked to JP1/NM.

Before you set up a quarantine system, you must have set up a client security control system with all the required core products.

Figure 13-1: Setting up a quarantine system linked to JP1/NM



## Legend:



: Perform these steps to set up a client security control system.



: These steps are required to set up a quarantine system.



: Required if you intend to use the JP1/NM quarantine support facility.

# JP1/Software Distribution SubManager may be used instead.

Install programs on the network control server in the order shown in Figure 13-1.

### 13.1.2 Setting up a network control server

Set up a network control server, installing and setting up the following programs:

- JP1/NM - Manager
- JP1/CSC - Agent

#### (1) Installing JP1/NM - Manager

Install JP1/NM - Manager on the network control server. For details about installing JP1/NM - Manager, see the manual *Job Management Partner 1/Network Monitor - Manager Description, User's Guide and Operator's Guide*.

#### (2) Setting up JP1/NM - Manager

To link JP1/NM - Manager with JP1/CSC, specify the following settings in the Integrated Management window of JP1/NM - Manager:

- Set the common login information for the treatment and monitoring servers.
- Create a treatment and monitoring server list.
- Set JP1 linkage.

The following table lists the items that can be set in the Integrated Management window of JP1/NM - Manager.

*Table 13-1: Items that can be set in the Integrated Management window of JP1/NM - Manager*

No.	Item	Contents set
1	Set the common login information for logging in to treatment and monitoring servers	Set the same login information used to log in from a Web browser to the treatment and monitoring servers. The common login information is as follows: <ul style="list-style-type: none"> <li>• User name</li> <li>• Password</li> </ul>
2	Create a treatment and monitoring server list	The list of treatment and monitoring servers is created as a CSV file.
3	Set up JP1 linkage	Perform the necessary settings to link to JP1/CSC. The items to be set are as follows: <ul style="list-style-type: none"> <li>• Select the <b>Update the permitted/blocked devices list through the link function</b> check box.</li> <li>• Select the <b>Update immediately by calling the API</b> check box.</li> </ul>

For details about how to perform these settings, see the manual *Job Management Partner 1/Network Monitor - Manager Description, User's Guide and Operator's*

*Guide.*

**(3) Installing JP1/CSC - Agent**

Install JP1/CSC - Agent on the network control server. Note that JP1/NM - Manager must be installed and set up on the network control server before you install JP1/CSC - Agent.

For details about installing JP1/CSC - Agent, see *5.7.1 Installing JP1/CSC - Agent*.

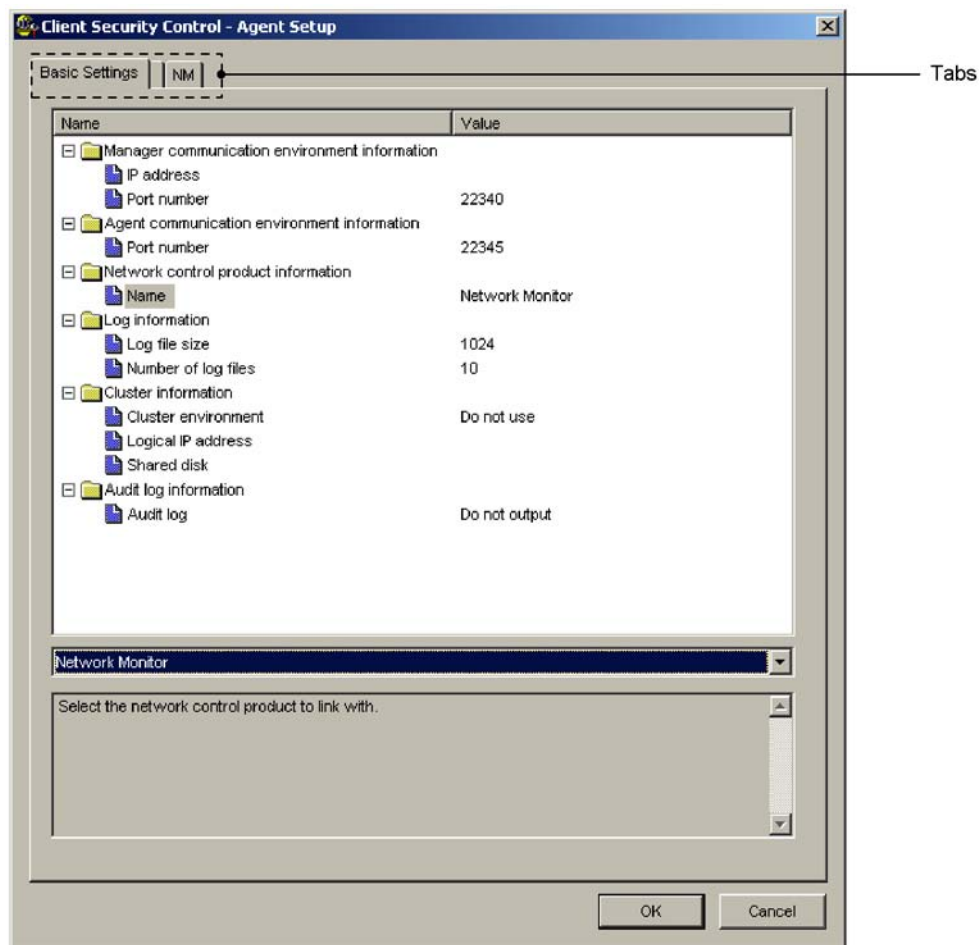
**(4) Setting up JP1/CSC - Agent**

After installing JP1/CSC - Agent, be sure to set up JP1/CSC - Agent before starting it.

You can set the information required for JP1/CSC - Agent setup by using the Client Security Control - Agent Setup dialog box.

The Client Security Control - Agent Setup dialog box has two pages, each of which is opened by clicking a tab. The following figure shows the Client Security Control - Agent Setup dialog box.

Figure 13-2: Client Security Control - Agent Setup dialog box



The following table describes the pages of the Client Security Control - Agent Setup dialog box.

Table 13-2: Pages of the Client Security Control - Agent Setup dialog box

Page	Description
<b>Basic Settings</b>	The JP1/CSC - Agent environment settings that have already been specified can be displayed or modified.



Page	Description
NM	<p>This page is used only if JP1/Network Monitor is linked. The format of the permitted-devices list registered in JP1/Network Monitor can be displayed or modified.</p> <p>This page appears if JP1/Network Monitor is specified for <b>Network control product information</b> on the <b>Basic Settings</b> page.</p>

Note:

The settings for linkage to JP1/Network Monitor are specified on the **Basic Settings** and **NM** pages in the Client Security Control - Agent Setup dialog box.

To display the Client Security Control - Agent Setup dialog box and edit the settings:

1. Click the **Start** button, and choose **Programs, Client Security Control**, and then **Agent Setup**.

The Client Security Control - Agent Setup dialog box appears.

2. Set values for the items.

When you select an item, a box appears below the item list. You can either enter a value or string directly in this box or select a value from the pull-down menu.

For details, see (a) *Operations that can be performed on the Basic Settings page* and (b) *Operations that can be performed on the NM page*.

3. Click the **OK** button.

The contents you specified are set for the JP1/CSC - Agent environment. The Client Security Control - Agent Setup dialog box closes.

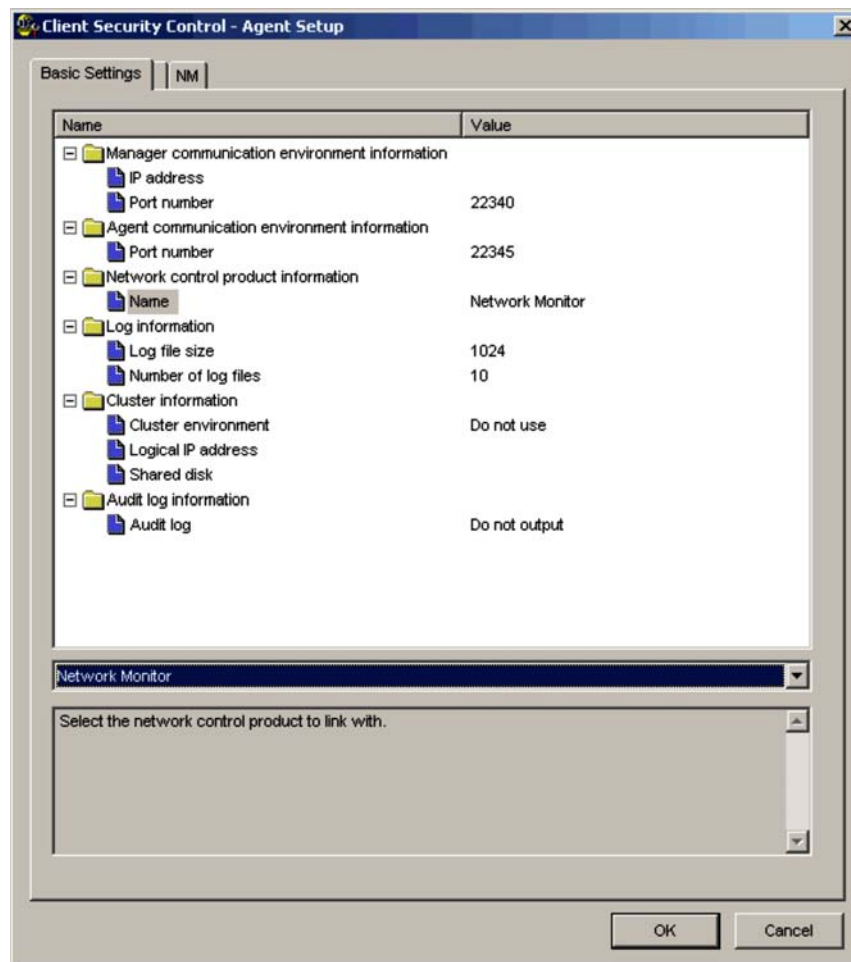
To close this dialog box without performing any environment settings, click the **Cancel** button.

#### (a) Operations that can be performed on the Basic Settings page

On the **Basic Settings** page, you can view or change the JP1/CSC - Agent environment settings.

The following figure shows the **Basic Settings** page.

Figure 13-3: Basic Settings page



The following table describes the items that can be displayed and set on the **Basic Settings** page.

Table 13-3: Items that can be displayed and set on the Basic Settings page

Item		Description	Specifiable values	Default for initial environment setup
Manager communication environment information	IP address	The IP address for JP1/CSC - Manager.	IPv4 format (xxx.xxx.xxx.xxx)	--
	Port number			

Item		Description	Specifiable values	Default for initial environment setup
	Port number	The port number JP1/CSC - Manager uses to communicate with JP1/CSC - Agent. Enter the same port number as specified in <b>Port number for receiving requests</b> under <b>Manager communication environment information</b> in the <b>Basic Settings</b> page of JP1/CSC - Manager.	1024 to 65535	22340
<b>Agent communication environment information</b>	Port number	The port number of JP1/CSC - Agent. Enter the same port number as that registered for <b>Port number</b> in the Add agent information window of JP1/CSC - Manager.	1024 to 65535	22345
<b>Network control product information</b>	Name	The name of the linked network control product.	Network Monitor	Network Monitor
<b>Log information</b>	Log file size	Specify the maximum size (in kilobytes) of the JP1/CSC - Agent log files.	1 to 2097151	1024
	Number of log files	Specify the maximum number of JP1/CSC - Agent log files.	1 to 999	10
<b>Cluster information</b>	Cluster environment	Specify whether to run JP1/CSC - Agent in a cluster environment.	<b>Use / Do not use</b>	<b>Do not use</b>
	Logical IP address	Specify a logical IP address to use in the cluster environment.	IPv4 format (xxx.xxx.xxx.xxx)	--
	Shared disk	Specify the path for the shared disk used in the cluster environment.	Full path	--
<b>Audit log information</b>	<b>Audit log</b>	Specify whether to output audit logs.	<b>Output / Do not output</b>	<b>Do not output</b>

Legend:

--: No default provided.

*Reference note:*

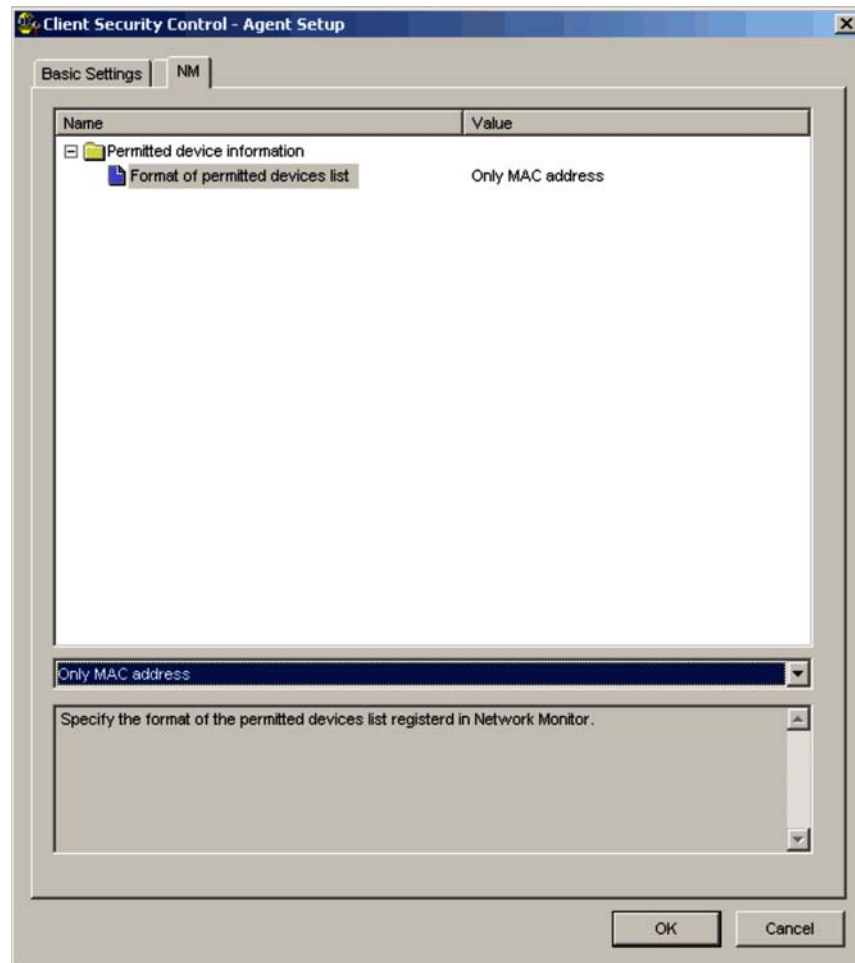
The log information contains information about startup and termination of JP1/CSC - Agent, as well as connection information for the network control product.

**(b) Operations that can be performed on the NM page**

On the **NM** page, you can view or change the format of the permitted-devices list to be registered in JP1/Network Monitor.

The following figure shows the **NM** page.

Figure 13-4: NM page



The following table describes the items that can be displayed and set on the **NM** page.

Table 13-4: Items that can be displayed and set on the Basic Settings page

Item		Description	Specifiable values	Default for initial environment setup
<b>Permitted-device information</b>	Format of the permitted-devices list	The format of the permitted-devices list to be registered in JP1/Network Monitor. <sup>#</sup>	<b>Only MAC address / MAC address and IP address</b>	<b>Only MAC address</b>

#:

For a network that uses DHCP to manage IP addresses, always specify **Only MAC address**.

### 13.1.3 Setting up a treatment or monitoring server

Set up a treatment server or a monitoring server.

If you intend to use the JP1/NM quarantine support facility, set up a treatment server. Install and set up the following programs on the treatment server:

- JP1/NM
- JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager

If you do not intend to use the JP1/NM quarantine support facility, set up a monitoring server. Install and set up the following program on the monitoring server:

- JP1/NM

To set up a treatment server, follow steps (1) to (4) below. To set up a monitoring server, follow steps (1) and (2) below.

#### (1) Installing JP1/NM

Install JP1/NM on the treatment or monitoring server. For details about installing JP1/NM, see the manual *Job Management Partner 1/Network Monitor Description, User's Guide and Operator's Guide*.

#### (2) Setting up JP1/NM

Set up JP1/NM. For details about setting up JP1/NM, see the manual *Job Management Partner 1/Network Monitor Description, User's Guide and Operator's Guide*.

The environment settings for JP1/NM are as follows:

- **Monitoring mode**  
Select **Monitor the network**.
- **Blocked Mode**  
Select **Do not block devices detected to be illegal**.

If you intend to use the JP1/NM quarantine support facility, specify the following setting:

- Quarantine support information  
Select **Quarantine support mode: ON**

**(3) Installing JP1/Software Distribution Client (relay system)**

Install JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager on the treatment server. For details about installing these products, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems.

**(4) Setting up JP1/Software Distribution Client (relay system)**

Set up JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager. For details about setting up these products, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems.

**13.1.4 Setting up a client**

If you intend to use the JP1/NM quarantine support facility, set up JP1/Software Distribution Client in the following manner.

**(1) Setting up JP1/Software Distribution Client**

Set up JP1/Software Distribution Client itself. For details, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems.

Set up to allow clients with restricted network access to communicate with JP1/Software Distribution Client (relay system) on the treatment server

As the connection destination (higher system) of the client, specify JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager.

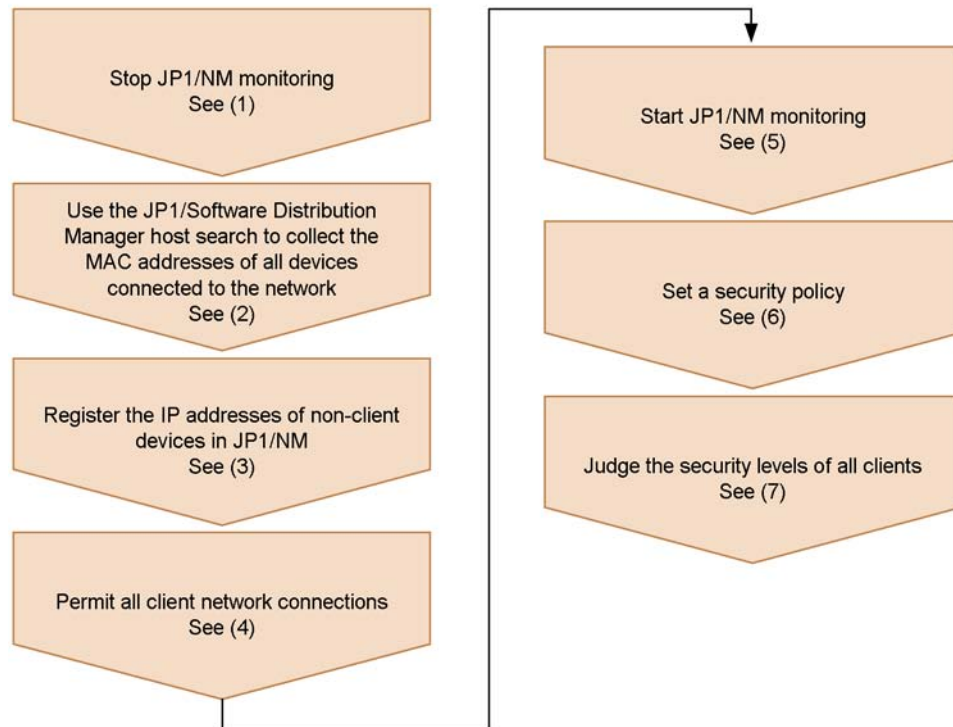
A client disconnected from the network cannot communicate with any device other than the treatment server. Therefore, JP1/Software Distribution Manager cannot directly implement security measures on the client, and the client cannot notify JP1/Software Distribution Manager of the latest inventory information.

By allowing the client to communicate with the treatment server, these tasks can be performed via JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager.

**13.1.5 Setting up the environment for operation**

Once the management server, network control server, treatment or monitoring server, and clients have been set up, to begin operating the quarantine system, set up the environment according to the procedures shown in the following figure.

Figure 13-5: Flow of setup before operation

**(1) Stopping JP1/NM monitoring**

From the Integrated Management window for JP1/NM - Manager, execute **Stop Network Monitor** on the treatment/monitoring server. Since this stops the treatment or monitoring server from monitoring the network, all client network connections will be permitted.

**(2) Using the JP1/Software Distribution Manager host search to collect the MAC addresses of all devices connected to the network**

Perform a host search from JP1/Software Distribution Manager to collect network configuration information for all devices connected to the network.

For details about the JP1/Software Distribution Manager host search, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems.

**(3) Registering the IP addresses of non-client devices in JP1/NM**

An administrator can register the IP addresses of non-client network connection devices in JP1/NM, using the information collected in (2) above. The IP addresses of the following devices are registered in JP1/NM:



- Network connection devices such as routers, printers, shared servers, and UNIX machines
- Management servers, network control servers, and treatment or monitoring servers

IP addresses of non-client devices are registered as **Fixed device** in the Integrated Management window of JP1/NM - Manager. IP addresses can also be registered by specifying a range, and MAC addresses can also be registered.

For details about how to register IP addresses and MAC addresses in JP1/NM - Manager, see the manual *Job Management Partner 1/Network Monitor - Manager Description, User's Guide and Operator's Guide*.

*Note:*

Be sure to register all IP addresses and MAC addresses. If there are routers or servers whose IP address or MAC address is not registered with JP1/NM, these devices will be shut off from the network and no longer accessible once monitoring is restarted.

#### **(4) Permitting all client network connections**

Check that JP1/Software Distribution Client is installed and set up on all clients. Then, select all clients in the PC List window of the Client Security Management window, and in **Network connection**, click the **Permit** button. This will automatically register all the client MAC addresses with JP1/NM, and permit network connections for these clients.

For details about permitting client network connections, see 9.3 *Controlling client network connections*.

*Note:*

Do not use JP1/NM directly to control client network connections. Always use the Client Security Management window of AIM.

#### **(5) Starting JP1/NM monitoring**

Perform the following environment setting for JP1/NM on the treatment or monitoring server:

- **Blocked Mode**

Select **Block all devices detected to be illegal**.

Once you have made this setting, execute **Start Network Monitor** for the treatment or monitoring server, from the JP1/NM - Manager on the network control server. This will start monitoring for all clients and network connection devices.

*Note:*

If any routers or servers were missed in step (3), communication with the entire subnetwork may be lost and the server may no longer be accessible when JP1/NM starts monitoring.

**(6) Setting a security policy**

Use the Security Policy Management window to set a judgment policy and action policy. For details about security policies, see *6. Managing Security Policies*.

Make sure that **Control network connection** is selected for the action policies.

**(7) Judging the security levels of all clients**

Perform security level judgment for all clients. In the PC List window of the Client Security Management window, select all clients and click the **Judge** button to judge their security levels. In the action policy settings in (6), if **Refuse connection** was selected for **Control network connection**, clients with the corresponding security level are automatically excluded from the network.

For details about how to judge client security levels, see *8.4 Judging a client security level*.

---

## 13.2 Setting up a quarantine system linked to an authentication server

---

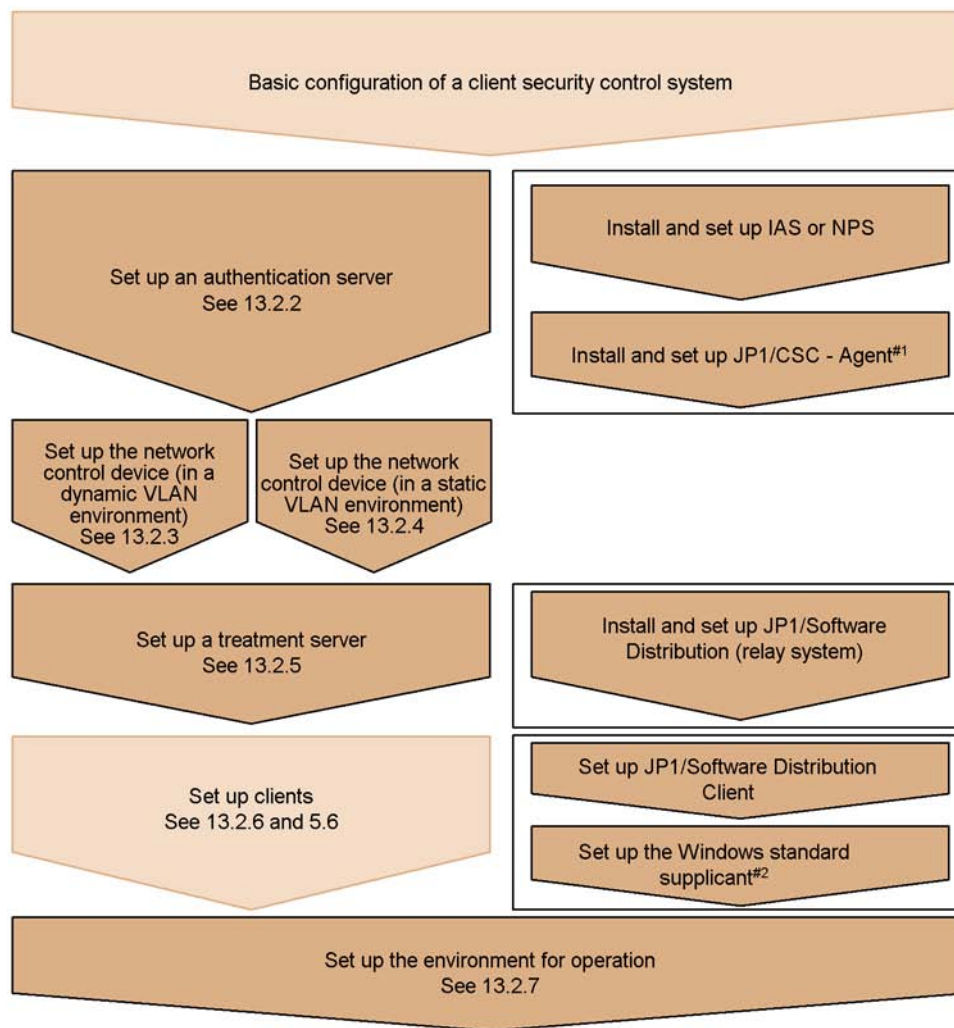
This section describes the procedure for setting up a quarantine system linked to an authentication server.

### 13.2.1 Flow of system setup

The following figure shows the procedures for setting up a quarantine system linked to an authentication server.

Before you set up a quarantine system, you must have set up a client security control system with all the required core products.

Figure 13-6: Setting up a quarantine system linked to an authentication server



Legend:

: Perform these steps to set up a client security control system.

: Perform these steps to set up a quarantine system.

IAS or NPS: Microsoft Internet Authentication Service or Network Policy Server

#1: Before installing and setting up JP1/CSC - Agent, configure the switch that supports IEEE 802.1X or MAC authentication.

#2: This product is not necessary when MAC authentication is used.

Install programs on the authentication server in the order shown in Figure 13-6.

## 13.2.2 Setting up an authentication server

This section describes how to set up an authentication server by installing and setting up the following programs:

- Microsoft Internet Authentication Service or Network Policy Server
- JP1/CSC - Agent

*Note:*

Before installing and setting up JP1/CSC - Agent, make sure that you have performed the operations described in *13.2.3 Setting up the network control device (dynamic VLAN environment)* or *13.2.4 Setting up the network control device (static VLAN environment)*.

### (1) Installing Microsoft Internet Authentication Service or Network Policy Server

Install Microsoft Internet Authentication Service or Network Policy Server on the authentication server. These products can be found on the installation media for the prerequisite version of Windows. For details about installing Microsoft Internet Authentication Service and Network Policy Server, refer to the documentation on the Microsoft Support site or Windows help.

### (2) Setting up Microsoft Internet Authentication Service or Network Policy Server

Set up Microsoft Internet Authentication Service or Network Policy Server. Perform the following settings before you set up Microsoft Internet Authentication Service or Network Policy Server to link with JP1/CSC:

- Connection request policy settings

Set the policy name and policy conditions.

- Remote access policy settings

Set the policy name, access method, and authentication method.

In a dynamic VLAN environment, for Tunnel-Pvt-Group-ID in the remote access policy, specify the VLAN-ID of the corporate network to which safe clients are connected. This VLAN-ID is used if a switch is used to create a VLAN.

- RADIUS client settings

Set the IP address, client vendor, shared key, and other items for the switch.

To set up Microsoft Internet Authentication Service and Network Policy Server to link with JP1/CSC:

Setting up to store passwords using reversible encryption

If IEEE 802.1X authentication is used, set an attribute that uses reversible encryption to store passwords. The procedure for setting this attribute differs

depending on whether Active Directory is installed on the authentication server.

- When Active Directory is installed

Open the **Domain Controller Security Policy** console, click **Security Settings**, **Account Policy**, and then **Password Policy**, and enable **Store passwords using reversible encryption**.

Any passwords that were registered before you enabled **Store passwords using reversible encryption** must be reset. To do this, open **Active Directory Users and Computers**, select **Users**, and then click the relevant user. You must then assign the password again.

- When Active Directory is not installed

Open the **Local Security Policy** console, click **Security Settings**, **Account Policy** and then **Password Policy**, and enable **Store passwords using reversible encryption**.

Setting the authentication protocol for remote access policies

If IEEE 802.1X authentication is used, select either **MD5-Challenge** or **Protected EAP [PEAP]** as the remote access policy authentication method. This setting is unnecessary if MAC authentication is used.

For details about setting up Microsoft Internet Authentication Service and Network Policy Server, refer to the documentation on the Microsoft Support site or Windows help.

### **(3) Installing JP1/CSC - Agent**

Install JP1/CSC - Agent on the authentication server.

For details about installing JP1/CSC - Agent, see *5.7.1 Installing JP1/CSC - Agent*.

*Note:*

If your OS is Windows Server 2008, the NETWORK SERVICE user must have Full Control access permission for the following folders:

- *JP1/CSC - Agent-installation-folder\log*
- *JP1/CSC - Agent-installation-folder\trace*
- *JP1/CSC - Agent-installation-folder\radius\log*

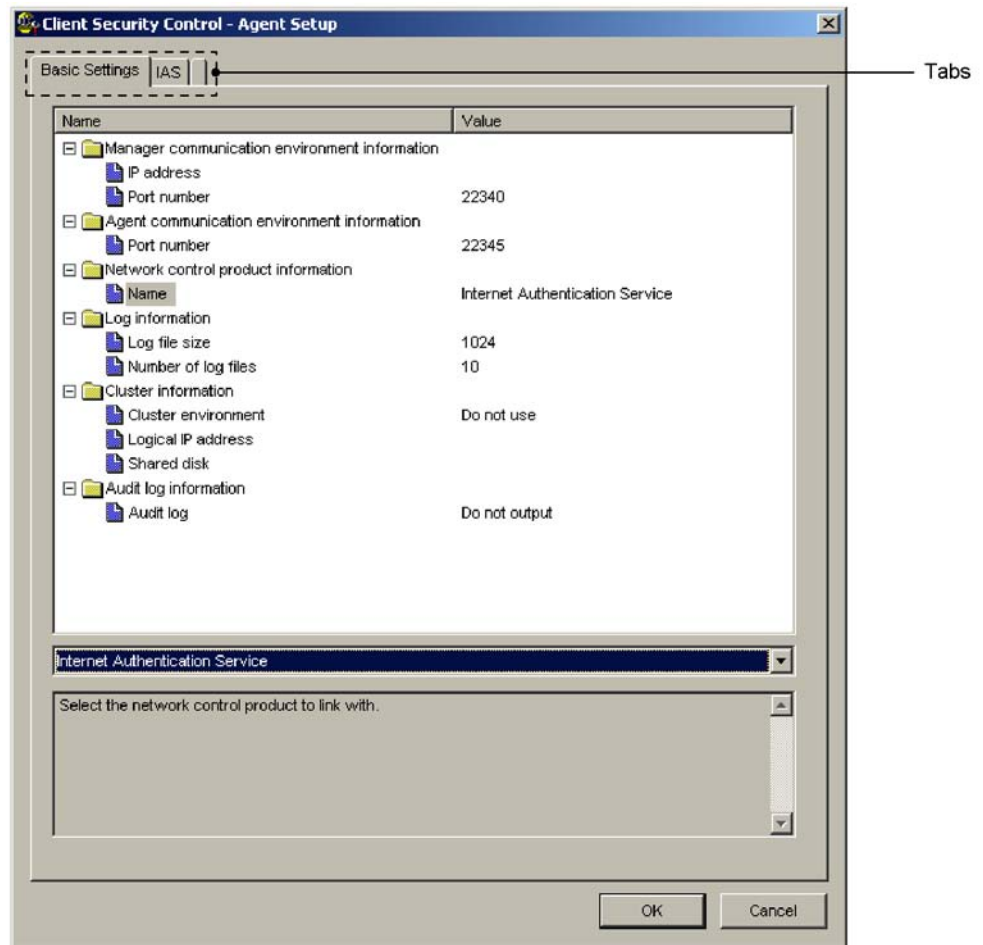
### **(4) Setting up JP1/CSC - Agent**

After installing JP1/CSC - Agent, be sure to set up JP1/CSC - Agent before starting it.

You can set the information required for JP1/CSC - Agent setup by using the Client Security Control - Agent Setup dialog box.

The Client Security Control - Agent Setup dialog box has two tabbed pages, which can be selected by clicking the corresponding tab. The following figure shows the Client Security Control - Agent Setup dialog box.

Figure 13-7: Client Security Control - Agent Setup dialog box



The following table lists the items that can be set in the Client Security Control - Agent Setup dialog box.

Table 13-5: Items that can be set in the Client Security Control - Agent Setup dialog box

Tab selected	Description
Basic Settings tab	This tab is used to display settings information for JP1/CSC - Agent environments already set up, and to change environment settings.

Tab selected	Description
<b>IAS</b> tab	<p>This tab is used only if linkage to an authentication server is used. It is used to display settings information for JP1/CSC - Agent environments, and to change environment settings.</p> <p>This page appears if <i>Internet Authentication Service</i> is specified for <b>Network control product information</b> on the <b>Basic Settings</b> page.</p>

#

The settings for linkage to an authentication server are specified on the **Basic Settings** and **IAS** pages in the Client Security Control - Agent Setup dialog box.

To display the Client Security Control - Agent Setup dialog box and edit the settings:

1. Click the **Start** button, and choose **Programs, Client Security Control**, and then **Agent Setup**.

The Client Security Control - Agent Setup dialog box appears.

2. Select the pages and set values for the items.

When you select an item, a box appears below the item list. You can either enter a value or string directly in this box or select a value from the pull-down menu.

For details, see (a) *Operations that can be performed on the Basic Settings page* and (b) *Operations that can be performed on the IAS page*.

3. Click the **OK** button.

The contents you specified are set for the JP1/CSC - Agent environment. The Client Security Control - Agent Setup dialog box closes.

To close this dialog box without performing any environment settings, click the **Cancel** button.

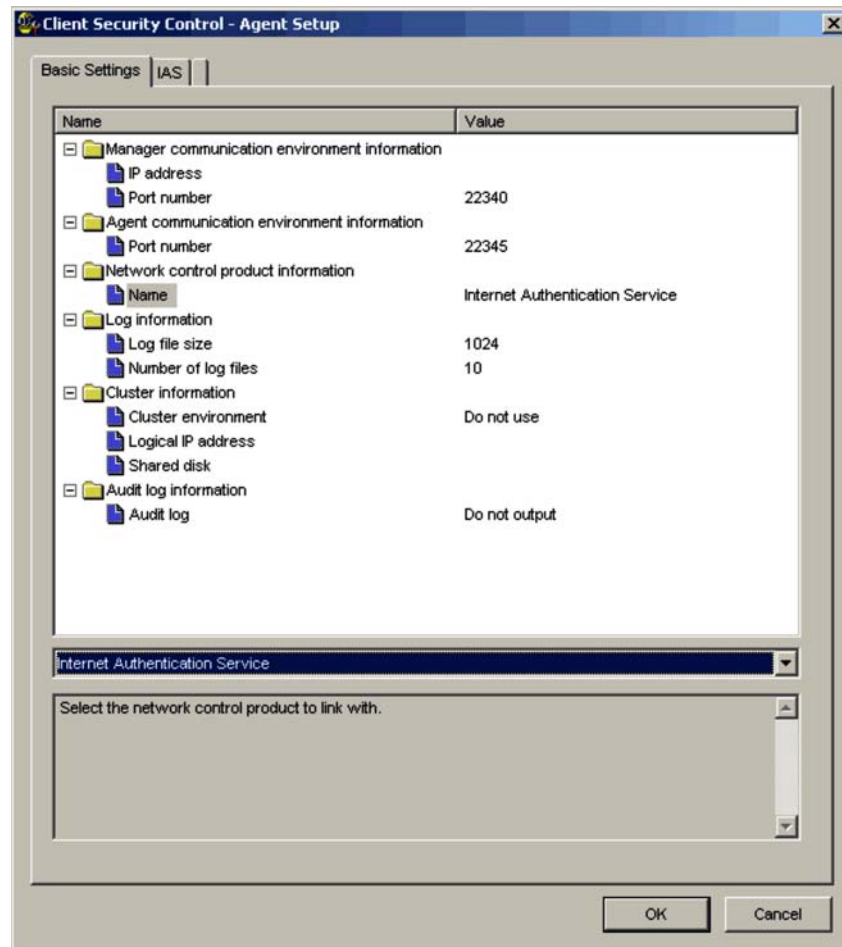
#### (a) Operations that can be performed on the Basic Settings page

Use the **Basic Settings** page to display and change the environment settings for JP1/CSC - Agent.

The following figure shows the **Basic Settings** page.



Figure 13-8: Basic Settings page



The following table lists the items that can be set in the **Basic Settings** page.

Table 13-6: Items that can be displayed and set on the Basic Settings page

Item		Description	Specifiable values	Default for initial environment setup
Manager communication environment information	IP address	The IP address for JP1/CSC - Manager.	IPv4 format (xxx.xxx.xxx.xxx)	--
	Port number			

Item		Description	Specifiable values	Default for initial environment setup
	Port number	The port number JP1/CSC - Manager uses to communicate with JP1/CSC - Agent. Enter the same port number as specified in <b>Port number for receiving requests</b> under <b>Manager communication environment information</b> , in the <b>Basic Settings</b> page of JP1/CSC - Manager.	1024 to 65535	22340
<b>Agent communication environment information</b>	Port number	The port number of JP1/CSC - Agent. Enter the same port number as that registered for <b>Port number</b> in the Add agent information window of JP1/CSC - Manager.	1024 to 65535	22345
<b>Network control product information</b>	Name	The name of the linked network control product.	Internet Authentication Service <sup>#</sup>	Network Monitor
<b>Log information</b>	Log file size	Specify the maximum size (in kilobytes) of the JP1/CSC - Agent log files.	1 to 2097151	1024
	Number of log files	Specify the maximum number of JP1/CSC - Agent log files.	1 to 999	10
<b>Cluster information</b>	Cluster environment	Specify whether to run JP1/CSC - Agent in a cluster environment.	<b>Use / Do not use</b>	<b>Do not use</b>
	Logical IP address	Specify a logical IP address to use in the cluster environment.	IPv4 format (xxx.xxx.xxx.xxx)	--
	Shared disk	Specify the path for the shared disk used in the cluster environment.	Full path	--
<b>Audit log information</b>	<b>Audit log</b>	Specify whether to output audit logs.	<b>Output / Do not output</b>	<b>Do not output</b>

Legend:

--: No default provided

#

For Network Policy Server also, specify Internet Authentication Service.

*Note:*

You must stop the Microsoft IAS service before selecting **Network control product information**. If you select this item while the Microsoft IAS service is running, an error message will appear when you click the **OK** button. This also applies to Network Policy Server.

*Reference note:*

The log information contains information about startup and termination of JP1/CSC - Agent, as well as connection information for the network control product.

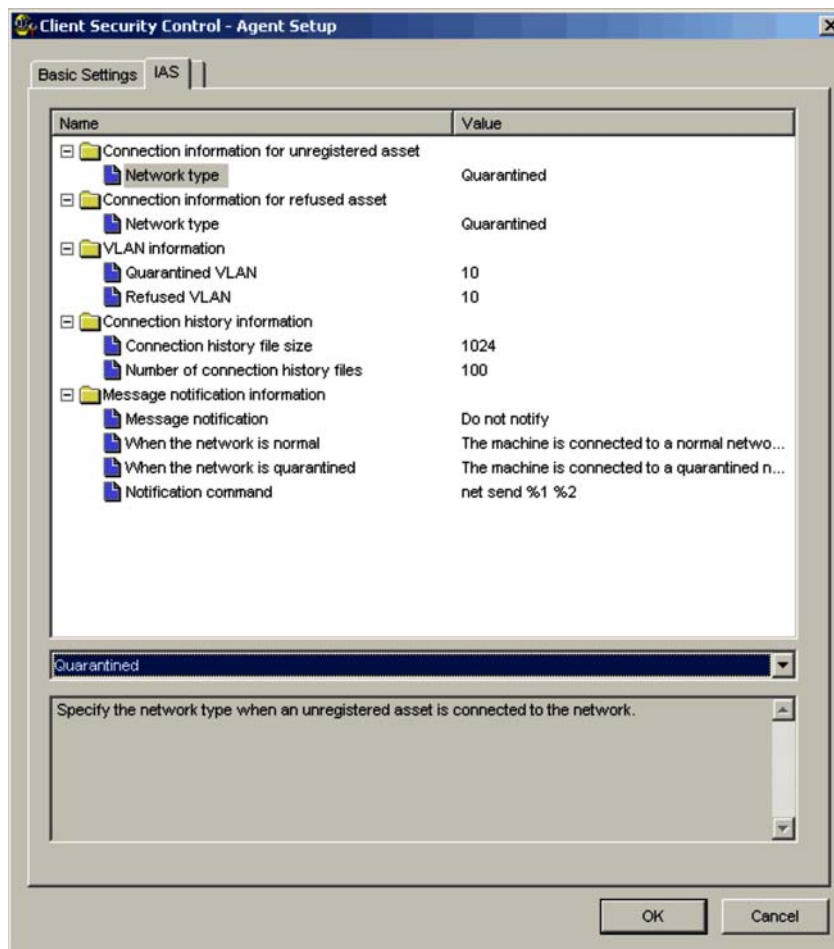
**(b) Operations that can be performed on the IAS page**

On the **IAS** page, you can view and change the JP1/CSC - Agent environment settings for linkage to an authentication server (Microsoft Internet Authentication Service or Network Policy Server).

Be sure to stop the Microsoft IAS before changing any settings on the **IAS** page. If you fail to do so, an error will occur, and the changes will not be applied. This also applies to Network Policy Server.

The following figure shows the **IAS** page.

Figure 13-9: IAS page



The following table lists the items that can be checked and set in the **IAS** page.

Table 13-7: Items that can be displayed and set on the IAS page

Item		Description	Specifiable values	Default for initial environment setup
Connection information for unregistered asset	Network type	Specify the connection destination for clients not registered in the connection control list. <ul style="list-style-type: none"> <li>To have such clients connect to the quarantined network, specify <b>Quarantined</b>.</li> <li>To deny such clients access to the network, specify <b>Refused</b>.</li> <li>To have such clients connect to the corporate network, specify <b>Normal</b>.</li> <li>To have such clients connect to the unauthenticated network, specify <b>Unauthenticated</b>.</li> </ul>	<b>Quarantined / Refused / Normal / Unauthenticated</b>	<b>Quarantined</b>
	Network type	Specify the connection destination for clients listed as rejected in the connection control list. <ul style="list-style-type: none"> <li>To have such clients connect to the quarantined network, specify <b>Quarantined</b>.</li> <li>To deny such clients access to the network, specify <b>Refused</b>.</li> <li>To have such clients connect to the unauthenticated network, specify <b>Unauthenticated</b>.</li> </ul>		
VLAN information <sup>#1</sup>	Quarantined VLAN	Specify the VLAN-ID of the quarantined network.	1 to 4095 <sup>#2</sup>	10
	Refused VLAN	Specify a VLAN-ID that is not assigned to any network on the switch.	1 to 4095 <sup>#2</sup>	10

Item		Description	Specifiable values	Default for initial environment setup
<b>Connection history information</b>	Connection history file size	The size of the file in which the connection history of clients is recorded. Specify the maximum size (in kilobytes).	1 to 2097151	1024
	Number of connection history files	Specify the maximum number of connection history files to be created.	1 to 999	100
<b>Message notification information</b>	Message notification <sup>#3,#4</sup>	Specify whether a message is to be sent notifying clients of the network to which they are connected.	<b>Notify / Do not notify</b>	<b>Do not notify</b>
	When the network is normal	Enter the body of the message to be sent to clients that are connected to the corporate network, as a string of 1,024 or fewer bytes.	Character string	The machine is connected to a normal network.
	When the network is quarantined	Enter the body of the message to be sent to clients that are connected to the quarantined network, as a string of 1,024 or fewer bytes.	Character string	The machine is connected to a quarantined network because a vulnerability was detected. Implement necessary measures, and restart the machine.
	Notification command	The command used to send notification messages to clients. Enter the command line as a string of 1,024 or fewer bytes.	Character string	net send %1 %2 <sup>#5</sup>

#1

You cannot set the VLAN-ID of the corporate network (normal VLAN) from JP1/CSC - Agent. The VLAN-ID specified for the Tunnel-Pvt-Group-ID attribute in the remote access policy of Microsoft Internet Authentication Service or

Network Policy Server is used for the corporate network.

#2

The valid range for VLAN-IDs depends on the switch model that you use. Be sure to specify a VLAN-ID for the refusal LAN that is within the valid range.

For details, see the manual for the switch.

#3

If you set message notification to **Notify**, a message is sent each time the client is authenticated (or re-authenticated).

#4

You cannot use message notification when the authentication server is running Windows Server 2008.

#5

%1 and %2 are variables that take the following values:

%1: The IP address of the client to which the message is sent.

%2: One of the character strings specified in message notification information, specific to either the normal network or quarantined network.

*Reference note:*

By setting **Connection information for unregistered asset** to **Refused**, you can prevent clients not in the connection control list and unauthorized PCs from connecting to the network.

However, when you add a new client to the network, information about the client is not automatically registered in the connection control list. In this case, inventory information must be obtained from an offline machine.

For details, see *14.2.6 Adding a new client to the network*.

### 13.2.3 Setting up the network control device (dynamic VLAN environment)

Set up the network control device (switch that supports IEEE 802.1X authentication). For details about setting up a switch, see the applicable manual for the switch.

- Setting for enabling IEEE 802.1X authentication  
Enable IEEE 802.1X authentication.
- Authentication interval settings  
Set the re-authentication interval, the EAP request frame transmission interval,

and the number of re-authentication attempts for IEEE 802.1X authentication.

By setting a re-authentication interval and an EAP request frame transmission interval, client authentication is performed periodically in response to authentication requests sent from the switch. This allows client network connections to be controlled in a timely manner when the connection control list is updated.

- RADIUS server settings

Set the IP address, port number, and shared key of the authentication server. Use the shared key you specified when setting up the RADIUS client in Microsoft IAS or Network Policy Server.

- VLAN settings

Set up the various VLANs, including the corporate network and the quarantined network. When you set up the corporate network, use the VLAN-ID you specified for the Tunnel-Pvt-Group-ID attribute in the remote access policy of Microsoft Internet Authentication Service or Network Policy Server.

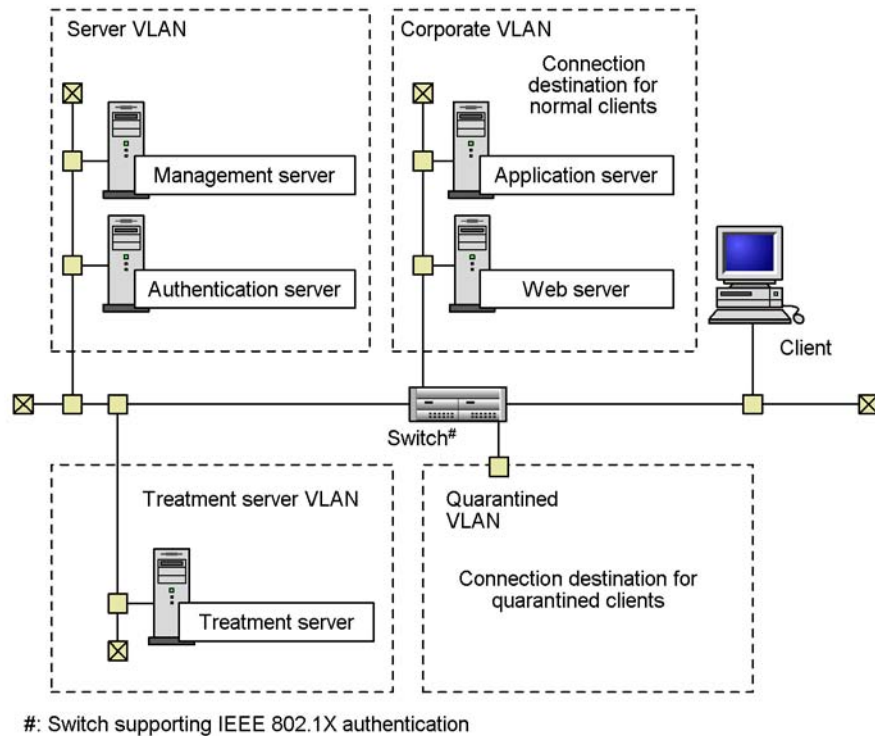
The following explains the VLANs to set up on the switch, and how to set up communication between the VLANs.

**(1) *Inter-VLAN communication settings specified on the switch***

The following figure shows the recommended VLAN configuration.



Figure 13-10: Recommended VLAN configuration



In this configuration four VLANs have been set up:

- **Corporate VLAN**  
A corporate network to which safe clients are connected. This network provides access to various servers including the job server and the Web server.
- **Quarantined VLAN**  
A quarantined network to which clients with a high security risk level are connected.
- **Treatment server VLAN**  
A network containing the treatment server.
- **Server VLAN**  
A network containing the management server and the authentication server.

The following table shows how communication takes place between VLANs.

*Table 13-8: Inter-VLAN communication settings*

No.	VLAN name	Corporate VLAN	Quarantined VLAN	Server VLAN	Treatment VLAN
1	Corporate VLAN	Yes	No	Yes	Yes
2	Quarantined VLAN	No	Yes	No	Yes
3	Server VLAN	Yes	No	Yes	Yes
4	Treatment server VLAN	Yes	Yes	Yes	Yes

Legend:

Yes: Communication can take place.

No: Communication cannot take place.

*Note:*

Be sure to set up communication between the VLANs as shown in Table 13-8.

When security measures are implemented on a client, or client inventory information is reported to a higher system, communication takes place in each case via the treatment server VLAN.

- When implementing security measures on clients  
Server VLAN → Treatment server VLAN → Quarantined VLAN
- When reporting inventory information for clients  
Quarantined VLAN → Treatment server VLAN → Server VLAN

#### 13.2.4 Setting up the network control device (static VLAN environment)

Set up the network control device (switch that supports IEEE 802.1X or MAC authentication). For details about how to setting up a switch, see the applicable manual for the switch.

IEEE 802.1X authentication

- Setting for enabling IEEE 802.1X authentication  
Enable IEEE 802.1X authentication.
- Authentication interval settings  
Set the re-authentication interval, the EAP request frame transmission interval, and the number of re-authentication attempts for IEEE 802.1X

authentication.

By setting a re-authentication interval and an EAP request frame transmission interval, client authentication is performed periodically in response to authentication requests sent from the switch. This allows client network connections to be controlled in a timely manner when the connection control list is updated.

- RADIUS server settings

Set the IP address, port number, and shared key of the authentication server. Use the shared key you specified when setting up the RADIUS client in Microsoft Internet Authentication Service or Network Policy Server.

- Access list settings

Set the access list that contains the connection control settings for the clients connected to the unauthenticated network.

#### MAC authentication

- Setting for enabling MAC authentication

Enable MAC authentication.

- Maximum connection time setting

By setting the maximum connection time for MAC authentication, client authentication is performed periodically in response to authentication requests sent from the switch. This allows client network connections to be controlled in a timely manner when the connection control list is updated.

- RADIUS server settings

Set the IP address, port number, and shared key of the authentication server. Use the shared key you specified when setting up the RADIUS client in Microsoft Internet Authentication Service or Network Policy Server.

- Access list settings

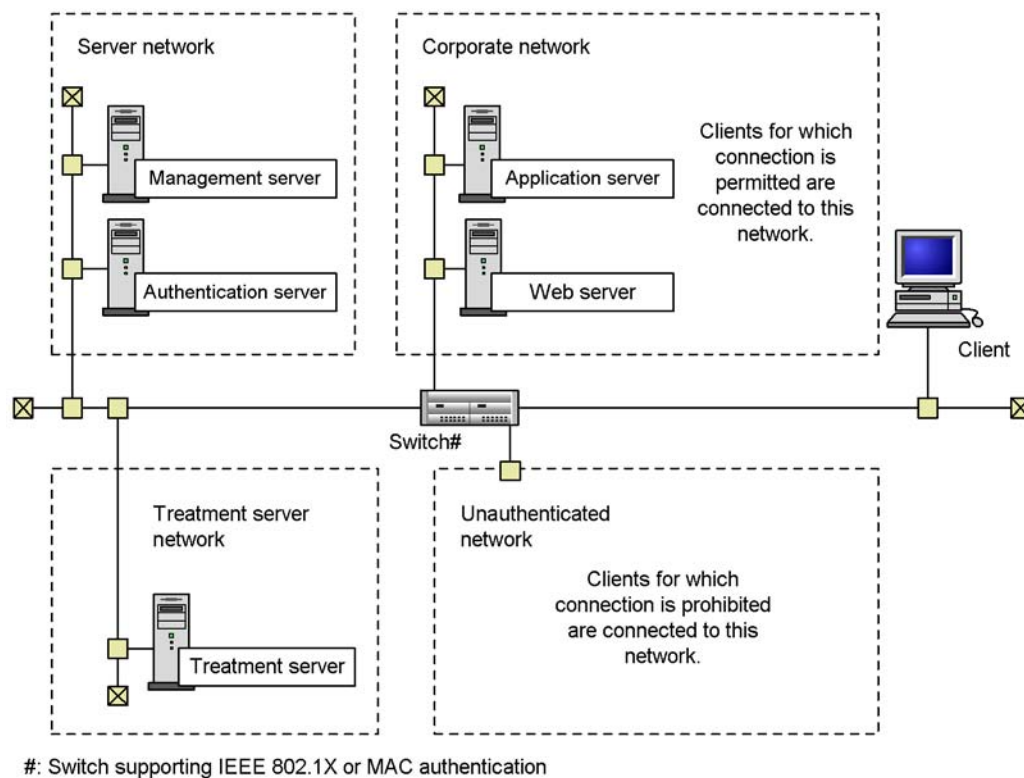
Set the access list that contains the connection control settings for the clients connected to the unauthenticated network.

The following explains the network configuration and access list settings.

#### **(1) Network configuration and access list settings**

The following figure shows the recommended network configuration.

Figure 13-11: Recommended network configuration



The following describes each network in the figure.

- Corporate network  
The intra-company network to which safe clients are connected. This network can contain the application server, Web server, and other network components.
- Unauthenticated network  
The network to which unsafe clients are connected as a security measure.
- Treatment server network  
The network to which the treatment server belongs.
- Server network  
The network to which the management server and authentication server belong.

The access list settings are specified as follows:

- Connection between the unauthenticated network and treatment server network is permitted.
- Connection between the unauthenticated network and server network is prohibited.
- Connection between the unauthenticated network and corporate network is prohibited.

### 13.2.5 Setting up a treatment server

Set up a treatment server by installing and setting up JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager. Also install and set up Microsoft Software Update Services and an anti-virus product on the treatment server, as necessary.

#### (1) *Installing JP1/Software Distribution Client (relay system)*

Install JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager on the treatment server. For details about installing these products, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems.

#### (2) *Setting up JP1/Software Distribution Client (relay system)*

Set up JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager. For details about setting up these products, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems.

### 13.2.6 Setting up a client

Set up each client by setting up the following programs:

IEEE 802.1X authentication

- JP1/Software Distribution Client
- Windows standard supplicant

Because this is pre-installed as standard in Windows, you need to perform setup only.

MAC authentication

- JP1/Software Distribution Client

#### (1) *Setting up JP1/Software Distribution Client*

The following explains the setup required for JP1/Software Distribution Client to link to an authentication server. For details about setting up JP1/Software Distribution Client, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems.

### Communication with JP1/Software Distribution Client (relay system) on the treatment server

As the connection destination (higher system) of a client, specify JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager on the treatment server.

If a client is connected to the quarantine or unauthenticated network, the client can only communicate with the treatment server. This configuration allows security measures to be implemented on the client and the latest inventory information to be reported to the higher system via JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager on the treatment server.

### Setup for polling the higher system after authentication (when the client OS is Windows)

JP1/Software Distribution Client includes a function that polls a higher system such as JP1/Software Distribution Manager at machine startup to check for the instructions from the higher system. However, if linkage to an authentication server is used, JP1/Software Distribution Client cannot communicate with the higher system until authentication is completed successfully. Accordingly, the polling attempt might fail.

To prevent a polling failure, first measure the time required for JP1/Software Distribution Client to log on to Windows after machine (OS) startup. Then, during JP1/Software Distribution Client setup, set JP1/Software Distribution Client to wait for that amount of time before starting polling.

Of the following settings, only the first is mandatory, but it is recommended that you set all three:

- In the **Default Running Status/Polling** panel, specify a time interval in **Maximum polling delay before or after starting the client**, and select **Start polling after waiting**.
- In the **Default Running Status/Polling** panel, select **Execute polling once every**, and specify a polling interval.
- In the **Retry Communication** panel, set **Retry count for establishing socket connection** and **Retry interval for establishing socket connection**.

### *Note:*

If you have set **The first polling is executed: Before the client starts** during JP1/Software Distribution Client setup, installation at startup is delayed by the setup for polling the higher system after authentication. As a result, the startup of programs registered in the **Software Distribution Client Startup** folder is also delayed.

**(2) Setting up the Windows standard supplicant**

If IEEE 802.1X authentication is used, set up the Windows standard supplicant.

Set up the Windows standard supplicant.

The following table lists the settings for the Windows standard supplicant. For details about setting up the supplicant, refer to the documentation on the Microsoft Support site or to Windows help.

*Table 13-9: Settings for Windows standard supplicant by OS*

OS	Setting	Description
Windows 2000	Starting the service	Start the following Windows service: <b>Wireless Configuration</b> The startup type is set to <b>Manual</b> by default.
	Enabling IEEE 802.1X authentication; choosing the EAP authentication method	Specify the following settings on the <b>Authentication</b> page of the <b>Local Area Connection Properties</b> dialog box: <ul style="list-style-type: none"> <li>• Select the <b>Enable IEEE 802.1X authentication for this network</b> check box.</li> <li>• From the drop-down menu, select <b>MD5-Challenge</b>.</li> </ul>
	Displaying an icon in the taskbar	On the <b>General</b> page of the <b>Local Area Connection Properties</b> dialog box, select the <b>Show icon in taskbar when connected</b> check box.
Windows XP	Starting the service	Start the following Windows service: <b>Wireless Zero Configuration</b> The startup type is set to <b>Automatic</b> by default. Check that the service has started.
	Enabling IEEE 802.1X authentication; choosing the EAP authentication method	Specify the following settings on the <b>Authentication</b> page of the <b>Local Area Connection Properties</b> dialog box: <ul style="list-style-type: none"> <li>• Select the <b>Enable IEEE 802.1X authentication for this network</b> check box.</li> <li>• From the drop-down menu, select <b>MD5-Challenge</b>.</li> </ul>
	Displaying an icon in the notification area	On the <b>General</b> page of the <b>Local Area Connection Properties</b> dialog box, select the <b>Show icon in notification area when connected</b> check box.

OS	Setting	Description
Windows Server 2003	Starting the service	Start the following Windows service: <b>Wireless Configuration</b> The startup type is set to <b>Automatic</b> by default. Check that the service has started.
	Enabling IEEE 802.1X authentication; choosing the EAP authentication method	Specify the following settings on the <b>Authentication</b> page of the <b>Local Area Connection Properties</b> dialog box: <ul style="list-style-type: none"> <li>Select the <b>Enable IEEE 802.1X authentication for this network</b> check box.</li> <li>From the drop-down menu, select <b>MD5-Challenge</b>.</li> </ul>
	Displaying an icon in the notification area	On the <b>General</b> page of the <b>Local Area Connection Properties</b> dialog box, select the <b>Show icon in notification area when connected</b> check box.
Windows Vista	Starting the service	Start the following Windows service: <b>Wired AutoConfig</b> The startup type is set to <b>Manual</b> by default.
	Enabling IEEE 802.1X authentication; choosing the EAP authentication method	Specify the following settings on the <b>Authentication</b> page of the <b>Local Area Connection Properties</b> dialog box: <ul style="list-style-type: none"> <li>Select the <b>Enable IEEE 802.1X authentication for this network</b> check box.</li> <li>From the drop-down menu, select <b>Protected EAP (PEAP)</b>.</li> </ul>
Windows Server 2008	Starting the service	Start the following Windows service: <b>Wired AutoConfig</b> The startup type is set to <b>Manual</b> by default.
	Enabling IEEE 802.1X authentication; choosing the EAP authentication method	Specify the following settings on the <b>Authentication</b> page of the <b>Local Area Connection Properties</b> dialog box: <ul style="list-style-type: none"> <li>Select the <b>Enable IEEE 802.1X authentication for this network</b> check box.</li> <li>From the drop-down menu, select <b>Protected EAP (PEAP)</b>.</li> </ul>
Windows 7	Starting the service	Start the following Windows service: <b>Wired AutoConfig</b> The startup type is set to <b>Manual</b> by default.
	Enabling IEEE 802.1X authentication; choosing the EAP authentication method	Specify the following settings on the <b>Authentication</b> page of the <b>Local Area Connection Properties</b> dialog box: <ul style="list-style-type: none"> <li>Select the <b>Enable IEEE 802.1X authentication for this network</b> check box.</li> <li>From the drop-down menu, select <b>Protected EAP (PEAP)</b>.</li> </ul>

#

In addition to these settings, it is recommended that you configure the Windows standard supplicant to initiate authentication after a restart by sending an



EAPOL-START packet to the switch. To set up the supplicant to send EAPOL-START packets, you will need to make changes to the registry. For details about the settings for sending EAPOL-START packets, see applicable information published by Microsoft.

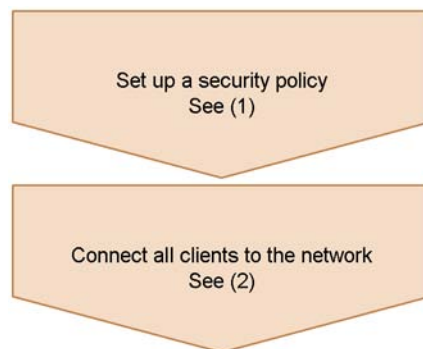
*Note:*

If the supplicant is not set up to send EAPOL-START packets, client authentication is performed at the authentication interval set on the switch (authentication does not start when the client is restarted).

### 13.2.7 Setting up the environment before operation can be started

After completing setup of the management server, authentication server, treatment server, network control devices, and clients, set up the environment before you start operation. The following figure shows the procedures for environment setup.

*Figure 13-12: Flow of setup before operation*



#### (1) Setting security policies

Use the Security Policy Management window to set a judgment policy and action policy. For details about setting security policies, see *6. Managing Security Policies*.

In the action policy, specify whether to permit or deny network connections for each security level. This ensures that the connection control list for JP1/CSC - Agent is updated, and client network connections can be directed to the appropriate network.

For details about how actions affect the connection control list, see *14.2.4(1) Types of information registered in the connection control list*.

#### (2) Connecting all clients to the network

Before a client can connect to the corporate network, information about the client must be registered in the client control list for JP1/CSC - Agent.

When a client is first introduced into the network, it is treated as an unregistered asset

because no information about it is found in the connection control list. In this case, the client is connected to the network specified by the **Connection information for unregistered asset** setting in JP1/CSC - Agent setup.

The following describes the **Quarantined**, **Refused**, **Normal**, and **Unauthenticated** settings that can be specified for **Connection information for unregistered asset**.

**(a) When Quarantined is set**

The client is connected to the quarantined network, where security measures are implemented on the client. The client is then connected to the corporate network.

To connect an unregistered client to the corporate network:

1. Initiate client authentication.

An authentication request is sent to the authentication server via the switch when the client is restarted, when the Windows standard supplicant service is restarted, or when client network connection that has been disabled is enabled. Note that if sending of EAPOL-START packets is not enabled, the switch requests client authentication at the authentication interval set on the switch.

2. Implement security measures on the client by communicating with the treatment server.

Security measures can be implemented on clients in the quarantined network, by communicating with the treatment server.

By using the software distribution facility of JP1/Software Distribution, the administrator can distribute software from JP1/Software Distribution Manager on the management server, using JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager on the treatment server as a relay system. Alternatively, the client can be provided with packages for the user to install.

For details about the software distribution facility of JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

When client inventory information is updated, the latest inventory information is reported to JP1/Software Distribution Manager running on the management server, via JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager running on the treatment server.

When the client is judged safe based on the judgment policy by JP1/CSC - Manager on the management server, an action (to permit a network connection) is implemented according to the action policy. The client information is then recorded as `Permit` in the JP1/CSC - Agent connection control list.

3. Re-authenticate the client.

An authentication request is sent to the authentication server via the switch when

the client is restarted, when the Windows standard supplicant service is restarted, or when client network connection that has been disabled is enabled. Note that if sending of EAPOL-START packets is not enabled, the switch requests client authentication at the authentication interval that is set on the switch.

After security measures have been completed, the client is registered as `Permit` in the connection control list of JP1/CSC - Agent on the authentication server, and can then connect to the corporate network.

#### (b) When Refused is set

The client cannot connect to the network. Use the offline machine management functionality provided by JP1/Software Distribution to implement security measures on the client. The client can then connect to the corporate network.

To connect a rejected client to the corporate network:

1. Initiate client authentication.

An authentication request is sent to the authentication server via the switch when the client is restarted, when the Windows standard supplicant service is restarted, or when client network connection that has been disabled is enabled. Note that if sending of EAPOL-START packets is not enabled, the switch requests client authentication at the authentication interval that is set on the switch.

Because **Connection information for unregistered asset** is set to **Refused**, the client cannot connect to the network.

2. Use the offline machine management functionality of JP1/Software Distribution to implement security measures on the client.

You can use the offline machine management functionality of JP1/Software Distribution to implement security measures on a client in an offline environment. The offline machine management functionality allows you to install software offline, and obtain inventory information from offline machines.

For details about the offline machine management functionality of JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

The inventory information obtained from the offline machine is sent to JP1/Software Distribution Manager on the management server, and the client is judged by JP1/CSC - Manager.

If the client is judged safe based on the security policy, an action (to permit a network connection) is implemented according to the action policy. The client information is then recorded as `Permitted` in the JP1/CSC - Agent connection control list.

3. Re-authenticate the client.

An authentication request is sent to the authentication server via the switch when the client is restarted, when the Windows standard supplicant service is restarted, or when client network connection that has been disabled is enabled. Note that if sending of EAPOL-START packets is not enabled, the switch requests client authentication at the authentication interval that is set on the switch.

After security measures have been completed, the client is registered as *Permitted* in the connection control list of JP1/CSC - Agent on the authentication server, and can then connect to the corporate network.

**(c) When Normal is set**

The client can already connect to the corporate network, and no special measures are necessary.

However, ensure that security measures have been implemented on the client before it connects to the network.

**(d) When Unauthenticated is set**

The client is first connected to the unauthenticated network. After security measures have been implemented in the unauthenticated network, the client can be connected to the corporate network.

To connect an unauthenticated client to the corporate network:

1. Initiate client authentication.

When the client is restarted or client network connection that has been disabled is enabled, an authentication request is sent to the authentication server via the switch. Note, however, that if the sending of EAPOL-START packets for IEEE 802.1X authentication is not set, the switch requests client authentication at the authentication interval that is set on the switch. If MAC authentication is used, the switch requests client authentication based on the maximum connection time set on the switch.

Because **Unauthenticated** is set for **Connection information for unregistered asset**, the client is connected to the unauthenticated network.

2. Implement security measures on the client by communicating with the treatment server.

Security measures for a client connected to the unauthenticated network are implemented through communication with the treatment server from the unauthenticated network.

When the software distribution function of JP1/Software Distribution is used, JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager on the treatment server can be used as a relay system. The relay system allows the administrator to distribute software from the management server (JP1/Software Distribution Manager) or allows the client user to install a

package.

For details about the software distribution function of JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

When the client inventory has been updated, the latest inventory information is reported to JP1/Software Distribution Manager on the management server via JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager.

JP1/CSC - Manager on the management server judges whether the client is safe based on the judgment policy. If the client is judged safe, an action (permit network connection) is performed according to the action policy settings. At this time, `Permitted` is registered as client information in the connection control list of JP1/CSC - Agent.

### 3. Re-authenticate the client.

When the client is restarted or when client network connection that has been disabled is enabled, an authentication request is sent to the authentication server via the switch. Note, however, that if sending of EAPOL-START packets for IEEE 802.1X authentication is not set, the switch requests client authentication at the authentication interval that is set on the switch. If MAC authentication is used, the switch requests client authentication based on the maximum connection time set on the switch.

Clients for which security measures have been implemented are registered as `Permitted` in the connection control list of JP1/CSC - Agent on the authentication server, and are able to connect to the corporate network.

### 13.3 Setting up a quarantine system linked to JP1/Software Distribution (AMT Linkage facility)

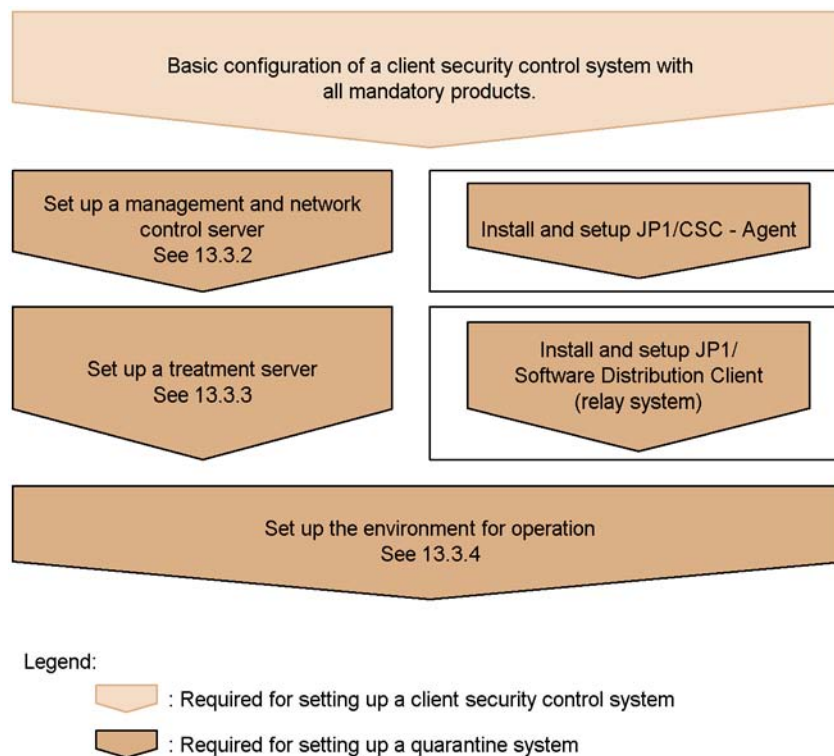
This section describes the procedure for setting up a quarantine system linked to JP1/Software Distribution (AMT Linkage facility).

#### 13.3.1 Flow of system setup

The following figure shows the procedure for setting up a quarantine system linked to JP1/Software Distribution (AMT Linkage facility).

Before you set up a quarantine system, you must have set up a client security control system with all the required core products.

*Figure 13-13: Setting up a quarantine system linked to JP1/Software Distribution (AMT Linkage facility)*



#### 13.3.2 Setting up a management and network control server

Set up a management and network control server by installing and setting up the

following program on the management server:

- JP1/CSC - Agent

### (1) **Confirming the system setup with the core products**

Confirm that the following programs have been installed and set up on the management server (called a *management and network control server* hereafter):

- JP1/Software Distribution Manager<sup>#</sup>
- .NET Framework 1.1 or 2.0
- Asset Information Manager (optional product)
- JP1/CSC - Manager

#

AMT Linkage facility Component of JP1/Software Distribution must be installed.

For details about installing and setting up each program, see 5. *Installation and Setup*.

### (2) **Installing JP1/CSC - Agent**

Install JP1/CSC - Agent on the management and network control server.

For details about installing JP1/CSC - Agent, see 5.7.1 *Installing JP1/CSC - Agent*.

### (3) **Setting up JP1/CSC - Agent**

After installing JP1/CSC - Agent, make sure that you set up JP1/CSC - Agent before you start it.

You can specify the information required for JP1/CSC - Agent setup by using the Client Security Control - Agent Setup dialog box.

To display the Client Security Control - Agent Setup dialog box and specify the settings:

1. Click the **Start** button, and choose **Programs, Client Security Control**, and then **Agent Setup**.

The Client Security Control - Agent Setup dialog box appears.

2. Set values for the items.

When you select an item, a box appears below the item list. In this box, you can enter a value or string, or select a value from the pull-down menu.

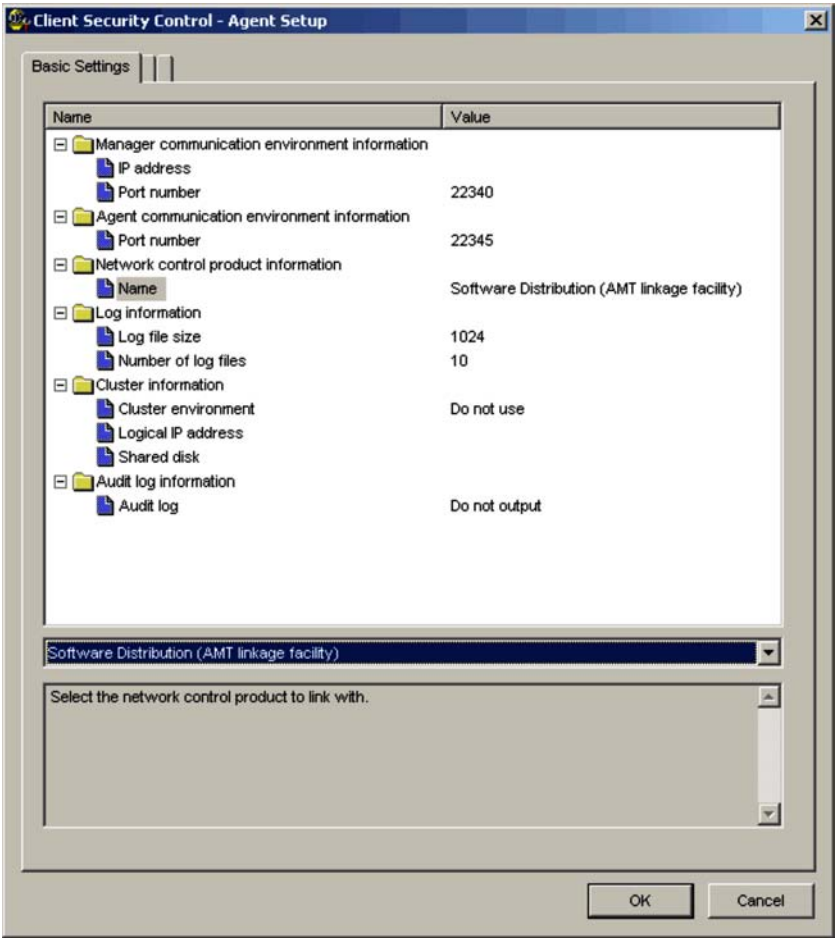
3. Click the **OK** button.

The information you have specified is set for the JP1/CSC - Agent environment. The Client Security Control - Agent Setup dialog box closes.

To close this dialog box without setting the environment, click the **Cancel** button.

The following figure shows the Client Security Control - Agent Setup dialog box.

Figure 13-14: Client Security Control - Agent Setup dialog box



The following table lists the items that can be set in the Client Security Control - Agent Setup dialog box.



*Table 13-10:* Items that can be set in the Client Security Control - Agent Setup dialog box

Items		Description	Specifiable values	Default for initial environment setup
<b>Manager communication environment information</b>	IP address	The IP address for JP1/CSC - Manager	IPv4 format (xxx.xxx.xxx.xxx)	--
	Port number	The port number that JP1/CSC - Manager uses to communicate with JP1/CSC - Agent. Enter the same port number as specified in <b>Port number for receiving requests</b> under <b>Manager communication environment information</b> , in the <b>Basic Settings</b> page of JP1/CSC - Manager.	1024 to 65535	22340
<b>Agent communication environment information</b>	Port number	The port number of JP1/CSC - Agent. Enter the same port number as that registered for <b>Port number</b> in the Add agent information window of JP1/CSC - Manager.	1024 to 65535	22345
<b>Network control product information</b>	Name	The name of the linked network control product.	Software Distribution (AMT linkage facility)	Network Monitor
<b>Log information</b>	Log file size	Specify the maximum size (in kilobytes) of the JP1/CSC - Agent log files.	1 to 2097151	1024
	Number of log files	Specify the maximum number of JP1/CSC - Agent log files.	1 to 999	10
<b>Cluster information</b>	Cluster environment	Specify whether to run JP1/CSC - Agent in a cluster environment.	<b>Use / Do not use</b>	<b>Do not use</b>
	Logical IP address	Specify a logical IP address to use in the cluster environment.	IPv4 format (xxx.xxx.xxx.xxx)	--

Items		Description	Specifiable values	Default for initial environment setup
	Shared disk	Specify the path for the shared disk used in the cluster environment.	Full path	--
<b>Audit log information</b>	<b>Audit log</b>	Specify whether to output audit logs.	<b>Output / Do not output</b>	<b>Do not output</b>

Legend:

--: No default provided

*Reference note:*

The log information contains information about startup and termination of JP1/CSC - Agent, as well as connection information for the network control product.

### 13.3.3 Setting up a treatment server

Set up a treatment server. On the treatment server, install and set up JP1/Software Distribution Client (relay system).

#### (1) Installing JP1/Software Distribution Client (relay system)

Install JP1/Software Distribution Client (relay system) on the treatment server. The AMT Linkage facility component of JP1/Software Distribution must also be installed at this time.

For details about installation, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems.

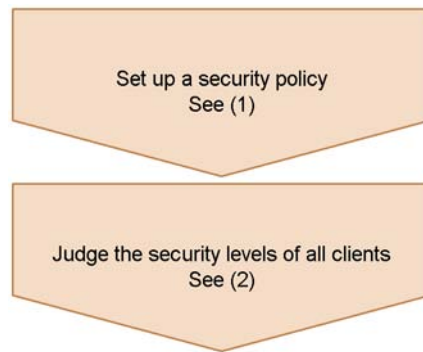
#### (2) Setting up JP1/Software Distribution Client (relay system)

Set up JP1/Software Distribution Client (relay system). If necessary, specify settings on the **AMT Linkage** page.

For details about installation, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems.

### 13.3.4 Setting up the environment for operation

After completing setup of the management and network control server, treatment server, and clients, set up the environment before starting operation. The following figure shows the procedure for setting up the environment.

*Figure 13-15: Flow of environment setup before operation***(1) Setting a security policy**

Use the Security Policy Management window to set a judgment policy and an action policy. For details about setting security policies, see *6. Managing Security Policies*.

Make sure that **Control network connection** is selected for the action policies.

**(2) Judging the security levels of all clients**

Judge the security levels of all clients. In the PC List window of the Client Security Management window, select all clients and click the **Judge** button to judge their security levels. In the action policy settings in (1), if **Refuse connection** is selected for **Control network connection**, clients with the corresponding security level are automatically excluded from the network.

For details about how to judge client security levels, see *8.4 Judging a client security level*.



## Chapter

---

# 14. Operating a Quarantine System

---

This chapter describes the operation of a quarantine system in JP1/CSC linked with different program products.

- 14.1 Operating a quarantine system linked to JP1/NM
- 14.2 Operating a quarantine system linked to an authentication server
- 14.3 Operating a quarantine system linked to JP1/Software Distribution (AMT Linkage facility)

---

## 14.1 Operating a quarantine system linked to JP1/NM

---

You can operate a quarantine system with JP1/NM in one of the following ways:

- Using the JP1/NM quarantine support facility

A client under network connection control is permitted to communicate only with the treatment server and other specific servers. This allows security measures to be implemented on the client in an online environment.

- Without using the JP1/NM quarantine support facility

Security measures are implemented on clients denied access to the network in an offline environment.

Examples of each usage are shown below.

### 14.1.1 Example of quarantine system operation using the JP1/NM quarantine support facility

The example below describes the quarantine process using the JP1/NM quarantine support facility.

This example is based on the following assumptions:

- Managed clients

Of clients A, B, and C, an unapplied patch is found only for client C.

- Security policy (judgment policy) setting

The security level for clients with unapplied patches is judged to be *Danger*.

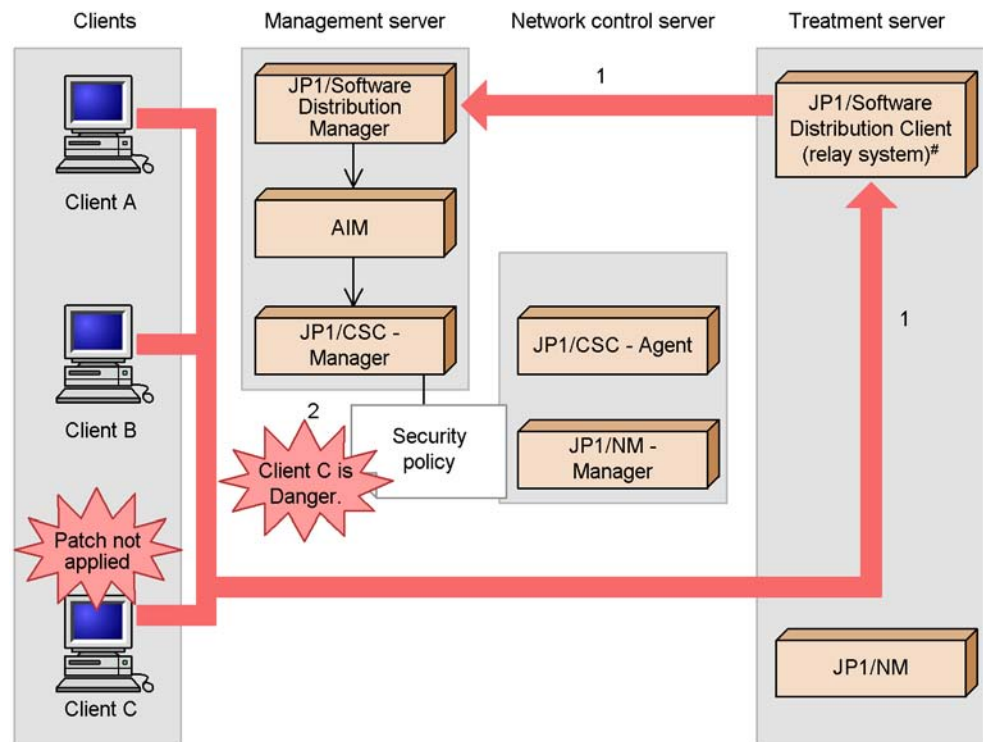
- Security policy (action policy) setting

- Clients whose security level is *Danger* are denied access to the network.
- Clients whose security level is *Safe* are permitted access to the network.

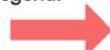

#### (1) *Inspection process*

In the inspection process, client security levels are judged, and clients that are a security risk are identified. The following figure shows the inspection process.

Figure 14-1: Inspection process



## Legend:

-  : Flow of inventory information
-  : Flow of control

#: JP1/Software Distribution SubManager 07-50 or later may be used instead.

JP1/NM can also be installed on another server, depending on the version. In Windows, JP1/NM 09-00 or later can be installed on another server. In Linux, JP1/NM 08-11 or later can be installed on another server.

1. Inventory information for clients is reported to JP1/Software Distribution Manager on the management server via JP1/Software Distribution Client (relay system)# on the treatment server.

Inventory information for clients A, B, and C is reported to JP1/Software Distribution Manager on the management server via JP1/Software Distribution Client (relay system)#.

#

JP1/Software Distribution SubManager 07-50 or later can also be used.

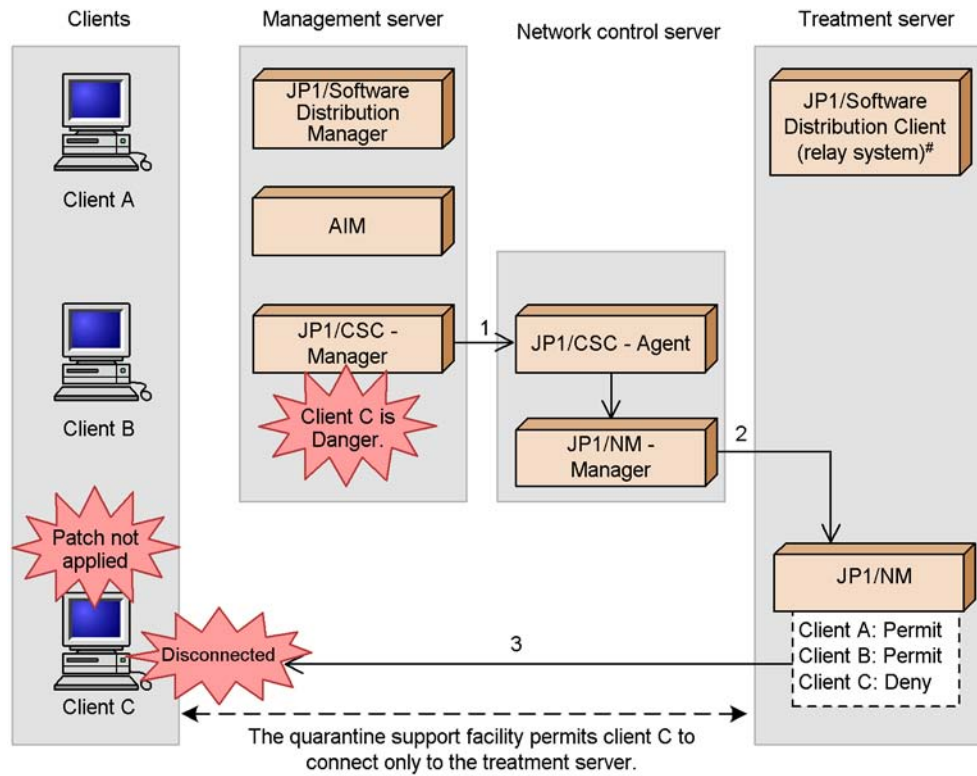
2. JP1/CSC - Manager on the management server judges client C to be *Danger*.

JP1/CSC - Manager on the management server compares the inventory information against the judgment policy, and judges client C to be *Danger*.

## (2) Isolation process

In the isolation process, client network connections are controlled based on the security policy. The following figure shows the isolation process.

Figure 14-2: Isolation process



Legend:

→ : Flow of control

#: JP1/Software Distribution SubManager 07-50 or later may be used instead.

JP1/NM can also be installed on another server, depending on the version. In Windows, JP1/NM 09-00 or later can be installed on another server. In Linux, JP1/NM 08-11 or later can be installed on another server.

1. JP1/CSC - Manager on the management server instructs the network control server to deny a network connection.



Based on the action policy, JP1/CSC - Manager on the management server instructs the network control server to deny a network connection.

2. The network control server instructs the treatment server to deny the network connection by client C.
3. The treatment server denies the network connection by client C.

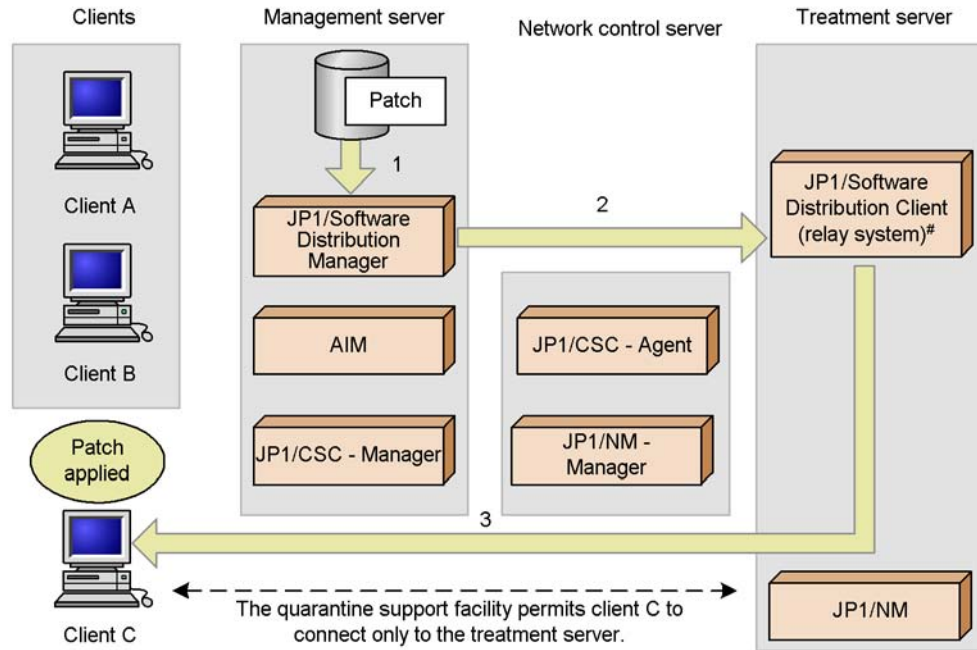
JP1/NM on the treatment server denies the network connection by client C. However, the JP1/NM quarantine support facility permits a connection between client C and the treatment server, allowing the two to communicate.

### **(3) Treatment process**

In the treatment process, security measures are implemented on clients denied access to the network. For details about how to implement security measures on clients, see *14.1.4 Implementing client security measures*.

The following figure shows the treatment process.

Figure 14-3: Treatment process



Legend:

: Flow of patch application

#: JP1/Software Distribution SubManager 07-50 or later may be used instead.

JP1/NM can also be installed on another server, depending on the version. In Windows, JP1/NM 09-00 or later can be installed on another server. In Linux, JP1/NM 08-11 or later can be installed on another server.

1. Package the patch and register it in JP1/Software Distribution Manager on the management server.  
Package the patch to be installed and register it in JP1/Software Distribution Manager on the management server.
2. Distribute the patch from JP1/Software Distribution Manager on the management server.  
In JP1/Software Distribution Manager on the management server, execute the patch distribution job. The patch is transferred to JP1/Software Distribution Client (relay system)# on the treatment server.
3. Remotely install the patch on client C from JP1/Software Distribution Client

(relay system)<sup>#</sup>.

The patch is installed on client C from JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server. By applying the distributed patch, security measures are implemented on client C.

#

JP1/Software Distribution SubManager 07-50 or later can also be used.

*Reference note:*

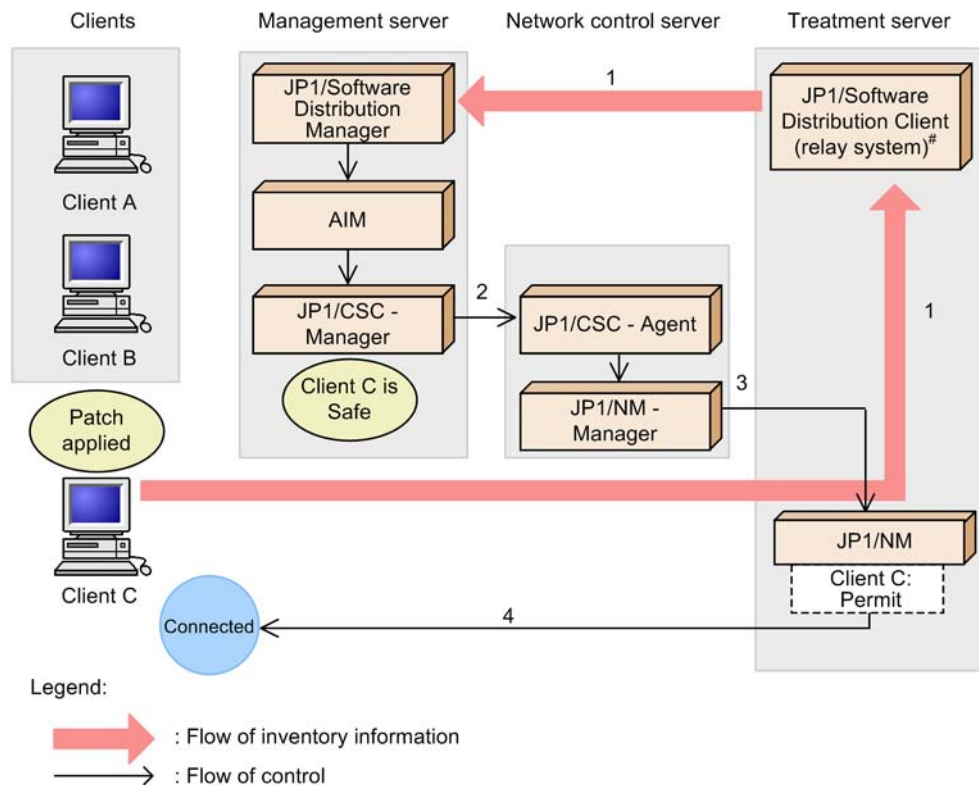
The user can also implement security measures on a client denied access to the network by manually selecting and installing packages registered with JP1/Software Distribution Manager on the management server.

**(4) Recovery process**

In the recovery process, clients for which security measures were implemented are judged again, and those judged *Safe* are reconnected to the network.

The following figure shows the recovery process.

Figure 14-4: Recovery process



#: JP1/Software Distribution SubManager 07-50 or later may be used instead.

JP1/NM can also be installed on another server, depending on the version. In Windows, JP1/NM 09-00 or later can be installed on another server. In Linux, JP1/NM 08-11 or later can be installed on another server.

1. Inventory information for client C is reported to JP1/Software Distribution Manager on the management server via JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server.

After the patch is applied, the latest inventory information for client C is reported to JP1/Software Distribution Manager on the management server via JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server.

#

JP1/Software Distribution SubManager 07-50 or later can also be used.

2. JP1/CSC - Manager on the management server judges client C to be safe, and instructs the network control server to permit a network connection.

JP1/CSC - Manager on the management server compares the inventory information against the security policy, and finds that all patches are applied. As a result, client C is judged to be *Safe*. JP1/CSC - Manager on the management server then instructs the network control server to permit a network connection based on the action policy.

3. The network control server instructs the treatment server to restore the network connection for client C.
4. The treatment server restores the network connection for client C.

JP1/NM on the treatment server restores the network connection for client C, allowing client C to access the network.

### 14.1.2 Operation without the JP1/NM quarantine support facility

The example below describes the quarantine process when the JP1/NM quarantine support facility is not used.

This example is based on the following assumptions:

- Managed clients

Of clients A, B, and C, an unapplied patch is found only for client C.

- Security policy (judgment policy) setting

The security level for clients with unapplied patches is judged to be *Danger*.

- Security policy (action policy) setting

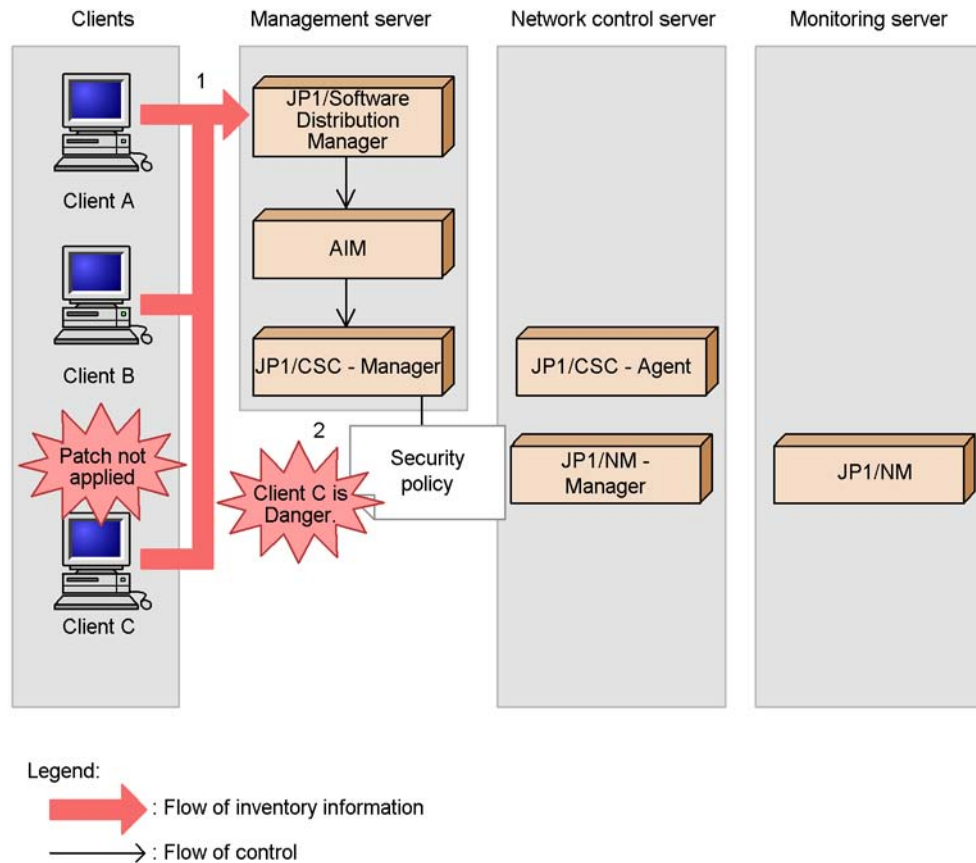
- Clients whose security level is *Danger* are denied access to the network.
- Clients whose security level is *Safe* are permitted access to the network.

#### (1) Inspection process

In the inspection process, client security levels are judged, and clients that are a security risk are identified.

The following figure shows the inspection process.

Figure 14-5: Inspection process



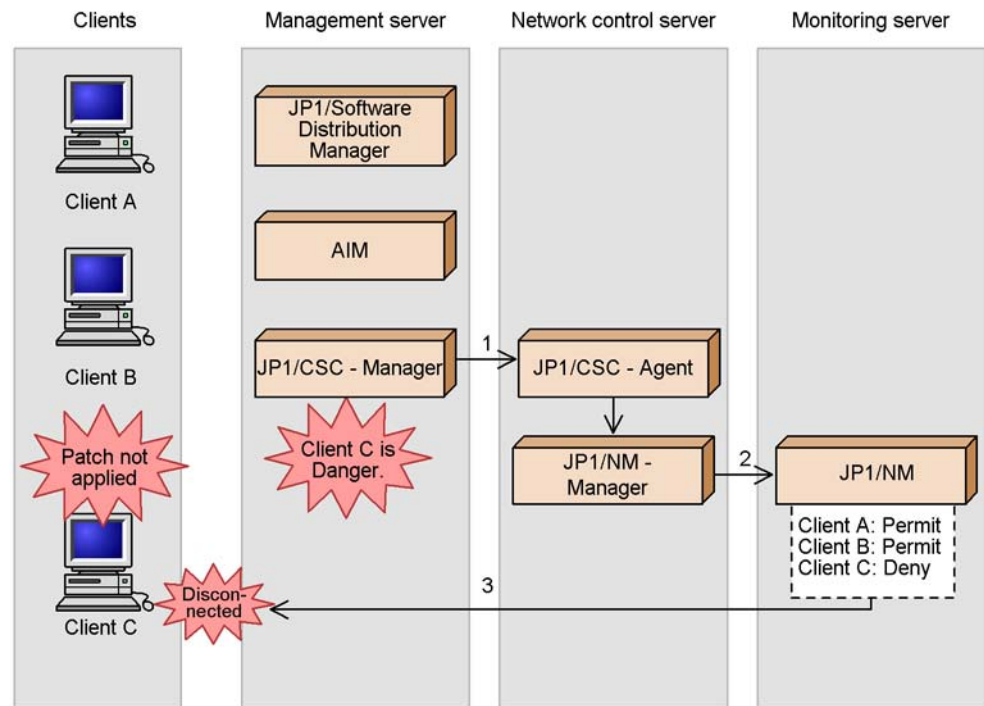
1. Inventory information for clients is reported to JP1/Software Distribution Manager on the management server.  
Inventory information for clients A, B, and C is reported to JP1/Software Distribution Manager on the management server.
2. JP1/CSC - Manager on the management server judges client C to be Danger.  
JP1/CSC - Manager on the management server compares the inventory information against the judgment policy, and judges client C to be *Danger*.

## (2) Isolation process

In the isolation process, client network connections are controlled based on the security policy.

The following figure shows the isolation process.

Figure 14-6: Isolation process



Legend:

—————> : Flow of control

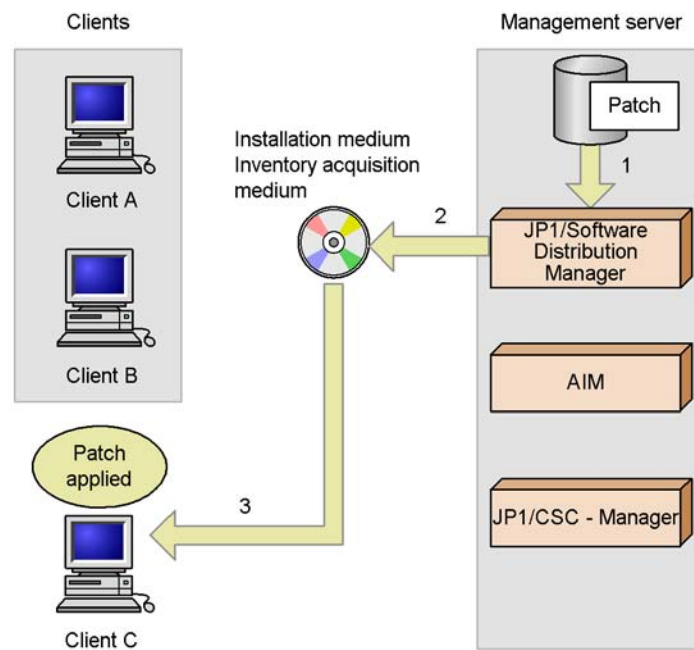
1. JP1/CSC - Manager on the management server instructs the network control server to deny a network connection.  
Based on the action policy, JP1/CSC - Manager on the management server instructs the network control server to deny a network connection.
2. The network control server instructs the monitoring server to deny the network connection by client C.
3. The monitoring server denies the network connection by client C.  
JP1/NM on the monitoring server denies the network connection by client C.

### (3) Treatment process

In the treatment process, security measures are implemented on clients denied access to the network. For details about how to implement security measures on clients, see *14.1.4 Implementing client security measures*.

The following figure shows the treatment process.

Figure 14-7: Treatment process



Legend:



1. Package the patch and register it in JP1/Software Distribution Manager on the management server.  
Package the patch you intend to install offline, and register it with JP1/Software Distribution Manager on the management server.
2. Prepare an installation medium and an inventory acquisition medium.  
Prepare an installation medium containing the patch you want to apply to client C, and an inventory acquisition medium on which to record the latest inventory information for client C.
3. Transport the media you prepared in step 2 to client C, and install the patch.  
Run the program on the installation medium to apply the patch to client C. This implements security measures on client C.

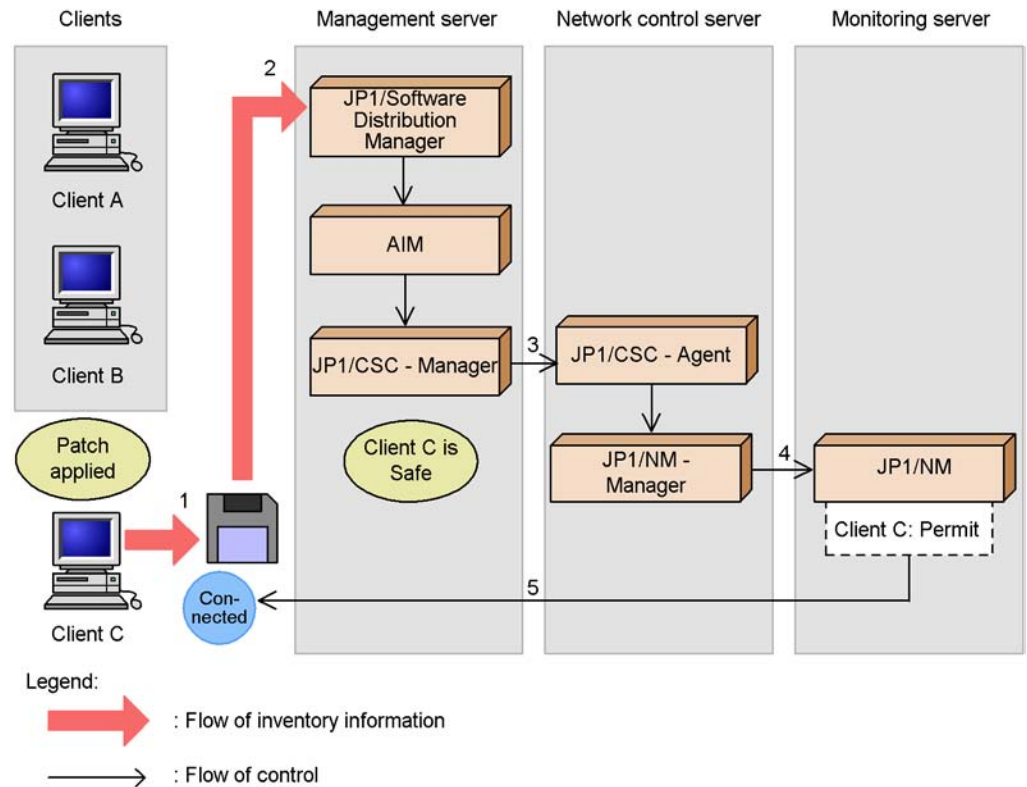


**(4) Recovery process**

In the recovery process, clients for which security measures were implemented are judged again, and those judged *Safe* are reconnected to the network.

The following figure shows the recovery process.

Figure 14-8: Recovery process



1. Save the latest inventory information for client C to the inventory acquisition medium.  
Run the program on the inventory acquisition medium. The latest inventory information for client C is written to the medium.
2. Transport the medium containing the inventory information for client C to JP1/Software Distribution Manager on the management server, and read the inventory information from the medium.  
JP1/Software Distribution Manager retrieves the latest inventory information for client C from the medium you prepared in step 1.

3. JP1/CSC - Manager on the management server judges client C to be Safe, and instructs the network control server to permit a network connection.

JP1/CSC - Manager compares the inventory information against the security policy, and finds that all patches are applied. As a result, client C is judged to be *Safe*. JP1/CSC - Manager then instructs the network control server to permit a network connection based on the action policy.

4. The network control server instructs the monitoring server to restore the network connection for client C.
5. The monitoring server restores the network connection for client C.

JP1/NM on the monitoring server restores the network connection for client C, allowing client C to access the network.

### 14.1.3 Tasks during operation of a quarantine system linked to JP1/NM

This subsection explains the tasks involved in running a quarantine system linked to JP1/NM.

The following table lists the tasks.

*Table 14-1: List of quarantine system tasks*

Tasks	Description	Type	Reference
Monitoring clients	Client security levels are judged and action histories are reviewed at the administrator's discretion.	M	<i>8. Monitoring Clients</i>
Implementing actions	Based on instructions from the administrator, clients with high security risk levels are denied access to the network, and clients that are declared safe have their network access restored.	M	<i>9. Dealing with Security Risks</i>
Evaluating client security	The status of security measures is checked for each client, and the adequacy of the security measures for a specific user or group is evaluated based on a points rating.	O	<i>10. Auditing Security</i>

Tasks	Description	Type	Reference
Implementing security measures on clients	Security measures are implemented on clients that have been denied access to the network after being judged a security risk. Security measures are implemented on clients either in an online environment through communication with the treatment server or in an offline environment.	M	<i>14.1.4 Implementing client security measures</i>
Changing the system configuration	When you add a new client to the network, information about the client is registered in JP1/NM.	O	<i>14.1.5 Adding new clients to the network</i>
	When you remove a client from the network while the quarantine system is running, information about the client is deleted from JP1/NM.	O	<i>14.1.7 Removing a client after operation has started</i>

Legend:

M: Indicates a mandatory task.

O: Indicates an optional task.

### 14.1.4 Implementing client security measures

When a client is judged a security risk and denied access to the network, security measures must be implemented on the client. Security measures are implemented differently depending on whether the JP1/NM quarantine support facility is used. This section describes how to implement security measures with and without the JP1/NM quarantine support facility.

#### (1) When using the JP1/NM quarantine support facility

To implement security measures on a client that is denied access to the network, execute the software distribution facility of JP1/Software Distribution.

By using this facility, the administrator can distribute software from JP1/Software Distribution Manager on the management server, using JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server as a relay system. Alternatively, the client can be provided with packages for the user to install.

For details about the software distribution facility, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows

systems.

#

JP1/Software Distribution SubManager 07-50 or later can also be used.

## (2) When not using the JP1/NM quarantine support facility

Security measures can be implemented on a client that is denied access to the network in either of two ways:

- Using the JP1/Software Distribution offline machine management facility
- Providing installation media to the client

Each method is described below.

### (a) Using the JP1/Software Distribution offline machine management facility

The offline machine management facility of JP1/Software Distribution allows you to install software offline and to obtain inventory information from offline machines. You can use this facility to implement client security measures in an offline environment.

For details about the offline machine management facility, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

### (b) Providing installation media to the client

A client user can use an installation medium or similar to implement security measures. However, after the security measures have been implemented, the client will still be unable to reconnect to the network. This is because the client is unable to notify the management server of the latest inventory information.

To reconnect the client to the network:

1. Implement the appropriate security measures.  
Apply the most recent patches for the client, or install the latest anti-virus product.
2. In the PC List window of the Client Security Management window, select the client to be reconnected to the network, and in **Network Connection**, click the **Permit** button.  
Network connections are permitted for the client.  
You can also execute a network control command (`cscnetctrl`) from the remote management server to permit network connections. For details about this command, see *cscnetctrl (controls network connections)* in 15. Commands.
3. Reconnect the client to the network.  
Physically reconnect the client to the network.
4. Collect the latest inventory information for the client.

The client inventory information updated by the security measures implemented in step 1 is collected by JP1/Software Distribution.

5. Using the latest inventory information for the client, judge the security level of the client according to the judgment policy.
6. Check the judgment results in the PC List window.

Using the PC List window, the administrator confirms that the security level of the client added to the network is *Safe*.

### 14.1.5 Adding new clients to the network

To add a new client to the network after starting operations with your quarantine system, you will first need to register the relevant MAC address with JP1/NM. The procedure differs depending on whether the JP1/NM quarantine support facility is used.

#### (1) When using the JP1/NM quarantine support facility

If you are using the JP1/NM quarantine support facility, you do not need to register the MAC address with JP1/NM when you add a new client to the network or add a LAN board to a client.

Inventory information for the new client is reported to the management server via JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server, and the security level of the client is judged. If the client is confirmed as *Safe*, the network control server is instructed to permit network connections for the client according to the action policy, and the client's MAC address is registered with JP1/NM automatically.

#

JP1/Software Distribution SubManager 07-50 or later can also be used.

#### (2) When not using the JP1/NM quarantine support facility

If you do not use the JP1/NM quarantine support facility, the MAC address will not be automatically registered with JP1/NM when you add a client to the network or a LAN board to a client.

As such, an administrator must register the MAC address of the new client or LAN board in JP1/NM from the Register Permitted PCs window.

Before you connect the new client to the network, first implement security measures for the client.

To connect a new client to the network:

1. Implement security measures for the client.  
Apply the most recent patches for the client, or install the latest anti-virus product.
2. Create a permitted-PC list file for the client to be added.

The administrator creates a permitted-PC list file containing the MAC address of the client to be added. For details about how to create a permitted-PC list file, see *14.1.6 Registering permitted PCs*.

3. In the Register Permitted PCs window of the Client Security Management window, register the permitted-PC list file.

The permitted-PC list file created in step 2 is registered in JP1/NM.

4. Connect the client to the network.

Physically connect the client to the network.

5. Collect the latest inventory information for the client.

The inventory information for the added client is collected by JP1/Software Distribution.

6. Using the latest inventory information for the client, judge the security level of the client according to the security policy.

7. Check the judgment results in the PC List window.

Using the PC List window, the administrator confirms that the security level of the client added to the network is *Safe*.

### 14.1.6 Registering permitted PCs

To add new clients to the network after starting operations with your quarantine system, you must register the MAC addresses in JP1/NM using the function for registering permitted PCs.

To register MAC addresses in JP1/NM, first create a permitted-PC list file containing the client MAC addresses. Then, register the file in the Register Permitted PCs window of the Client Security Control window in AIM.

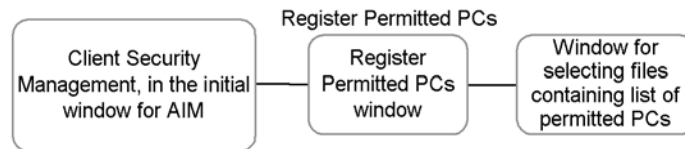
*Note:*

To add a device such as a router, printer, or Solaris machine to the network, from the Integrated Management window of JP1/NM - Manager, add the IP address or MAC address as a **Fixed device**. If an administrator mistakenly denies a network connection from the PC List window for a device registered from the Integrated Management window of JP1/NM - Manager, the status of the device appears as **Refuse** in the PC List window, but the actual network connection is still permitted.

#### (1) Transitions of windows used to register permitted PCs

The following figure shows the transitions of windows used to register permitted PCs.

Figure 14-9: Transitions of windows used to register permitted PCs



To open the initial window of AIM, log in to AIM as a user with the CSC administrator role. For details about opening the initial window of AIM, see 8.1 *Transitions of windows used for client monitoring*.

## (2) Creating a permitted-PC list file

A permitted-PC list file contains the MAC addresses of new clients and the added LAN boards for which network connections are to be permitted.

The following table shows the format of the permitted-PC list file.

Table 14-2: Format of permitted-PC list file

No.	Item	Description
1	MAC address <sup>#</sup>	Write the MAC address of the new client or added LAN board. Write one MAC address per line, represented by a 12-digit hexadecimal number. One of the following delimiters can be used every second digit: <ul style="list-style-type: none"> <li>• Hyphen (-)</li> <li>• Colon (:)</li> <li>• Space</li> </ul>
2	Comment	Lines beginning with a hash symbol (#) are treated as comments. The hash symbol cannot be used except at the start of a line.

#

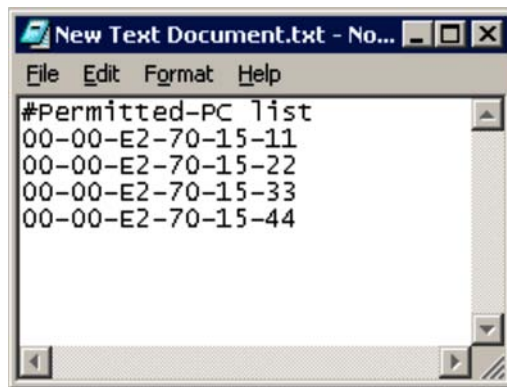
In the permitted-PC list file, do not specify the MAC addresses of clients and LAN boards already subjected to security management. If the MAC addresses of such clients and LAN boards are registered in JP1/NM, keep in mind that their network connections are permitted even when their status is displayed as **Refuse** in the PC List window.

*Note:*

- Make sure that there are no spaces or tabs before or after MAC addresses in the permitted-PC list file.
- Include a line feed in the last line of the permitted-PC list file.

The following figure shows an example of the permitted-PC list file.

*Figure 14-10:* Example of permitted-PC list file



### **(3) Registering permitted PCs**

Clients whose network connections are to be permitted are registered in JP1/NM from the Register Permitted PCs window.

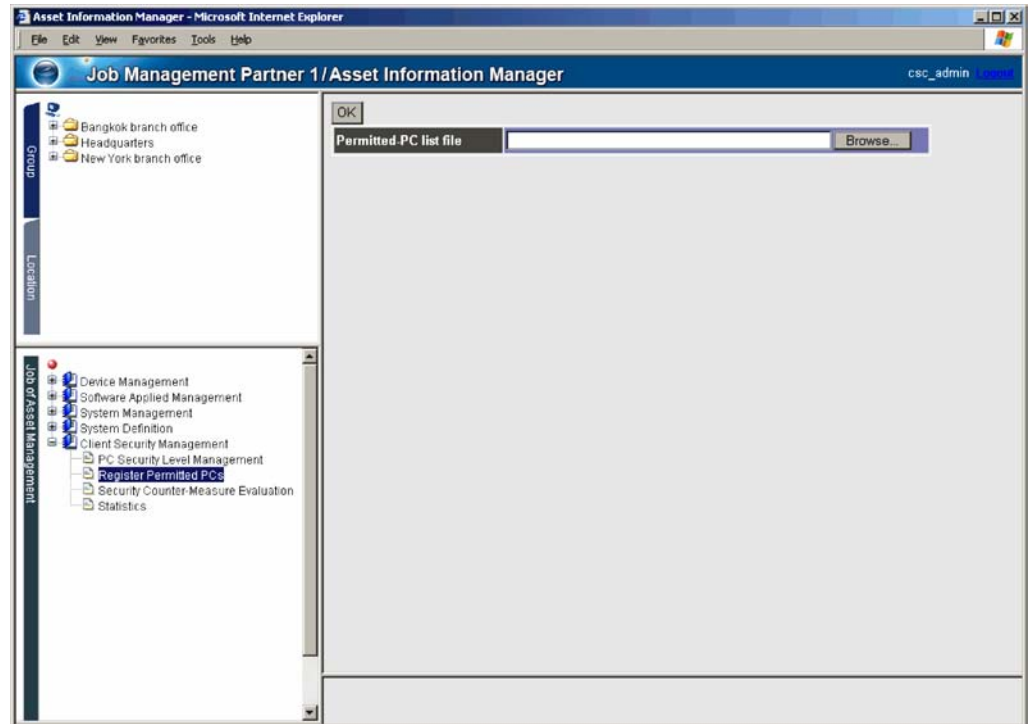
To register a client whose network connections are to be permitted in JP1/NM:

1. From the job menu in the initial window of AIM, choose **Client Security Management** and then **Register Permitted PCs**.

The Register Permitted PCs window appears.



Figure 14-11: Register Permitted PCs window

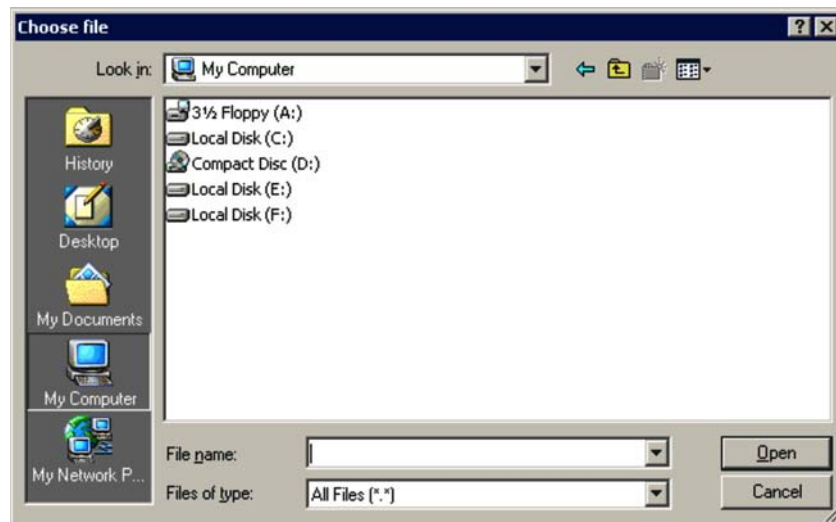


2. Enter the name of the permitted-PC list file.

In **Permitted-PC list file**, enter the full path of the permitted-PC list file.

Alternatively, click the **Browse** button to display a window where you can select the file.

The following figure shows the window where you can select the permitted-PC list file.



3. In the Register Permitted PCs window, click the **OK** button.

A message box appears asking you to confirm whether to allow the clients in the permitted-PC list file to connect to the network.

4. Click the **OK** button.

The clients in the permitted-PC list file are connected to the network, and the Action Message dialog box appears. If an error message is displayed, see *17.4.3 Messages in the Register Permitted PCs window* and act accordingly.

5. Click the **Close** button.

The Action Message dialog box closes.

### 14.1.7 Removing a client after operation has started

After you have started operations with your quarantine system, the removal of clients because of asset disposal or other reasons can be performed in either of the following ways:

- With automatic denial of network connection enabled
- With automatic denial of network connection disabled

This procedure is the same regardless of whether you use the JP1/NM quarantine support facility.

#### **(1) With automatic denial of network connection enabled**

1. In JP1/CSC - Manager setup, enable network connections to be denied automatically when a client is removed from the network.

To automatically deny network connections when a client is removed, enter the following setting in the Client Security Control - Manager Setup dialog box:

- In the **Basic Settings** page, under **Asset deletion information**, set the **Automatic refusal of network connection** attribute to **Execute**.

2. Remove the client.

JP1/NM automatically denies the client connection to the network.

3. In the Device List window of AIM, select the asset information of the client you removed, and set the device status to **Erase**.

For details about how to set the device status to **Erase**, see the manual *Job Management Partner 1/Asset Information Manager Administrator's Guide*.

Note that if the management server is configured using Asset Information Manager Subset Component of JP1/Software Distribution Manager, this step is unnecessary because the device status changes to **Erase** as soon as you remove the client.

4. Use the data maintenance task to delete asset information with the **Erase** status.

For details about data maintenance, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

## **(2) With automatic denial of network connection disabled**

1. In JP1/CSC - Manager setup, prevent network connections from being denied automatically when a client is removed from the network.

To prevent network connections from being denied automatically when a client is removed, specify the following setting in the Client Security Control - Manager Setup dialog box:

- In the **Basic Settings** page, under **Asset deletion information**, set the **Automatic refusal of network connection** attribute to **Do not execute**.

2. In the PC List window of the Client Security Management window, select the client you want to remove. Then, in **Network connection**, click the **Refuse** button.

JP1/NM denies the client connection to the network.

3. Remove the client.

4. In the Device List of AIM, select the asset information of the client you removed, and set the device status to **Erase**.

For details about how to set the device status to **Erase**, see the manual *Job Management Partner 1/Asset Information Manager Administrator's Guide*.

Note that if the management server is configured using Asset Information

Manager Subset Component of JP1/Software Distribution Manager, this step is unnecessary because the device status changes to **Erase** as soon as you remove the client.

5. Use the data maintenance task to delete asset information with the **Erase** status.  
For details about data maintenance, see the manual *Job Management Partner 1/ Asset Information Manager Planning and Setup Guide*.

## 14.2 Operating a quarantine system linked to an authentication server

You can operate a quarantine system linked to an authentication server in any of the following ways:

- Using IEEE 802.1X authentication in a dynamic VLAN environment
- Using IEEE 802.1X authentication in a static VLAN environment
- Using MAC authentication in a static VLAN environment

The following subsections provide operation examples for two of these: IEEE 802.1X authentication used in a dynamic VLAN environment and MAC authentication used in a static VLAN environment.

### 14.2.1 Example of operating a quarantine system linked to an authentication server in a dynamic VLAN environment (IEEE 802.1X authentication)

This subsection uses an operation example to explain the quarantine processes of a quarantine system linked to an IEEE 802.1X authentication server in a dynamic VLAN environment.

This example is based on the following assumptions:

- Authentication server

The authentication server OS is Windows Server 2003.

Note that if the authentication server OS is Windows Server 2008, managed clients cannot receive messages that report the destination network for connection.

- Managed clients

- Of clients A and B, an unapplied patch is found only for client B.
- Client C will be newly added to the network.

- Security policy (judgment policy) setting

The security level for clients with unapplied patches is judged to be *Danger*.

- Security policy (action policy) setting

- Clients whose security level is *Danger* are denied access to the network.
- Clients with any security level other than *Danger* are permitted access to the network.

■ JP1/CSC - Agent setup

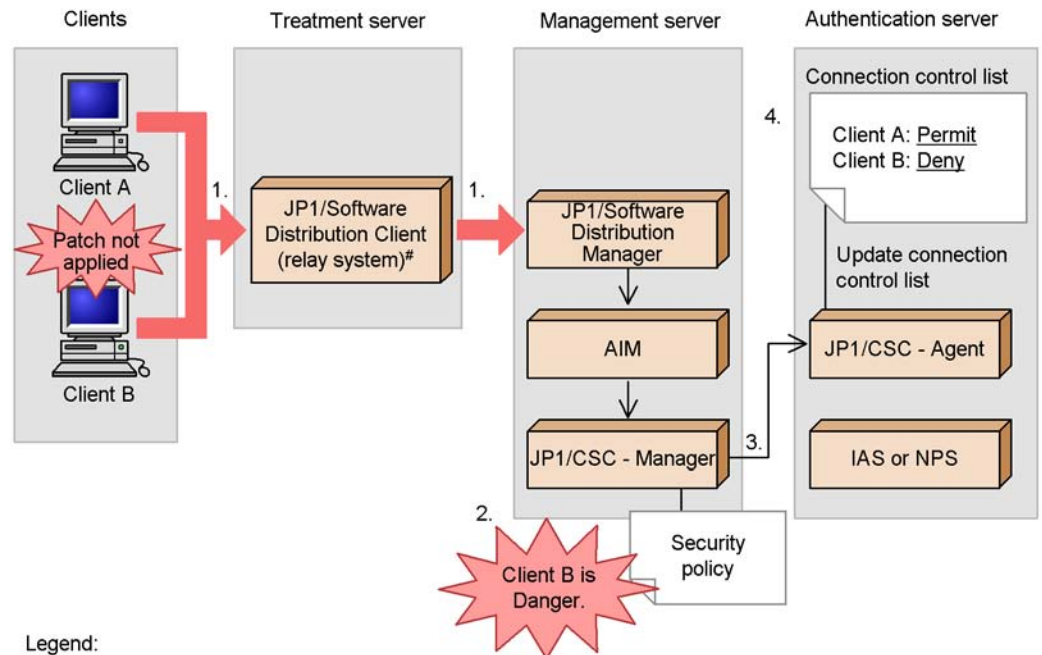
- The **Network type** of **Connection information for unregistered asset** is set to **Quarantined**.
- The **Network type** of **Connection information for refused asset** is set to **Quarantined**.
- **Message notification** under **Message notification information** is set to **Notify**.

**(1) Authentication/inspection process**

In the authentication/inspection process, clients that are a security risk are identified, and clients are authenticated.

The following figure shows the authentication/inspection process (client judgment).

Figure 14-12: Authentication/inspection process (client judgment)



1. Inventory information for clients is reported to JP1/Software Distribution Manager on the management server via JP1/Software Distribution Client (relay system)# on the treatment server.  
Inventory information for clients A and B is reported to JP1/Software Distribution Manager on the management server via JP1/Software Distribution Client (relay system)# on the treatment server.

#

JP1/Software Distribution SubManager 07-50 or later can also be used.

2. JP1/CSC - Manager on the management server judges client B to be *Danger*.  
JP1/CSC - Manager on the management server compares the inventory

information against the judgment policy, and judges client B to be *Danger*.

3. JP1/CSC - Manager on the management server instructs JP1/CSC - Agent on the authentication server to permit (client A) and deny (client B) network connections.

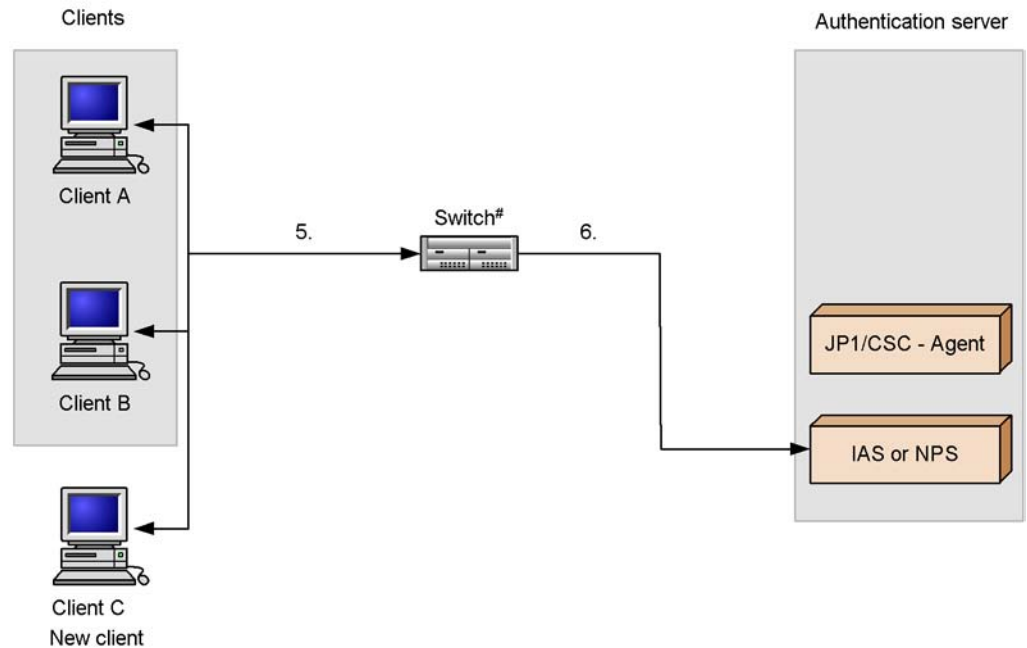
Based on the action policy, JP1/CSC - Manager on the management server instructs JP1/CSC - Agent on the authentication server to allow client A access to the network, but deny access for client B.

4. JP1/CSC - Agent on the authentication server updates the connection control list.  
JP1/CSC - Agent updates the network control list to reflect the action implemented on JP1/CSC - Manager, by setting client A to *Permit* and client B to *Deny*.

The following figure shows the authentication/inspection process (client authentication).



Figure 14-13: Authentication/inspection process (client authentication)



Legend:

IAS or NPS : Microsoft Internet Authentication Service or Network Policy Server

→ : Flow of authentication request

#: Switch supporting IEEE 802.1X authentication

#### 5. Begin client authentication.

When the client is restarted, or when the Windows standard supplicant service is restarted or the client network connection is enabled, an authentication request is sent via the switch to Microsoft IAS or Network Policy Server on the authentication server.

If sending of EAPOL-START packets<sup>#</sup> has not been set, the switch requests client authentication based on the authentication interval set on the switch.

In this example, a new client (client C) will be added to the network.

#

For details about configuring the supplicant to send EAPOL-START packets, see the description immediately following the table in 13.2.6(2) *Setting up the Windows standard supplicant*.

6. The switch sends client authentication requests to Microsoft IAS or Network Policy Server on the authentication server.

The switch requests authentication of clients A, B, and C from Microsoft IAS or Network Policy Server on the authentication server.

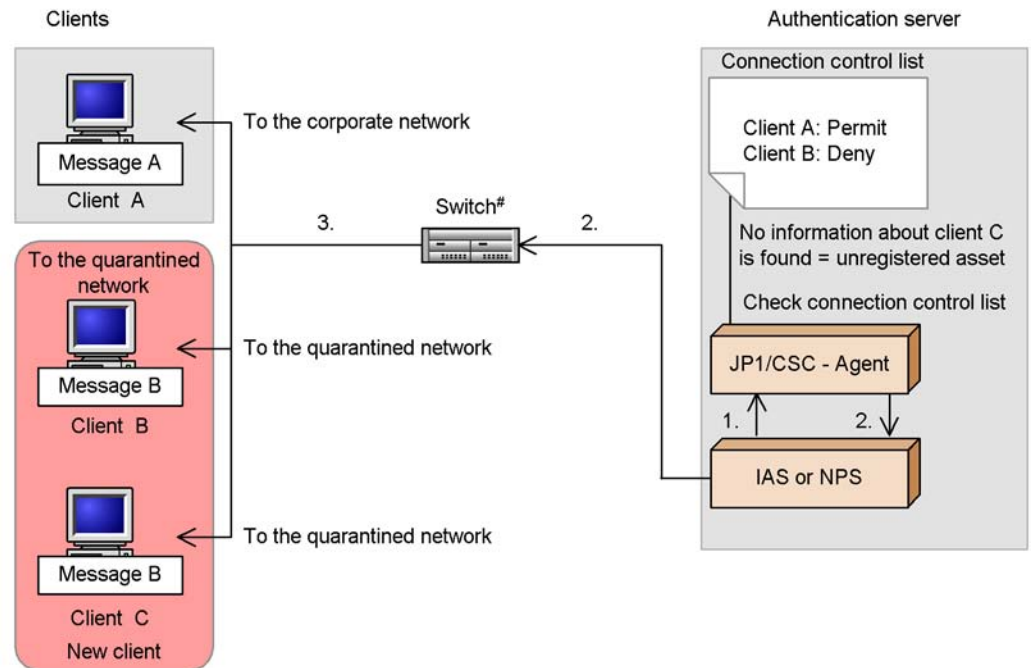
Clients A, B, and C are authenticated according to the IEEE 802.1X standard, based on a user ID and password.

## **(2) Isolation process**

In the isolation process, client network connections are controlled based on the security policy.

The following figure shows the isolation process.

Figure 14-14: Isolation process



## Legend:

IAS or NPS : Microsoft Internet Authentication Service or Network Policy Server

→ : Flow of control

Message A : Message sent when the client is connected to the corporate network.

Message B : Message sent when the client is connected to the quarantined network.

#: Switch supporting IEEE 802.1X authentication

1. Microsoft IAS or Network Policy Server on the authentication server requests JP1/CSC - Agent to check the connection control list.  
After clients A, B, and C have been authenticated, Microsoft IAS or Network Policy Server on the authentication server requests JP1/CSC - Agent to check the connection control list.
2. JP1/CSC - Agent checks the connection control list, and returns the VLAN-IDs of the clients' connection destinations to Microsoft IAS or Network Policy Server. Microsoft IAS or Network Policy Server then reports these VLAN-IDs to the switch.  
JP1/CSC - Agent on the authentication server checks the connection control list

for information about clients A, B, and C. In this case, client A is listed as `Permit`, and client B is listed as `Deny`. As no information about client C is listed in the connection control list, client C is deemed an unregistered asset.

JP1/CSC - Agent returns the VLAN-ID of the quarantined network to Microsoft IAS or Network Policy Server.

Microsoft Internet Authentication Service or Network Policy Server reports to the switch the quarantine network's VLAN-ID received by JP1/CSC - Agent and the corporate network's VLAN-ID managed by Microsoft Internet Authentication Service or Network Policy Server.

3. The switch switches the connection destinations of the clients.

The switch decides the connection destination for each client based on the VLAN-IDs received from Microsoft IAS or Network Policy Server on the authentication server.

Client A is connected to the corporate network, and clients B and C are connected to the quarantined network. A message is sent to the clients, notifying them of their connection destination.

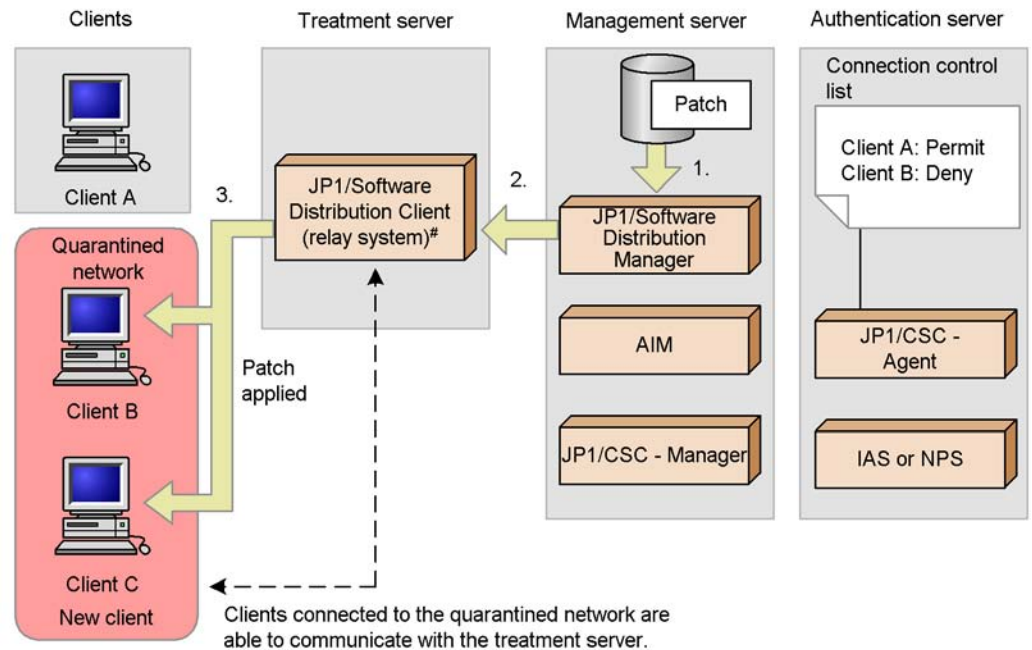
You must now implement security measures on clients B and C, which are connected to the quarantined network.

### **(3) Treatment process**

In the treatment process, security measures are implemented on clients denied access to the network. For details about how to implement security measures on clients, see *14.2.5 Implementing security measures on a client*.

The following figure shows the treatment process.

Figure 14-15: Treatment process



## Legend:

IAS or NPS : Microsoft Internet Authentication Service or Network Policy Server

: Flow of patch

#: JP1/Software Distribution SubManager 07-50 or later may be used instead.

1. Package the patches, and then register the package in JP1/Software Distribution Manager on the management server.

Package the patches to be installed, and register the package in JP1/Software Distribution Manager on the management server.

2. Distribute the patches from JP1/Software Distribution Manager on the management server.

On JP1/Software Distribution Manager, execute the patch distribution job. The patches are transferred to JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server.

3. Remotely install the patches on the clients from JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server.

Because clients in the quarantined network are permitted to communicate with

JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server, the patches are installed on the client from JP1/Software Distribution Client (relay system)<sup>#</sup>. By applying the distributed patch, security measures are implemented on the client.

#

JP1/Software Distribution SubManager 07-50 or later can also be used.

*Reference note:*

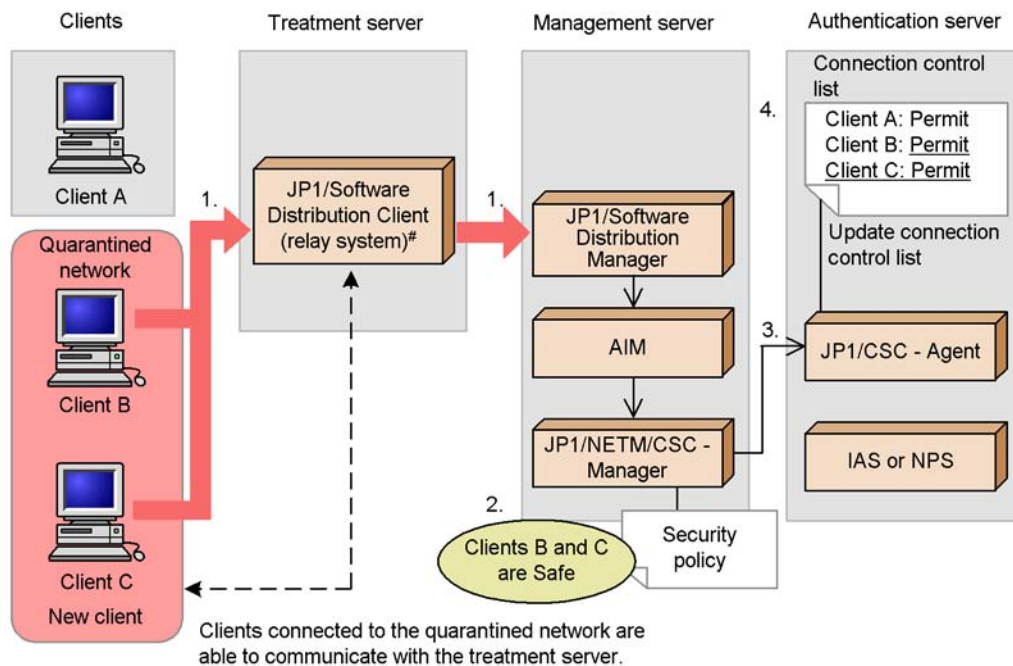
The user can also implement security measures on a client denied access to the network by manually selecting and installing packages registered with JP1/Software Distribution Manager on the management server.

**(4) Recovery process**

In the recovery process, clients for which security measures have been implemented are judged and authenticated again, and those judged *Safe* are reconnected to the network.

The following figure shows the recovery process (repeating client judgment).

Figure 14-16: Recovery process (repeating client judgment)



## Legend:

IAS or NPS : Microsoft Internet Authentication Service or Network Policy Server

: Flow of inventory information

: Flow of control

\_ (underline) : Information newly registered in the connection control list

#: JP1/Software Distribution SubManager 07-50 or later may be used instead.

1. Inventory information for the clients is reported to JP1/Software Distribution Manager on the management server via JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server.

After the patch is applied, the latest inventory information for clients B and C is reported to JP1/Software Distribution Manager on the management server via JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server.

#

JP1/Software Distribution SubManager 07-50 or later can also be used.

2. JP1/CSC - Manager on the management server judges clients B and C to be safe.

JP1/CSC - Manager on the management server compares the inventory information against the judgment policy, and finds that all patches are applied. As a result, clients B and C are judged to be *Safe*.

3. JP1/CSC - Manager on the management server instructs JP1/CSC - Agent on the authentication server to permit network connections (for clients B and C).

Based on the action policy, JP1/CSC - Manager on the management server instructs JP1/CSC - Agent on the authentication server to allow clients B and C access to the network.

4. JP1/CSC - Agent on the authentication server updates the connection control list.

JP1/CSC - Agent on the authentication server updates the connection control list, by implementing an action involving network connection permission.

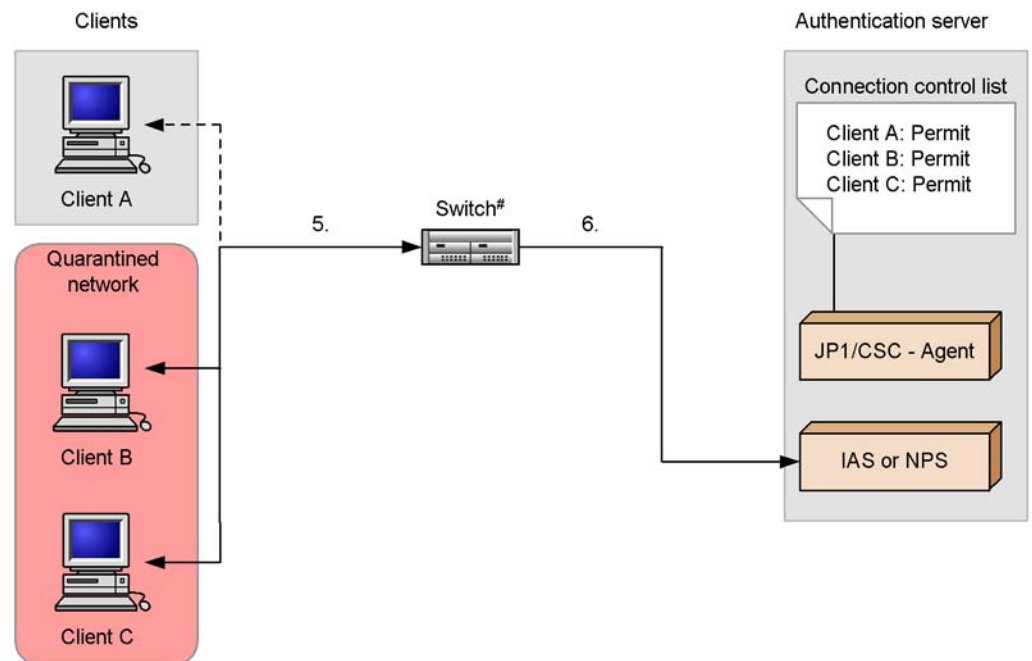
The existing connection information for client B in the connection control list is changed from *Refuse* to *Permit*.

Because there is no information about client C in the list, JP1/CSC - Agent registers the MAC address and IP address obtained as part of the inventory information for client C, and sets the connection information for client C to *Permit*.

The following figure shows the recovery process (repeating client authentication).



Figure 14-17: Recovery process (repeating client authentication)



## Legend:

IAS or NPS : Microsoft Internet Authentication Service or Network Policy Server

—————▶ : Flow of authentication request

-----▶ : Flow of authentication request at re-authentication of client A

#: Switch supporting IEEE 802.1X authentication

## 5. Initiate client re-authentication.

Client re-authentication is performed so that client B and client C can be connected to the corporate network.

When the client is restarted, the Windows standard supplicant service is restarted, or the client network connection is enabled, an authentication request is sent via the switch to Microsoft IAS or Network Policy Server on the authentication server.

If sending of EAPOL-START packets<sup>#</sup> has not been set, the switch requests client authentication based on the authentication interval set on the switch.

If client authentication is initiated based on the *authentication interval setting* of

*the switch*, client A will be re-authenticated as well as clients B and C.

#

For details about configuring the supplicant to send EAPOL-START packets, see the description immediately following the table in 13.2.6(2) *Setting up the Windows standard supplicant*.

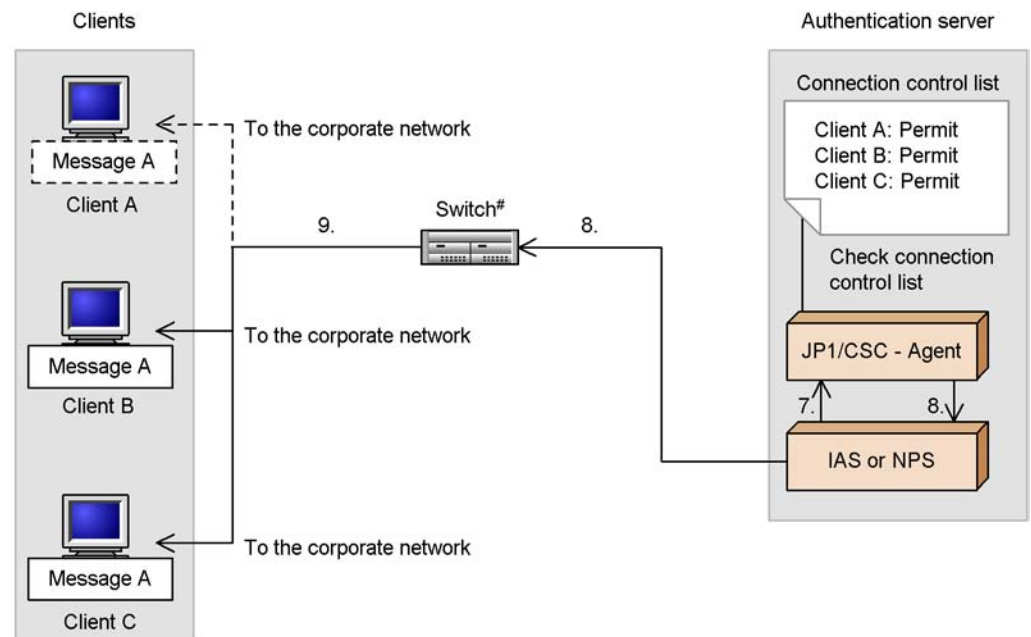
6. The switch sends client authentication requests to Microsoft IAS or Network Policy Server on the authentication server.

The switch requests authentication of clients B and C from Microsoft IAS or Network Policy Server on the authentication server.

Clients B and C are authenticated according to the IEEE 802.1X standard, based on a user ID and password. However, the user ID and password for client A will not be checked, as it has already successfully completed the authentication process.

The following figure shows the recovery process (reconnecting clients to the network).

Figure 14-18: Recovery process (reconnecting clients to the network)



## Legend:

IAS or NPS : Microsoft Internet Authentication Service or Network Policy Server

—&gt; : Flow of control

- - -&gt; : Flow of authentication request at re-authentication of client A.

Message A

 : Message sent when the client is connected to the corporate network.

Message A

 : Message sent when client A is re-authenticated.

#: Switch supporting IEEE 802.1X authentication

7. Microsoft IAS or Network Policy Server on the authentication server requests JP1/CSC - Agent to check the connection control list.

When user authentication of client B and client C has been completed, Microsoft IAS or Network Policy Server on the authentication server requests JP1/CSC - Agent to check the connection control list.

8. JP1/CSC - Agent on the authentication server checks the connection control list, and returns the VLAN-IDs of the clients' connection destinations to Microsoft IAS or Network Policy Server. Microsoft IAS or Network Policy Server then reports these VLAN-IDs to the switch.

JP1/CSC - Agent on the authentication server checks the connection control list for information about clients B and C. In this case, clients B and C are listed as *Permit*.

JP1/CSC - Agent then notifies Microsoft IAS or Network Policy Server that these clients should be connected to the corporate network, and Microsoft IAS or Network Policy Server reports the VLAN-ID of the corporate network to the switch.

9. The switch switches the connection destinations of the clients.

The switch decides the connection destination for each client based on the VLAN-IDs received from Microsoft IAS or Network Policy Server on the authentication server.

Clients B and C are connected to the corporate network, and a message is sent to the clients notifying them of their connection destination. If authentication was initiated based on the *authentication interval setting of the switch*, a message will also be sent to client A.

### 14.2.2 Example of operating a quarantine system linked to an authentication server in a static VLAN environment (MAC authentication)

This subsection uses an operation example to explain the quarantine processes of a quarantine system linked to a MAC authentication server in a static VLAN environment.

This example is based on the following assumptions:

- Authentication server

The authentication server OS is Windows Server 2003.

Note that if the authentication server OS is Windows Server 2008, managed clients cannot receive messages that report the destination network for connection.

- Managed clients

- Of clients A and B, an unapplied patch is found only for client B.
- Client C will be added to the network.

- Security policy (judgment policy) setting

The security level for clients with unapplied patches is judged to be *Danger*.

- Security policy (action policy) setting

- Clients whose security level is *Danger* are denied access to the network.
- Clients with any security level other than *Danger* are permitted access to the

network.

■ JP1/CSC - Agent setup

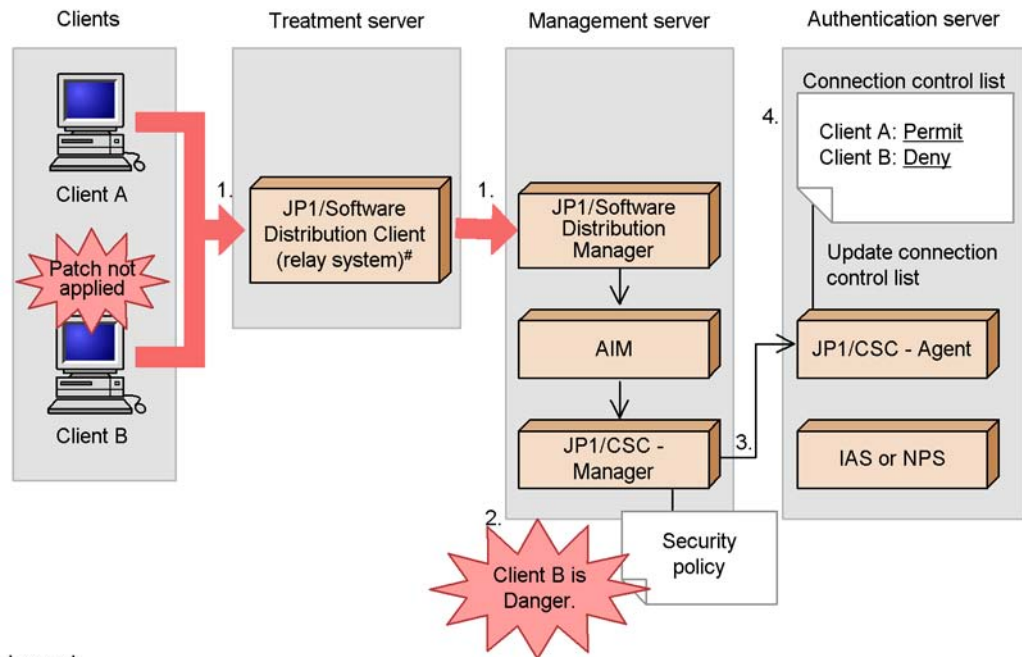
- The **Network type** of **Connection information for unregistered asset** is set to **Unauthenticated**.
- The **Network type** of **Connection information for refused asset** is set to **Unauthenticated**.
- **Message notification** under **Message notification information** is set to **Notify**.

**(1) Authentication/inspection process**

In the authentication/inspection process, clients that are a security risk are identified, and clients are authenticated.

The following figure shows the authentication/inspection process (client judgment).

Figure 14-19: Authentication/inspection process (client judgment)



Legend:

IAS or NPS : Microsoft Internet Authentication Service or Network Policy Server

Red arrow : Flow of inventory information

Black arrow : Flow of control

— (underline) : Information newly registered in the connection control list

#: JP1/Software Distribution SubManager 07-50 or later may be used instead.

1. Inventory information for clients is reported to JP1/Software Distribution Manager on the management server via JP1/Software Distribution Client (relay system)# on the treatment server.

Inventory information for clients A and B is reported to JP1/Software Distribution Manager on the management server via JP1/Software Distribution Client (relay system)# on the treatment server.

#

JP1/Software Distribution SubManager 07-50 or later can also be used.

2. JP1/CSC - Manager on the management server judges client B to be *Danger*.

JP1/CSC - Manager on the management server compares the inventory information against the judgment policy, and judges client B to be *Danger*.

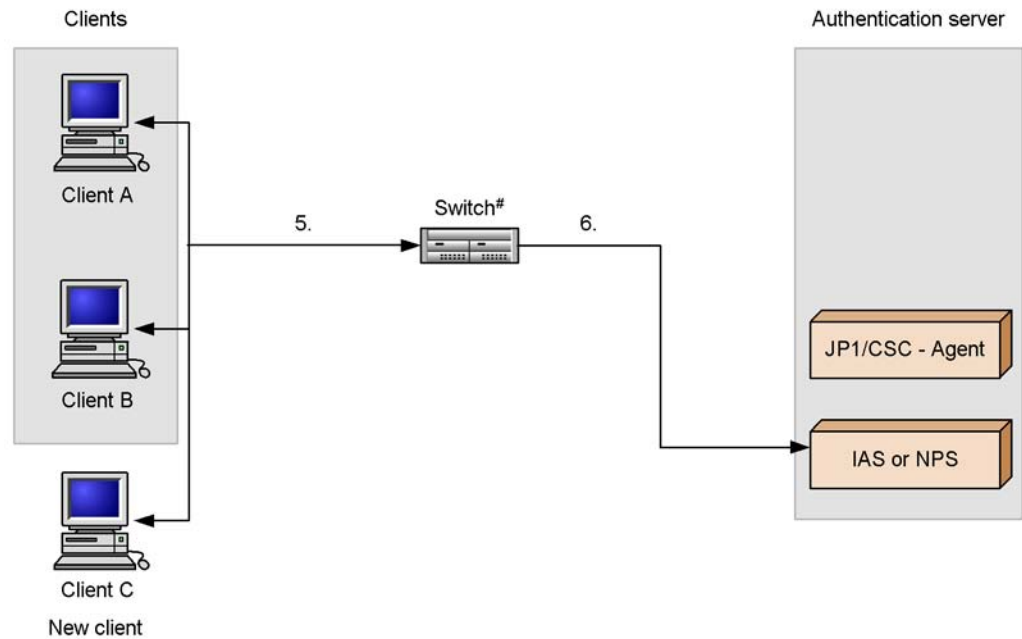
3. JP1/CSC - Manager on the management server instructs JP1/CSC - Agent on the authentication server to permit (client A) and deny (client B) network connections.

Based on the action policy, JP1/CSC - Manager on the management server instructs JP1/CSC - Agent on the authentication server to allow client A access to the network, but deny access for client B.

4. JP1/CSC - Agent on the authentication server updates the connection control list.

JP1/CSC - Agent updates the network control list to reflect the action implemented on JP1/CSC - Manager, by setting client A to *Permit* and client B to *Deny*.

The following figure shows the authentication/inspection process (client authentication).

*Figure 14-20: Authentication/inspection process (client authentication)***Legend:**

IAS or NPS : Microsoft Internet Authentication Service or Network Policy Server

→ : Flow of authentication request

#: Switch supporting MAC authentication

5. The switch starts client authentication.

When the client is restarted or when client network connection that has been disabled is enabled, an authentication request is sent via the switch to Microsoft Internet Authentication Service or Network Policy Server on the authentication server. In addition, the switch requests client authentication based on the maximum connection time set on the switch.

In this example, a new client (client C) will also be added to the network.

6. The switch sends client authentication requests to Microsoft Internet Authentication Service or Network Policy Server on the authentication server.

The switch requests authentication of clients A, B, and C from Microsoft Internet Authentication Service or Network Policy Server on the authentication server.

Clients A, B, and C are authenticated based on their MAC addresses.

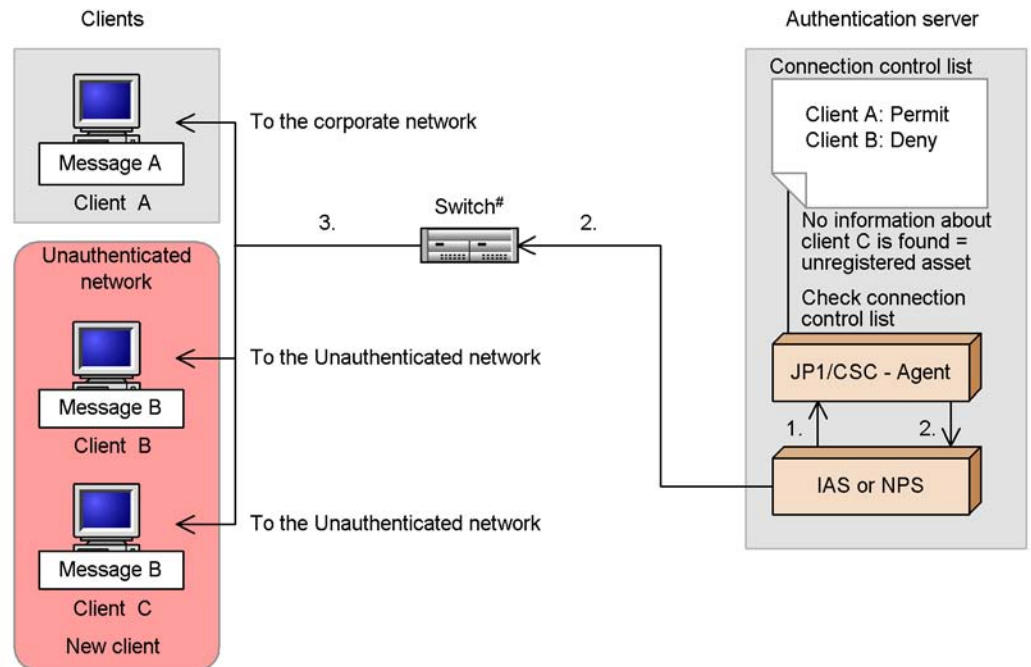


## (2) Isolation process

In the isolation process, client network connections are controlled based on the security policy.

The following figure shows the isolation process.

Figure 14-21: Isolation process



Legend:

IAS or NPS : Microsoft Internet Authentication Service or Network Policy Server

→ : Flow of control

Message A : Message sent when the client is connected to the corporate network.

Message B : Message sent when the client is connected to the unauthenticated network.

#: Switch supporting MAC authentication

1. Microsoft Internet Authentication Service or Network Policy Server on the authentication server requests JP1/CSC - Agent to check the connection control list.

After clients A, B, and C have been authenticated, Microsoft Internet Authentication Service or Network Policy Server on the authentication server

requests JP1/CSC - Agent to check the connection control list.

2. JP1/CSC - Agent on the authentication server checks the connection control list, and returns the client authentication results<sup>#</sup> to Microsoft Internet Authentication Service or Network Policy Server. Microsoft Internet Authentication Service or Network Policy Server then reports the client authentication results to the switch.

JP1/CSC - Agent on the authentication server checks the connection control list for information about clients A, B, and C. In this case, client A is listed as `Permit`, and client B is listed as `Deny`. Because no information about client C is listed in the connection control list, client C is deemed an unregistered asset.

JP1/CSC - Agent returns the authentication results to Microsoft Internet Authentication Service or Network Policy Server.

Microsoft Internet Authentication Service or Network Policy Server reports the received authentication results to the switch.

#

Results of judging whether to permit or deny connection to the corporate network based on the connection control list

3. The switch controls the connection destinations of the clients.

The switch controls the connection destination for each client based on the authentication results received by Microsoft Internet Authentication Service or Network Policy Server on the authentication server.

Client A is connected to the corporate network, and clients B and C are connected to the unauthenticated network. A message is sent to the clients, notifying them of their connection destination.

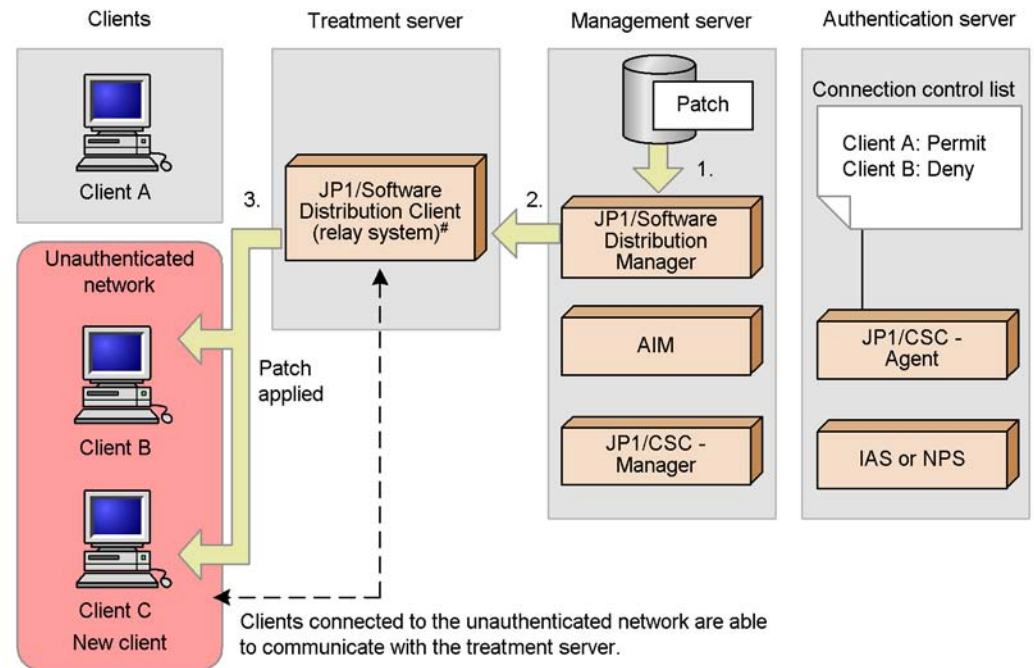
You must now implement security measures on clients B and C, which are connected to the unauthenticated quarantined network.

### **(3) Treatment process**

In the treatment process, security measures are implemented on clients whose network connection is controlled. For details about how to implement security measures on clients, see *14.2.5 Implementing security measures on a client*.

The following figure shows the treatment process.

Figure 14-22: Treatment process



Legend:

IAS or NPS : Microsoft Internet Authentication Service or Network Policy Server

Yellow arrow : Flow of patch

#: JP1/Software Distribution SubManager 07-50 or later may be used instead.

1. The administrator packages the patch and registers the package in JP1/Software Distribution Manager on the management server.  
The administrator packages the patch to be installed and registers the package in JP1/Software Distribution Manager on the management server.
2. JP1/Software Distribution Manager on the management server distributes the patch.  
JP1/Software Distribution Manager on the management server executes a patch distribution job. The patch is transferred to JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server.
3. The patch is remotely installed from JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server to the clients.

Because clients in the unauthenticated network are permitted to communicate with JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server, the patch is installed on the clients from JP1/Software Distribution Client (relay system). Application of the distributed patch implements security measures on the clients.

#

JP1/Software Distribution SubManager 07-50 or later can also be used.

*Reference note:*

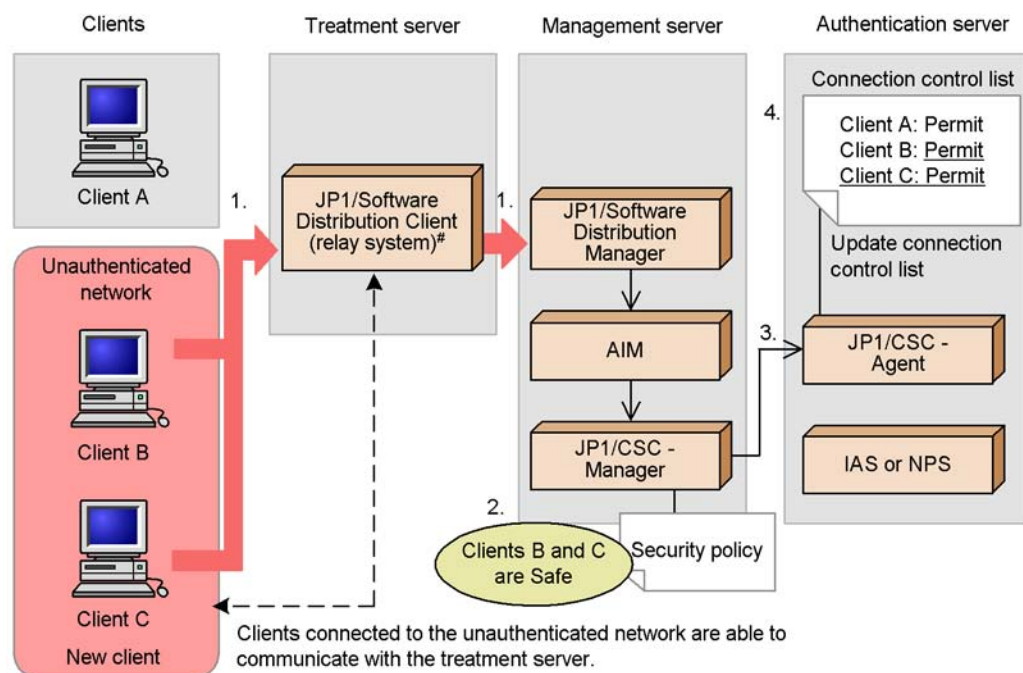
For a client whose network connection is controlled, the client user can also implement security measures by manually selecting and installing packages registered in JP1/Software Distribution Manager on the management server.

**(4) Recovery process**

In the recovery process, clients for which security measures have been implemented are judged and authenticated again, and those judged *Safe* are reconnected to the network.

The following figure shows the recovery process (repeating client judgment).

Figure 14-23: Recovery process (repeating client judgment)



## Legend:

IAS or NPS : Microsoft Internet Authentication Service or Network Policy Server

: Flow of inventory information

: Flow of control

\_ (underline) : Information newly registered in the connection control list

#: JP1/Software Distribution SubManager 07-50 or later may be used instead.

1. Inventory information for the clients is reported to JP1/Software Distribution Manager on the management server via JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server.

After the patch is applied, the latest inventory information for clients B and C is reported to JP1/Software Distribution Manager on the management server via JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server.

#

JP1/Software Distribution SubManager 07-50 or later can also be used.

2. JP1/CSC - Manager on the management server judges clients B and C to be safe.

JP1/CSC - Manager on the management server compares the inventory information against the judgment policy, and finds that all patches are applied. As a result, clients B and C are judged to be *Safe*.

3. JP1/CSC - Manager on the management server instructs JP1/CSC - Agent on the authentication server to permit network connections (for clients B and C).

Based on the action policy, JP1/CSC - Manager on the management server instructs JP1/CSC - Agent on the authentication server to allow clients B and C access to the network.

4. JP1/CSC - Agent on the authentication server updates the connection control list.

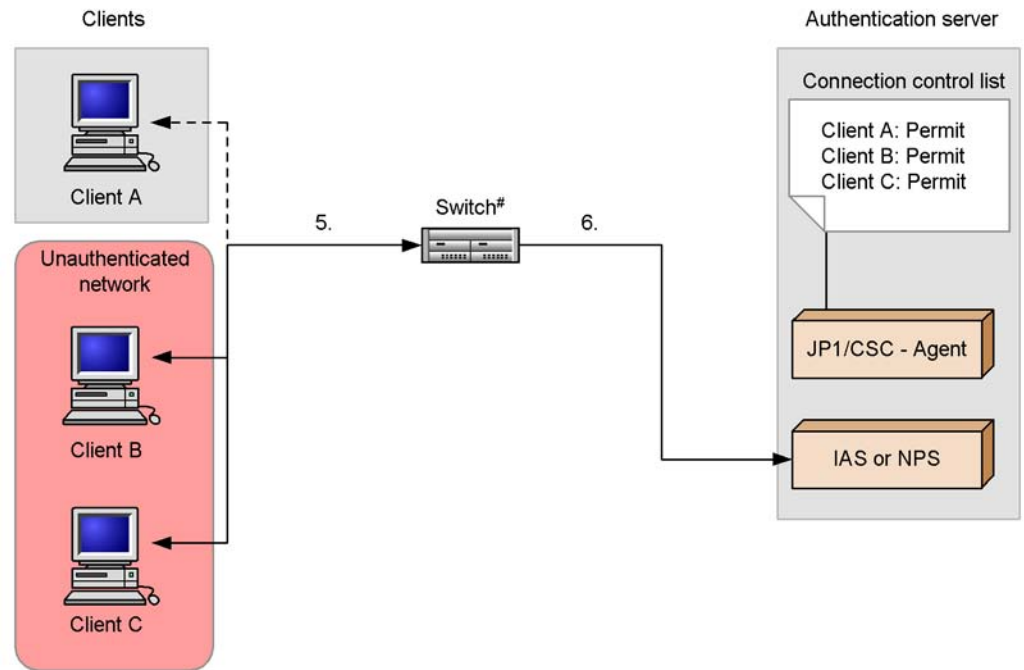
JP1/CSC - Agent on the authentication server updates the connection control list, by implementing an action involving network connection permission.

The existing connection information for client B in the connection control list is changed from *Refuse* to *Permit*.

Because there is no information about client C in the list, JP1/CSC - Agent registers the MAC address and IP address obtained as part of the inventory information for client C, and sets the connection information for client C to *Permit*.

The following figure shows the recovery process (repeating client authentication).

Figure 14-24: Recovery process (repeating client authentication)



## Legend:

IAS or NPS : Microsoft Internet Authentication Service or Network Policy Server

—→ : Flow of authentication request

- - - - -→ : Flow of authentication request at re-authentication of client A

#: Switch supporting MAC authentication

## 5. Client re-authentication starts.

Client re-authentication is performed so that client B and client C can be connected to the corporate network.

When the client is restarted or when client network connection that has been disabled is enabled, an authentication request is sent via the switch to Microsoft Internet Authentication Service or Network Policy Server on the authentication server. In addition, the switch requests client authentication based on the maximum connection time set on the switch.

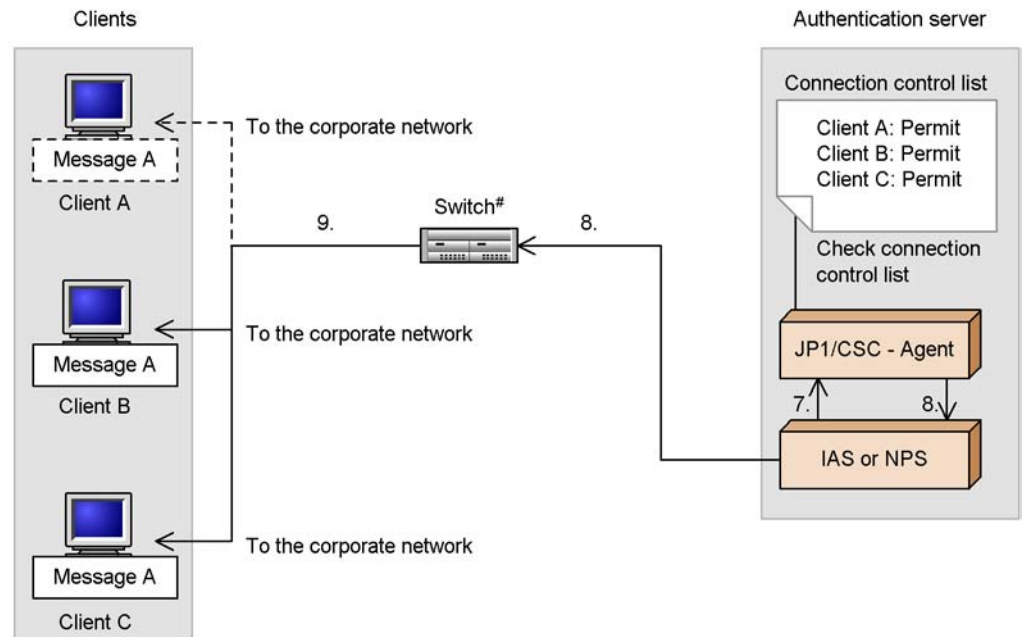
If client authentication is initiated based on the maximum connection time set on the switch, client A will be re-authenticated, as will clients B and C.

6. The switch sends a client authentication request to Microsoft Internet Authentication Service or Network Policy Server on the authentication server.  
The switch requests authentication of clients B and C from Microsoft Internet Authentication Service or Network Policy Server on the authentication server.  
Clients B and C are authenticated based on their MAC addresses. However, the MAC address of client A is not re-authenticated because client A has already been successfully authenticated.

The following figure shows the recovery process (reconnecting clients to the network).



Figure 14-25: Recovery process (reconnecting clients to the network)



## Legend:

IAS or NPS : Microsoft Internet Authentication Service or Network Policy Server

—→ : Flow of control

- - - -&gt; : Flow of authentication request at re-authentication of client A.

Message A	: Message sent when the client is connected to the corporate network.
-----------	---

Message A	: Message sent when client A is re-authenticated.
-----------	---

#: Switch supporting MAC authentication

7. Microsoft Internet Authentication Service or Network Policy Server on the authentication server requests JP1/CSC - Agent to check the connection control list.

When authentication of client B and client C has been completed, Microsoft Internet Authentication Service or Network Policy Server on the authentication server requests JP1/CSC - Agent to check the connection control list.

8. JP1/CSC - Agent on the authentication server checks the connection control list,

and returns the client authentication results to Microsoft Internet Authentication Service or Network Policy Server. Microsoft Internet Authentication Service or Network Policy Server then reports the client authentication results to the switch.

JP1/CSC - Agent on the authentication server checks the connection control list for information about clients B and C. In this case, clients B and C are listed as `Permit`, and client B is listed as `Deny`.

JP1/CSC - Agent reports the authentication results to Microsoft Internet Authentication Service or Network Policy Server. Microsoft Internet Authentication Service or Network Policy Server then reports the authentication results to the switch.

9. The switch switches the connection destinations of the clients.

The switch decides the connection destination for each client based on the authentication results received by Microsoft Internet Authentication Service or Network Policy Server on the authentication server.

Clients B and C are connected to the corporate network, and a message is sent to the clients notifying them of their connection destination. If client authentication is performed based on the maximum connection time set on *the switch*, a message that reports the connection destination network will also be sent to client A.

### 14.2.3 Tasks during operation of a quarantine system linked to an authentication server

This subsection explains the tasks involved in running a quarantine system linked to an authentication server.

The following table lists the tasks.

*Table 14-3: List of quarantine system tasks*

Tasks	Description	Type	Reference
Monitoring clients	Client security levels are judged and action histories are reviewed at the administrator's discretion.	M	8. <i>Monitoring Clients</i>
Implementing actions	Based on instructions from the administrator, clients with high security risk levels are denied access to the network, and clients that are declared safe have their network access restored.	M	9. <i>Dealing with Security Risks</i>

Tasks	Description	Type	Reference
Evaluating client security	The status of security measures is checked for each client, and the adequacy of the security measures for a specific user or group is evaluated based on a points rating.	O	<i>10. Auditing Security</i>
Managing connection control list	Actions related to network connection control are registered in the connection control list. As a result, the network connections of clients that are judged a security risk are controlled according to the information in the connection control list. Administrators must manage the connection control list, and will need to be familiar with its structure.	M	<i>14.2.4 Managing the connection control list</i>
Implementing security measures on clients	Security measures are implemented on clients that have been denied access to the network after being judged a security risk. Security measures are implemented on clients in the quarantined network or unauthenticated network through communication with the treatment server.	M	<i>14.2.5 Implementing security measures on a client</i>
Changing the system configuration	When you add a new client to the network, information about the client is registered in the connection control list.	O	<i>14.2.6 Adding a new client to the network</i>

Tasks	Description	Type	Reference
	When you remove a client from the network while the quarantine system is running, information about the client is deleted from the linked product and the connection control list.	O	<i>14.2.7 Removing clients after operation has started</i>
Managing connection history information for clients	You can manage the connection history of clients subjected to network connection control. This includes information relating to times at which clients were connected to the network, and the network to which they were connected.	O	<i>14.2.8 Managing network connection histories for clients</i>

Legend:

M: Indicates a mandatory task.

O: Indicates an optional task.

#### 14.2.4 Managing the connection control list

A quarantine system linked to an authentication server controls network connections from clients based on the *connection control list* of JP1/CSC - Agent.

This subsection describes the following aspects of the connection control list:

- The contents of the connection control list
- The timing of updates to the connection control list
- Precautions regarding controlling network connections from the connection control list
- Commands for managing the connection control list
- Editing the connection control list

##### (1) *Types of information registered in the connection control list*

Information is registered or updated in the connection control list whenever an action relating to network connection control is implemented. When a client is authenticated, the client's connection destination is determined by the contents of the connection

control list.

The following information in the connection control list can be updated by actions.

- Network connection information

The status of the network connection, as Permit, Deny, or Refuse in the emergency.

- MAC address

The MAC address for managing the client.

- IP address

The IP address for sending notification messages to the client.

The following table lists the contents of the connection control list that are registered or updated by certain actions.

*Table 14-4:* Contents of the connection control list registered or updated by actions

No.	Action	Contents of the connection control list			
		Registered as Permit	Registered as Deny	Registered as Refuse in the emergency	Not registered
1	Permit network connections	Connection information is unchanged. If the IP address has changed, the new address is recorded.	Connection information is changed from Deny to Permit. If the IP address has changed, the new address is recorded.	Connection information is changed from Refuse in the emergency to Permit. If the IP address has changed, the new address is recorded.	The MAC address and IP address are added, and the connection information is registered as Permit.
2	Deny network connections	Connection information is changed from Permit to Deny. If the IP address has changed, the new address is recorded.	Connection information is unchanged. If the IP address has changed, the new address is recorded.	Connection information is unchanged. If the IP address has changed, the new address is recorded.	The MAC address and IP address are added, and the connection information is registered as Deny.

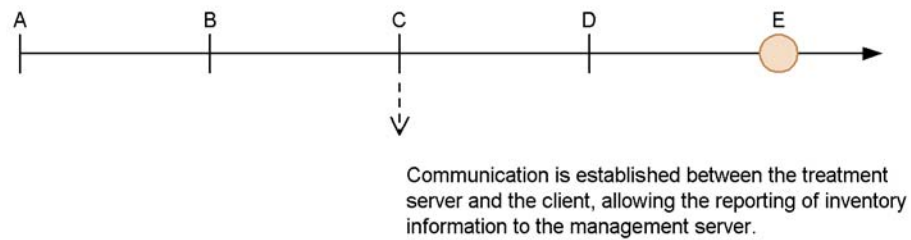
No.	Action	Contents of the connection control list			
		Registered as Permit	Registered as Deny	Registered as Refuse in the emergency	Not registered
3	Implement emergency denial of network connections	Connection information is changed from Permit to Refuse in the emergency. If the IP address has changed, the new address is recorded.	Connection information is unchanged. If the IP address has changed, the new address is recorded.	Connection information is unchanged. If the IP address has changed, the new address is recorded.	The MAC address and IP address are added, and the connection information is registered as Refuse in the emergency.

## (2) When the connection control list is updated

The connection control list is updated when an action is implemented as a result of a security level judgment. However, clients cannot notify the management server of the latest inventory information, since they are unable to connect to the network until authenticated by the authentication server.

The following figure shows the timing at which the connection control list is updated.

Figure 14-26: Timing of updates to connection control list



- A: The client attempts to connect to the network (authentication is initiated).
- B: The client is authenticated by the authentication server.
- C: The client is connected to the corporate, quarantined, or unauthenticated network.
- D: JP1/CSC - Manager on the management server judges the security level of the client, and executes the appropriate action.
- E: The connection control list is updated.

Legend:

→ : Flow of time

○ : Timing of update to connection control list

As shown above, the connection control list is updated with the latest inventory information after the client is connected to the network.

*Note:*

At the next authentication, network connection control is performed based on the latest inventory information.

**(3) Notes on network connection control based on the connection control list**

Control of network connection from a client based on the connection control list is performed when the client is successfully authenticated by IEEE 802.1X or MAC authentication.

After the client has been authenticated, network connection control is automatically applied to the client user. Therefore, we recommend that you specify the following two settings for client user notifications:

Set up an action policy to send notification messages to client users.

Set up an action policy to send messages alerting users that security measures must be implemented, when the client security level is *Warning* or *Caution*. For example, if you want to send notification messages to clients whose security level is *Caution*, specify the following settings in the action policy:

- Select **Send message to user in the Notification to PC user area**.
- Select **Permit connection in the Control PC network connection area**.

Remember to set the action policy to permit connections. If you fail to do so, the action policy will not update the connection control list.

For details, see *6.10 Setting an action for each security level*, and *6.12 Editing a client user notification message*.

Set the message notification information in JP1/CSC - Agent setup.

In the action policy's message notification information, set message notification to **Notify**, and set messages informing users that their connection destination has been changed and what action they should take.

For details, see *13.2.2(4)(b) Operations that can be performed on the IAS page*.

You cannot use message notification when JP1/CSC - Agent is running on Windows Server 2008.

*Note:*

Do not set message notification information in JP1/CSC - Agent setup if your network environment includes a DHCP server.

By default, message notification is performed using the IP address of the client. If the network environment includes a DHCP server, messages may inadvertently be sent to the wrong client.

**(4) Commands for managing the connection control list**

The following table lists the commands used to manage the connection control list.

*Table 14-5: Connection control list management commands*

No.	Command	Description
1	<code>cscrexport</code>	Exports a connection control list to a CSV file. You can use the exported file to check the contents of the connection control list and edit client information.
2	<code>cscrimport</code>	Imports an exported file created by the administrator, or a connection control list exported by the <code>cscrexport</code> command, into JP1/CSC - Agent. Use this command to import a connection control list you edited as a CSV text file, or to restore the connection control list from a backup.
3	<code>cscrdelete</code>	Deletes client information from the connection control list. Use this command when you want to remove a client from the network.

For details about how to use these commands, see *15. Commands*.

**(5) Editing the connection control list**

Ordinarily the connection control list is updated by JP1/CSC - Agent on the authentication server. However, administrators can also create and edit connection control lists as text files in CSV format.

When you have created a connection control list, you can import the data using the `cscrimport` command. For details about the connection control list and its format, see *16.16 Import file*.

**14.2.5 Implementing security measures on a client**

When a client is judged a security risk and denied access to the network, security measures must be implemented on the client.

Clients whose network connections are being controlled are connected to the network specified for the **Connection information for refused asset** attribute in JP1/CSC - Agent setup.

When **Connection information for refused asset** is set to **Quarantined**:

Security measures are implemented on the client in the quarantined network.



When **Connection information for refused asset** is set to **Unauthenticated**:

Security measures are implemented on the client in the unauthenticated network.

When **Connection information for refused asset** is set to **Refused**:

Security measures are implemented on the client in an offline environment.

This subsection describes the procedures for each setting.

### **(1) Implementing security measures for clients in the quarantined or unauthenticated network**

Security measures for a client connected to the quarantined or unauthenticated network are implemented through communication with the treatment server from the quarantined or unauthenticated network.

By using the software distribution facility of JP1/Software Distribution, the administrator can distribute software from JP1/Software Distribution Manager on the management server, using JP1/Software Distribution Client (relay system) or JP1/Software Distribution SubManager on the treatment server as a relay system. Alternatively, the client can be provided with packages for the user to install.

For details about the software distribution facility of JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

*Reference note:*

You can also use SUS or an anti-virus product installed on the treatment server to implement security measures on clients.

### **(2) Implementing client security measures in an offline environment**

You can implement security measures on clients that are denied access to the network by using the offline machine management facility of JP1/Software Distribution.

This facility allows you to install software offline and obtain inventory information from offline machines.

For details about the offline machine management facility of JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

## **14.2.6 Adding a new client to the network**

Before you can add a client to the network, information about the client must be registered in the client control list for JP1/CSC - Agent.

When a client is first introduced into the network, it is treated as an unregistered asset because no information about it is found in the connection control list. In this case, the client is connected to the network specified by the **Connection information for**

**unregistered asset** setting in JP1/CSC - Agent setup.

The following explains the operations you need to perform for each of the **Connection information for unregistered asset** settings (**Quarantined**, **Rejected**, **Normal**, and **Unauthenticated**).

*Note:*

You cannot use the function for registering permitted PCs to add clients to the network.

#### (a) When Quarantined is set

The client is connected to the quarantined network, where security measures are implemented on the client. The client is then connected to the corporate network.

To connect an unregistered client to the corporate network:

1. Initiate client authentication.

An authentication request is sent to the authentication server via the switch when the client is restarted, when the Windows standard supplicant service is restarted, or when client network connection that has been disabled is enabled. Note that if sending of EAPOL-START packets is not enabled, the switch requests client authentication at the authentication interval that is set on the switch.

Because **Connection information for unregistered asset** is set to **Quarantined**, the client is connected to the quarantined network.

2. Implement security measures on the client by communicating with the treatment server.

Security measures can be implemented on clients in the quarantined network, by communicating with the treatment server.

By using the software distribution facility of JP1/Software Distribution, the administrator can distribute software from JP1/Software Distribution Manager on the management server, using JP1/Software Distribution Client (relay system) on the treatment server as a relay system. Alternatively, the client can be provided with packages for the user to install.

For details about the software distribution facility of JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

When client inventory information is updated, the latest inventory information is reported to JP1/Software Distribution Manager running on the management server, via JP1/Software Distribution Client (relay system)<sup>#</sup> running on the treatment server.

When the client is judged safe based on the judgment policy by JP1/CSC -

Manager on the management server, an action (to permit a network connection) is implemented according to the action policy. The client information is then recorded as `Permit` in the JP1/CSC - Agent connection control list.

#

JP1/Software Distribution SubManager 07-50 or later can also be used.

### 3. Re-authenticate the client.

An authentication request is sent to the authentication server via the switch when the client is restarted, when the Windows standard supplicant service is restarted, or when client network connection that has been disabled is enabled. Note that if sending of EAPOL-START packets is not enabled, the switch requests client authentication at the authentication interval that is set on the switch.

After security measures have been completed, the client is registered as `Permit` in the connection control list of JP1/CSC - Agent on the authentication server, and can then connect to the corporate network.

## (b) When Rejected is set

The client cannot connect to the network. Use the offline machine management functionality provided by JP1/Software Distribution to implement security measures on the client. The client can then connect to the corporate network.

To connect a rejected client to the corporate network:

### 1. Initiate client authentication.

An authentication request is sent to the authentication server via the switch when the client is restarted, when the Windows standard supplicant service is restarted, or when client network connection that has been disabled is enabled. Note that if sending of EAPOL-START packets is not enabled, the switch requests client authentication at the authentication interval that is set on the switch.

Because **Connection information for unregistered asset** is set to **Refused**, the client cannot connect to the network.

### 2. Use the offline machine management functionality of JP1/Software Distribution to implement security measures on the client.

You can use the offline machine management functionality of JP1/Software Distribution to implement security measures on a client in an offline environment. The offline machine management functionality allows you to install software offline, and obtain inventory information from offline machines.

For details about the offline machine management functionality of JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

The inventory information obtained from the offline machine is sent to JP1/

Software Distribution Manager on the management server, and the client is judged by JP1/CSC - Manager.

If the client is judged safe based on the security policy, an action (to permit a network connection) is implemented according to the action policy. The client information is then recorded as `Permit` in the JP1/CSC - Agent connection control list.

3. Re-authenticate the client.

An authentication request is sent to the authentication server via the switch when the client is restarted, when the Windows standard supplicant service is restarted, or when client network connection that has been disabled is enabled. Note that if sending of EAPOL-START packets is not enabled, the switch requests client authentication at the authentication interval that is set on the switch.

After security measures have been completed, the client is registered as `Permit` in the connection control list of JP1/CSC - Agent on the authentication server, and can then connect to the corporate network.

**(c) When Normal is set**

The client can already connect to the corporate network, and no special measures are necessary.

However, ensure that security measures have been implemented on the client before it connects to the network.

**(d) When Unauthenticated is set**

To connect the client to the corporate network:

1. Initiate client authentication.

When the client is restarted or client network connection that has been disabled is enabled, an authentication request is sent to the authentication server via the switch. Note, however, that if sending of EAPOL-START packets for IEEE 802.1X authentication is not set, the switch requests client authentication at the authentication interval that is set on the switch. If MAC authentication is used, the switch requests client authentication based on the maximum connection time set on the switch.

Because **Unauthenticated** is set for **Connection information for unregistered asset**, the client is connected to the unauthenticated network.

2. Implement security measures on the client by communicating with the treatment server.

Security measures for a client connected to the unauthenticated network are implemented through communication with the treatment server from the unauthenticated network.

When the software distribution function of JP1/Software Distribution is used, JP1/Software Distribution Client (relay system)<sup>#</sup> on the treatment server can be used as a relay system. The relay system allows the administrator to distribute software from JP1/Software Distribution Manager on the management server or allows the client user to install a package.

For details about the software distribution function of JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

When the client inventory is updated, the latest inventory information is reported to JP1/Software Distribution Manager on the management server via JP1/Software Distribution Client (relay system)<sup>#</sup>.

JP1/CSC - Manager on the management server judges whether the client is safe based on the judgment policy. If the client is judged safe, action (permit network connection) is performed according to the action policy settings. At this time, *Permitted* is registered as client information in the connection control list of JP1/CSC - Agent.

#

JP1/Software Distribution SubManager 07-50 or later can also be used.

### 3. Re-authenticate the client.

When the client is restarted or client network connection that has been disabled is enabled, an authentication request is sent to the authentication server via the switch. Note, however, that if sending of EAPOL-START packets for IEEE 802.1X authentication is not set, the switch requests client authentication at the authentication interval that is set on the switch. If MAC authentication is used, the switch requests client authentication based on the maximum connection time set on the switch.

After security measures have been completed, the client is registered as *Permit* in the connection control list of JP1/CSC - Agent on the authentication server, and is able to connect to the corporate network.

## 14.2.7 Removing clients after operation has started

After you have started operations with your quarantined system, the removal of clients because of asset disposal or other reasons can be performed in either of the following ways:

- With automatic denial of network connection enabled
- With automatic denial of network connection disabled

**(1) With automatic denial of network connection enabled**

1. In JP1/CSC - Manager setup, enable network connections to be denied automatically when a client is removed from the network.

To automatically deny network connections when a client is removed, specify the following setting in the Client Security Control - Manager Setup dialog box:

- In the **Basic Settings** page, under **Asset deletion information**, set the **Automatic refusal of network connection** attribute to **Execute**.

2. Remove the client.

The client is automatically denied connection to the network in the connection control list of JP1/CSC - Agent.

3. In the Device List window of AIM, select the asset information of the client you want to remove, and set the device status to **Erase**.

For details about how to set the device status to **Erase**, see the manual *Job Management Partner 1/Asset Information Manager Administrator's Guide*.

Note that if the management server is configured using Asset Information Manager Subset Component of JP1/Software Distribution Manager, this step is unnecessary because the device status changes to **Erase** as soon as you remove the client.

4. Use the data maintenance task to delete asset information with the **Erase** status.

For details about data maintenance, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

5. Execute the `cscrdelete` command.

The network connection information, MAC address and IP address of the client you want to remove is deleted from the connection control list of JP1/CSC - Agent. For details about the `cscrdelete` command, see *cscrdelete (deletes information about a specified client from the connection control list)* in 15. *Commands*.

**(2) With automatic denial of network connection disabled**

1. In JP1/CSC - Manager setup, prevent network connections from being denied automatically when a client is removed from the network.

To prevent network connections from being denied automatically when a client is removed, specify the following setting in the Client Security Control - Manager Setup dialog box:

- In the **Basic Settings** page, under **Asset deletion information**, set the **Automatic refusal of network connection** attribute to **Do not execute**.

2. In the PC List window of the Client Security Management window, select the

client you want to remove. Then, in **Network connection**, click the **Refuse** button.

The client control list of JP1/CSC - Agent is updated to indicate that the client is to be denied connection to the network.

3. Remove the client.
4. In the Device List of AIM, select the asset information of the client you removed, and set the device status to **Erase**.

For details about how to set the device status to **Erase**, see the manual *Job Management Partner 1/Asset Information Manager Administrator's Guide*.

Note that if the management server is configured using Asset Information Manager Subset Component of JP1/Software Distribution Manager, this step is unnecessary because the device status changes to **Erase** as soon as you remove the client.

5. Use the data maintenance task to delete asset information with the **Erase** status.

For details about data maintenance, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

6. Execute the `cscrdelete` command.

The network connection information, MAC address and IP address of the client you want to remove is deleted from the connection control list of JP1/CSC - Agent. For details about the `cscrdelete` command, see *cscrdelete (deletes information about a specified client from the connection control list)* in 15. *Commands*.

### 14.2.8 Managing network connection histories for clients

You can use a *connection history file* to manage client connection histories. By periodically reviewing client connection files, the administrator can retroactively manage the status of client network connections.

Because connection history files are in CSV format, you can easily compile statistical data by importing the file into a spreadsheet application. You can use this ability to audit client network connection logs.

The following table shows the folder where connection history files are created, and the file names given to the files.

*Table 14-6:* Folder and file name of connection history file

Folder name	File name
<i>JP1/CSC - Agent-installation-folder</i> \radius\log	cscracslog*.log <sup>#</sup>

**Legend:**

*installation-folder*: The folder in which you installed JP1/CSC -Agent. The default installation folder for JP1/CSC - Agent is as follows (when the OS is installed under C:\):

For Windows Server 2003 (x64):

C:\Program Files(x86)\HITACHI\jplnetmcsca

For other OSs:

C:\Program Files\HITACHI\jplnetmcsca

#

The asterisk (\*) indicates the connection history file number from 1 to 999.

**Number of connection history files** can be specified in the **IAS** page of the JP1/CSC - Agent Setup dialog box.

For details about how to set the number of connection history files, see *13.2.2(4)(b) Operations that can be performed on the IAS page*.

A connection history file contains connection history records. The format of a connection history file and the items in a connection history record are as follows:

Format of connection history file

```
Connection-history-name-record ↓
Connection-history-record ↓
Connection-history-record ↓
:
:
```

Legend: ↓: Line feed code

Items in a connection history record

Connection history records are output in CSV format. The items in a connection history record appear in the order shown in the following table:

*Table 14-7: Items written in a connection history record*

No.	Item	Description
1	TIME	The date and time when the client connected to the network, in the format <i>YYYYMMDDhhmmss.nnn</i> . Example: November 15th 2005, 13:50:55.111 20051115135055.111



No.	Item	Description
2	MAC	The MAC address of the client PC. Example: If the MAC address is 00-00-E2-70-15-11 00:00:E2:70:15:11
3	IP	The IP address of the client PC. Example: If the IP address is 192.168.2.1 192.168.2.1
4	STAT	The type of network to which the client was connected (one of the following constants): <ul style="list-style-type: none"> <li>• Normal (corporate network)</li> <li>• Quarantine (quarantined network)</li> <li>• Refused (denied connection to the network)</li> <li>• Unauthorized (unauthenticated network)</li> </ul>
5	VLAN	The VLAN-ID of the network to which the client was connected, as a value from 1 to 4095. Note that NULL is recorded if the client was connected to the unauthenticated network.

---

## 14.3 Operating a quarantine system linked to JP1/Software Distribution (AMT Linkage facility)

---

This section describes how to operate a quarantine system linked to JP1/Software Distribution (AMT Linkage facility).

### 14.3.1 Example of quarantine system operation linked to JP1/Software Distribution (AMT Linkage facility)

The example below describes the operation of a quarantine system linked to JP1/Software Distribution (AMT Linkage facility) in terms of the quarantine process.

This example is based on the following assumptions:

- Managed clients

Of the clients, A, B, and C, only client C is found to have an unapplied patch.

- Security policy (judgment policy) setting

The security level for clients with unapplied patches is judged to be *Danger*.

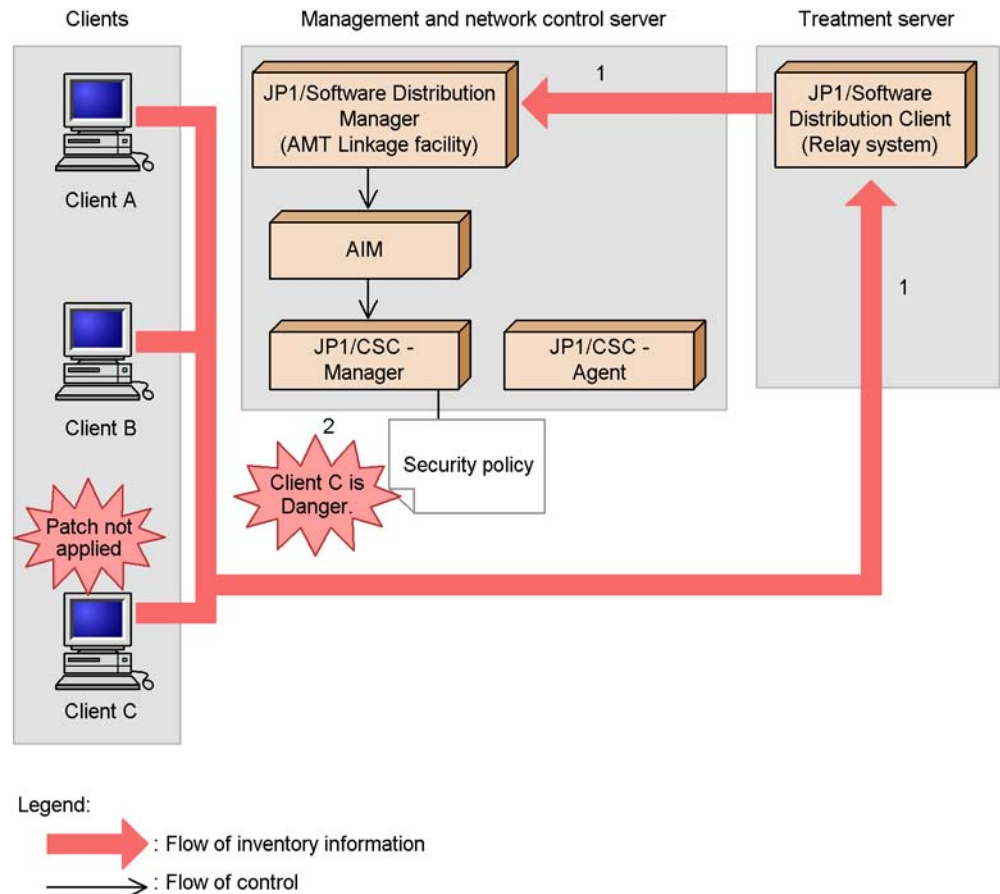
- Security policy (action policy) settings

- Clients whose security level is *Danger* are denied access to the network.
- Clients whose security level is *Safe* are permitted access to the network.

#### **(1) Inspection process**

In the inspection process, clients that are a security risk are identified, and clients are authenticated. The following figure shows the inspection process.

Figure 14-27: Inspection process



1. Inventory information for clients is reported to JP1/Software Distribution Manager on the management and network control server via JP1/Software Distribution Client (relay system) on the treatment server.

The inventory information for clients A, B, and C is reported to JP1/Software Distribution Manager on the management and network control server via JP1/Software Distribution Client (relay system) on the treatment server.

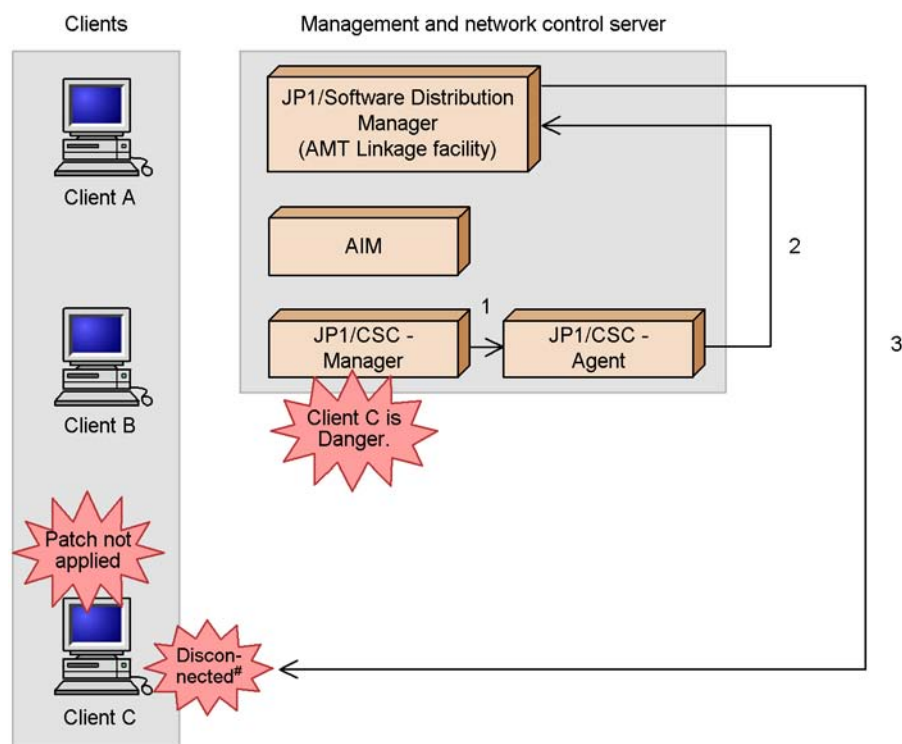
2. JP1/CSC - Manager on the management and network control server judges the security level of client C to be *Danger*.

JP1/CSC - Manager on the management and network control server compares the inventory information against the judgment policy, and judges the security level of client C to be *Danger*.

**(2) Isolation process**

In the isolation process, client network connections are controlled based on the security policy. The following figure shows the isolation process.

Figure 14-28: Isolation process



Legend:

→ : Flow of control

# Specific ports (such as JP1/Software Distribution ports) are not disconnected.

1. JP1/CSC - Manager on the management and network control server instructs JP1/CSC - Agent to deny network connections.  
Based on the action policy, JP1/CSC - Manager on the management and network control server instructs JP1/CSC - Agent to deny connections.
2. JP1/CSC - Agent on the management and network control server instructs JP1/Software Distribution Manager to deny client C network connections.
3. The AMT Linkage facility of JP1/Software Distribution Manager denies client C

network connections.

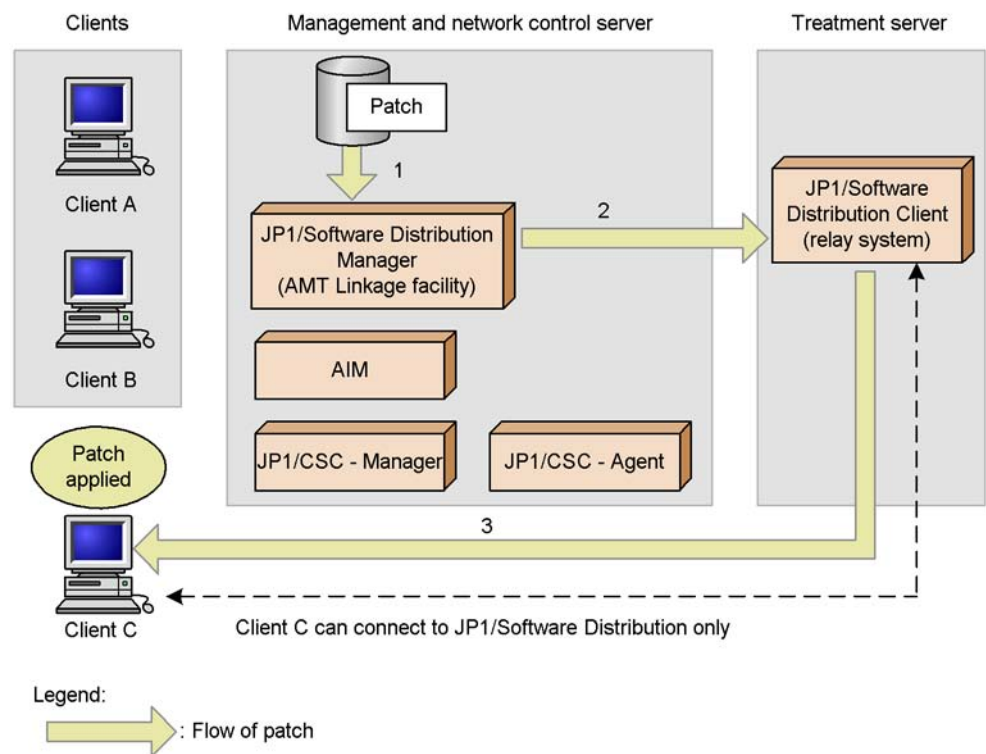
Communication with client C is disconnected, except for specific ports such as JP1/Software Distribution ports.

### (3) Treatment process

In the treatment process, security measures are implemented on clients denied access to the network. For details about how to implement security measures on clients, see *14.3.3 Implementing client security measures*.

The following figure shows the treatment process.

Figure 14-29: Treatment process



1. Package the patch and register it in JP1/Software Distribution Manager on the management and network control server.  
Package the patch to be installed and register it in JP1/Software Distribution Manager on the management and network control server.
2. Distribute the patch from JP1/Software Distribution Manager on the management and network control server.

In JP1/Software Distribution Manager on the management and network control server, execute the patch distribution job. The patch is transferred to JP1/Software Distribution Client (relay system) on the treatment server.

3. Remotely install the patch on client C from JP1/Software Distribution Client (relay system) on the treatment server.

The patch is installed on client C from JP1/Software Distribution Client (relay system) on the treatment server. Security measures are implemented on client C with the application of the distributed patch.

*Reference note:*

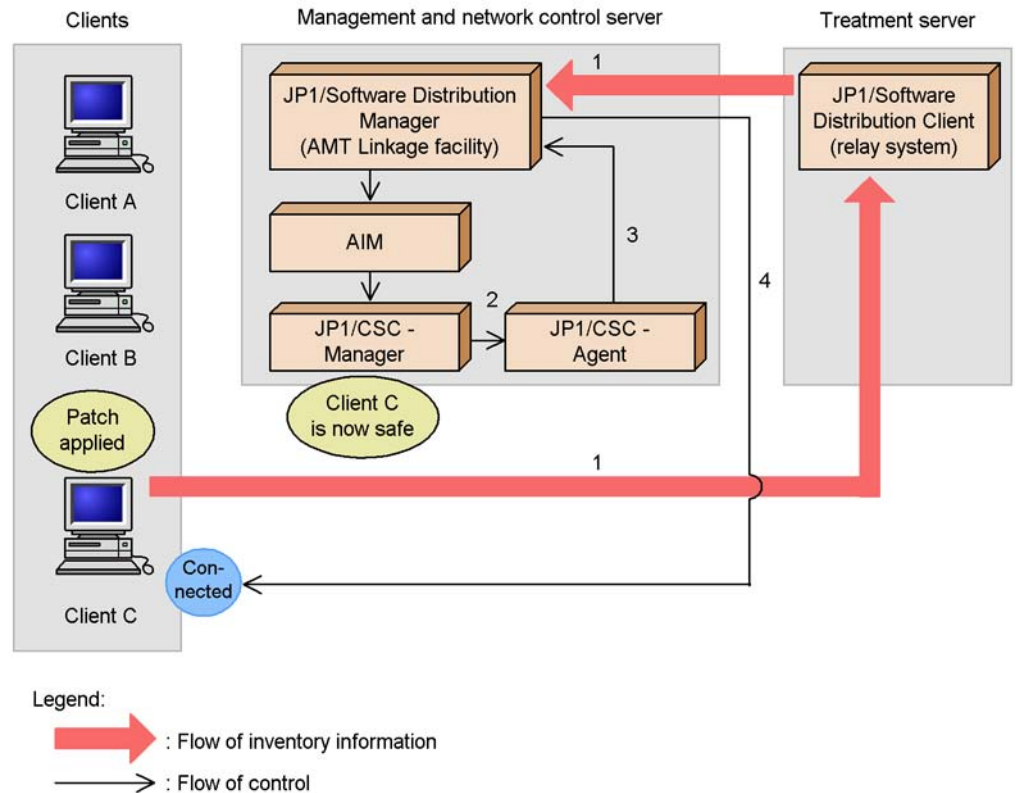
The client user can also implement security measures on a client denied access to the network by manually selecting and installing packages registered with JP1/Software Distribution Manager on the management and network control server.

**(4) Recovery process**

In the recovery process, clients for which security measures have been implemented are judged again, and those judged *Safe* are reconnected to the network.

The following figure shows the recovery process.

Figure 14-30: Recovery process



1. Inventory information for client C is reported to JP1/Software Distribution Manager on the management and network control server via JP1/Software Distribution Client (relay system) on the treatment server.

After the patch is applied, the latest inventory information for client C is reported to JP1/Software Distribution Manager on the management and network control server via JP1/Software Distribution Client (relay system) on the treatment server.

2. JP1/CSC - Manager on the management and network control server judges client C to be *Safe*, and instructs JP1/CSC - Agent to permit a network connection.

JP1/CSC - Manager on the management and network control server compares the inventory information against the security policy, and finds that all patches have been applied. As a result, the security level of the client C is judged to be *Safe*. JP1/CSC - Manager on the management and network control server then instructs JP1/CSC - Agent to permit a network connection based on the action policy.

3. JP1/CSC - Agent on the management and network control server instructs JP1/

Software Distribution Manager to permit a network connection for client C.

4. The AMT Linkage facility of JP1/Software Distribution Manager permits a network connection for client C.

This allows client C to access the network.

### 14.3.2 Tasks during operation of a quarantine system linked to JP1/Software Distribution (AMT Linkage facility)

This subsection explains the tasks involved in running a quarantine system linked to JP1/Software Distribution (AMT Linkage facility).

The following table lists the tasks.

*Table 14-8: List of quarantine system tasks*

Tasks	Description	Type	Reference
Monitoring clients	Client security levels are judged and action histories are reviewed at the administrator's discretion.	M	8. <i>Monitoring Clients</i>
Implementing actions	Based on instructions from the administrator, clients with high security risk levels are denied access to the network, and clients that are declared safe have their network access restored.	M	9. <i>Dealing with Security Risks</i>
Evaluating client security	The status of security measures is checked for each client, and the adequacy of the security measures for a specific user or group is evaluated based on a points rating.	O	10. <i>Auditing Security</i>
Implementing security measures on clients	Security measures are implemented on clients that have been denied access to the network after being judged a security risk. Security measures are implemented on clients in an online environment through communication with the treatment server.	M	14.3.3 <i>Implementing client security measures</i>



Tasks	Description	Type	Reference
Changing the system configuration	No special tasks are required on the quarantine system. A new client is added to the network.	O	<i>14.3.4 Adding new clients to the network</i>
	When you remove a client from the network while the quarantine system is running, the client is denied access to the network.	O	<i>14.3.5 Removing a client after operation has started</i>

Legend:

M: Indicates a mandatory task.

O: Indicates an optional task.

### 14.3.3 Implementing client security measures

When a client is judged to be a security risk and denied access to the network, security measures must be implemented on the client.

Security measures can be implemented on a client that is denied access to the network by executing the software distribution facility of JP1/Software Distribution.

By using this facility, the administrator can distribute software from JP1/Software Distribution Manager on the management and network control server, using JP1/Software Distribution Client (relay system) on the treatment server as a relay system. Alternatively, the client can be provided with packages for the user to install.

For details about the software distribution facility, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows systems.

### 14.3.4 Adding new clients to the network

When you add a new client to the network after starting operations with your quarantine system, inventory information for the new client is reported to the management and network control server via JP1/Software Distribution Client (relay system) on the treatment server. Then the security level of the client is judged.

If the client is judged to be *Safe*, the added client is permitted to connect to the network.

### 14.3.5 Removing a client after operation has started

After your quarantine system has begun operation, the removal of clients for asset disposal or other reasons can be performed in either of the following ways:

- With automatic denial of network connection enabled

- With automatic denial of network connection disabled

**(1) With automatic denial of network connection enabled**

1. In JP1/CSC - Manager setup, enable the automatic denial of network connections when a client is removed from the network.

To automatically deny network connections when a client is removed, enter the following setting in the Client Security Control - Manager Setup dialog box:

- In the **Basic Settings** page, under **Asset deletion information**, set the **Automatic refusal of network connection** attribute to **Execute**.

2. Remove the client.

The AMT Linkage facility of JP1/Software Distribution Manager automatically denies the client connection to the network.

3. In the Device List window of AIM, select the asset information of the client you removed, and set the device status to **Erase**.

For details about how to set the device status to **Erase**, see the manual *Job Management Partner 1/Asset Information Manager Administrator's Guide*.

Note that if Asset Information Manager Subset Component of JP1/Software Distribution Manager has been used to configure the management and network control server, this step is unnecessary because the device status changes to **Erase** as soon as you remove the client.

4. Use the data maintenance task to delete asset information with the **Erase** status.

For details about data maintenance, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

**(2) With automatic denial of network connection disabled**

1. In JP1/CSC - Manager setup, prevent network connections from being denied automatically when a client is removed from the network.

To prevent network connections from being denied automatically when a client is removed, specify the following setting in the Client Security Control - Manager Setup dialog box:

- In the **Basic Settings** page, under **Asset deletion information**, set the **Automatic refusal of network connection** attribute to **Do not execute**.

2. In the PC List window of the Client Security Management window, select the client you want to remove. Then, in **Network connection**, click the **Refuse** button.

The AMT Linkage facility of JP1/Software Distribution Manager denies the client connection to the network.

3. Remove the client.
4. In the Device List window of Asset Information Manager, select the asset information of the client you removed, and set the device status to **Erase**.

For details about how to set the device status to **Erase**, see the manual *Job Management Partner 1/Asset Information Manager Administrator's Guide*.

Note that if Asset Information Manager Subset Component of JP1/Software Distribution Manager has been used to configure the management and network control server, this step is unnecessary because the device status changes to **Erase** as soon as you remove the client.

5. Use the data maintenance task to delete asset information with the **Erase** status.

For details about data maintenance, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.



## **Chapter**

---

# **15. Commands**

---

This chapter describes the commands provided by JP1/CSC and their use.

List of commands  
Command details

---

## List of commands

---

The following table lists the commands that can be used with JP1/CSC.

*Table 15-1: List of JP1/CSC commands*

Command name	Description	Server for execution	Required Permission
cscaction	Implements actions for a specified client based on the result of the latest security level judgment.	JP1/CSC - Manager	Administrator
cscassign	Assigns security policies to clients.	JP1/CSC - Manager	Administrator
cscexportcount	Outputs statistics for specified groups to a file in CSV format. Statistics can be output from a number of different perspectives.	JP1/CSC - Manager	Administrator
cscexportplist	Outputs PC list information (asset information and judgment results for clients whose security levels were judged on the specified date) to a CSV file.	JP1/CSC - Manager	Administrator
cscjudge	Judges security levels.	JP1/CSC - Manager	Administrator
cscnetctrl	Permits or immediately blocks network connections by a specified client.	JP1/CSC - Manager Remote Option	Administrator
cscnwmaintenance	Maintains a list of permitted devices for JP1/NM - Manager.	JP1/CSC - Manager	Administrator
cscpatchupdate	Updates patch information in judgment policies registered in JP1/CSC - Manager that relate to security updates.	JP1/CSC - Manager	Administrator
cscpolexport	Outputs judgment policy settings to a text file.	JP1/CSC - Manager	Administrator
cscpolimport	Updates judgment policy settings.	JP1/CSC - Manager	Administrator

<b>Command name</b>	<b>Description</b>	<b>Server for execution</b>	<b>Required Permission</b>
cscrdelete	Deletes information about a specified client from the connection control list.	JP1/CSC - Agent	Administrator
cscrexport	Exports a connection control list.	JP1/CSC - Agent	Administrator
cscrimport	Imports a connection control list.	JP1/CSC - Agent	Administrator
cscsetup	Sets up JP1/CSC - Manager.	JP1/CSC - Manager	Administrator
cscstorecount	Stores statistical information in the asset management database about the status of security measures for individual groups.	JP1/CSC - Manager	Administrator
Command used in a user-defined action	A command executed as a user-defined action. This command is created by an administrator.	JP1/CSC - Manager	Administrator

---

## Command details

---

This section explains the directory in which commands are stored, as well as the format and order in which commands are explained.

### Command directory

The directory for JP1/CSC commands is as follows:

*JP1/CSC - Manager-installation-folder\bin*

### Format of command explanation

The subsections used when explaining each command are as follows:

#### Function

Explains the command function.

#### Format

Explains the command format.

#### Server for execution

Indicates the server on which the command can be executed.

#### Required permissions

Indicates the permissions required to execute the command.

#### Command directory

Indicates the location in which the command resides.

#### Arguments

Explains the command arguments.

#### Notes

Explains any notes.

#### Output messages

Explains the messages displayed on the standard output or standard error output in response to a command input. Note that messages indicating that the system administrator should be contacted indicate that the administrator should take appropriate action, or contact the appropriate Hitachi party.

#### Return values

Explains the values returned by the command.

Note that some items may not be explained for some commands. For example,



arguments are not explained for commands without arguments.

### **Order of command explanations**

The commands are listed in alphabetical order.

---

## cscaction (implements actions for a specified client)

---

### Function

This command implements actions for a specified client based on the result of the latest security level judgment.

The clients for which actions are to be implemented can be specified in any of three ways:

- Specify the name of an asset number file so that actions are implemented for the clients corresponding to the asset numbers specified in the file.
- Specify the name of a search condition file so that actions are implemented for the clients belonging to the groups specified in the file.
- Specify all clients as the target of the actions.

The name of an action policy used for implementing actions can also be specified.

### Format

```
cscaction {-f asset-number-file-name|-k search-condition-file-name|-all} [-a action-policy-name] [-ns]
```

### Server for execution

JP1/CSC - Manager

### Required permissions

Administrator permissions

### Command directory

*JP1/CSC - Manager-installation-folder*\bin

### Arguments

- -f *asset-number-file-name*

Specify by full path the name of the asset number file containing the asset numbers of the clients for which actions are to be implemented. When this argument is specified, actions are implemented for only those clients specified in the file.

Create the asset number file with any file name in any directory on the management server.

For details about the asset number file, see *16.5 Asset number file*.

- -k *search-condition-file-name*

Specify by full path the name of the search condition file containing the names of the

groups to which the target clients belong. When this argument is specified, the security levels of all clients in the groups specified in the file are judged.

Create the search condition file in any directory on the management server, using any file name.

For details about the search condition file, see *16.6 Search condition file*.

■ **-all**

Performs actions for all clients registered in JP1/CSC - Manager.

■ **-a *action-policy-name***

Specify the name of the action policy used for implementing actions. You cannot specify the initial policy as the action policy.

To specify an action name that includes spaces, enclose the entire name in double quotation marks ("").

When this argument is omitted, the action policy assigned to the specified clients is used.

■ **-ns**

Also performs actions for clients for which security level judgment was skipped.

When this argument is omitted, actions are not implemented for clients whose security level was not judged.

## Notes

- Execute this command when JP1/CSC setup is completed and the asset management database of AIM is active.
- Execute this command when JP1/CSC - Manager is active.
- This command cannot be executed when the result of the security level judgment is **Unknown**, no judgment item is found, or the security level has not been judged yet.

## Output messages

For details about the messages displayed, see *17.3 List of JP1/CSC messages*.

## Return values

Return value	Description
0	Command processing terminated normally.
1	No connection to JP1/CSC - Manager could be established.
3	The specified command arguments are incorrect.

cscaction (implements actions for a specified client)

Return value	Description
4	The specified file could not be accessed.
5	You do not have execution permissions for the command.
6	JP1/CSC - Manager has not been set up.
7	The asset information file contains an error.
8	A database access error occurred.
9	The search condition file contains an error.
10	No clients meeting the conditions specified in the search condition file were found.
11	AIM is not installed.
12	The action policy name is invalid.
13	A policy that cannot be assigned is specified.
255	An error other than those listed above has occurred.

---

## cscassign (assigns security policies to clients)

---

### Function

This command assigns judgment policies and action policies to clients according to the contents in a policy assignment definition file.

Before you execute this command, you must specify the recipients and the names of the policies to be assigned in the policy assignment definition file.

For details about this file, see *16.7 Policy assignment definition file*.

### Format

```
cscassign -f policy-assignment-definition-file-name
```

### Server for execution

JP1/CSC - Manager

### Required permissions

Administrator permissions

### Command directory

*JP1/CSC - Manager-installation-folder\bin*

### Arguments

- -f *policy-assignment-definition-file-name*

Specify the policy assignment definition file name by full path.

### Notes

- Execute this command when JP1/CSC setup is completed and the asset management database of AIM is active.

### Output messages

For details about the messages displayed, see *17.3 List of JP1/CSC messages*.

### Return values

Return value	Description
0	The policies were assigned successfully.
3	The specified command arguments are incorrect.
4	The specified file could not be accessed.

cscassign (assigns security policies to clients)

Return value	Description
5	You do not have execution permissions for the command.
6	JP1/CSC - Manager has not been set up.
7	The policy assignment definition file contains an error.
8	A database access error occurred.
9	There is no such asset information in the asset management database.
10	A policy specified in the assignment definition file does not exist.
11	AIM is not installed.
12	A policy specified in the policy assignment definition file cannot be assigned.
13	No clients have been registered in JP1/CSC - Manager.
255	An error other than those listed above has occurred.

---

## cscexportcount (outputs statistics on the status of security measures)

---

### Function

This command outputs statistics relating to the status of security measures for specified groups to a CSV file. Statistics can be output from a variety of perspectives.

### Format

```
cscexportcount[ -d| -w[ day-of-week]| -m][ -s total-start-date][ -e total-end-date][ -k search-condition-file-name][ -r group-level][ -c type-of-totals][ -o output-file-name]
```

### Server for execution

JP1/CSC - Manager

### Required permissions

Administrator permissions

### Command directory

*JP1/CSC - Manager-installation-folder\bin*

### Arguments

■ -d

Specify this argument to accumulate statistics on a daily basis.

■ -w *day-of-week*

Specify this argument to accumulate statistics on a weekly basis. Also specify the day of the week from which to start the weekly totals, as a numeral from 1 to 7. If you do not specify a day of the week, the weekly totals will begin on Sunday.

The following table shows which numerals correspond to which days of the week.

Argument	Description
1	Start weekly totals on Sunday.
2	Start weekly totals on Monday.
3	Start weekly totals on Tuesday.
4	Start weekly totals on Wednesday.
5	Start weekly totals on Thursday.

Argument	Description
6	Start weekly totals on Friday.
7	Start weekly totals on Saturday.

When statistics are accumulated weekly, the totals may reflect data from a shorter period depending on the collection period and the day on which the week starts. The following shows an example of such a situation:

■ Totals compiled when 10/1 (Mon) to 11/15 (Thu) is specified as the period to total, and weeks start on Wednesday.

```

Week 1: 10/1 (Mon) to 10/2 (Tue)      (2 days)
Week 2: 10/3 (Wed) to 10/9 (Tue)
Week 3: 10/10 (Wed) to 10/16 (Tue)
Week 4: 10/17 (Wed) to 10/23 (Tue)
Week 5: 10/24 (Wed) to 10/30 (Tue)
Week 6: 10/31 (Wed) to 11/6 (Tue)
Week 7: 11/7 (Wed) to 11/13 (Tue)
Week 8: 11/14 (Wed) to 11/15 (Thu)   (2 days)

```

■ -m

Specify this argument to accumulate statistics on a monthly basis.

When statistics are accumulated monthly, the totals may reflect data from a shorter period depending on the collection period. The following shows an example of such a situation:

■ Totals compiled when 2007/10/20 to 2008/2/15 is specified as the period to total

```

October 2007 10/20 to 10/31 (11 days)
November 2007 11/1 to 11/30
December 2007 12/1 to 12/31
January 2008 1/1 to 1/31
February 2008 2/1 to 2/15 (15 days)

```

■ -s *total-start-date*

Specify the start date for the totals, in the format *YYYY/MM/DD*. When this argument is omitted, the date of the oldest statistics stored in the asset management database is used as the start date.

■ -e *total-end-date*

Specify the end date for the totals, in the format *YYYY/MM/DD*. When this argument is omitted, the date of the most recent statistics stored in the asset management



database is used as the end date.

■ **-k** *search-condition-file-name*

Specify by full path the name of the search condition file containing the names of the groups for which statistics are to be accumulated.

Create the search condition file in any directory on the management server, using any file name. For details about the search condition file, see *16.6 Search condition file*.

■ **-r** *group-level*

Specify the level of the group for which statistics will be accumulated, as a numeral from 0 to 256. Note that you cannot specify the **-r** argument if 3 is specified in the **-c** argument.

When this argument is omitted and value other than 3 is specified for the **-c** argument, group level 1 is used.

Specify the level of groups under the groups specified by the **-k** option (level 0). For example, if `Sales Dept.` and `Accounting Dept.` exist under `Head Office` and you want to output statistics for **Head Office/Sales Dept.** and **Head Office/Accounting Dept.**, specify `Head Office` as the group name and specify 1 for the group level.

■ **-c** *type-of-totals*

Specify the perspective from which to accumulate the statistics, as a numeral from 1 to 3 or 101 to 110. When this argument is omitted, countermeasure usage is totaled across all judgment items.

The following table shows which numeral corresponds to which type of total.

Argument	Description
1	Totals evaluation points.
2	Totals countermeasure usage across all judgment items.
3	Totals countermeasure usage for individual judgment items.
101	Totals countermeasure usage for the first user-defined judgment item.
102	Totals countermeasure usage for the second user-defined judgment item.
103	Totals countermeasure usage for the third user-defined judgment item.
104	Totals countermeasure usage for the fourth user-defined judgment item.
105	Totals countermeasure usage for the fifth user-defined judgment item.
106	Totals countermeasure usage for the sixth user-defined judgment item.
107	Totals countermeasure usage for the seventh user-defined judgment item.

Argument	Description
108	Totals countermeasure usage for the eighth user-defined judgment item.
109	Totals countermeasure usage for the ninth user-defined judgment item.
110	Totals countermeasure usage for the tenth user-defined judgment item.

■ -o *output-file-name*

Specify by full path the name of the output file (CSV format) for the statistics. This file can have the extension `.txt` or `.csv`. To specify a file name that includes spaces, enclose the entire name in double quotation marks (").

When this argument is omitted, the output file will be created with one of the following file names in the current folder in which the command was executed:

Item	Output file name	Description
1	<code>cscjudgemark.csv</code>	Output file name when evaluation points is specified as the type of total
2	<code>cscetotal.csv</code>	Output file name when countermeasure usage across all judgment items is specified as the type of total
3	<code>cscjudgeitems.csv</code>	Output file name when countermeasure usage per judgment item is specified as the type of total
4	<code>cscuseritemnnn.csv</code> <sup>#</sup>	Output file name when countermeasure usage for user-defined judgment items is specified as the type of total

#

*nnn* is a number from 101 to 110, corresponding to the value specified for the `-c` option.

## Notes

- Execute this command when JP1/CSC setup has completed and the asset management database of AIM is active.
- If a file with the same name already exists in the output destination folder, the file is overwritten.
- If the statistics to be output are not found, no file is created when this command is executed. If a file has already been created in the output destination folder, the file is left unchanged.
- You cannot specify a folder in a shared folder or on a network drive as the output target.
- If none of the arguments `-d`, `-w`, or `-m` are specified, statistics are accumulated on

a monthly basis.

## Output messages

For details about the messages displayed, see *17.3 List of JPI/CSC messages*.

## Return values

Return value	Description
0	Command processing terminated normally.
3	The specified command arguments are incorrect.
4	The specified file could not be accessed.
5	You do not have execution permissions for the command.
6	JPI/CSC - Manager has not been set up.
7	A date is specified incorrectly.
8	A database access error occurred.
9	The search condition file contains an error.
10	The specified group does not exist, or no groups belong to the specified group.
11	AIM is not installed.
12	No statistics meeting the specified conditions were found.
255	An error other than those listed above has occurred.

---

## cscexportplist (outputs PC list information)

---

### Function

This command outputs to a CSV file PC list information that contains asset information and judgment results for clients whose security levels were judged on the specified date and time.

### Format

```
cscexportplist[ -j "security-level-judgment-date" ][ -k
search-condition-file-name ]
[ -o file-output-destination-folder ][ -s ][ -l number-of-lines ]
```

### Server for execution

JP1/CSC - Manager

### Required permissions

Administrator permissions

### Command directory

*JP1/CSC - Manager-installation-folder*\bin

### Arguments

- -j "*security-level-judgment-date*"

Specify the security level judgment date for which you want to output PC list information. Use *YYYY/MM/DD hh:mm:ss* format enclosed in double quotation marks (").

The asset information and judgment results for the clients whose security levels were judged at the date and time specified here will be output to the PC list information file.

For details about the date of security level judgment you can specify, see *judgment-date*=*[ security-level-judgment-date ]* output to the JP1/CSC - Manager log file or the PC List window of the Client Security Management window.

When this argument is omitted, the latest information will be output for all clients registered in JP1/CSC.

- -k *search-condition-file-name*

Specify by full path the name of the search condition file containing the names of the groups to which the clients subject to the output of information belong. When this argument is specified, the asset information and judgment results of all clients in the groups specified in the search condition file are output to the PC list information file.

Create the search condition file in any directory on the management server, using any file name.

For details about the search condition file, see *16.6 Search condition file*.

When this argument is omitted, information for all clients registered in JP1/CSC - Manager will be output to the PC list information file.

■ -o *file-output-destination-folder*

Specify by full path the output destination folder for the PC list information file.

To specify a path that includes spaces, enclose the entire path in double quotation marks ("").

When this argument is omitted, the PC list information will be created in the current folder in which the command was started.

For details about the PC list information, see *16.10 PC list information file*.

■ -s

Specify this argument to output the items related to the judgment results *Danger*, *Warning*, *Caution*, *Safe*, and *Unknown* to the judgment result file for PC list information.

When this argument is not specified, the items related to the judgment results *Danger*, *Warning*, *Caution*, and *Unknown* will be output to the judgment result file.

■ -l *number-of-lines* (specifiable range: 1-2147483647)

Specify the maximum number of lines that can be output to the PC list information file. If the number of lines exceeds the maximum, the remaining lines will be output to another file. If this argument is omitted, all lines will be output to one file.

File names are assigned according to the following rules:

First file: *fileName.csv*

Second file: *fileName2.csv*

Nth file: *fileNameN.csv*

Legend:

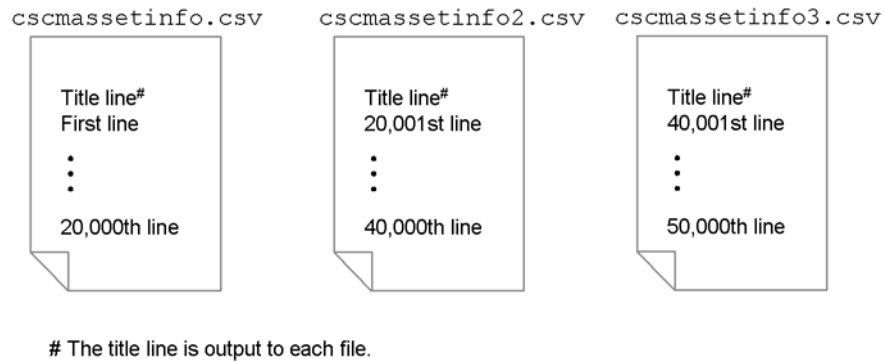
*fileName*: File name of an asset information list file or a judgment result file

The following shows an example of outputting a file:

Asset information list file: *cscmassetinfo.csv*

Number of output lines: 50000

Number of lines specified by -l: 20000



## Notes

- If you specify the `-j` and `-k` arguments, information for the following clients is output to the PC list information file:  
Clients whose security levels were judged on the specified date of security level judgment and that belong to the groups specified in the search condition file.
- Even when the date of security level judgment contained in the JP1/CSC - Manager log file is specified in the `-j` argument, output of PC list information might fail if the judgment and action history saved in the database has wrapped around and been overwritten from the beginning.
- Execute this command when the asset management database of AIM is active. Note that this command can be executed even when JP1/CSC - Manager is inactive.
- If a file with the same name already exists in the output destination folder, the file is overwritten.
- If information to be output is not found, no file is created when this command is executed. If a file has already been created in the output destination folder, the file is not changed.
- Specifying too small value in the `-l` argument could result in the creation of many PC list information files.

## Output messages

For details about the messages displayed, see *17.3 List of JP1/CSC messages*.

**Return values**

<b>Return value</b>	<b>Description</b>
0	Command processing terminated normally.
3	The specified command arguments are incorrect.
4	The specified file could not be accessed.
5	You do not have execution permissions for the command.
6	JP1/CSC - Manager has not been set up.
7	The format of the security level judgment date is incorrect.
8	A database access error occurred.
9	The search condition file contains an error.
10	PC list information corresponding to the security level judgment date was not found. Alternatively, no clients belong to the groups specified in the search condition file.
11	AIM is not installed.
12	No clients have been registered in JP1/CSC - Manager.
15	A judgment history cannot be acquired.
255	An error other than those listed above has occurred.

---

## cscjudge (judges security levels)

---

### Function

This command judges the security levels of clients.

The clients whose security levels are to be judged can be specified in any of three ways:

- Specify the name of an asset number file to judge the clients corresponding to the asset numbers written in the file.
- Specify the name of a search condition file to judge the clients belonging to the groups written in the file.
- Specify `all` to judge all clients.

### Format

```
cscjudge {-f asset-number-file-name |-k search-condition-file-name |-all} [-s]
```

### Server for execution

JP1/CSC - Manager

### Required permissions

Administrator permissions

### Command directory

*JP1/CSC - Manager-installation-folder*\bin

### Arguments

#### ■ -f *asset-number-file-name*

Specify by full path the name of the asset number file containing the asset numbers of the clients to be judged. When this argument is specified, the security levels of only those clients specified in the file are judged.

Create the asset number file with any file name in any directory on the management server.

For details about this file, see *16.5 Asset number file*.

#### ■ -k *search-condition-file-name*

Specify by full path the name of the search condition file containing the names of the groups to which the clients to be judged belong. When this argument is specified, the security levels of all clients in the groups specified in the file are judged.



Create the search condition file in any directory on the management server, using any file name.

For details about this file, see *16.6 Search condition file*.

■ -all

Judges the security levels of all clients registered in JP1/CSC - Manager.

■ -s

Skips security level judgment and action implementation for clients whose inventory information has not been updated since the last time security levels were judged.

When this argument is omitted, the command uses the setting specified for **Perform judgment if asset information is not updated** in the JP1/CSC - Manager setup window.

## Notes

- You can check the security level judgment results in the Client Security Management window of AIM or in the JP1/CSC - Manager log. If linkage is performed to JP1/IM, the security level judgment results are also sent to JP1/IM.

## Output messages

For details about the messages displayed, see *17.3 List of JP1/CSC messages*.

## Return values

Return value	Description
0	Command processing terminated normally.
1	No connection to JP1/CSC - Manager could be established.
3	The specified command arguments are incorrect.
4	The specified file could not be accessed.
5	You do not have execution permissions for the command.
6	JP1/CSC - Manager has not been set up.
7	The asset information file contains an error.
8	A database access error occurred.
9	The search condition file contains an error.
10	No clients meeting the conditions specified in the search condition file were found.
11	AIM is not installed.

cscjudge (judges security levels)

Return value	Description
255	An error other than those listed above has occurred.

---

## cscnetctrl (controls network connections)

---

### Function

This command permits or immediately denies access to the network by a specified client.

You must specify the client by one or more of the following: MAC address, IP address, or host name. The client specification is handled according to the following rules:

- When a MAC address is specified, the client is identified by MAC address only.
- When only an IP address is specified, the client is identified by IP address.
- When only a host name is specified, the client is identified by host name.
- When both an IP address and host name are specified, the client is identified by both IP address and host name.

### Format

```
cscnetctrl {-p|-r}{ {-m MAC-address [-i IP-address] [-h host-name]
                    |-i IP-address [-m MAC-address] [-h host-name]
                    |-h host-name [-m MAC-address] [-i IP-address]}
                    |-f network-connection-control-list-file-name}
```

### Server for execution

JP1/CSC - Manager Remote Option

### Required permissions

Administrator permissions

### Command directory

*JP1/CSC - Manager-Remote-Option-installation-folder\bin*

### Arguments

#### ■ -p

Permits network connections by the specified client.

#### ■ -r

Immediately blocks network connections by the specified client.

#### ■ -m *MAC-address*

Specify the MAC address of the client whose network connections are to be controlled.

To specify multiple MAC addresses, use the format -f

*network-connection-control-list-file-name.*

■ **-i** *IP-address*

Specify the IP address of the client whose network connections are to be controlled.

To specify multiple IP addresses, use the format **-f** *network-connection-control-list-file-name.*

■ **-h** *host-name*

Specify the host name of the client whose network connections are to be controlled as a character string of 1 to 64 bytes.

To specify multiple host names, use the format **-f** *network-connection-control-list-file-name.*

■ **-f** *network-connection-control-list-file-name*

Specify by full path the name of the network connection control list file containing the MAC addresses, IP addresses, or host names of the clients whose network connections are to be controlled.

For details about this file, see *16.15 Network connection control list file.*

## Notes

- Execute this command when JP1/CSC - Manager is active.
- Execute this command after registering the IP address of the remote management server on which the command is to be executed with JP1/CSC - Manager.
- An immediate denial request by this command takes precedence over other actions when processed by JP1/CSC - Manager.
- To clear an immediate denial executed by this command, the administrator must explicitly grant network connection, either by this command or by instruction in the Client Security Management window. Network connection permission as the result of a subsequent security level judgment does not clear an immediate denial already in force.

## Output messages

For details about the messages displayed, see *17.3 List of JP1/CSC messages.*

## Return values

Return value	Description
0	Command processing terminated normally.
1	The specified command arguments are incorrect.
2	You do not have execution permissions for the command.

Return value	Description
3	The format of a MAC address is incorrect.
4	The format of an IP address is incorrect.
5	The length of a host name is incorrect.
6	The specified file could not be accessed.
7	JP1/CSC - Manager - Remote Option has not been set up.
8	The network connection control list file contains an error.
9	JP1/CSC - Manager is inactive.
10	The IP address of JP1/CSC - Manager could not be authenticated.
11	Network connection control processing in JP1/CSC - Manager failed.
255	An error other than those listed above has occurred.

---

## cscnwmaintenance (maintains a list of permitted devices)

---

### Function

This command deletes MAC addresses not registered in the AIM network information from the list of permitted devices for JP1/NM - Manager.

### Format

```
cscnwmaintenance[ -f MAC-addresses-not-removed-definition-file-name]
```

### Server for execution

JP1/CSC - Manager

### Required permissions

Administrator permissions

### Command directory

*JP1/CSC - Manager-installation-folder*\bin

### Arguments

- *-f MAC-addresses-not-removed-definition-file-name*

Specify by full path the name of the definition file that contains MAC addresses not subject to deletion. This file contains the MAC addresses that are not to be removed. When this argument is specified, the MAC addresses specified in this definition file are not deleted from the list of permitted devices for JP1/NM - Manager. If this argument is omitted, all MAC addresses not registered in the AIM network information are deleted from the list of permitted devices for JP1/NM - Manager.

Specify this argument when a MAC address has been registered in JP1/NM - Manager but has not been registered in the ATM network information because, for example, the MAC address was registered in the Register Permitted PCs window for JP1/CSC.

For details about the definition file of MAC addresses not subject to deletion, see *16.20 Definition file of MAC addresses not subject to deletion*.

### Output messages

For details about the messages that are displayed, see *17.3 List of JP1/CSC messages*.

### Return values

Return value	Description
0	Command processing terminated normally.
3	The specified command arguments are incorrect.

Return value	Description
4	The specified file could not be accessed.
5	You do not have execution permissions for the command.
6	JP1/CSC - Manager has not been set up.
7	The definition file of MAC addresses not subject to deletion contains an error.
8	A database access error occurred.
11	AIM is not installed.
20	JP1/NM - Manager is not installed.
21	An error occurred in JP1/NM - Manager.
255	An error other than those listed above has occurred.

---

## cscpatchupdate (updates patch information for judgment policies relating to security updates)

---

### Function

This command updates patch information in judgment policies registered in JP1/CSC - Manager that relate to security updates. When this command is executed, patch information that can be replaced with, for example, the latest cumulative patch information is also deleted.

Before executing this command, you must first acquire patch information files using JP1/Software Distribution. For details about acquiring patch information files, see the manual *Job Management Partner 1/Software Distribution Description and Planning Guide*, for Windows systems.

### Format

```
cscpatchupdate[ -f patch-update-condition-file-name][ -n  
judgment-policy-name]
```

### Server for execution

JP1/CSC - Manager

### Required permissions

Administrator permissions

### Command directory

*JP1/CSC - Manager-installation-folder*\bin

### Arguments

- -f *patch-update-condition-file-name*

Specify by full path the name of the patch update condition file containing the conditions for updating patch information. When this argument is omitted, the patch information in the judgment policy is updated under the conditions that would apply if all settings in the patch update condition file were omitted.

For details about the patch update condition file, see *16.11 Patch update condition file*.

- -n *judgment-policy-name*

Specify the name of the judgment policy to update. You cannot specify the initial policy.

To specify a judgment policy name that includes spaces, enclose the entire name in double quotation marks ("").



When this argument is omitted, all judgment policies except the initial policy are updated.

## Notes

- Execute this command when JP1/CSC setup has completed and the asset management database of AIM is active.
- This command requires version 08-10 or later of JP1/Software Distribution Manager.
- To run this command, MSXML 4.0 Service Pack 2 or MSXML 6.0 must be installed on the management server.
- If the patch information generated from the contents of the patch information file already exists in the judgment policy, the judgment policy is left unchanged.
- When this command is executed, patch information that will be replaced by, for example, the latest cumulative patch is deleted.
- If patch information was added to the judgment policy by using a patch information update command whose version is earlier than 09-50, use the following procedure to re-register the patch information.
  1. Delete all patch information that was registered by the patch information update command from the judgment policy.
  2. Set the following values in the patch information update condition file:
 

```
Patch_Update_Cond=1
```

```
Patch_Version=1
```
  3. Specify the patch information update condition file described in step 2 and execute the patch information update command.
- The OS type set in the judgment policy by the patch information update command differs according to the command version. The following shows the correspondence between a version earlier than 09-50 and version 09-50 or later.

No.	OS type for versions earlier than 09-50	CPU type	OS type for version 09-50 or later
1	Windows 2000	None	Windows 2000
2	Windows XP	32-bit	Windows XP

No.	OS type for versions earlier than 09-50	CPU type	OS type for version 09-50 or later
3	<ul style="list-style-type: none"> <li>Windows Server 2003, Standard Edition</li> <li>Windows Server 2003, Enterprise Edition</li> <li>Windows Server 2003, Datacenter Edition</li> <li>Windows Server 2003, Standard x64 Edition</li> <li>Windows Server 2003, Enterprise x64 Edition</li> <li>Windows Server 2003, Datacenter x64 Edition</li> </ul>	32-bit	<ul style="list-style-type: none"> <li>Windows Server 2003, Standard Edition</li> <li>Windows Server 2003, Enterprise Edition</li> <li>Windows Server 2003, Datacenter Edition</li> </ul>
		64-bit (x64)	<ul style="list-style-type: none"> <li>Windows Server 2003, Standard x64 Edition</li> <li>Windows Server 2003, Enterprise x64 Edition</li> <li>Windows Server 2003, Datacenter x64 Edition</li> </ul>
4	Windows Vista	32-bit	Windows Vista (32-bit)
		64-bit	Windows Vista (64-bit)
5	Windows Server 2008	32-bit	Windows Server 2008 (32-bit)
		64-bit	Windows Server 2008 (64-bit)
6	Windows 7	32-bit	Windows 7 (32-bit)
		64-bit	Windows 7 (64-bit)
7	Windows Server 2008 R2	None	Windows Server 2008 R2

## Output messages

For details about the messages displayed, see *17.3 List of JPI/CSC messages*.

## Return values

Return value	Description
0	The policy was updated successfully.
1	Some policies were updated successfully.
3	The specified command arguments are incorrect.
5	You do not have execution permissions for the command.

Return value	Description
6	JP1/CSC - Manager has not been set up.
8	A database access error occurred.
11	AIM is not installed.
20	JP1/Software Distribution Manager is not installed.
21	Your version of JP1/Software Distribution Manager is 08-02 or earlier.
22	The patch information file could not be accessed.
23	The patch information file contains an error.
24	The patch management file could not be accessed.
25	The patch management file contains an error.
26	The patch update condition file could not be accessed.
27	The patch update condition file contains an error.
28	The specified policy does not exist.
29	The specified policy cannot be updated.
30	The version of your MSXML is 4.0 Service Pack 1 or earlier.
255	An error other than those listed above has occurred.

---

## cscpolexport (exports judgment policies)

---

### Function

This command exports judgment policy settings to the text file that has the specified file name. You can use this command when editing multiple judgment policies at one time.

### Format

```
cscpolexport -j judgment-policy-name [ -f policy-export-file-name ]
```

### Server for execution

JP1/CSC - Manager

### Required permissions

Administrator permissions

### Command directory

*JP1/CSC - Manager-installation-folder*\bin

### Arguments

- **-j *judgment-policy-name***

Specify the name of the judgment policy to be exported.

To specify a judgment policy name that includes spaces, enclose the entire name in double quotation marks ("").

- **-f *policy-export-file-name***

Specify by full path the name of the policy export file. If this argument is omitted, an output file named *judgment-policy-ID*.txt will be created in the current folder in which the command was started. For example, if the judgment policy ID is 00000101, the name of the created file is 00000101.txt. For details about the policy export file, see *16.18 Judgment policy information file*.

### Notes

- Execute this command when JP1/CSC - Manager setup has finished and the asset management database of AIM is active.
- If a file with the same name already exists in the output destination folder, the file will be overwritten.

### Output messages

For details about the messages that are displayed, see *17.3 List of JP1/CSC messages*.

**Return values**

<b>Return value</b>	<b>Description</b>
0	The policy was exported successfully.
2	You do not have execution permissions for the command.
3	The specified command arguments are incorrect.
4	JP1/CSC - Manager has not been set up.
5	AIM is not installed.
6	The specified file could not be accessed.
8	A database access error occurred.
10	The specified policy does not exist.
255	An error other than those listed above has occurred.

---

## cscpolimport (updates judgment policy settings)

---

### Function

This command updates the judgment policy settings.

### Format

```
cscpolimport {-v anti-virus-product-policy-import-file | -j  
judgment-policy-name -f policy-import-file-name}
```

### Server for execution

JP1/CSC - Manager

### Required permissions

Administrator permissions

### Command directory

*JP1/CSC - Manager-installation-folder*\bin

### Arguments

- **-v *anti-virus-product-policy-import-file-name***

Specify either of the following files by full path:

- Anti-virus product policy import file

This file is created by the administrator and contains anti-virus product information to be imported to the judgment policies.

- Policy import execution file (manual)

This file is created when the remote management server detects that information about the anti-virus product (the version of the virus definition file or detection engine) has been updated.

If you specify the -v, -j, and -f options together, a command error occurs.

For details about the policy import file for anti-virus products, see *16.13 Anti-virus product policy import file*. For the file name and location of the policy import execution file (manual), see *16.14 Policy import execution file (manual)*.

- **-j *judgment-policy-name***

Specify the name of the judgment policy whose information you want to import.

To specify a judgment policy name that includes spaces, enclose the entire name in double quotation marks ("").

■ `-f policy-import-file-name`

Specify by full path the name of the policy import file that contains the judgment policy information to be imported. If you specify the `-f` option, you must also specify the `-j` option.

For details about the policy import file, see *16.18 Judgment policy information file*.

## Notes

- Execute this command when JP1/CSC - Manager setup is completed and the asset management database of AIM is active.
- When the policy import file for anti-virus products contains multiple lines, the judgment policy settings are updated in order, starting from the first line. When multiple updates refer to the same policy name, only the last update in the file will be valid.
- A specified judgment policy is updated if it contains the anti-virus product name specified in the policy import file for anti-virus products. If the judgment policy does not contain the anti-virus product name, the anti-virus product name and the information set in the policy import file are added to the judgment policy.

## Output messages

For details about the messages displayed, see *17.3 List of JP1/CSC messages*.

## Return values

Return value	Description
0	The policies were imported successfully.
1	Some policies were imported successfully.
2	You do not have execution permissions for the command.
3	The specified command arguments are incorrect.
4	JP1/CSC - Manager has not been set up.
5	AIM is not installed.
6	The specified file could not be accessed.
7	The judgment policy import file contains an error.
8	A database access error occurred.
9	None of the settings in the policy import file could be imported.
10	The specified policy does not exist.
11	A policy that cannot be updated was specified.

cscpolimport (updates judgment policy settings)

Return value	Description
255	Policy import failed for a reason other than the above.



---

## cscrdelete (deletes information about a specified client from the connection control list)

---

### Function

This command deletes client information from the connection control list.

### Format

```
cscrdelete {-a MAC-address|-l MAC-address-list-file-name}
```

### Server for execution

JP1/CSC - Agent

### Required permissions

Administrator permissions

### Command directory

*JP1/CSC - Agent-installation-folder*\radius\bin

### Arguments

■ -a *MAC-address*

Specify the MAC address of the client to be deleted from the connection control list.

■ -l *MAC-address-list-file-name*

Specify by full path the name of the MAC address list file containing the MAC addresses of the clients to be deleted from the connection control list.

For details about this file, see *16.17 MAC address list file*.

### Notes

- Execute this command when JP1/CSC - Agent is stopped.
- Execute this command when Microsoft IAS or Network Policy Server is stopped.
- An error occurs if a MAC address written in the MAC address list file does not appear in the connection control list.

### Output messages

For details about the messages displayed, see *17.3 List of JP1/CSC messages*.

cscrdelete (deletes information about a specified client from the connection control list)

## Return values

Return value	Description
0	Command processing terminated normally.
1	An error occurred during command processing.

---

## cscrexport (exports a connection control list)

---

### Function

This command exports a connection control list from JPI/CSC - Agent to a CSV file under a specified file name. You can use this command to back up a connection control list, for example.

### Format

```
cscrexport [-f export-file-name]
```

### Server for execution

JPI/CSC - Agent

### Required permissions

Administrator permissions

### Command directory

*JPI/CSC - Agent-installation-folder*\radius\bin

### Arguments

■ None specified

When no arguments are specified, the connection control list is exported to the default path.

The default path and export file name are as follows:

*JPI/CSC-Agent-installation-folder*\radius\dat\cscrexport.csv

■ -f *export-file-name*

Specify the export file (CSV format) by full path.

### Notes

- If the specified export path points to an existing file, the file will be overwritten.

### Output messages

For details about the messages displayed, see *17.3 List of JPI/CSC messages*.

### Return values

Return value	Description
0	Command processing terminated normally.

csclexport (exports a connection control list)

Return value	Description
1	An error occurred during command processing.

---

## cscrimport (imports a connection control list)

---

### Function

This command imports a connection control list exported by the `cscrexport` command.

### Format

```
cscrimport -f import-file-name
```

### Server for execution

JP1/CSC - Agent

### Required permissions

Administrator permissions

### Command directory

*JP1/CSC - Agent-installation-folder*\radius\bin

### Arguments

- `-f import-file-name`

Specify the file to be imported by full path.

For details about the import file, see *16.16 Import file*.

### Notes

- Execute this command when JP1/CSC - Agent is stopped.

### Output messages

For details about the messages displayed, see *17.3 List of JP1/CSC messages*.

### Return values

Return value	Description
0	Command processing terminated normally.
1	An error occurred during command processing.

---

## cscsetup (sets up JP1/CSC - Manager)

---

### Function

This command performs initial setup after new JP1/CSC - Manager is installed. Execute this command to create JP1/CSC management information in the asset management database, and perform initial setup. You must also execute the `cscsetup` command when upgrading JP1/CSC - Manager. This also upgrades JP1/CSC management information in the asset management database. At this time, the set values of the previous version are inherited.

Execute this command as a member of the Administrators group.

### Format

`cscsetup`

### Server for execution

JP1/CSC - Manager

### Required permissions

Administrator permissions

### Command directory

*JP1/CSC - Manager-installation-folder\bin*

### Notes

- Execute this command when AIM setup is completed and the asset management database of AIM is active. You must also stop the World Wide Web Publishing Service (the service provided by the management server).
- If the asset management database contains a significant amount of asset information, the command may take some time until termination.

### Output messages

For details about the messages displayed, see *17.3 List of JP1/CSC messages*.

### Return values

Return value	Description
0	Command processing terminated normally.
1	An error occurred during command processing.

---

## cscstorecount (stores statistics about the status of security measures)

---

### Function

This command stores statistics in the asset management database. Information stored by this command includes evaluation points, the number of clients at a particular security level, and the status of security measures for particular groups.

### Format

cscstorecount

### Server for execution

JP1/CSC - Manager

### Required permissions

Administrator permissions

### Command directory

*JP1/CSC - Manager-installation-folder\bin*

### Notes

- Execute this command when JP1/CSC setup has completed and the asset management database of AIM is active.
- If this command is executed more than once in one day, only the results from the last time the command is executed are stored in the asset management database.

### Output messages

For details about the messages displayed, see *17.3 List of JP1/CSC messages*.

### Return values

Return value	Description
0	Command processing terminated normally.
3	The specified command arguments are incorrect.
5	You do not have execution permissions for the command.
6	JP1/CSC - Manager has not been set up.
8	A database access error occurred.
11	AIM is not installed.

cscstorecount (stores statistics about the status of security measures)

Return value	Description
12	There is no information about security measures to be stored in the asset management database.
255	An error other than those listed above has occurred.



---

## Command used in a user-defined action

---

### Function

This command is executed as a user-defined action in an action policy. It is optionally created by an administrator in the form of an executable file (\*.exe) or batch file (\*.bat). Any command name can be specified.

To execute this command, in the Edit Action Policy window you must select the **Execute the specified command** check box and set **Action, Command**, and the other items. For details about the Edit Action Policy window, see *6.10 Setting an action for each security level*.

### Format

```
command -CSC_polname:policy-name -CSC_level:security-level[  
-CSC_folder:temp-folder-path -CSC_result:judgment-result-format]
```

### Server for execution

JP1/CSC - Manager

### Required permissions

Administrator permissions

### Command directory

Any directory on the management server.

### Arguments

These arguments are set by JP1/CSC - Manager at execution of a user-defined command, based on the settings in the Edit Action Policy window.

■ *command*

Indicates the full path of the command (\*.exe or \*.bat) for the user-defined action.

■ -CSC\_polname:*policy-name*

Indicates the name of the action policy in which the command for the user-defined action is specified.

■ -CSC\_level:*security-level*

Indicates the security level that triggered execution of the command for the user-defined action.

- **Danger:** The command was executed for a security level judged **Danger**.
- **Warning:** The command was executed for a security level judged **Warning**.

- **Caution:** The command was executed for a security level judged **Caution**.
- **Safe:** The command was executed for a security level judged **Safe**.

■ `-CSC_folder:temp-folder-path`

Indicates the full path of the folder containing the asset information file and judgment result file for security level.

At command execution, the *temp-folder-path* is replaced with *JP1/CSC - Manager-installation-folder\usr\YYYYMMDDhhmmssnnn*. The folder set in this argument is deleted by JP1/CSC after execution of the command specified in the user-defined action.

For details about the asset information file, see *16.8 Asset information file*. For details about the judgment result file for security level, see *16.9 Judgment result file for security level*.

■ `-CSC_result:judgment-result-format`

Indicates the format of the judgment result file for security level, which was passed to the command.

- **Simple:** The format of the file was specified as **Summary**.
- **Detail:** The format of the file was specified as **Details**.

For details about this file, see *16.9 Judgment result file for security level*.

## Notes

- Do not create commands for user-defined actions as resident commands. Because user-defined commands are executed each time the particular action is implemented, creating them as resident commands would consume a significant amount of the system resources, and system operation could become unstable.

## Chapter

---

# 16. Definition Files

---

This chapter describes the various definition files used in running a client security control system.

- 16.1 List of definition files
- 16.2 Judgment policy definition files
- 16.3 Mail address definition file
- 16.4 Product name definition file
- 16.5 Asset number file
- 16.6 Search condition file
- 16.7 Policy assignment definition file
- 16.8 Asset information file
- 16.9 Judgment result file for security level
- 16.10 PC list information file
- 16.11 Patch update condition file
- 16.12 Statistics output file
- 16.13 Anti-virus product policy import file
- 16.14 Policy import execution file (manual)
- 16.15 Network connection control list file
- 16.16 Import file
- 16.17 MAC address list file
- 16.18 Judgment policy information file
- 16.19 Excluded user definition file
- 16.20 Definition file of MAC addresses not subject to deletion

## 16.1 List of definition files

The following table shows the various definition files using in running a client security control system.

*Table 16-1:* Definition files used in JP1/CSC operation

No.	Definition file	Description	Ref.
1	Judgment policy definition files	Used when defining a judgment policy by importing settings. The following definition files can be imported to judgment policies: <ul style="list-style-type: none"> <li>• Definition file of excluded security updates</li> <li>• Definition file for mandatory security updates</li> <li>• Definition file for mandatory service pack</li> <li>• Anti-virus products definition file</li> <li>• Prohibited software definition file</li> <li>• Mandatory software definition file</li> <li>• User definition file</li> </ul>	16.2
2	Mail address definition file	Used when importing the email addresses of administrators to the Settings for Email Address dialog box.	16.3
3	Product name definition file	Used to register product names for the product name combo box in the Add (patch information) dialog box or the Update (patch information) dialog box used for setting the judgment policy for security updates.	16.4
4	Asset number file	Used in the <code>-f</code> option of the security level judgment command ( <code>cscjudge</code> ) when specifying which clients to judge.	16.5
5	Search condition file	Used in the <code>-k</code> option of the following commands when specifying a target group for command execution: <ul style="list-style-type: none"> <li>• Action command (<code>cscaction</code>)</li> <li>• Security level judgment command (<code>cscjudge</code>)</li> <li>• PC list information output command (<code>cscexportplist</code>)</li> <li>• Statistics output command (<code>cscexportcount</code>)</li> </ul>	16.6
6	Policy assignment definition file	Used when executing the security policy assignment command ( <code>cscassign</code> ).	16.7

No.	Definition file	Description	Ref.
7	Asset information file	Passed to a command as input information at execution of an action when <b>Pass the asset information to the command</b> is selected under <b>Action for the user definition</b> in the Edit Action Policy window.	16.8
8	Judgment result file for security level	Passed to a command as input information at execution of an action when <b>Pass the judgment result to the command</b> is selected under <b>Action for the user definition</b> in the Edit Action Policy window.	16.9
9	PC list information file	Created when the PC list information output command ( <code>cscexportpclist</code> ) is executed. Asset information and judgment results for clients whose security levels were judged on the specified date and time are output as PC list information in CSV format.	16.10
10	Patch update condition file	Used in the <code>-f</code> option of the judgment policy update command for security updates ( <code>cscpatchupdate</code> ) when specifying the conditions for updating patch information.	16.11
11	Statistics output file	Created when the statistics output command ( <code>cscexportcount</code> ) is executed. The status of security measures for the specified groups is accumulated from various perspectives and output to the file as statistics in CSV format.	16.12
12	Anti-virus product policy import file	Contains the items to be updated at automatic update of judgment policies for anti-virus products.	16.13
13	Policy import execution file (manual)	Contains the items to be updated at automatic update of judgment policies for anti-virus products. This file is generated automatically by the remote management server.	16.14
14	Network connection control list file	Specifies the clients whose network connections are to be controlled from JP1/CSC - Manager Remote Option.	16.15
15	Import file	Contains information to be imported by the connection control list import command ( <code>cscimport</code> ).	16.16
16	MAC address list file	Used in the asset deletion command ( <code>cscrdelete</code> ) when batch-deleting asset information from a connection control list in JP1/CSC - Agent.	16.17

## 16. Definition Files

No.	Definition file	Description	Ref.
17	Judgment policy information file	Contains policy information to be imported by the judgment policy update command ( <code>cscpolimport</code> ).	16.18
18	Excluded user definition file	Used to specify user accounts that are to be excluded from the judgment defined by the password-related information in the PC security settings.	16.19
19	Definition file of MAC addresses not subject to deletion	Specifies the MAC addresses that will not be deleted when the <code>-f</code> option of the permitted device list maintenance command ( <code>cscnwmaintenance</code> ) is specified.	16.20

## 16.2 Judgment policy definition files

When a large amount of information needs to be defined for the judgment items in the judgment policies you are editing, you can define the information in a file in advance, and then import the file.

The following definition files can be imported to judgment policies:

- Definition file of excluded security updates
- Definition file for mandatory security updates
- Definition file for mandatory service pack
- Anti-virus products definition file
- Prohibited software definition file
- Mandatory software definition file
- User definition file

Create each definition file in CSV format. The files can be created with any file name in any directory.

### 16.2.1 Import destination of judgment policy definition files

The following table shows the import destination of each judgment policy definition file.

*Table 16-2: Import destination of judgment policy definition files*

No.	Definition file	Judgment item	Import destination
1	Definition file of excluded security updates	<b>Security updates</b>	Definition of Excluded Security Updates dialog box
2	Definition file of mandatory security updates	<b>Security updates</b>	<b>Patch</b> page of the Definition of Mandatory Security Updates dialog box
3	Definition file of mandatory service packs	<b>Security updates</b>	<b>Service pack</b> page of the Definition of Mandatory Security Updates dialog box
4	Anti-virus products definition file	<b>Anti-virus products</b>	Edit Judgment Policy (Anti-Virus Product) window
5	Prohibited software definition file	<b>Prohibited software</b>	Edit Judgment Policy (Prohibited Software) window

No.	Definition file	Judgment item	Import destination
6	Mandatory software definition file	<b>Mandatory software</b>	Edit Judgment Policy (Mandatory Software) window
7	User definition file	<b>User definition</b>	Edit Judgment Policy (User Definition) window

The format is the same for each definition file. The format and precautions are as follows:

- Enclose setting values in double quotation marks ("). To omit a setting value, specify " ".
- To specify a double quotation mark (") in a definition file, use two consecutively (" ").
- Use a comma (,) to separate setting values.
- Multiple parameters can be specified.
- Be sure to include a linefeed (0x0d0a) at the end of each parameter line. Note that lines consisting only of a linefeed are ignored.

## 16.2.2 List of setting values

This section contains lists of the setting values used in each definition file.

### (1) List of OS types

The following table lists the OS types.

Table 16-3: List of OS types

No.	OS type	Setting value
1	All OSs	0000
2	Windows NT Workstation	0001
3	Windows NT Server	0002
4	Windows NT	0003
5	Windows 95 <sup>#</sup>	0004
6	Windows 98	0005
7	Windows 2000 Professional	0006
8	Windows 2000 Server	0007



No.	OS type	Setting value
9	Windows 2000 Advanced Server	0008
10	Windows 2000 Datacenter Server	0009
11	Windows 2000	0010
12	Windows Me	0011
13	Windows XP Home Edition	0012
14	Windows XP Professional	0013
15	Windows XP	0014
16	Windows Server 2003, Standard Edition	0015
17	Windows Server 2003, Enterprise Edition	0016
18	Windows Server 2003	0017
19	Windows Server 2003, Datacenter Edition	0018
20	Windows Server 2003 (32bit)	0019
21	Windows Server 2003, Standard x64 Edition	0020
22	Windows Server 2003, Enterprise x64 Edition	0021
23	Windows Server 2003, Datacenter x64 Edition	0022
24	Windows Server 2003 (64bit)	0023
25	Windows Vista Business	0025
26	Windows Vista Enterprise	0026
27	Windows Vista Ultimate	0027
28	Windows Vista	0028
29	Windows Server 2008 Standard	0029
30	Windows Server 2008 Enterprise	0030
31	Windows Server 2008 Datacenter	0040
32	Windows Server 2008	0031
33	Windows Server 2008 R2 Standard	0032
34	Windows Server 2008 R2 Enterprise	0033
35	Windows Server 2008 R2 Datacenter	0034

No.	OS type	Setting value
36	Windows Server 2008 R2	0035
37	Windows 7 Professional	0036
38	Windows 7 Enterprise	0037
39	Windows 7 Ultimate	0038
40	Windows 7	0039
41	Windows Vista Business x64 Edition	0041
42	Windows Vista Enterprise x64 Edition	0042
43	Windows Vista Ultimate x64 Edition	0043
44	Windows Vista(32bit)	0044
45	Windows Vista(64bit)	0045
46	Windows Server 2008 Standard without Hyper-V	0046
47	Windows Server 2008 Enterprise without Hyper-V	0047
48	Windows Server 2008 Datacenter without Hyper-V	0048
49	Windows Server 2008 Standard x64 Edition	0049
50	Windows Server 2008 Enterprise x64 Edition	0050
51	Windows Server 2008 Datacenter x64 Edition	0051
52	Windows Server 2008 Standard without Hyper-V x64 Edition	0052
53	Windows Server 2008 Enterprise without Hyper-V x64 Edition	0053
54	Windows Server 2008 Datacenter without Hyper-V x64 Edition	0054
55	Windows Server 2008(32bit)	0055
56	Windows Server 2008(64bit)	0056
57	Windows 7 Professional x64 Edition	0057
58	Windows 7 Enterprise x64 Edition	0058
59	Windows 7 Ultimate x64 Edition	0059
60	Windows 7(32bit)	0060
61	Windows 7(64bit)	0061

#

This is used only for JP1/Software Distribution Client Version 6.

## (2) List of service packs

The following table lists the service packs.

Table 16-4: List of service packs

No.	Service pack	Setting value
1	No specification	0
2	Service Pack 1	1
3	Service Pack 2	2
4	Service Pack 3	3
5	Service Pack 4	4
6	Service Pack 5	5
7	Service Pack 6	6
8	All	100

## (3) List of security levels

The following table lists the security levels.

Table 16-5: List of security levels

No.	Security level	Setting value
1	<b>Danger</b>	400
2	<b>Warning</b>	300
3	<b>Caution</b>	200

## (4) List of products

The following table lists the products.

Table 16-6: List of products

No.	Product	Setting value
1	No specification	0
2	Microsoft Internet Explorer	1

No.	Product	Setting value
3	Other products	99

**(5) List of classes**

The following table lists the classes.

*Table 16-7:* List of classes

No.	Class	Setting value
1	Asset information	1
2	Hardware information	2

**(6) List of comparison conditions**

The following table lists the comparison conditions.

*Table 16-8:* List of comparison conditions

No.	Comparison condition	Setting value	Property type	
			String	Numeric and date/time
1	Match all the words	1	Yes	No
2	Match part of the words	2	Yes	No
3	Match beginning of the words	3	Yes	No
4	Match end of the words	4	Yes	No
5	Match	5	No	Yes
6	Not less than	6	Yes	Yes
7	Not greater than	7	Yes	Yes
8	Do not match	8	Yes	Yes

Legend:

Yes: Can be used.

No: Cannot be used.

**(7) List of treatments when no value is set for a property**

The following table shows the system processing when no value is set for a property in a comparison condition.

*Table 16-9:* List of treatments when no value is set for a property

No.	Comparison condition	Setting value
1	Treat the judgment condition as met.	1
2	Treat the judgment condition as not met.	2
3	Do not judge this condition.	3
4	Treat the security level as unknown.	4

**16.2.3 Definition file of excluded security updates**

This file defines information to be imported to security update programs that are excluded from the judgment item **Security updates**. The following table lists the items and setting values that can be specified in this file.

*Table 16-10:* Items and setting values that can be specified in the definition file of excluded security updates

No.	Item	Setting value
1	<b>Parameter ID</b>	ExpUpProgram
2	<b>Update number</b>	Specify the update number without its MS prefix.
3	<b>Article ID number</b>	Specify the article ID number without its prefix (for example, KB or Q).

Be sure to enter the update number and article ID number.

The following figure shows an example of the definition file of excluded security updates.

```

"ExpUpProgram","04-027","884933" ↓
"ExpUpProgram","04-035","885881" ↓
"ExpUpProgram","04-039","888258" ↓
"ExpUpProgram","04-042","885249" ↓
"ExpUpProgram","05-003","871250" ↓

.
.
.

```

Legend:

↓ : Linefeed code

### 16.2.4 Definition file for mandatory security updates

This file defines information to be imported to mandatory security updates (patch information) in the judgment item **Security updates**. The following table lists the items and setting values that can be specified in this file.

*Table 16-11:* Items and setting values that can be specified in the definition file for mandatory security updates

No.	Item	Setting value	Required
1	<b>Parameter ID</b>	NeedUpProgram	Yes
2	<b>Update number</b>	Specify the update number without its MS prefix.	Yes
3	<b>Article ID number</b>	Specify the article ID number without its prefix (for example, KB or Q).	Yes
4	<b>OS for mandatory security updates</b>	Specify the target OS type. For details about the setting values for OS types, see Table 16-3 <i>List of OS types</i> .	Yes
5	<b>OS service pack for mandatory security updates</b>	Specify the service pack of the target OS type. For details about the setting values for service packs, see Table 16-4 <i>List of service packs</i> . Specify <b>No specification</b> if <b>All OSs</b> is specified for <b>OS for mandatory security updates</b> .	Yes

No.	Item	Setting value	Required
6	<b>Product code for mandatory security updates</b>	Specify the product code. For details about the setting values for product codes, see <i>Table 16-6 List of products</i> .	Yes
7	<b>Product version for mandatory security updates</b>	Specify the product version, using a string with 60 or fewer bytes. Do not specify anything if <b>Product name for mandatory security updates</b> is set to <b>No specification</b> .	No
8	<b>Product service pack for mandatory security updates</b>	Specify the product service pack. For details about the setting values for service packs, see <i>Table 16-4 List of service packs</i> . Specify <b>No specification</b> if <b>Product name for mandatory security updates</b> is set to <b>No specification</b> .	Yes
9	<b>Security level</b>	Specify the security level. For details about the setting values for security levels, see <i>Table 16-5 List of security levels</i> .	Yes
10	<b>Product name for mandatory security updates</b>	When 99 (other products) is specified in No. 6, specify the product name for mandatory security updates, using a string of 255 or fewer bytes.	No
11	<b>Comparison condition</b>	When 99 (other products) is specified in No. 6, specify the comparison condition for the product name for mandatory security updates. You can specify 1 ( <b>Match all the words</b> ) or 3 ( <b>Match beginning of the words</b> ).	No

The following figure shows an example of the definition file for mandatory security updates.

```

"NeedUpProgram", "04-040", "889293", "0010", "4", "1", "6.0", "1", "400", "", "" ↓
"NeedUpProgram", "04-040", "889293", "0014", "4", "1", "6.0", "1", "400", "", "" ↓
"NeedUpProgram", "05-001", "890175", "0010", "0", "0", "", "0", "400", "", "" ↓
"NeedUpProgram", "05-001", "890175", "0014", "0", "0", "", "0", "400", "", "" ↓
"NeedUpProgram", "05-001", "890175", "0017", "0", "0", "", "0", "400", "", "" ↓
"NeedUpProgram", "05-002", "891711", "0010", "0", "0", "", "0", "400", "", "" ↓
"NeedUpProgram", "05-002", "891711", "0014", "0", "0", "", "0", "400", "", "" ↓
"NeedUpProgram", "05-002", "891711", "0017", "0", "0", "", "0", "400", "", "" ↓
"NeedUpProgram", "06-001", "909354", "0010", "100", "99", "1.0.0", "0", "400", "SoftwareA", "1" ↓
.
.
.

```

Legend:

↓ : Linefeed code

### 16.2.5 Definition file for mandatory service packs

This file defines information to be imported to mandatory security updates (service pack information) in the judgment item **Security updates**. The following table lists the items and setting values that can be specified in this file.

#### (1) Product service packs

The following table lists the items and setting values for product service packs that can be defined in the definition file for mandatory service packs.

Table 16-12: Product service pack items and setting values

No.	Item	Setting value	Required
1	<b>Parameter ID</b>	NeedUpServicePackProduct	Yes
2	<b>Product name</b>	Specify the product name. For details about the setting values for product names, see Table 16-6 <i>List of products</i> .	Yes
3	<b>Product version</b>	Specify the product version, using a string with 60 or fewer bytes.	No



No.	Item	Setting value	Required
4	<b>Product service pack</b>	Specify the product service pack. For details about the setting values for service packs, see Table 16-4 <i>List of service packs</i> . Note that <b>No specification</b> cannot be specified.	Yes
5	<b>Product service pack condition</b>	Specify 0 to include only service packs that match <b>Product service pack</b> . Specify 1 to include all other service packs than <b>Product service pack</b> .	Yes
6	<b>OS</b>	Specify the type of OS. For details about the setting values for types of OSs, see Table 16-3 <i>List of OS types</i> .	Yes
7	<b>OS service pack</b>	Specify the service pack of the target OS type. For details about the setting values for service packs, see Table 16-4 <i>List of service packs</i> . Specify <b>No specification</b> if <b>All OSs</b> is specified for <b>OS for mandatory security updates</b> .	Yes
8	<b>Security level</b>	Specify the security level. For details about the setting values for security levels, see Table 16-5 <i>List of security levels</i> .	Yes

## (2) OS service packs

The following table lists the items and setting values for OS service packs that can be defined in the definition file for mandatory service packs.

Table 16-13: OS service pack items and setting values

No.	Item	Setting value	Required
1	<b>Parameter ID</b>	NeedUpServicePackOS	Yes

No.	Item	Setting value	Required
2	<b>OS</b>	Specify the type of OS. For details about the setting values for types of OSs, see Table 16-3 <i>List of OS types</i> . Note that <b>All OSs</b> cannot be specified.	Yes
3	<b>OS service pack</b>	Specify the OS service pack. For details about the setting values for service packs, see Table 16-4 <i>List of service packs</i> . Note that <b>No specification</b> cannot be specified.	Yes
4	<b>OS service pack condition</b>	Specify 0 to include only service packs that match <b>OS service pack</b> . Specify 1 to include all other service packs than <b>OS service pack</b> .	Yes
5	<b>Security level</b>	Specify the security level. For details about the setting values for security levels, see Table 16-5 <i>List of security levels</i> .	Yes

The following figure shows an example of the definition file for mandatory service packs.

```
"NeedUpServicePackProduct","1","6.0","1","0","0010","4","400" ↓
"NeedUpServicePackProduct","1","6.0","1","0","0014","1","400" ↓
"NeedUpServicePackOS","0010","4","1","300" ↓
"NeedUpServicePackOS","0003","6","0","400" ↓
"NeedUpServicePackOS","0014","1","1","200" ↓

.
.
.
```

Legend:  
↓ : Linefeed code

### 16.2.6 Anti-virus products definition file

This file defines information to be imported to anti-virus products in the judgment item **Anti-virus products**. The following table lists the items and setting values that can be specified in this file.

*Table 16-14:* Items and setting values that can be specified in the anti-virus products definition file

No.	Item	Setting value	Required
1	<b>Parameter ID</b>	VirusProduct	Yes
2	<b>Anti-virus product name</b>	Specify the name of the anti-virus product, using a string with 255 or fewer bytes.	Yes
3	<b>Product version</b>	Specify the version of the anti-virus product, using a string with 255 or fewer bytes.	No
4	<b>Engine version</b>	Specify the engine version of the anti-virus product, using a string with 255 or fewer bytes.	No
5	<b>Virus definition file version</b>	Specify the version of the virus definition file, using a string with 255 or fewer bytes.	No
6	<b>Determine that PCs with no resident anti-virus products are at risk</b>	Specify 0 to not judge residency, or 1 to judge residency.	Yes
7	<b>Security level</b>	Specify the security level. For details about the setting values for security levels, see Table 16-5 <i>List of security levels</i> .	Yes

The following figure shows an example of the anti-virus products definition file.

```

"VirusProduct","AntiVirus Corporate Edition 9.0","1","400" ↓
"VirusProduct","Symantec Client Security","1","400" ↓
"VirusProduct","VirusScan 4.5.1","1","400" ↓
"VirusProduct","VirusScan Enterprise 8.0i","1","400" ↓
"VirusProduct","VirusScan TC 6.1.0","0","400" ↓
"VirusProduct","NetShield 4.5","1","400" ↓
"VirusProduct","PC-cillin 2002","1","400" ↓
"VirusProduct","PC-cillin 2003","1","400" ↓
"VirusProduct","OfficeScan Corp. Win9x","1","400" ↓
"VirusProduct","OfficeScan Corp. WinNT","1","400" ↓
"VirusProduct","ServerProtect Normal Server","1","400" ↓
"VirusProduct","F-Secure Anti-Virus Client Security","0","400" ↓
.
.
.

```

Legend:

↓ : Linefeed code

### 16.2.7 Prohibited software definition file

This file defines information to be imported to prohibited software in the judgment item **Prohibited software**. The following table lists the items and setting values that can be specified in this file.

*Table 16-15: Items and setting values that can be specified in the prohibited software definition file*

No.	Item	Setting value	Required
1	<b>Parameter ID</b>	UnjustSoftware	Yes
2	<b>Software name</b>	Specify the name of the prohibited software, using a string with 255 or fewer bytes.	Yes
3	<b>Version</b>	Specify the version of the prohibited software, using a string with 60 or fewer bytes.	No
4	<b>OS</b>	Specify the type of OS. For details about the setting values for types of OSs, see Table 16-3 <i>List of OS types</i> .	Yes
5	<b>Security level</b>	Specify the security level. For details about the setting values for security levels, see Table 16-5 <i>List of security levels</i> .	Yes

No.	Item	Setting value	Required
6	<b>Comparison condition</b>	Specify the comparison condition for the software name. The following values are available: <ul style="list-style-type: none"> <li>• 1 (<b>Match all the words</b>)</li> <li>• 2 (<b>Match part of the words</b>)</li> <li>• 3 (<b>Match beginning of the words</b>)</li> <li>• 4 (<b>Match end of the words</b>)</li> </ul>	Yes

The following figure shows an example of the prohibited software definition file.

```
"UnjustSoftware","baseballgame","", "0000", "300", "2" ↓
"UnjustSoftware","cardgame","", "0000", "200", "2" ↓
"UnjustSoftware","chessgame","", "0000", "200", "3" ↓
.
.
.
```

Legend:  
↓ : Linefeed code

## 16.2.8 Mandatory software definition file

This file defines information to be imported to mandatory software in the judgment item **Mandatory software**. The following table lists the items and setting values that can be specified in this file.

*Table 16-16:* Items and setting values that can be specified in the mandatory software definition file

No.	Item	Setting value	Required
1	<b>Parameter ID</b>	NeedSoftware	Yes
2	<b>Software name<sup>#</sup></b>	Specify the name of the mandatory software, using a string with 255 or fewer bytes.	Yes
3	<b>Version<sup>#</sup></b>	Specify the version of the mandatory software, using a string with 60 or fewer bytes.	No
4	<b>OS</b>	Specify the type of OS. For details about the setting values for types of OSs, see Table 16-3 <i>List of OS types</i> .	Yes

No.	Item	Setting value	Required
5	<b>Security level</b>	Specify the security level. For details about the setting values for security levels, see Table 16-5 <i>List of security levels</i> .	Yes
6	<b>Software group name</b>	Specify the group name, using a string of 255 or fewer bytes. If nothing is entered, the software name defined at the beginning of the file will be set.	No

#

To specify multiple software names, enter the software names as many times as the number of software items to be specified, using the following format:

```
" " "software-name-1" " " , " "software-name-2" " " , " "software-name-3" " " , ... "
```

To specify multiple versions, enter the versions as many times as the number of versions to be specified, using the following format:

```
" " "version-1" " " , " "version-2" " " , " "version-3" " " , ... "
```

Specify the software names in order, so that they correspond to the versions.

The following figure shows an example of the mandatory software definition file.

```
"NeedSoftware", ""Software1"", ""Software2"", ""1.0"", ""2.0"", ""0000", "200", "Group1" ↓
.
.
.
```

Legend:

↓ : Linefeed code

### 16.2.9 User definition file

This file defines information to be imported to a user-specific security requirement in the judgment item **User Definition**. The following table lists the items and setting values that can be specified in this file.

Table 16-17: Items and setting values that can be specified in a user definition file

No.	Item	Setting value	Required
1	<b>Parameter ID</b>	UserDefJudge	Yes

No.	Item	Setting value	Required
2	<b>Judgment item name</b>	Specify the name of the user-defined judgment item, using a string with 255 or fewer bytes.	Yes
3	<b>Class<sup>#</sup></b>	Specify the class of the asset management database of AIM to be used in the judgment. For the setting values, see Table 16-7 <i>List of classes</i> .	Yes
4	<b>Property<sup>#</sup></b>	Specify the display name of the property to be used in the judgment. For the setting values, see Table 6-30 <i>List of classes and properties that can be used in user-defined judgments</i> .	Yes
5	<b>Comparison condition<sup>#</sup></b>	Specify a comparison condition. For the setting values, see Table 16-8 <i>List of comparison conditions</i> .	Yes
6	<b>Comparison value<sup>#</sup></b>	<ul style="list-style-type: none"> <li>Property attribute of numeric type Type a positive number of 1 to 19 digits, or a negative number of no more than 20 digits beginning with a hyphen (-).</li> <li>Property attribute of string type Type a character string (other than a line feed code) no larger than the property size. For details about property sizes, see Table 6-30 <i>List of classes and properties that can be used in user-defined judgments</i>.</li> <li>Property attribute of date/time type Set one or more of the following items: Year: 1 to 9999 Month: 1 to 12 Day: 1 to 31 Hour: 0 to 23 Minute: 0 to 59 Second: 0 to 59</li> </ul>	Yes

No.	Item	Setting value	Required
7	<b>Treatment when value is not set for property<sup>#</sup></b>	Specify the processing when no value is set for the property. For the setting values, see Table 16-9 <i>List of treatments when no value is set for a property</i> .	Yes
8	<b>Security level</b>	Specify the security level. For the setting values, see Table 16-5 <i>List of security levels</i> .	Yes

Legend:

Yes: Mandatory (must be specified)

#

To specify multiple classes, properties, comparison conditions, comparison values, or processing options for unspecified properties, specify each item in succession in the following format:

```
" " "Class-name1" " , " "Class-name2" " , " "Class-name3" " , . . . "
" " "Property-name1" " , " "Property-name2" " , " "Property-name3" " , . . . "
" " "Comparison-condition1" " , " "Comparison-condition2" " , " "Comparison-c
ondition3" " , . . . "
" " "Processing-option1" " , " "Processing-option2" " , " "Processing-option3" " ,
. . . "
```

When specifying multiple definitions, specify the items in each line in corresponding order.

The following figure shows an example of a user definition file.



```

"UserDefJudge","Automatic logon setting","Asset information","Automatic logon","5","0","2","300" ↓
"UserDefJudge","WindowsUpdate execution time","Hardware asset information","WindowsUpdate execution
date","6","2006-01-09-*-*","4","400" ↓
"UserDefJudge","Power-saving CPU","""Hardware asset information""","Hardware asset information""",
""CPU""","CPU""","8","8","28694","28695","4","4","200" ↓

:

```

Legend:

↓ : Line feed code

## 16.3 Mail address definition file

A mail address definition file is used when importing the email addresses of administrators to the Settings for Email Address dialog box. In this file, define the administrator email addresses to which the security level judgment results will be sent by email.

When the mail address definition file is imported to the Settings for Email Address dialog box, the administrator email addresses are added to the **Email address to be notified** list.

Create the file with any file name in any directory.

### (1) Synopsis

```
email-address ↓
email-address ↓
:
:
```

Legend: ↓: Line feed code

### (2) Definition contents

The following table shows the contents to define in this file.

Table 16-18: Definition contents of a mail address definition file

No.	Item	Setting value
1	Email address	Specify the email address of the administrator, using a string of 64 or fewer bytes.

Note the following coding conventions:

- You can write multiple lines in the file.
- End every line with a line feed code. The line feed code is 0x0d0a. Lines containing only a line feed code are ignored.
- You can import a maximum of 100 email addresses.

### (3) Specification example

```
shisan_ichiroh@aaa.com ↓
:
:
shisan_hachiroh@bbb.co.jp ↓
```

## 16.4 Product name definition file

The product name definition file is used to register product names for the product name combo box in the Add (patch information) dialog box or the Update (patch information) dialog box used for setting the judgment policy for security updates. The product names defined in this file are displayed in the pull-down menu of the combo box.

Define the software names registered as asset information in AIM in this file.

When a product name is entered and patch information is added or changed in the Add (patch information) dialog box or Update (patch information) dialog box, that product name is automatically registered in the product name definition file. If the product name definition file does not exist, it is created automatically.

The file name and the folder in which it resides are as follows.

File name	Folder
cscmproduct.conf	JPI/CSC - Manager-installation-folder\conf

For details about the Add (patch information) dialog box and Update (patch information) dialog box, see 6.3.2 *Performing judgment by a specified security update*.

### (1) Synopsis

```
product-name ↓
product-name ↓
:
```

Legend: ↓: Line feed code

### (2) Definition contents

The following table shows the contents to define in this file.

*Table 16-19: Definition contents of a product name definition file*

No.	Item	Setting value
1	Product name	Specify the product name, using a string of 255 or fewer bytes.

Note the following coding conventions:

- The file can contain multiple lines.

- Every line must end with a line feed code, which is 0x0d0a. Any lines containing only a line feed code are ignored.
- When **Microsoft Internet Explorer** or **No specification** is defined as the product name, the specification is ignored.
- When the same product name is entered more than once, only one specification is valid.

**(3) Specification example**

```
SoftwareA ↓  
SoftwareB ↓  
  :  
  :  
SoftwareC ↓
```

# 16.5 Asset number file

This file is used in the `-f` option of the security level judgment command (`cscjudge`) when specifying the clients whose security levels are to be judged. Define the asset numbers of those clients in the file. Create the file with any file name in any directory.

## (1) Synopsis

```
asset-number ↓
asset-number ↓
:
:
```

Legend: ↓: Line feed code

## (2) Definition contents

The following table shows the contents to define in this file.

Table 16-20: Definition contents of an asset number file

No.	Item	Setting value
1	Asset number	Define the asset numbers of the clients to be judged, one per line.

Note the following coding conventions:

- You can write multiple lines in the file.
- End every line with a line feed code. The line feed code is `0x0d0a`. Lines containing only a line feed code are ignored.
- You can define a maximum of 65,535 asset numbers.

## (3) Specification example

```
1000000001 ↓
1000000002 ↓
1000000003 ↓
1000000004 ↓
:
:
9999999999 ↓
```

## 16.6 Search condition file

This file is used to specify a target group for command execution. Define the name of the group in the file. Create the file with any file name in any directory.

This file is used in the `-k` option of the following commands:

- Action command (`cscaction`)
- Security level judgment command (`cscjudge`)
- PC list information output command (`cscexportpclist`)
- Statistics output command (`cscexportcount`)

### (1) Synopsis

`Group_Fullname=group-name ↓`

Legend: ↓: Line feed code

### (2) Definition contents

The following table shows the contents to define in this file.

*Table 16-21: Definition contents of a search condition file*

No.	Parameter	Item	Setting value
1	Group_Fullname	Group name (full path)	Specify the name of the group to subject to command execution, using a string of 512 or fewer bytes. When groups are in a hierarchy, specify the path from the highest level, delimiting each part with a forward slash (/).

Note the following coding conventions:

- Lines beginning with the hash symbol (#) are treated as comments.
- The security levels of clients whose group name begins with the specified group name will be judged.
- Specify each part of the group name correctly.

For example, to judge the security level of clients in the group *Sales Department*, which comes under group *Yokohama Office*, specify `Yokohama_Office/Sales_Department`. If any part is incomplete, as in `Yokohama_Office/Sales`, even though part of the specified path may match an existing group name,

no matching group (clients) will be found and judgment will not be performed.

- You cannot specify multiple parameters. If you specify multiple parameters, the last specified condition is valid.
- End the parameter line with a line feed code. The line feed code is 0x0d0a. Lines containing only a line feed code are ignored.

*Reference note:*

The following table shows the clients that will be judged for each group name specification, when *Sales Department* is a group under the *Yokohama Office* group.

No.	Specified group name	Applicable clients
1	Yokohama_Office/Sales_Department	Clients belonging to Sales_Department.
2	Yokohama_Office/Sales	None
3	Yokohama_Office	Clients belonging to Yokohama_Office including those in Sales_Department.

**(3) Specification example**

Group\_Fullname=Head\_Office/Sales\_Department/Sales1 ↓

## 16.7 Policy assignment definition file

This file is used when executing the security policy assignment command (`cscassign`). Define the policy recipients and the policy names in this file. Create the file with any file name in any directory.

### (1) Synopsis

```
category,keyword,judgment-policy-name,action-policy-name,option{ 0|1 } ↓
category,keyword,judgment-policy-name,action-policy-name,option{ 0|1 } ↓
:
:
```

Legend: ↓: Line feed code

### (2) Definition contents

The following table shows the contents to define in this file.

Table 16-22: Definition contents of a policy assignment definition file

No.	Item	Setting value
1	Category	Specify the policy recipients. ALL: All clients PC: Clients with the asset number specified in <i>keyword</i> . GROUP: Clients in the group specified in <i>keyword</i> .
2	Keyword	Specify a keyword for searching for clients. The specifiable contents depend on the value specified in <i>category</i> , as follows: ALL specified in <i>category</i> Omit. If specified, a syntax error occurs. PC specified in <i>category</i> Specify the client's asset number using a string with 60 or fewer bytes. GROUP specified in <i>category</i> Specify the group name (path from the highest level) using a string with 512 or fewer bytes. Delimit each part of the path with a forward slash (/).
3	Judgment policy name	Specify the name of the judgment policy to assign to the specified clients using a string with 128 or fewer bytes. Omit this item if you do not want to assign a judgment policy.
4	Action policy name	Specify the name of the action policy to assign to the specified clients using a string with 128 or fewer bytes. Omit this item if you do not want to assign an action policy.



No.	Item	Setting value
5	Option	Specify the client search method based on the keyword. This item is valid only when GROUP is specified in <i>category</i> . 0: Match word beginning 1: Match exactly The default is 0.

Note the following coding conventions:

- Lines beginning with the hash symbol (#) are treated as comments.
- When specifying group names by keyword, you must specify each part of the group name correctly, even if you specify 0 (match word beginning) in *option*.  
For example, to assign a policy to group *Sales Department*, which comes under group *Yokohama Office*, specify `Yokohama_Office/Sales_Department`. If any part is incomplete, as in `Yokohama_Office/Sales`, even though part of the specified path may match an existing group name, no matching group (clients) will be found and the policy will not be assigned.
- You can write multiple lines in the file.
- End every line with a line feed code. The line feed code is 0x0d0a. Lines containing only a line feed code are ignored.

*Reference note:*

The following table shows the clients that will be assigned the policy when a group name is specified in *keyword* and *Sales Department* is a group under the *Yokohama Office* group.

No.	Group name specified in <i>keyword</i>	Applicable clients
1	<code>Yokohama_Office/Sales_Department</code>	Clients belonging to <code>Sales_Department</code> .
2	<code>Yokohama_Office/Sales</code>	None
3	<code>Yokohama_Office</code>	Clients belonging to <code>Yokohama_Office</code> including those in <code>Sales_Department</code> .

### (3) Specification example

```
ALL,,(default policy),(default policy) ↓
GROUP,Head_Office/Sales_Department/Sales1,,ActionPolicy1,0 ↓
```

## 16. Definition Files

PC,1000000001,JudgmentPolicyB,ActionPolicy2 ↓

## 16.8 Asset information file

This file is passed to a user-specified command when **Pass the asset information to the command** is selected under **Action for the user definition** in the Edit Action Policy window.

Asset information set by JP1/CSC, such as asset numbers and host names, is set in this file. The file name and the folder in which it resides are as follows.

File name	Folder
cscmassetinfo.dat	JP1/CSC - Manager-installation-folder\usr\YYYYMMDDhhmmssnn#

#

Command execution date and time.

The folder containing an asset information file is deleted by JP1/CSC after execution of the command specified in the user-defined action.

### (1) Synopsis

```
"asset-number" , "host-name" , "IP-address" , "user-name" , "group" , "MAC-address" , "OS-information" , "location" , "JP1/Software-Distribution-host-ID" ↓
:
```

Legend: ↓: Line feed code

Syntax of the asset information file

Note the following:

- Items are delimited with commas ( , ).
- Each item value is enclosed with double quotation marks ( "). Two double quotation marks in succession ( " ") mean that the value is omitted.
- A double quotation mark ( " ) appearing within an item value string is set as two double quotation marks ( " " ).
- The line feed code is 0x0d0a.

### (2) Definition contents

The following table shows the contents set in this file.

Table 16-23: Contents of an asset information file

No.	Item	Value set
1	Asset number	Asset number of the client, set as a string of 120 or fewer bytes.
2	Host name	Host name of the client, set as a string of 128 or fewer bytes.
3	IP address	IP address of the client, set as a string of 15 or fewer bytes.
4	User name	User name of the client, set as a string of 510 or fewer bytes.
5	Group	Group name of the client, set as a string of 1,024 or fewer bytes.
6	MAC address	MAC address of the client, set as a string of 17 or fewer bytes.
7	OS information	OS used by the client, set as a string of 400 or fewer bytes.
8	Location	Location in which the client is installed, set as a string of 1,024 or fewer bytes.
9	JP1/Software Distribution host ID	Host ID information when inventory information is received, set as a string of 256 or fewer bytes.

When multiple IP addresses or MAC addresses have been allocated to a client, only the IP address or MAC address appearing in the PC List window of the Client Security Management window is set.

### (3) Specification example

```
"0000000001","General Affairs 001","100.20.150.40","John
Brown","Head_Office/
General_Affairs_Department","00:1A:2B:3C:4D:5E","Windows 2000
Server","Head Office 2F","#giqlm9lasl694r1b89ljaj38q20" ↓
```

## 16.9 Judgment result file for security level

This file is passed to a user-specified command when **Pass the judgment result to the command** is selected under **Action for the user definition** in the Edit Action Policy window.

The file name and the folder in which it resides are as follows.

Table 16-24: File names and folder of a judgment result files

No.	Category	File name	Folder
1	Judgment result (summary) file	cscmresult.dat	JP1/CSC - Manager-installation-folder\usr\YYYYM MDDhhmmssnn <sup>#</sup>
2	Judgment result (security updates) file	cscmupresult.dat	
3	Judgment result (anti-virus product) file	cscmvrsresult.dat	
4	Judgment result (prohibited software) file	cscmunjustresult.dat	
5	Judgment result (mandatory software) file	cscmneedjdgrslt.dat	
6	Judgment result (user definition) file	cscmusrjdgrslt.dat	
7	Judgment result (PC security settings) file	cscmpcsecurityresult.dat	

#

Command execution date and time.

The folder containing judgment result files is deleted by JP1/CSC after execution of the command specified in the user-defined action.

Syntax of judgment result files

Each file has the same syntax. Note the following:

- Items are delimited with commas (,).

- Each item value is enclosed with double quotation marks ("). Two double quotation marks in succession (" ") mean that the value is omitted.
- A double quotation mark (") appearing within an item value string is set as two double quotation marks (" ").
- The line feed code is 0x0d0a.
- An empty file is created if all applicable clients were judged `Safe` or were excluded by the judgment policy. However, judgment results are still output to a judgment result (anti-virus product) file when all clients are judged `Safe`.

### 16.9.1 Judgment result (summary) file

This file is passed to the command if the user selected **Pass the judgment result to the command** in the **Action for the user definition** area of the Edit Action Policy window, regardless of whether the user selected **Summary** or **Details**.

This file is set by JP1/CSC. It contains asset numbers and security level judgment results.

#### (1) Synopsis

```
"asset-number" , "PC-judgment-result" , "security-level-of-security-update" , "security-level-of-anti-virus-product" , "security-level-of-prohibited-software" , "security-level-of-mandatory-software" , "security-level-of-user-definition" , "security-level-of-PC-security-settings" ↓
:
:
```

Legend: ↓: Line feed code

#### (2) Definition contents

The following table shows the contents set in this file.

Table 16-25: Contents of a judgment result (summary) file

No.	Item	Value set
1	Asset number	Asset number of the client whose security level was judged, set as a string of 120 or fewer bytes.
2	PC judgment result	Security level set as one of the following codes: 100: Safe 200: Caution 300: Warning 400: Danger

No.	Item	Value set
3	Security level of security update	Security risk level of the security update, set as one of the following codes: 010: Not applicable 100: Safe 150: Unknown 200: Caution 300: Warning 400: Danger
4	Security level of anti-virus product	Security risk level of the anti-virus product, set as one of the following codes: 010: Not applicable 100: Safe 150: Unknown 200: Caution 300: Warning 400: Danger
5	Security level of prohibited software	Security risk level of the prohibited software, set as one of the following codes: 010: Not applicable 100: Safe 150: Unknown 200: Caution 300: Warning 400: Danger
6	Security level of mandatory software	Security risk level of the mandatory software, set as one of the following codes: 010: Not applicable 100: Safe 150: Unknown 200: Caution 300: Warning 400: Danger
7	Security level of user definition	Security risk level of the user-defined judgment item, set as one of the following codes: 010: Not applicable 100: Safe 150: Unknown 200: Caution 300: Warning 400: Danger

No.	Item	Value set
8	Security level of PC security settings	Security risk level of the PC security settings, set as one of the following codes: 010: Not applicable 100: Safe 150: Unknown 200: Caution 300: Warning 400: Danger

**(3) Specification example**

```
"1000000001", "400", "100", "150", "200", "400", "300", "100" ↓
"1000000002", "400", "300", "400", "200", "200", "010", "200" ↓
"1000000003", "300", "300", "200", "150", "200", "100", "300" ↓
```

**16.9.2 Judgment result (security updates) file**

This file contains detailed information about security updates. It is passed to the command as input information at execution of the specified action if the user selected **Pass the judgment result to the command** and **Details** in the **Action for the user definition** area of the Edit Action Policy window.

This file is set by JP1/CSC. It contains information for judging security updates (judgment policies) and security level judgment results.

**(1) Synopsis**

```
"asset-number", "security-update-type", "update-number", "article-ID", "OS", "
OS-service-pack", "judgment-condition", "product", "product-version", "product-
service-pack", "judgment-condition", "security-level" ↓
:
:
```

Legend: ↓: Line feed code

**(2) Definition contents**

The following table shows the contents set in this file.

*Table 16-26: Contents of a judgment result (security updates) file*

No.	Item	Value set
1	Asset number	Asset number of the client whose security level was judged, set as a string of 120 or fewer bytes.



No.	Item		Value set
2	Security update type <sup>#</sup>		Security update type, set as one of the following codes: 1: Patch 2: OS service pack 3: Product service pack
3	Patch	Update number	Information about an unapplied patch detected by the security update judgment, set as a string of 32 or fewer bytes. Note that the update number, without its MS prefix, is set. Example: MS06-001 is set as 06-001.
4		Article ID	Information about an unapplied patch detected by the security update judgment, set as a string of 32 or fewer bytes. Note that the article ID, without its prefix (for example, KB or Q), is set. Example: KB911565 is set as 911565.
5	OS service pack	OS	Information (OS) about an unapplied OS service pack detected by the security update judgment, set as a code. For the codes, see Table 16-3 <i>List of OS types</i> .
6		Service pack	Information (service pack) about an unapplied OS service pack detected by the security update judgment, set as a code. For the codes, see Table 16-4 <i>List of service packs</i> .
7		Judgment condition	Information (judgment condition) about an unapplied OS service pack detected by the security update judgment, set as a code. 0: Match 1: Later

No.	Item		Value set
8	Product service pack	Product	Information (product) about an unapplied product service pack detected by the security update judgment, set as a code. 1 is the only value set. For the codes, see Table 16-6 <i>List of products</i> .
9		Product version	Information (product version) about an unapplied product service pack detected by the security update judgment, set as a string with 120 or fewer bytes.
10		Product service pack	Information (product service pack) about an unapplied product service pack detected by the security update judgment, set as a code. For the codes, see Table 16-4 <i>List of service packs</i> .
11		Judgment condition	Information (judgment condition) about an unapplied product service pack detected by the security update judgment, set as a code. 0: Match 1: Later
12	Security level		Security level set as one of the following codes: 100: Safe 200: Caution 300: Warning 400: Danger

#

Only information about the item set as the security update type is set in a judgment result (security updates) file.

### (3) Specification example

```
"1000000001","1","06-007","913446","","","","","","","300"
↓
"1000000001","2","","","12","1","0","","","","","300" ↓
"1000000001","3","","","","","1","6","1","0","300" ↓
"1000000002","1","06-007","913446","","","","","","","300"
↓
```

### 16.9.3 Judgment result (anti-virus product) file

This file contains detailed information about anti-virus products. It is passed to the command as input information at execution of the specified action if the user selected **Pass the judgment result to the command** and **Details** in the **Action for the user**

**definition** area of the Edit Action Policy window.

This file is set by JP1/CSC. It contains information for judging anti-virus products (judgment policies) and security level judgment results.

### (1) Synopsis

```
"asset-number" , "product-version-result" , "engine-version-result" , "virus-definition-file-version-result" , "resident-settings-result" , "security-level" ↓
:
:
```

Legend: ↓: Line feed code

### (2) Definition contents

The following table shows the contents set in this file.

*Table 16-27: Contents of a judgment result (anti-virus product) file*

No.	Item	Value set
1	Asset number	Asset number of the client whose security level was judged, set as a string of 120 or fewer bytes.
2	Product version result	Judgment result for the product version, set as one of the following codes: 0: No problem 1: Problem found 2: Unknown 3: Not applicable
3	Engine version result	Judgment result for the engine version, set as one of the following codes: 0: No problem 1: Problem found 2: Unknown 3: Not applicable
4	Virus definition file version result	Judgment result for the virus definition file version, set as one of the following codes: 0: No problem 1: Problem found 2: Unknown 3: Not applicable

No.	Item	Value set
5	Resident setting result	Judgment result for the anti-virus product resident setting, set as one of the following codes: 0: No problem 1: Problem found 2: Unknown 3: Not applicable
6	Security level	Security level set as one of the following codes: 100: Safe 200: Caution 300: Warning 400: Danger

## Notes

- All anti-virus products installed on the client are judged. In the judgment result, the security level is the lowest security risk among the products. If an unknown result is found for a product, the judgment result for another anti-virus product is taken as the security level.
- When an anti-virus product is uninstalled, the judgment result for items 2 to 5 is 1 (problem found).
- When the judgment result for an anti-virus product is Safe, the judgment result for items 2 to 5 is 0 (no problem).
- When an anti-virus product installed on the client is not set in the judgment policy, the judgment result for items 2 to 5 is 3 (not applicable).

**(3) Specification example**

```
"1000000001", "1", "0", "0", "1", "400" ↓
"1000000002", "1", "1", "2", "1", "400" ↓
"1000000003", "1", "1", "1", "1", "400" ↓
"1000000004", "3", "3", "3", "3", "010" ↓
```

**16.9.4 Judgment result (prohibited software) file**

This file contains detailed information about prohibited software. It is passed to the command as input information at execution of the specified action if the user selected **Pass the judgment result to the command** and **Details** in the **Action for the user definition** area of the Edit Action Policy window.

This file is set by JP1/CSC. It contains information for judging prohibited software (judgment policies) and security level judgment results.

**(1) Synopsis**

```
"asset-number" , "software-name" , "version" , "security-level" ↓
:
:
```

Legend: ↓: Line feed code

**(2) Definition contents**

The following table shows the contents set in this file.

*Table 16-28: Contents of a judgment result (prohibited software) file*

No.	Item	Value set
1	Asset number	Asset number of the client whose security level was judged, set as a string of 120 or fewer bytes.
2	Software name	Name of the prohibited software installed on the client, set as a string of 510 or fewer bytes.
3	Version	Version of prohibited software installed on the client, set as a string of 120 or fewer bytes.
4	Security level	Security level set as one of the following codes: 100: Safe 200: Caution 300: Warning 400: Danger

**(3) Specification example**

```
"10000000001" , "baseballgame" , "1.0" , "400" ↓
"10000000001" , "cardgame" , "2.0" , "400" ↓
"10000000002" , "chessgame" , "2.0" , "400" ↓
```

**16.9.5 Judgment result (mandatory software) file**

This file contains detailed information about mandatory software. It is passed to the command as input information at execution of the specified action if the user selected **Pass the judgment result to the command** and **Details** in the **Action for the user definition** area of the Edit Action Policy window.

This file is set by JP1/CSC. It contains information for judging mandatory software (judgment policies) and security level judgment results.

**(1) Synopsis**

```
"asset-number" , "group-name" , "software-name" , "version" , "security-level" ↓
:
:
```

Legend: ↓: Line feed code

**(2) Definition contents**

The following table shows the contents set in this file.

*Table 16-29: Contents of a judgment result (mandatory software) file*

No.	Item	Value set
1	Asset number	Asset number of the client whose security level was judged, set as a string of 120 or fewer bytes.
2	Group name	Group name of mandatory software not installed on the client, set as a string of 510 or fewer bytes.
3	Software name	Software name of mandatory software not installed on the client, set as a string of 510 or fewer bytes.
4	Version	Version of mandatory software not installed on the client, set as a string of 120 or fewer bytes.
5	Security level	Security level set as one of the following codes: 100: Safe 200: Caution 300: Warning 400: Danger

**(3) Specification example**

```
"1000000001" , "Group A" , "Software A" , "" , "300" ↓
"1000000002" , "Group A" , "Software A" , "" , "300" ↓
"1000000003" , "Group B" , "Software B" , "" , "300" ↓
```

**16.9.6 Judgment result (user definition) file**

This file contains detailed information about a user definition. It is passed to the command as input information at execution of the specified action if the user selected **Pass the judgment result to the command** and **Details** in the **Action for the user definition** area of the Edit Action Policy window.

The information for judging user definitions (judgment policies) and security level

judgment results set in this file is set by JP1/CSC.

### (1) Synopsis

```
"asset-number" , "judgment-item" , "security-level" ↓
:
:
```

Legend: ↓: Line feed code

### (2) Definition contents

The following table shows the contents set in this file.

*Table 16-30: Contents of a judgment result (user definition) file*

No.	Item	Value set
1	Asset number	Asset number of the client whose security level was judged, set as a string of 120 or fewer bytes.
2	Judgment item	Name of the judgment item judged as <b>Danger</b> , <b>Warning</b> , or <b>Caution</b> by the user-defined judgment, set as a string of 510 or fewer bytes.
3	Security level	Security level set as one of the following codes: 100: Safe 200: Caution 300: Warning 400: Danger

### (3) Specification example

```
"1000000001" , "Automatic logon" , "300" ↓
"1000000001" , "Power-saving CPU" , "200" ↓
"1000000002" , "Automatic logon" , "300" ↓
```

## 16.9.7 Judgment result (PC security settings) file

This file contains detailed information about PC security settings. It is passed to the command as input information at execution of the specified action if the user selected **Pass the judgment result to the command** and **Details** in the **Action for the user definition** area of the Edit Action Policy window.

This file is set by JP1/CSC. It contains information for judging PC security settings (judgment policies) and security level judgment results.

**(1) Synopsis**

```
"asset-number" , "judgment-item" , "setting" , "security-level" ↓
:
:
```

Legend: ↓: Line feed code

**(2) Definition contents**

The following table shows the contents set in this file.

*Table 16-31: Contents of a judgment result (PC security settings) file*

No.	Item	Value set
1	Asset number	Asset number of the asset whose security level was judged, set as a string of 120 or fewer bytes.
2	Judgment item	Name of the judgment item judged as <i>Danger</i> , <i>Warning</i> , or <i>Caution</i> by the PC security setting judgment, set as a string of 256 or fewer bytes.
3	Setting	The setting, taken from inventory information, for a judgment item judged as <i>Danger</i> , <i>Warning</i> , or <i>Caution</i> by the judgment of PC security settings. This item is set as a string of 6,144 or fewer bytes. This item is blank if no setting exists.
4	Security level	Security level set as one of the following codes: 100: Safe 200: Caution 300: Warning 400: Danger

**(3) Specification example**

```
"1000000001","Vulnerable password","user1;user2","400" ↓
"1000000001","Shared folder settings","", "400" ↓
"1000000002","Days since the password was
updated","admin","400" ↓
```



## 16.10 PC list information file

A PC list information file is created when the PC list information output command (`cscexportplist`) is executed.

Asset information and judgment results for clients whose security levels were judged on the specified date and time are output as PC list information in CSV format. The administrator can use the PC list information file to manage PC security levels.

The PC list information files consist of an asset information list file and judgment result files (one file for each type of judgment result). The contents of the files are the same as the information displayed in the Client Security Management window.

The following table lists the PC list information files.

*Table 16-32: PC list information files*

No.	Item name	File name	Description
1	Asset information list file	cscmassetinfo.csv	The information displayed in the PC List window of the Client Security Management window
2	Judgment result file (security updates)	cscmupresult.csv	The information displayed in each details window of the Client Security Management window
3	Judgment result file (anti-virus products)	cscmvrsresult.csv	
4	Judgment result file (prohibited software)	cscmunjustresult.csv	
5	Judgment result file (mandatory software)	cscmneedjdgrslt.csv	
6	Judgment result file (user definition)	cscmusrjdgrslt.csv	
7	Judgment result file (PC security settings)	cscmpcsecurityresult.csv	

Each file has the same syntax. Note the following:

- Items are delimited with commas ( , ).
- Each item value is enclosed in double quotation marks ( "). Two double quotation marks in succession ( " " ) indicate an omitted value.
- A double quotation mark ( " ) appearing within an item value string is set as two double quotation marks ( " " ).

- The line feed code is 0x0d0a.
- A title line containing the item names in a PC list information file is set at the beginning of the file.
- Items output to a judgment result file vary depending on the argument specified in the PC list information output command (`cscexportplist`).

When the `-s` option is not specified:

Information related to the judgment results *Danger*, *Warning*, *Caution*, and *Unknown* is output. Information related to the judgment results *Safe* and *Not applicable* is not output. When the judgment results for all the assets are *Safe* or *Not applicable*, a judgment result file is not created.

When the `-s` option is specified:

Information related to the judgment results *Danger*, *Warning*, *Caution*, *Safe*, and *Unknown* is output. Information related to the judgment result *Not applicable* is not output. When the judgment results for all the assets are *Not applicable*, a judgment result file is not created.

- For the asset information list file, all assets subject to the security level judgment are output irrespective of the security level.

For details about the PC list information output command (`cscexportplist`), see `cscexportplist` (outputs PC list information) in 15. Commands.

### 16.10.1 Asset information list file

The following shows the information output to an asset information list file, and a display example.

#### (1) Output information

The following table shows the information that is output.

Table 16-33: Information output to an asset information list file

No.	Item	With a security level judgment date specified	Without a security level judgment date specified
1	Asset No.	Latest	Latest
2	Host name	Latest	Latest
3	IP address	Latest	Latest
4	User name	Latest	Latest
5	Group name	Latest	Latest
6	PC security level	History	Latest

No.	Item	With a security level judgment date specified	Without a security level judgment date specified
7	PC security level judgment date	History	Latest
8	Number of consecutive times for the same security level	Latest	Latest
9	Number of consecutive days for the same security level	Latest	Latest
10	MAC address	Latest	Latest
11	Warning date	History	Latest
12	Network connection status	History	Latest
13	Update date of network connection status	History	Latest
14	Execution date of user definition	History	Latest
15	Security level of security updates	History	Latest
16	Security level of anti-virus products	History	Latest
17	Security level of prohibited software	History	Latest
18	Security level of mandatory software	History	Latest
19	Security level of PC security settings	History	Latest
20	Security level of user definition	History	Latest
21	OS	Latest	Latest
22	Location	Latest	Latest
23	Security management	Latest	Latest
24	Evaluation point	History	Latest
25	Judgment policy	History	Latest
26	Renewal date of judgment policy	Latest	Latest
27	Assigned date of judgment policy	Latest	Latest
28	Action policy	History	Latest

No.	Item	With a security level judgment date specified	Without a security level judgment date specified
29	Renewal date of action policy	Latest	Latest
30	Assigned date of action policy	Latest	Latest

Legend:

Latest: The latest information when the command is executed

History: Information that exists during the specified security level judgment

*Reference note:*

The settings specified in AIM are applied to the items output to an asset information list file, their output order, and the item names shown in the title line.

- Output items and output order

The items output to the asset information list file and their output order are the items and output order specified as the format applied to the CSC administrator in **PC Security Level Management** in the Customize Job Windows window. If no format applies to the CSC administrator, all items shown in Table 16-33 are output in the order they appear in the table.

- Item names

The item names shown in the title line output to the asset information list file are the names specified in the Customize Managed Items window of AIM.

For details about the Customize Job Windows window and Customize Managed Items window, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

## (2) Definition information

The following table shows the information set in this file.

"asset-No." , "host-name" , "IP-address" , "user-name" , "group-name" , "PC-security-level" , "PC-security-level-judgment-date" , "number-of-consecutive-times-for-the-same-security-level" , "number-of-consecutive-days-for-the-same-security-level" , "MAC-address" , "warning-date" , "network-connection-status" , "update-date-of-network-connection-status" , "execution-date-of-user-definition" , "security-level-of-security-updates" , "security-level-of-anti-virus-products" , "security-level-of-prohibited-software" , "security-level-of-mandatory-software" , "security-level-of-PC-security-settings" , "security-level-of-user-definition" , "OS" , "location" , "security-management" , "evaluation-point" , "judgment-policy" , "renewal-date-of-judgment-policy"

, "assigned-date-of-judgment-policy" , "action-policy" , "renewal-date-of-action-policy" , "assigned-date-of-action-policy" ↓

Legend: ↓: Line feed code

### (3) File output example

The following shows an example of file output.

```
"10000000001" , "vm2ksrvSP4" , "192.168.136.111" , "" , "" , "Warning" , "2006/03/23 19:55:59" , "1" , "1" , "00:0c:29:a1:2a:72" , "" , "-" , "" , "" , "Warning" , "Not applicable" , "Not applicable" , "Not applicable" , "Not applicable" , "Not applicable" , "Microsoft Windows 2000 Server" , "" , "Valid" , "50" , "(default policy)" , "2006/03/23 19:55:40" , "" , "(default policy)" , "2006/03/23 19:53:42" , "" ↓
```

## 16.10.2 Judgment result file (security updates)

The following shows the information output to a judgment result file (security updates) and a display example.

### (1) Output information

The following table shows the information that is output.

Table 16-34: Information output to a judgment result (security updates) file

No.	Item
1	Asset No.
2	Security level for security updates
3	PC security level judgment date
4	OS
5	Service pack
6	Judgment conditions
7	Security updates information
8	Security level

Note:

When there is more than one security update for which information is to be output, multiple lines are output. The information for each line is the same for Nos. 1 to 6, but different for Nos. 7 and 8.

**(2) Definition information**

The following table shows the information set in this file.

```
"asset-No." , "security-level-for-security-updates" , "PC-security-level-judgment-date" , "OS" , "service-pack" , "judgment-conditions" , "security-updates-information" , "security-level" ↓
```

Legend: ↓: Line feed code

**(3) File output example**

The following shows an example of file output.

```
"1000000001" , "Unknown" , "2006/03/30 15:32:22" , "Windows XP Professional" , "Service Pack 1" , "Specified security updates" , "01-001(123456)" , "Unknown" ↓
"1000000001" , "Unknown" , "2006/03/30 15:32:22" , "Windows XP Professional" , "Service Pack 1" , "Specified security updates" , "01-002(654321)" , "Unknown" ↓
```

**16.10.3 Judgment result file (anti-virus products)**

The following shows the information output to a judgment result file (anti-virus products), and a display example.

**(1) Output information**

The following table shows the information that is output.

*Table 16-35: Information output to a judgment result file (anti-virus products)*

No.	Item		Item names on the title line
1	Asset No.		Asset No.
2	Security level for anti-virus products		Security level for anti-virus products
3	PC security level judgment date		PC security level judgment date
4	Installation information	Product name	Product name (installed)
5		Product version	Product version (installed)
6		Engine version	Engine version (installed)
7		Virus definition file version	Virus definition file version (installed)
8		Resident status	Resident status

No.	Item		Item names on the title line
9	Policy information and judgment result	Product name	Product name (policy)
10		Product version	Product version (policy)
11		Engine version	Engine version (policy)
12		Virus definition file version	Virus definition file version (policy)
13		Nonresident judgment	Nonresident judgment
14		Security level	Security level

Notes:

- When there is more than one multiple anti-virus product for which information is to be output, multiple lines are output. The information for each line is the same for Nos. 1 to 8, but different for Nos. 9 to 14.
- When multiple anti-virus products are installed on the client, multiple lines are output. The information for each line is the same for Nos. 1 to 3, but different for Nos. 4 to 14. If the `-s` option is not specified and the judgment result for No. 2 is **Safe**, no judgment results are output.
- If a product other than the specified anti-virus products has been installed, items for Nos. 9 to 14 are not output because there is no policy information that can be used for judgment.

## (2) Definition information

The following table shows the information set in this file.

"asset-No." , "security-level-for-anti-virus-products" , "PC-security-level-judgment-date" , "product-name<sup>#1</sup>" , "product-version<sup>#1</sup>" , "engine-version<sup>#1</sup>" , "virus-definition-file-version<sup>#1</sup>" , "resident-status" , "product-name<sup>#2</sup>" , "product-version<sup>#2</sup>" , "engine-version<sup>#2</sup>" , "virus-definition-file-version<sup>#2</sup>" , "nonresident-judgment" , "security-level" ↓

Legend: ↓: Line feed code

#1

Information related to installation

#2

Information related to policy and judgment results

**(3) File output example**

The following shows an example of file output.

```
"1000000001","Danger"," 2006/03/30 16:25:19","AntiVirus
Corporate Edition 9.0","9.0.310","51.3.0.11",
"20060327.006","Resident","AntiVirus Corporate Edition
9.0","9.0.310","51.3.0.11","20060327.007","Judge","Danger" ↓
```

**16.10.4 Judgment result file (prohibited software)**

The following shows the information output to a judgment result file (prohibited software), and a display example.

**(1) Output information**

The following table shows the information that is output.

*Table 16-36: Information output to a judgment result file (prohibited software)*

No.	Item
1	Asset No.
2	Security level for prohibited software
3	PC security level judgment date
4	Prohibited software name
5	Install status
6	Installed version
7	Prohibited version
8	Security level

Note:

When there is more than one prohibited software product for which information is to be output, multiple lines are output. The information for each line is the same for Nos. 1 to 3, but different for Nos. 4 to 8.

**(2) Definition information**

The following table shows the information set in this file.

```
"asset-No." , "security-level-for-prohibited-software" , "PC-security-level-judgment-
date" , "prohibited-software-name" , "install-status" , "installed-version" , "prohibit
ed-version" , "security-level" ↓
```

Legend: ↓: Line feed code



**(3) File output example**

The following shows an example of file output.

```
"1000000001", "Caution", "2006/03/30 16:43:51", "JP1/Software
Distribution Client -
Base", "Installed", "0800", "0800", "Caution" ↓
```

**16.10.5 Judgment result file (mandatory software)**

The following shows the information output to a judgment result file (mandatory software), and a display example.

**(1) Output information**

The following table shows the information that is output.

*Table 16-37: Information output to a judgment result file (mandatory software)*

No.	Item
1	Asset No.
2	Security level for mandatory software
3	PC security level judgment date
4	Software group name
5	Mandatory software name
6	Install status
7	Installed version
8	Mandatory version
9	Security level of software
10	Security level of group

Note:

When there is more than one prohibited software product for which information is to be output, multiple lines are output. The information for each line is the same for Nos. 1 to 3, but different for Nos. 4 to 10.

**(2) Definition information**

The following table shows the information set in this file.

```
"asset-No." , "
security-level-for-mandatory-software" , "PC-security-level-judgment-date" , "softw
are-group-name" , "mandatory-software-name" , "install-status" , "installed-version"
```

" , "mandatory-version" , "security-level-of-software" , " security-level-of-group" ↓

Legend: ↓ : Line feed code

### (3) File output example

The following shows an example of file output.

```
"1000000001" , "Caution" , "2006/03/30 17:05:57" , "JP1/Software
Distribution
Client" , " , "Installed" , "0800" , "0810" , "Caution" , "Caution" ↓
```

## 16.10.6 Judgment result file (user definition)

The following shows the information output to a judgment result file (user definition), and a display example.

### (1) Output information

The following table shows the information that is output.

Table 16-38: Information output to a judgment result file (user definitions)

No.	Item
1	Asset No.
2	Security level for user definition
3	PC security level judgment date
4	Judgment item
5	Class
6	Property
7	Value
8	Comparison condition
9	Comparison value
10	Result
11	Security level

Notes:

- When there is more than one judgment item for which information is to be output, multiple lines are output. The information for each line is the same for Nos. 1 to 3, but different for Nos. 4 to 11.

- When multiple judgment conditions are specified for the judgment item, multiple lines are output. The information for each line is the same for Nos. 1 to 4, but different for Nos. 5 to 11.

## (2) Definition information

The following table shows the information set in this file.

```
"asset-No." , "security-level-for-user-definition" , "PC-security-level-judgment-date" , "judgment-item" , "class" , "property" , "value" , "comparison-condition" , "comparison-value" , "result" , "security-level" ↓
```

Legend: ↓: Line feed code

## (3) File output example

The following shows an example of file output.

```
"1000000001" , "Caution" , "2008/02/19 13:48:18" , "Power-saving CPU" , "Hardware information" , "CPU" , "28681" , "Do not match" , "28694" , "Failed" , "Caution" ↓
"1000000001" , "Caution" , "2008/02/19 13:48:18" , "Power-saving CPU" , "Hardware information" , "CPU" , "28681" , "Do not match" , "28695" , "Failed" , "Caution" ↓
```

## 16.10.7 Judgment result file (PC security settings)

The following shows the information output to a judgment result file (PC security settings) and a display example.

### (1) Output information

The following table shows the information that is output.

Table 16-39: Information output to a judgment result (PC security settings) file

No.	Item
1	Asset No.
2	Security level for PC security settings
3	PC security level judgment date
4	Group
5	Judgment items
6	Values
7	Judgment conditions
8	Security level

Note:

- When there is more than one judgment item for which information is to be output, multiple lines are output. In this case, the information for each line is the same for Nos. 1 to 3, but different for Nos. 4 to 8.
- When there is more than one judgment item for the group, multiple lines are output. In this case, the information for each line is the same for Nos. 1 to 4, but different for Nos. 5 to 8.

## **(2) Definition information**

The following table shows the information defined in this file.

"asset-No." , "security-level-for-PC-security-settings" , "PC-security-level-judgment-date" , "group" , "judgment-items" , "values" , "judgment-conditions" , "security-level" ↓

Legend: ↓ : Line feed code

## **(3) File output example**

The following shows an example of file output.

"1000000001" , "Caution" , "2006/07/04 18:20:22" , "Automatic updates" , "Settings for Windows automatic updates" , "Disabled" , "-" , "Caution" ↓

---

## 16.11 Patch update condition file

---

This file is used in the `-f` option of the judgment policy update command for security updates (`cscpatchupdate`). It defines the conditions for updating patch information by specifying information such as the release date of the patch and the OS to which it applies. The file also defines security levels tied to the priority of the patch. Create the file with any file name in any directory.

### (1) Synopsis

```
Patch_Release_Start=release-date-(start) ↓
Patch_Release_End=release-date-(end) ↓
Patch_Release_Period=release-period ↓
Patch_Product=product-type ↓
Patch_Class=class ↓
Patch_OS=target-OS ↓
Patch_Serious=severity-rating ↓
Patch_Update_Cond=update-condition ↓
Patch_Version=processing-dependent-on-patch-information-file-version ↓
Patch_Delay=update-delay-time ↓
Patch_Emergency=security-level-setting-(critical) ↓
Patch_Importance=security-level-setting-(important) ↓
Patch_Warning=security-level-setting-(moderate) ↓
Patch_Caution=security-level-setting-(low) ↓
Patch_Nothing=security-level-setting-(unspecified) ↓
```

Legend: ↓: Line feed code

### (2) Definition contents

The following table shows the contents set in this file.

Table 16-40: Contents of a patch update condition file

No.	Parameter	Setting item	Setting value
1	Patch_Release_Start	Release date (start)	Specify the first and last release dates, in the format YYYY/MM/DD.
2	Patch_Release_End	Release date (end)	<p>If you specify only a start date, patch information is updated for all patches released since that date.</p> <p>If you specify only an end date, patch information is updated for all patches released up to that date.</p> <p>If you specify a start and end date, patch information is updated for all patches released between those dates.</p> <p>If you omit both dates, patch information is updated for all patches regardless of their release dates.</p>
3	Patch_Release_Period	Release period	<p>Specify a release period as a numeral from 0 to 100.</p> <p>Patch information will be updated for all patches whose release date falls within the specified number of days from when the command was executed.</p> <p>If you specify a release date in the patch update condition file, the release period is ignored.</p> <p>When omitted, patch information is updated for all patches regardless of when they were released.</p>
4	Patch_Product	Product type	<p>Specify the product types for which to update patch information.</p> <p>0: All (OS and software products) 1: OS 2: Software products</p> <p>When omitted, patch information is updated for operating systems and software products.</p>

No.	Parameter	Setting item	Setting value
5	Patch_Class	Class	Specify one or more classes of patch for which to update patch information. 0: All patches 1: Critical updates 2: Security updates 8: Security rollups When omitted, patch information is updated for security updates.
6	Patch_OS	Target OS	Specify one or more operating systems for which to update patch information. 0: All 1: Windows 2000 2: Windows XP 4: Windows Server 2003 8: Windows Server 2003 Datacenter 16: Windows Vista 32: Windows Server 2008 64: Windows 7 128: Windows Server 2008 R2 When omitted, patch information is updated for all operating systems.
7	Patch_Serious	Severity rating	Specify one or more patch severity ratings for which to update patch information. 0: All 1: Critical 2: Important 3: Moderate 4: Low 5: Unspecified When omitted, patch information is updated for patches whose severity rating is critical or important.

No.	Parameter	Setting item	Setting value
8	Patch_Update_Cond	Update condition	Specify whether to update patch information only for patches added since the last time the command was executed. 0: Only patches added since last execution 1: All patches If you omit this setting, patch information is updated only for patches added since the last time the command was executed. If you set a release period that predates the last time the command was executed, specify 1 for this item.
9	Patch_Version	Processing dependent on patch information file version	Specify whether to update patch information if the patch information file has not changed since the last time the command was executed. 0: Do not update patch information. 1: Update patch information. When omitted, patch information is not updated.
10	Patch_Delay	Update delay time	Specify an update delay time, as a numeral from 0 to 100. Processing is executed after the specified number of days have elapsed from the date of the patch information file. If you do not specify an update delay time, patch information is updated without delay.
11	Patch_Emergency	Security level setting (critical)	The security level to assign to patches whose severity rating is critical. Specify one of the following codes: 200: Caution 300: Warning 400: Danger When omitted, 300 (Warning) is set.



No.	Parameter	Setting item	Setting value
12	Patch_Importance	Security level setting (important)	The security level to assign to patches whose severity rating is important. Specify one of the following codes: 200: Caution 300: Warning 400: Danger When omitted, 300 (Warning) is set.
13	Patch_Warning	Security level setting (moderate)	The security level to assign to patches whose severity rating is moderate. Specify one of the following codes: 200: Caution 300: Warning 400: Danger When omitted, 200 (Caution) is set.
14	Patch_Caution	Security level setting (low)	The security level to assign to patches whose severity rating is low. Specify one of the following codes: 200: Caution 300: Warning 400: Danger When omitted, 200 (Caution) is set.
15	Patch_Nothing	Security level setting (unspecified)	The security level to assign to patches whose severity rating is unspecified. Specify one of the following codes: 200: Caution 300: Warning 400: Danger When omitted, 200 (Caution) is set.

Note the following coding conventions:

- Lines beginning with a hash symbol (#) are treated as comments.
- End every line with a line feed code. The line feed code is 0x0d0a. Lines containing only a line feed code are ignored.

### (3) Specification example

```
Patch_Release_Start=2007/03/01 ↓
Patch_Release_End=2008/03/31 ↓
Patch_Release_Period=0 ↓
Patch_Product=0 ↓
Patch_Class=0 ↓
Patch_OS=0 ↓
Patch_Serious=0 ↓
Patch_Update_Cond=0 ↓
Patch_Version=0 ↓
Patch_Delay=0 ↓
Patch_Emergency=400 ↓
Patch_Importance=400 ↓
Patch_Warning=300 ↓
Patch_Caution=200 ↓
Patch_Nothing=200 ↓
```

## 16.12 Statistics output file

A statistics output file is created when the statistics output command (`cscexportcount`) is executed.

The status of security measures for the specified groups is accumulated from various perspectives and output to the file as statistics in CSV format.

There are four types of statistics output file: evaluation point files, countermeasure usage files, countermeasure usage details files, and countermeasure usage files for user-defined judgment items. Each of these files contains statistics accumulated from a different perspective. The contents of the files are the same as the information displayed in the Client Security Management window.

The following table lists the statistics output files.

*Table 16-41: Statistics output files*

No.	Item name	File name	Description
1	Evaluation point file	<code>cscjudgemark.csv</code>	Statistics accumulated from the perspective of evaluation points
2	Countermeasure usage file	<code>cscmupresult.csv</code>	Statistics from the perspective of the overall countermeasure usage for all judgment items
3	Countermeasure usage details file	<code>cscmvrresult.csv</code>	Statistics from the perspective of countermeasure usage for specific judgment items
4	Countermeasure usage file for user-defined judgment items	<code>cscuseritemnnn#.csv</code>	Statistics reflecting the countermeasure usage for user-defined judgment items

#

*nnn* is a number from 101 to 110, corresponding to the value specified for the `-c` option of the statistics output command (`cscexportcount`).

Each file has the same syntax. Note the following:

- Each item value is enclosed in double quotation marks ("). Two double quotation marks in succession (" ") indicate an omitted value.
- A double quotation mark (") appearing within an item value string is set as two double quotation marks (" ").
- A title line containing the item names in the statistics output file is set at the beginning of the file.

- Items output to the statistics output file vary depending on the arguments specified in the statistics output command (`cscexportcount`).

When the `-d` option is specified

The file contains statistics totaled by day.

When the `-w` option is specified

The file contains statistics totaled by week.

When the `-m` option is specified

The file contains statistics totaled by month.

For details about the statistics output command (`cscexportcount`), see *cscexportcount (outputs statistics on the status of security measures)* in 15. *Commands*.

### 16.12.1 Evaluation point file

The following shows the information output to an evaluation point file, and shows display examples.

#### (1) Output information

The following table shows the information that is output.

*Table 16-42: Information output to an evaluation point file*

No.	Item	Description
1	Group	The name of the group
2	Date (day)	When statistics are totaled by day, a date is output for each day.
3	Date (week)	When statistics are totaled by week, the first date to be output is the start date for totals. Subsequent dates correspond to the same specified day of the week in each subsequent week.
4	Date (month)	When statistics are totaled by month, a date is output for each month.
5	Evaluation points	The average evaluation points over the period

#### (2) Definition information

The following information is set in this file.

"Group" , "date" , "date" , "date" , "date" , "date" , "date" , ... ↓

"group-name" , "evaluation-points" , "evaluation-points" , "evaluation-points" , "evaluation-points" , "evaluation-points" , "evaluation-points" , ... ↓

Legend: ↓: Line feed code

### (3) File output example

The following shows an example of file output when statistics are totaled by day.

```
"Group", "2007/10/01", "2007/10/02", "2007/10/03", "2007/10/04" ↓
"General_Affairs_Department", "20", "25", "20", "27" ↓
"Sales_Department", "15", "20", "10", "20" ↓
```

The following shows an example of file output when statistics are totaled by week.

```
"Group", "2007/10/01", "2007/10/03", "2007/10/10", "2007/10/
17", "2007/10/24" ↓
"General_Affairs_Department", "20", "25", "20", "27", "24" ↓
"Sales_Department", "15", "20", "10", "20", "28" ↓
```

Note:

When statistics are totaled by week, the first date indicates the start date for totals, and subsequent dates indicate the same specified day of the week in each successive week.

The following shows an example of file output when statistics are totaled by month.

```
"Group", "2007/10", "2007/11", "2007/12", "2008/01", "2008/02" ↓
"General_Affairs_Department", "20", "25", "20", "27", "24" ↓
"Sales_Department", "20", "25", "10", "27", "24" ↓
```

## 16.12.2 Countermeasure usage file

The following shows the information output to a countermeasure usage file, and shows display examples.

### (1) Output information

Table 16-43: Information output to a countermeasure usage file

No.	Item	Description
1	Group	The name of the group
2	Date (day)	When statistics are totaled by day, a date is output for each day.
3	Date (week)	When statistics are totaled by week, the first date to be output is the start date for totals. Subsequent dates correspond to the same specified day of the week in each subsequent week.
4	Date (month)	When statistics are totaled by month, a date is output for each month.

No.	Item	Description
5	Countermeasure usage	The overall countermeasure usage across all judgment items

## (2) Definition information

The following information is set in this file.

```
"Group" , "date" , "date" , "date" , "date" , "date" , "date" , ... ↓
"group-name" , "countermeasure-usage" , "countermeasure-usage" , "countermeasure-usage" , "countermeasure-usage" , "countermeasure-usage" , "countermeasure-usage" , "countermeasure-usage" , ... ↓
```

Legend: ↓: Line feed code

## (3) File output example

The following shows an example of file output when statistics are totaled by day.

```
"Group" , "2007/10/01" , "2007/10/02" , "2007/10/03" , "2007/10/04" ↓
"General_Affairs_Department" , "20.5" , "25.5" , "20.2" , "27.5" ↓
"Sales_Department" , "15.3" , "20.5" , "10.2" , "20.0" ↓
```

The following shows an example of file output when statistics are totaled by week.

```
"Group" , "2007/10/01" , "2007/10/03" , "2007/10/10" , "2007/10/17" , "2007/10/24" ↓
"General_Affairs_Department" , "20.5" , "25.2" , "20.5" , "27.5" , "24.5" ↓
"Sales_Department" , "15.5" , "20.2" , "10.2" , "20.5" , "28.5" ↓
```

Note:

When statistics are totaled by week, the first date indicates the start date for totals, and subsequent dates indicate the same specified day of the week in each successive week.

The following shows an example of file output when statistics are totaled by month.

```
"Group" , "2007/10" , "2007/11" , "2007/12" , "2008/01" , "2008/02" ↓
"General_Affairs_Department" , "20.2" , "25.5" , "20.3" , "27.5" , "24.6" ↓
"Sales_Department" , "20.5" , "25.3" , "10.2" , "27.5" , "24.5" ↓
```

### 16.12.3 Countermeasure usage details file

The following shows the information output to a countermeasure usage details file, and

shows display examples.

### (1) Output information

Table 16-44: Information output to a countermeasure usage details file

No.	Item	Description
1	Judgment item	The name of the judgment item
2	Date (day)	When statistics are totaled by day, a date is output for each day.
3	Date (week)	When statistics are totaled by week, the first date to be output is the start date for totals. Subsequent dates correspond to the same specified day of the week in each subsequent week.
4	Date (month)	When statistics are totaled by month, a date is output for each month.
5	Countermeasure usage	Countermeasure usage for each judgment item

### (2) Definition information

The following information is set in this file.

```
"Judgment item", "date", "date", "date", "date", "date", ... ↓
"Overall", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", ... ↓
"Security
updates", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", ... ↓
"Anti-virus
products", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", ... ↓
"Prohibited
software", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", ... ↓
"Mandatory
software", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", ... ↓
"PC security
settings", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", ... ↓
"User
definition", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", "countermeasure-usage", ... ↓
```

Legend: ↓ : Line feed code

### (3) File output example

The following shows an example of file output when statistics are totaled by day.

```
"Judgment item","2007/10/01","2007/10/02","2007/10/03","2007/10/04" ↓
"Overall","20.5","25.0","31.8","27.5" ↓
"Security updates","20.5","25.0","20.8","27.0" ↓
"Anti-virus products","15.0","20.5","10.8","20.4" ↓
"Prohibited software","20.5","24.0","21.8","27.5" ↓
"Mandatory software","14.0","25.5","11.8","20.4" ↓
"PC security settings","20.5","25.0","31.8","27.5" ↓
"User definition","13.0","15.5","11.8","20.4" ↓
```

The following shows an example of file output when statistics are totaled by week.

```
"Judgment item","2007/10/01","2007/10/03","2007/10/10","2007/10/17" ↓
"Overall","20.5","25.0","31.8","27.5" ↓
"Security updates","20.5","25.0","20.8","27.0" ↓
"Anti-virus products","15.0","20.5","10.8","20.4" ↓
"Prohibited software","20.5","24.0","21.8","27.5" ↓
"Mandatory software","14.0","25.5","11.8","20.4" ↓
"PC security settings","20.5","25.0","31.8","27.5" ↓
"User definition","13.0","15.5","11.8","20.4" ↓
```

Note:

When statistics are totaled by week, the first date indicates the start date for totals, and subsequent dates indicate the same specified day of the week in each successive week.

The following shows an example of file output when statistics are totaled by month.

```
"Judgment item","2007/10","2007/11","2007/12","2008/01","2008/02" ↓
"Overall","20.5","25.0","31.8","27.5" ↓
"Security updates","20.5","25.0","20.8","27.0" ↓
"Anti-virus products","15.0","20.5","10.8","20.4" ↓
"Prohibited software","20.5","24.0","21.8","27.5" ↓
"Mandatory software","14.0","25.5","11.8","20.4" ↓
"PC security settings","20.5","25.0","31.8","27.5" ↓
"User definition","13.0","15.5","11.8","20.4" ↓
```



## 16.12.4 Countermeasure usage file for user-defined judgment items

The following shows the information output to a countermeasure usage file for user-defined judgment items, and shows display examples.

### (1) Output information

Table 16-45: Information output to a countermeasure usage file for user-defined judgment items

No.	Item	Description
1	Group	The name of the group
2	Date (day)	When statistics are totaled by day, a date is output for each day.
3	Date (week)	When statistics are totaled by week, the first date to be output is the start date for totals. Subsequent dates correspond to the same specified day of the week in each subsequent week.
4	Date (month)	When statistics are totaled by month, a date is output for each month.
5	Countermeasure usage	Countermeasure usage for user-defined judgment items

### (2) Definition information

The following information is set in this file.

```
"Group" , "date" , "date" , "date" , "date" , "date" , "date" , ... ↓
"group-name" , "countermeasure-usage" , "countermeasure-usage" , "countermeasu
re-usage" , "countermeasure-usage" , "countermeasure-usage" , "countermeasure-u
sage" , ... ↓
```

Legend: ↓: Line feed code

### (3) File output example

The following shows an example of file output when statistics are totaled by day.

```
"Group" , "2007/10/01" , "2007/10/02" , "2007/10/03" , "2007/10/04" ↓
"General_Affairs_Department" , "20.5" , "20.5" , "33.3" , "33.3" ↓
"Sales_Department" , "15.3" , "15.3" , "15.3" , "20.0" ↓
```

The following shows an example of file output when statistics are totaled by week.

```
"Group" , "2007/10/01" , "2007/10/03" , "2007/10/10" , "2007/10/
17" , "2007/10/24" ↓
"General_Affairs_Department" , "20.5" , "20.5" , "33.3" , "33.3" , "33.3
" ↓
```

```
"Sales_Department", "15.5", "15.5", "20.5", "20.5", "28.5" ↓
```

Note:

When statistics are totaled by week, the first date indicates the start date for totals, and subsequent dates indicate the same specified day of the week in each successive week.

The following shows an example of file output when statistics are totaled by month.

```
"Group", "2007/10", "2007/11", "2007/12", "2008/01", "2008/02" ↓  
"General_Affairs_Department", "20.2", "25.5", "30.3", "35.5", "35.5"  
" ↓  
"Sales_Department", "20.5", "25.3", "30.2", "30.2", "34.5" ↓
```

## 16.13 Anti-virus product policy import file

This file is specified in the judgment policy update command (`cscpolimport`). Define information such as anti-virus product names and virus definition file versions in this file. Create the file with any file name in any directory.

### (1) Synopsis

```
operation , category , judgment-policy-name , anti-virus-product-name , product-version , engine-version , virus-definition-file-version , Danger-judgment-for-PCs-with-non-resident-anti-virus-products , security-level ↓
:
```

Legend: ↓: Line feed code

### (2) Definition contents

The following table shows the contents to define in this file.

Table 16-46: Definition contents of an anti-virus product policy import file

No.	Item	Setting value
1	Operation	Specify the command operation. The setting value is U.
2	Category	Specify the update category. ALL: Update all policies. POLICY: Update the policy specified in <i>judgment-policy-name</i> .
3	Judgment policy name	For the POLICY category, specify the name of the judgment policy using a string with 128 or fewer bytes. This item cannot be specified for the ALL category.
4	Anti-virus product name	Specify the name of the anti-virus product, using a string with 255 or fewer bytes. The judgment policy is updated if it contains the specified anti-virus product name. Otherwise, the anti-virus product name is added as a new line in the judgment policy.
5	Product version	Specify the product version, using a string with 255 or fewer bytes. When omitted, the setting for this item is not updated.
6	Engine version	Specify the engine version in 255 or fewer bytes, using alphanumeric characters and symbols. When omitted, the setting for this item is not updated.

No.	Item	Setting value
7	Virus definition file version	Specify the virus definition file version in 255 or fewer bytes, using alphanumeric characters and symbols. When omitted, the setting for this item is not updated.
8	Danger judgment for PCs with nonresident anti-virus products	Specify whether to judge the security level of clients that have nonresident anti-virus products as <i>Danger</i> . 0: Do not perform 1: Perform When omitted, the setting for this item is not updated. When an anti-virus product name is added to the judgment policy, 0 (do not perform) is set.
9	Security level	Security level set as one of the following codes: 200: Caution 300: Warning 400: Danger When omitted, the setting for this item is not updated. When an anti-virus product name is added to the judgment policy, 400 (Danger) is set.

Note the following coding conventions:

- Lines beginning with a hash symbol (#) are treated as comments. The hash symbol cannot be used except at the start of a line.
- You can write multiple lines in the file.
- End every line with a line feed code. The line feed code is 0x0d0a. Lines containing only a line feed code are ignored.

### (3) Specification example

```
U,POLICY,(default policy),AntiVirus Corporate Edition
9.0,9.0.3.100,51.3.0.11,20060225.000,1,400 ↓
```

---

## 16.14 Policy import execution file (manual)

---

This file is specified in the judgment policy update command (`cscpolimport`) when the judgment policies for anti-virus products are to be updated automatically.

This file is set by JP1/CSC. It contains anti-virus product names, virus definition file versions, and other settings.

The file name of the policy import execution file (manual) and the folder in which it resides are as follows.

File name	Folder
<code>cscmpolimport.dat</code>	<i>JP1/CSC - Manager-installation-folder\spool</i>

For details about how to update judgment policies automatically, see *6.4.6 Updating judgment policies for anti-virus products automatically or manually*. For details about the judgment policy update command (`cscpolimport`), see *cscpolimport (updates judgment policy settings)* in *15. Commands*.

## 16.15 Network connection control list file

This file specifies the clients whose network connections are to be controlled from JP1/CSC - Manager Remote Option. In this file, specify one or more of the following to identify each client: MAC address, IP address, or host name. The client specification is handled according to the following rules:

- When a MAC address is specified, the client is identified by MAC address only.
- When only an IP address is specified, the client is identified by IP address.
- When only a host name is specified, the client is identified by host name.
- When both an IP address and host name are specified, the client is identified by both IP address and host name.

Create the file with any file name in any directory.

### (1) Synopsis

```
MAC-address , IP-address , host-name ↓
MAC-address , IP-address , host-name ↓
:
:
```

Legend: ↓ : Line feed code

### (2) Definition contents

The following table shows the contents to define in this file.

Table 16-47: Definition contents of a network connection control list file

No.	Item	Setting value
1	MAC address	Write the MAC addresses of the clients whose network connections are to be controlled, one address per line. Specify each MAC address as 12 hexadecimal digits. MAC addresses are not case sensitive. You can use a delimiter after every second digit. Only one type of delimiter can be used in one MAC address. Hyphens (–) or colons (:) can be used as the delimiter, or you can write the addresses without any delimiter. Note that spaces cannot be used as a delimiter.
2	IP address	Specify the IP address corresponding to the MAC address in IPv4 format (xxx.xxx.xxx.xxx).

No.	Item	Setting value
3	Host name	Specify the host name of the client using a string with 64 or fewer bytes.

Note the following coding conventions:

- You can write multiple lines in the file.
- End every line with a line feed code. The line feed code is 0x0d0a. Lines containing only a line feed code are ignored.

**(3) Specification example**

```
00:11:22:33:44:11,192.168.1.111,client01 ↓
00:11:22:33:44:22,192.168.1.222,client02 ↓
00:11:22:33:44:33,192.168.1.333,client03 ↓
00:11:22:33:44:44,, ↓
,192.168.1.444, ↓
,,client04 ↓
```

## 16.16 Import file

This file is specified when executing the connection control list import command (`cscrimport`). Its contents are imported as a connection control list.

When the command for exporting a connection control list (`cscrexport`) is executed, an export file is output in the same format as the import file.

The import file is a text file in CSV format, and can be created with any file name in any directory.

### (1) Synopsis

```
MAC-address , IP-address , connection-status { 1 | 2 } ↓
MAC-address , IP-address , connection-status { 1 | 2 } ↓
:
:
```

Legend: ↓: Line feed code

### (2) Definition contents

The following table shows the contents to define in this file.

Table 16-48: Definition contents of an import file

No.	Item	Setting value
1	MAC address <sup>#</sup>	Write the MAC addresses of the clients whose information is to be imported, one address per line. Specify each MAC address as 12 hexadecimal digits. MAC addresses are not case sensitive. You can use a delimiter after every second digit. Only one type of delimiter can be used in one MAC address. The following delimiters can be used: <ul style="list-style-type: none"> <li>• Hyphen (-)</li> <li>• Colon (:)</li> <li>• Space</li> </ul>
2	IP address	Specify the IP address corresponding to the MAC address.
3	Connection status	Specify the connection status (permit or deny). 1: Deny 2: Permit

<sup>#</sup>

In the file output by the export command (`cscrexport`), the digits are delimited



with colons (:).

Note the following coding conventions:

- You can write multiple lines in the file.
- End every line with a line feed code. The line feed code is 0x0d0a. Lines containing only a line feed code are ignored.

### (3) *Specification example*

No delimiter used:

```
0000E2701623,192.168.2.10,1 ↓
0000E2701624,192.168.2.11,1 ↓
0000E2701625,192.168.2.12,1 ↓
0000E2701626,192.168.2.13,1 ↓
0000E2701627,192.168.2.14,2 ↓
0000E2701628,192.168.2.15,2 ↓
0000E2701628,192.168.2.16,2 ↓
0000E2701629,192.168.2.17,1 ↓
0000E2701630,192.168.2.18,1 ↓
```

Colon (:) used as the delimiter:

```
00:00:E2:70:16:23,192.168.2.10,1 ↓
00:00:E2:70:16:24,192.168.2.11,1 ↓
00:00:E2:70:16:25,192.168.2.12,1 ↓
00:00:E2:70:16:26,192.168.2.13,1 ↓
00:00:E2:70:16:27,192.168.2.14,2 ↓
00:00:E2:70:16:28,192.168.2.15,2 ↓
00:00:E2:70:16:28,192.168.2.16,2 ↓
00:00:E2:70:16:29,192.168.2.17,1 ↓
00:00:E2:70:16:30,192.168.2.18,1 ↓
```

## 16.17 MAC address list file

This file is used in the asset deletion command (`cscrdelete`) when batch-deleting asset information from a connection control list in JP1/CSC - Agent. Define the MAC addresses of the clients to be deleted in this file. Create the file with any file name in any directory.

### (1) Synopsis

```
MAC-address ↓
MAC-address ↓
:
```

Legend: ↓: Line feed code

### (2) Definition contents

The following table shows the contents to define in this file.

*Table 16-49: Definition contents of a MAC address list file*

No.	Item	Setting value
1	MAC address	<p>Write the MAC addresses of the clients to be deleted from the connection control list, one address per line. Specify each MAC address as 12 hexadecimal digits. MAC addresses are not case sensitive. You can use a delimiter after every second digit. Only one type of delimiter can be used in one MAC address. The following delimiters can be used:</p> <ul style="list-style-type: none"> <li>• Hyphen (-)</li> <li>• Colon (:)</li> <li>• Space</li> </ul>

Note the following coding conventions:

- Lines beginning with the hash symbol (#) are treated as comments. The hash symbol cannot be used except at the start of a line.
- You can write multiple lines in the file.
- End every line with a line feed code. The line feed code is 0x0d0a. Lines containing only a line feed code are ignored.

### (3) Specification example

No delimiter used:

```
0000E2701622 ↓  
0000E2701623 ↓  
0000E2701624 ↓  
0000E2701625 ↓
```

Hyphen (-) used as the delimiter:

```
00-00-E2-70-16-22 ↓  
00-00-E2-70-16-23 ↓  
00-00-E2-70-16-24 ↓  
00-00-E2-70-16-25 ↓
```

## 16.18 Judgment policy information file

This file is specified for execution of the judgment policy update command (`cscpolimport`). Its contents are imported as judgment policy information.

When the judgment policy export command (`cscrexport`) is executed, an export file is output in the same format as this file.

The judgment policy information file is a text file, and can be created with any file name in any directory.

### (1) Synopsis

Each item in the judgment policy information file is specified in a separate section.

Each section has the same syntax. Note the following coding conventions:

- The sections in the file and the lines in a section can be specified in any order.
- Every line other than the section name line must start with a parameter ID.
- Lines beginning with a hash symbol (#) are treated as comments.
- Each setting value other than the section name must be enclosed in double quotation marks ("). To omit the value, specify two double quotation marks in succession (" ").
- To specify a double quotation mark (") in a character string in the definition file, specify two double quotation marks in succession (" ").
- Use a comma (,) to separate setting values.
- End every parameter line with a line feed code. The line feed code is (0x0d0a). Lines containing only a line feed code are ignored.

The following describes the format of each section.

#### (a) [Policy Information]

```
"Version" , "version" ↓
```

#### (b) [Security updates]

```
"Option" , "judgment-option" ↓
"Conditon" , "judgment-condition" ↓
"Latest Level" , "security-level" ↓
"Exclude Option" , "exclusion-option" ↓
"ExpUpProgram" , "security-information-number" , "document-number" ↓
```

"NeedUpProgram" , "security-information-number" , "document-number" , "target-OS" , "OS-service-pack" , "product-code" , "product-version" , "product-service-pack" , "security-level" , "product-name" , "comparison-condition" ↓  
 "NeedUpServicePackProduct" , "product-name" , "product-version" , "product-service-pack" , "service-pack-condition" , "OS-type" , "OS-service-pack" , "security-level" ↓  
 "NeedUpServicePackOS" , "OS-type" , "OS-service-pack" , "service-pack-condition" , "security-level" ↓

### (c) [Anti-virus products]

"Option" , "judgment-option" ↓  
 "VirusProduct" , "anti-virus-product-name" , "product-version" , "engine-version" , "virus-definition-file-version" , "determine-that-PCs-with-no-resident-anti-virus-products-are-at-risk" , "security-level" ↓

### (d) [Prohibited software]

"Option" , "judgment-option" ↓  
 "UnjustSoftware" , "software-name" , "version" , "OS-type" , "security-level" , "comparison-condition" ↓

### (e) [Mandatory software]

"Option" , "judgment-option" ↓  
 "NeedSoftware" , "software-name" , "version" , "OS-type" , "security-level" , "group-name" ↓  
 "DMClient" , "judgment-option" , "version" , "security-level" ↓  
 "DMSubManager" , "judgment-option" , "version" , "security-level" ↓  
 "DMRelayManager" , "judgment-option" , "version" , "security-level" ↓

### (f) [PC security settings]

"Option" , "judgment-option" ↓  
 "PCSecurity" , "group-name" , "group-judgment-option" , "item-name" , "item-judgment-option" , "judgment-condition" , "comparison-value" , "security-level" , "treatment-if-item-is-not-applicable" ↓

**(g) [User definition]**

```
"Option" , "judgment-option"  ↓
"UserDefJudge" , "judgemnt-item-name" , "class" , "property" , "comparison-con
dition" , "comparison-value" , "treatment-when-value-is-not-set-for-property" , "sec
urity-level"  ↓
```

**(2) Definition contents**

Note the following when specifying information in the definition.

- Sections other than the [Policy Information] section can be omitted. If a section is omitted, the judgment items corresponding to that section will not be updated.
- If you omit optional items and import the definition to the judgment policy, the information for those items that is registered in the judgment policy is deleted.

The following describes the information to be defined for each section.

**(a) [Policy Information]**

The following table describes the information to be defined in the [Policy Information] section.

*Table 16-50: Contents of the [Policy Information] section*

No.	Parameter ID	Item	Setting item	Required
1	Version	Version	090100	Yes

**(b) [Security updates]**

The [Security updates] section corresponds to the judgment item **Security updates**.

The following table describes the information to be defined in the [Security updates] section.

*Table 16-51: Contents of the [Security updates] section*

No.	Parameter ID	Item	Setting value	Required
1	Option	Judgment option	Specify whether security updates are to be judged. 0: Not to be judged 1: To be judged	Yes

No.	Parameter ID	Item	Setting value	Required
2	Conditon	Judgment condition	Specify the judgment condition. 1: Whether the latest security update has been applied to the client is judged. 2: Whether the security update specified by the administrator has been applied to the client is judged.	Yes
3	Latest Level	Security level	Specify as one of the following codes the security level that is set when 1 is specified for the judgment condition and the latest security update has not been applied: 200: Caution 300: Warning 400: Danger	Yes
4	Exclude Option	Exclusion option	Specify whether to exclude a specific program when 1 is specified for the judgment condition. 0: Not excluded 1: Excluded	Yes
5	ExpUpProgram	Security information number	Specify the information to be imported to the security updates that will be excluded. For details about the setting values, see Table 16-10.	No
6		document number		

No.	Parameter ID	Item	Setting value	Required
7	NeedUpProgram	Security information number	Specify the information to be imported to the mandatory security updates (patch information). For details about the setting values, see Table 16-11.	No
8		Document number		
9		Target OS		
10		OS service pack		
11		Product code		
12		Product version		
13		Product service pack		
14		Security level		
15		Product name		
16		Comparison condition		
17	NeedUpService PackProduct	Product name	Specify the product service pack information to be imported to mandatory security updates (service pack information). For details about the setting values, see Table 16-12.	No
18		Product version		
19		Product service pack		
20		Service pack condition		
21		OS type		
22		OS service pack		
23		Security level		
24	NeedUpService PackOS	OS type	Specify the OS service pack information to be imported to mandatory security updates (service pack information). For details about the setting values, see Table 16-13.	No
25		OS service pack		
26		Service pack condition		
27		Security level		



**(c) [Anti-virus products]**

The [Anti-virus products] section corresponds to the judgment item **Anti-virus products**.

The following table describes the information to be defined in the [Anti-virus products] section.

*Table 16-52: Contents of the [Anti-virus products] section*

No.	Parameter ID	Item	Setting value	Required
1	Option	Judgment option	Specify whether anti-virus products are to be judged. 0: Not to be judged 1: To be judged	Yes
2	VirusProduct	Anti-virus product name	Specify the information to be imported to the anti-virus products that will be judged. For details about the setting values, see Table 16-14.	No
3		Product version		
4		Engine version		
5		Virus definition file version		
6		Determine that PCs with no resident anti-virus products are at risk		
7		Security level		

**(d) [Prohibited software]**

The [Prohibited software] section corresponds to the judgment item **Prohibited software**.

The following table describes the information to be defined in the [Prohibited software] section.

Table 16-53: Contents of the [Prohibited software] section

No.	Parameter ID	Item	Setting value	Required
1	Option	Judgment option	Specify whether unauthorized software is to be judged. 0: Not to be judged 1: To be judged	Yes
2	UnjustSoftware	Software name	Specify the information to be imported to the unauthorized software that will be judged. For details about the setting values, see Table 16-15.	No
3		Version		
4		OS type		
5		Security level		
6		Comparison condition		

**(e) [Mandatory software]**

The [Mandatory software] section corresponds to the judgment item **Mandatory software**.

The following table describes the information to be defined in the [Mandatory software] section.

Table 16-54: Contents of the [Mandatory software] section

No.	Parameter ID	Item	Setting value	Required
1	Option	Judgment option	Specify whether the mandatory software is to be judged. 0: Not to be judged 1: To be judged	Yes
2	NeedSoftware	Software name	Specify the information to be imported to the mandatory software that will be judged. For details about the setting values, see Table 16-16.	No
3		Version		
4		OS type		
5		Security level		
6		Group name		

No.	Parameter ID	Item	Setting value	Required
7	DMClient	Judgment option	Specify whether JP1/Software Distribution Client is to be judged. 0: Not to be judged 1: To be judged	Yes
8		Version	Specify the version of JP1/Software Distribution Client as a string of 60 or fewer bytes.	
9		Security level	Specify the security level as one of the following codes: 200: Caution 300: Warning 400: Danger	
10	DMSubManager	Judgment option	Specify whether JP1/Software Distribution SubManager is to be judged. 0: Not to be judged 1: To be judged	Yes
11		Version	Specify the version of JP1/Software Distribution SubManager, as a string of 60 or fewer bytes.	
12		Security level	Specify the security level as one of the following codes: 200: Caution 300: Warning 400: Danger	
13	DMRelayManager	Judgment option	Specify whether JP1/Software Distribution Manager (relay manager) is to be judged. 0: Not to be judged 1: To be judged	Yes
14		Version	Specify the version of JP1/Software Distribution Manager (relay manager) as a string of 60 or fewer bytes.	
15		Security level	Specify the security level as one of the following codes: 200: Caution 300: Warning 400: Danger	

**(f) [PC security settings]**

The [PC security settings] section corresponds to the judgment item **PC security settings**.

The following table describes the information to be defined in the [PC security settings] section.

*Table 16-55: Contents of the [PC security settings] section*

No.	Parameter ID	Item	Setting value	Required
1	Option	Judgment option	Specify whether the PC security settings are to be judged. 0: Not to be judged 1: To be judged	Yes

No.	Parameter ID	Item	Setting value	Required
2	PCSecurity	Group name <sup>#</sup>	Specify the group name. For details about the setting values, see Table 16-56.	No
3		Group judgment option	Specify whether the specified group is to be judged. If a group containing multiple items is specified for <i>group-name</i> , specify the same value for all items in the group. 0: Not to be judged 1: To be judged	
4		Item name <sup>#</sup>	Specify the judgment item name. For details about the setting values, see Table 16-56.	
5		Item judgment option	Specify whether the specified judgment item is to be judged. If a group containing only one item is specified for <i>group-name</i> , specify the same value that is specified for <i>group-judgment-option</i> . 0: Not to be judged 1: To be judged	
6		Judgment condition <sup>#</sup>	Specify the judgment condition. For details about the setting values, see Table 16-56.	
7		Comparison value <sup>#</sup>	Specify the comparison value. For details about the setting values, see Table 16-56.	
8		Security level	Specify the security level as one of the following codes: 200: Caution 300: Warning 400: Danger	
9		Treatment if item is not applicable	Specify the desired behavior if the judgment item does not exist. You can specify one of the following values: 1: The specified security level is set. 2: Judged <i>Safe</i> . 3: Judged <i>Not applicable</i> . 4: Judged <i>Unknown</i> .	

#

The following shows details of the setting values and the corresponding item names in the PC security settings.

Table 16-56: Details of the setting values in the [PC security settings] section

No.	Corresponding item name	Setting values in the [PC security settings] section			
		Group name	Item name	Judgment condition	Comparison value
1	Guest account settings	Accounts	Guest account settings	1: Guest account exists and is enabled. 2: Guest exists.	--
2	Vulnerable password	Passwords	Vulnerable password	--	--
3	Password that never expires		Password that never expires	--	--
4	Days since the password was updated		Days since the password was updated	--	1 to 1000
5	Automatic logon	Logon	Automatic logon settings	--	--
6	Power-on password		Power-on password settings	1: Power-on password is not set. 2: Power-on password is not set or is not installed.	--
7	Shared folder settings	Shares	Shared folder settings	--	--
8	Restrictions on anonymous connections	Anonymous connections	Anonymous connections are restricted	--	--
9	Status of unnecessary services	Services	Unnecessary services are running	--	--

No.	Corresponding item name	Setting values in the [PC security settings] section			
		Group name	Item name	Judgment condition	Comparison value
10	Windows firewall settings	Firewall	Windows Firewall Settings	1: The Windows firewall is disabled. 2: The Windows firewall is disabled or allows exceptions.	--
11	Windows automatic update settings	Automatic updates	Settings for Windows automatic updates	--	--
12	Screensaver settings	Screensaver	Screensaver settings	--	--
13	Password protection		Password protection of screensaver	--	--
14	Drive encryption by BitLocker	Drive Encryption	BitLocker Drive Encryption	1: The system drive is not encrypted. 2: A drive is not encrypted.	--

Legend:

--: No setting

#### (g) [User definition]

The [User definition] section corresponds to the judgment item **User definition**.

The following table describes the information to be defined in the [User definition] section.

Table 16-57: Contents of the [User definition] section

No.	Parameter ID	Item	Setting value	Required
1	Option	Judgment option	Specify whether user definitions are to be judged. 0: Not to be judged 1: To be judged	Yes

No.	Parameter ID	Item	Setting value	Required
2	UserDefJudge	Judgment item name	Specify the information to be imported to the user definition that will be judged. For details about the setting values, see Table 16-17.	No
3		Class		
4		Property		
5		Comparison condition		
6		Comparison value		
7		Treatment when value is not set for property		
8		Security level		

**(3) Specification example**

```

[Policy Information] ↓
"Version","090100" ↓
[Security updates] ↓
"Option","1" ↓
"Conditon","2" ↓
"Latest Level","300" ↓
"Exclude Option","0" ↓
"ExpUpProgram","09-032","923854" ↓
"ExpUpProgram","09-033","923855" ↓
"NeedUpProgram","09-040","998765","0000","0","0","","0","300",
"","","" ↓
"NeedUpProgram","09-050","998855","0039","0","1","7.0","0","30
0","","" ↓
"NeedUpProgram","09-060","999855","0028","1","99","2003","0","
300","SoftA","3" ↓
"NeedUpServicePackOS","0014","2","1","200" ↓
"NeedUpServicePackOS","0028","1","0","400" ↓
"NeedUpServicePackProduct","1","6.0","1","0","0000","0","300"
↓
[Anti-virus products] ↓
"Option","1" ↓
"VirusProduct","AntiVirus
A","10.2.1.5","5.2.3.001","20100215.001","1","400" ↓

```



```

"VirusProduct","AntiVirus B","","","0","300" ↓
[Prohibited software] ↓
"Option","1" ↓
"UnjustSoftware","SoftA","","0000","200","2" ↓
"UnjustSoftware","SoftB","0100","0200","300","1" ↓
[Mandatory software] ↓
"Option","0" ↓
"NeedSoftware","""SoftC""","""","0000","200","SoftC" ↓
"NeedSoftware","""SoftD""","SoftE""","0100","0200""","0017
","200","SoftDE" ↓
"DMClient","1","0910","200" ↓
"DMSubManager","0","","200" ↓
"DMRelayManager","0","","200" ↓
[PC security settings] ↓
"Option","1" ↓
"PCSecurity","Accounts","1","Guest account
settings","1","1","","200","3" ↓
"PCSecurity","Passwords","1","Vulnerable
password","0","","","300","1" ↓
"PCSecurity","Passwords","1","Password that never
expires","0","","","300","3" ↓
"PCSecurity","Passwords","1","Days since the password was
updated","0","","180","200","4" ↓
"PCSecurity","Logon","0","Automatic logon
settings","0","","","200","3" ↓
"PCSecurity","Logon","0","Power-on password
settings","0","1","","200","3" ↓
"PCSecurity","Shares","0","Shared folder
settings","0","","","200","3" ↓
"PCSecurity","Firewall","0","Windows Firewall
Settings","0","1","","200","3" ↓
"PCSecurity","Automatic updates","0","Settings for Windows
automatic updates","0","","","200","3" ↓
"PCSecurity","Screensaver","0","Screensaver
settings","0","","","200","3" ↓
"PCSecurity","Screensaver","0","Password protection of
screensaver","0","","","200","3" ↓
"PCSecurity","Drive Encryption","1","BitLocker Drive
Encryption","1","2","","400","2" ↓
[User definition] ↓
"Option","1" ↓
"UserDefJudge","ItemA","""asset-information""","""asset-number""","""

```

```
"1""", ""100000001""", ""4""", "200" ↓  
"UserDefJudge", "ItemB", ""asset-information"" , ""hardware-asset-informat  
ion  
"" , ""device-status"" , ""free-disk-space"" , ""2"" , ""7"" , ""100"" , ""  
100000"" , ""1"" , ""4"" , "200" ↓
```

## 16.19 Excluded user definition file

The excluded user definition file is used to exclude specific user accounts from password-related judgment of the PC security settings (vulnerable password, password that never expires, and the number of days since the password was updated). Accordingly, the user accounts specified in this file are excluded from the password-related judgment in the PC security settings.

The file name and the folder where it is located are as follows.

File name	Folder
cscm_excludeuser.conf	JPI/CSC - Manager-installation-folder\conf

### (1) Synopsis

```

user-account-name ↓
user-account-name ↓
:
:

```

Legend: ↓: Line feed code

### (2) Definition contents

The following table describes the information to be defined in the file.

Table 16-58: Contents of the excluded user definition file

No.	Item	Setting value
1	User account name	Specify the user account name as a string of 256 or fewer bytes.

Note the following coding conventions.

- You can write multiple lines in the file.
- Lines beginning with a semicolon (;) are treated as comments.
- End every line with a line feed code. The line feed code is 0x0d0a. Lines containing only a line feed code are ignored.

### (3) Specification example

```

User1 ↓
:
:

```

## 16. Definition Files

User5 ↓

## 16.20 Definition file of MAC addresses not subject to deletion

This file specifies the MAC addresses that will not be deleted by the permitted device list maintenance command (`cscnwmaintenance`) with the `-f` option specified. Define the MAC addresses that are not to be deleted in this file. Create the file with any file name in any directory.

### (1) Synopsis

```
MAC-address ↓
MAC-address ↓
:
```

Legend: ↓: Line feed code

### (2) Definition contents

The following table describes the information to be defined in the file.

*Table 16-59:* Contents of the definition file of MAC addresses not subject to deletion

No.	Item	Setting value
1	MAC address	<p>Write the MAC addresses not to be deleted.</p> <p>Write one MAC address per line, represented by a 12-digit hexadecimal number. One of the following delimiters can be used every second digit:</p> <ul style="list-style-type: none"> <li>• Hyphen (-)</li> <li>• Colon (:)</li> <li>• Space</li> </ul>

Note the following coding conventions.

- Lines beginning with a hash symbol (#) are treated as comments.
- You can write multiple lines in the file.
- End every parameter line with a line feed code. The line feed code is (0x0d0a). Lines containing only a line feed code are ignored.

### (3) Specification example

```
00:11:22:33:44:55 ↓
66:77:88:99:AA:BB ↓
:
```

## 16. Definition Files

CC:DD:EE:FF:00:11 ↓

## Chapter

---

# 17. Messages

---

This chapter describes the message output by JP1/CSC and the messages displayed in the Client Security Management window of AIM.

- 17.1 Format of messages
- 17.2 List of output destinations of messages
- 17.3 List of JP1/CSC messages
- 17.4 List of messages in the Client Security Management window

---

## 17.1 Format of messages

---

This section describes the format of messages that are output by JP1/CSC and the format of message explanations in the manual.

### 17.1.1 Format of output messages

This subsection describes the format of messages that are output by JP1/CSC. A message consists of a message ID and message text.

The format of an output message is as follows:

*KDSLnnnn-Z message-text*

The components of the message ID are as follows:

K

System identifier

DSL

Indicates the message is output by JP1/CSC.

*nnnn*

Serial number of the message

Z

Type of the message

E: Error message

W: Warning message

I: Information message

### 17.1.2 Format of message explanations

This subsection describes the format of message explanations in this manual.

Messages are written starting from the smallest message ID. Italic characters in the messages are variables. When JP1/CSC is linked with JP1/IM, JP1/CSC sends some messages to JP1/IM as JP1 events. Those messages are accompanied by event IDs.

#### **message-ID (event-ID)**

*message-text*

*message-explanation*

(S)

Indicates the action performed by the system.



(O)

Indicates the action to be performed by the user when the message is output.

## 17.2 List of output destinations of messages

The JP1/CSC messages are output to the following output destinations:

- Manager log (JP1/CSC - Manager log)
- Remote Option log (JP1/CSC - Manager Remote Option log)
- Agent log (JP1/CSC - Agent log)
- JP1/IM
- Event log
- Standard output
- Standard error output
- Audit log

### 17.2.1 Output destinations of JP1/CSC - Manager messages

The following table lists the output destination of each JP1/CSC - Manager message.

*Table 17-1:* Output destinations of JP1/CSC - Manager messages

Message ID	Output destination					
	Manager log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL0001-I	Y	--	--	--	--	Y
KDSL0002-E	Y	--	--	--	--	--
KDSL0004-E	Y	--	--	--	--	--
KDSL0005-E	Y	--	--	--	--	--
KDSL0006-E	Y	--	--	--	--	--
KDSL0007-E	Y	--	--	--	--	--
KDSL0008-E	Y	--	--	--	--	--
KDSL0009-E	Y	--	--	--	--	--
KDSL0010-I	Y	Y	--	--	--	Y
KDSL0011-E	--	--	Y	--	--	--
KDSL0012-E	Y	Y	Y	--	--	--

Message ID	Output destination					
	Manager log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL0013-E	Y	Y	Y	--	--	--
KDSL0014-E	Y	Y	Y	--	--	--
KDSL0015-E	Y	Y	Y	--	--	--
KDSL0020-I	Y	Y	--	--	--	Y
KDSL0021-E	Y	Y	--	--	--	--
KDSL0022-E	Y	Y	--	--	--	--
KDSL0023-W	Y	Y	--	--	--	--
KDSL0024-E	Y	Y	--	--	--	--
KDSL0028-E	Y	Y	--	--	--	--
KDSL0041-E	Y	Y	--	--	--	--
KDSL0042-E	Y	Y	--	--	--	--
KDSL0043-E	Y	Y	--	--	--	--
KDSL0045-W	Y	--	--	--	--	--
KDSL0046-E	Y	Y	--	--	--	--
KDSL0047-W	Y	--	--	--	--	--
KDSL0050-I	Y	Y	--	--	--	--
KDSL0051-W	Y	Y	--	--	--	--
KDSL0052-E	Y	Y	--	--	--	--
KDSL0053-E	Y	Y	--	--	--	--
KDSL0054-E	Y	Y	--	--	--	--
KDSL0100-I	Y	--	--	--	--	--
KDSL0101-I	Y	--	--	--	--	--
KDSL0104-I	Y	Y	--	--	--	Y
KDSL0106-E	Y	Y	--	--	--	--
KDSL0107-E	Y	Y	--	--	--	--

Message ID	Output destination					
	Manager log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL0108-E	Y	Y	--	--	--	--
KDSL0109-W	Y	--	--	--	--	--
KDSL0110-W	Y	--	--	--	--	--
KDSL0111-W	Y	--	--	--	--	--
KDSL0112-W	Y	--	--	--	--	--
KDSL0113-W	Y	--	--	--	--	--
KDSL0114-W	Y	--	--	--	--	--
KDSL0115-E	Y	Y	--	--	--	--
KDSL0116-W	Y	--	--	--	--	--
KDSL0117-W	Y	--	--	--	--	--
KDSL0118-W	Y	--	--	--	--	--
KDSL0119-W	Y	--	--	--	--	--
KDSL0120-W	Y	--	--	--	--	--
KDSL0150-E	Y	Y	--	--	--	--
KDSL0151-E	Y	Y	--	--	--	--
KDSL0152-E	Y	Y	--	--	--	--
KDSL0153-E	Y	Y	--	--	--	--
KDSL0154-E	Y	Y	--	--	--	--
KDSL0155-E	Y	Y	--	--	--	--
KDSL0156-E	Y	Y	--	--	--	--
KDSL0157-E	Y	Y	--	--	--	--
KDSL0160-I	Y	--	--	--	--	--
KDSL0161-I	Y	--	--	--	--	--
KDSL0162-I	Y	--	--	--	--	--
KDSL0163-I	Y	--	--	--	--	--

Message ID	Output destination					
	Manager log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL0164-I	Y	--	--	--	--	--
KDSL0165-I	Y	--	--	--	--	--
KDSL0166-I	Y	--	--	--	--	--
KDSL0167-I	Y	--	--	--	--	--
KDSL0170-E	Y	Y	--	--	--	--
KDSL0171-E	Y	Y	--	--	--	--
KDSL0173-E	Y	Y	--	--	--	--
KDSL0174-E	Y	Y	--	--	--	--
KDSL0175-E	Y	Y	--	--	--	--
KDSL0176-E	Y	Y	--	--	--	--
KDSL0177-E	Y	Y	--	--	--	--
KDSL0178-E	Y	Y	--	--	--	--
KDSL0179-E	Y	Y	--	--	--	--
KDSL0180-E	Y	Y	--	--	--	--
KDSL0191-E	Y	Y	--	--	--	--
KDSL0192-E	Y	Y	--	--	--	--
KDSL0193-E	Y	Y	--	--	--	--
KDSL0194-I	Y	--	--	--	--	--
KDSL0195-I	Y	--	--	--	--	--
KDSL0196-E	Y	Y	--	--	--	--
KDSL0500-I	Y	--	--	--	--	--
KDSL0501-I	Y	--	--	--	--	--
KDSL0505-I	--	Y	--	--	--	--
KDSL0510-I	Y	Y	--	--	--	Y
KDSL0511-I	Y	Y	--	--	--	Y

Message ID	Output destination					
	Manager log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL0520-E	Y	Y	--	--	--	--
KDSL0521-E	Y	Y	--	--	--	--
KDSL0522-E	Y	Y	--	--	--	--
KDSL0523-E	Y	Y	--	--	--	--
KDSL0524-E	Y	Y	--	--	--	--
KDSL0525-E	Y	Y	--	--	--	--
KDSL0526-E	Y	Y	--	--	--	--
KDSL0527-W	Y	--	--	--	--	--
KDSL0550-I	Y	--	--	--	--	--
KDSL0551-I	Y	--	--	--	--	--
KDSL0560-W	Y	--	--	--	--	--
KDSL0561-I	Y	--	--	--	--	--
KDSL0562-W	Y	--	--	--	--	--
KDSL0570-E	Y	Y	--	--	--	--
KDSL0571-E	Y	Y	--	--	--	--
KDSL0572-E	Y	Y	--	--	--	--
KDSL0573-E	Y	Y	--	--	--	--
KDSL0574-W	Y	--	--	--	--	--
KDSL0575-E	Y	Y	--	--	--	--
KDSL0576-E	Y	Y	--	--	--	--
KDSL0577-E	Y	Y	--	--	--	--
KDSL0578-E	Y	Y	--	--	--	--
KDSL0600-I	Y	--	--	--	--	--
KDSL0601-I	Y	--	--	--	--	--
KDSL0610-W	Y	--	--	--	--	--

Message ID	Output destination					
	Manager log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL0611-W	Y	--	--	--	--	--
KDSL0612-W	Y	--	--	--	--	--
KDSL0613-W	Y	--	--	--	--	--
KDSL0614-W	Y	--	--	--	--	--
KDSL0615-W	Y	--	--	--	--	--
KDSL0620-E	Y	Y	--	--	--	--
KDSL0621-E	Y	Y	--	--	--	--
KDSL0622-E	Y	Y	--	--	--	--
KDSL0623-E	Y	Y	--	--	--	--
KDSL0624-E	Y	Y	--	--	--	--
KDSL0625-E	Y	Y	--	--	--	--
KDSL0650-I	Y	--	--	--	--	--
KDSL0651-I	Y	--	--	--	--	--
KDSL0652-I	Y	--	--	--	--	--
KDSL0653-I	Y	--	--	--	--	--
KDSL0670-E	Y	Y	--	--	--	--
KDSL0671-E	Y	Y	--	--	--	--
KDSL0672-E	Y	Y	--	--	--	--
KDSL0673-E	Y	Y	--	--	--	--
KDSL0674-E	Y	--	--	--	--	--
KDSL0675-E	Y	--	--	--	--	--
KDSL0676-E	Y	--	--	--	--	--
KDSL0677-E	Y	--	--	--	--	--
KDSL0680-I	Y	--	--	--	--	--
KDSL0681-I	Y	--	--	--	--	--

Message ID	Output destination					
	Manager log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL0682-E	Y	Y	--	--	--	--
KDSL0683-E	Y	Y	--	--	--	--
KDSL0684-E	Y	Y	--	--	--	--
KDSL0685-E	Y	Y	--	--	--	--
KDSL0686-E	Y	Y	--	--	--	--
KDSL0687-E	Y	Y	--	--	--	--
KDSL0750-I	Y	--	--	--	--	--
KDSL0751-I	Y	--	--	--	--	--
KDSL0752-I	Y	--	--	--	--	--
KDSL0753-W	Y	--	--	--	--	--
KDSL0754-E	Y	Y	--	--	--	--
KDSL0755-E	Y	Y	--	--	--	--
KDSL0756-W	Y	--	--	--	--	--
KDSL0757-W	Y	--	--	--	--	--
KDSL0758-W	Y	--	--	--	--	--
KDSL0760-E	Y	Y	--	--	--	--
KDSL0800-E	--	--	--	--	--	Y
KDSL0801-E	--	--	--	--	--	Y
KDSL0802-E	--	--	--	--	--	Y
KDSL0998-E	Y	Y	--	--	--	--
KDSL0999-E	Y	Y	--	--	--	--
KDSL1000-I	Y	--	--	Y	--	--
KDSL1001-E	Y	--	--	--	Y	--
KDSL1003-E	--	--	--	--	Y	--
KDSL1004-E	Y	--	--	--	Y	--



Message ID	Output destination					
	Manager log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL1005-E	Y	--	--	--	Y	--
KDSL1006-E	Y	--	--	--	Y	--
KDSL1007-E	Y	--	--	--	Y	--
KDSL1008-I	Y	--	--	Y	--	--
KDSL1050-I	Y	--	--	Y	--	--
KDSL1051-E	Y	--	--	--	Y	--
KDSL1052-E	Y	--	--	--	Y	--
KDSL1053-E	--	--	--	--	Y	--
KDSL1054-E	Y	--	--	--	Y	--
KDSL1055-E	Y	--	--	--	Y	--
KDSL1056-E	Y	--	--	--	Y	--
KDSL1057-E	Y	--	--	--	Y	--
KDSL1058-E	Y	--	--	--	Y	--
KDSL1059-W	Y	--	--	--	Y	--
KDSL1060-E	Y	--	--	--	Y	--
KDSL1080-I	Y	--	--	Y	--	Y
KDSL1081-E	--	--	--	--	Y	--
KDSL1082-E	Y	--	--	--	Y	--
KDSL1083-E	Y	--	--	--	Y	--
KDSL1084-E	Y	--	--	--	Y	--
KDSL1085-E	Y	--	--	--	Y	--
KDSL1086-E	Y	--	--	--	Y	--
KDSL1087-E	Y	--	--	--	Y	--
KDSL1088-W	Y	--	--	--	Y	--
KDSL1089-E	Y	--	--	--	Y	--

Message ID	Output destination					
	Manager log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL1090-E	Y	--	--	--	Y	--
KDSL1091-E	Y	--	--	--	Y	Y
KDSL1110-I	Y	--	--	Y	--	Y
KDSL1111-E	--	--	--	--	Y	--
KDSL1112-E	Y	--	--	--	Y	--
KDSL1113-E	Y	--	--	--	Y	--
KDSL1114-E	Y	--	--	--	Y	--
KDSL1115-E	Y	--	--	--	Y	--
KDSL1116-E	Y	--	--	--	Y	--
KDSL1117-W	Y	--	--	--	Y	--
KDSL1118-W	Y	--	--	--	Y	--
KDSL1119-W	Y	--	--	--	Y	--
KDSL1120-E	Y	--	--	--	Y	Y
KDSL1130-I	Y	--	--	Y	--	Y
KDSL1131-E	Y	--	--	--	Y	--
KDSL1132-E	Y	--	--	--	Y	--
KDSL1133-E	Y	--	--	--	Y	--
KDSL1134-E	Y	--	--	--	Y	--
KDSL1135-E	Y	--	--	--	Y	--
KDSL1136-E	Y	--	--	--	Y	--
KDSL1137-E	Y	--	--	--	Y	--
KDSL1138-E	Y	--	--	--	Y	--
KDSL1139-E	Y	--	--	--	Y	--
KDSL1140-E	Y	--	--	--	Y	--
KDSL1141-E	Y	--	--	--	Y	--

Message ID	Output destination					
	Manager log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL1142-E	Y	--	--	--	Y	--
KDSL1143-E	Y	--	--	--	Y	--
KDSL1144-E	Y	--	--	--	Y	--
KDSL1145-E	Y	--	--	--	Y	--
KDSL1200-I	Y	--	--	Y	--	Y
KDSL1201-E	Y	--	--	--	Y	--
KDSL1202-E	--	--	--	--	Y	--
KDSL1203-E	--	--	--	--	Y	--
KDSL1204-E	Y	--	--	--	Y	--
KDSL1205-W	Y	--	--	--	Y	--
KDSL1206-E	Y	--	--	--	Y	--
KDSL1207-E	Y	--	--	--	Y	--
KDSL1208-E	Y	--	--	--	Y	--
KDSL1209-E	Y	--	--	--	Y	--
KDSL1210-E	Y	--	--	--	Y	--
KDSL1220-E	Y	--	--	--	Y	Y
KDSL1250-I	Y	--	--	Y	--	--
KDSL1251-E	Y	--	--	--	Y	--
KDSL1252-E	Y	--	--	--	Y	--
KDSL1253-E	--	--	--	--	Y	--
KDSL1254-E	--	--	--	--	Y	--
KDSL1256-E	Y	--	--	--	Y	--
KDSL1257-E	Y	--	--	--	Y	--
KDSL1258-E	Y	--	--	--	Y	--
KDSL1259-W	Y	--	--	--	Y	--

Message ID	Output destination					
	Manager log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL1260-E	Y	--	--	--	Y	--
KDSL1261-E	Y	--	--	--	Y	--
KDSL1262-E	Y	--	--	--	Y	--
KDSL1270-E	Y	--	--	--	Y	--
KDSL1300-I	Y	--	--	Y	--	Y
KDSL1301-E	--	--	--	--	Y	--
KDSL1302-E	--	--	--	--	Y	--
KDSL1303-E	Y	--	--	--	Y	--
KDSL1304-E	Y	--	--	--	Y	--
KDSL1305-E	Y	--	--	--	Y	--
KDSL1310-E	Y	--	--	--	Y	Y
KDSL1350-I	Y	--	--	Y	--	Y
KDSL1351-E	Y	--	--	--	Y	--
KDSL1352-E	--	--	--	--	Y	--
KDSL1353-E	--	--	--	--	Y	--
KDSL1354-E	Y	--	--	--	Y	--
KDSL1355-E	Y	--	--	--	Y	--
KDSL1356-W	Y	--	--	--	Y	--
KDSL1357-E	Y	--	--	--	Y	--
KDSL1358-W	Y	--	--	--	Y	--
KDSL1359-E	Y	--	--	--	Y	--
KDSL1370-E	Y	--	--	--	Y	Y
KDSL1450-I	Y	--	--	Y	--	Y
KDSL1451-E	--	--	--	--	Y	--
KDSL1452-E	--	--	--	--	Y	--

Message ID	Output destination					
	Manager log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL1453-E	Y	--	--	--	Y	--
KDSL1454-E	Y	--	--	--	Y	--
KDSL1455-E	Y	--	--	--	Y	--
KDSL1456-E	Y	--	--	--	Y	--
KDSL1457-E	Y	--	--	--	Y	--
KDSL1458-E	Y	--	--	--	Y	--
KDSL1459-E	Y	--	--	--	Y	--
KDSL1460-E	Y	--	--	--	Y	--
KDSL1461-E	Y	--	--	--	Y	--
KDSL1462-E	Y	--	--	--	Y	--
KDSL1463-E	Y	--	--	--	Y	--
KDSL1464-E	Y	--	--	--	Y	--
KDSL1465-I	Y	--	--	Y	--	--
KDSL1466-I	Y	--	--	Y	--	--
KDSL1467-E	Y	--	--	--	Y	--
KDSL1468-W	Y	--	--	--	Y	--
KDSL1469-E	Y	--	--	--	Y	Y
KDSL1500-I	Y	--	--	Y	--	Y
KDSL1501-E	Y	--	--	--	Y	--
KDSL1502-E	Y	--	--	--	Y	--
KDSL1503-E	Y	--	--	--	Y	--
KDSL1504-E	Y	--	--	--	Y	--
KDSL1505-E	Y	--	--	--	Y	--
KDSL1506-E	Y	--	--	--	Y	--
KDSL1507-E	Y	--	--	--	Y	Y

Message ID	Output destination					
	Manager log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL1600-I	Y	--	--	Y	--	Y
KDSL1601-E	--	--	--	--	Y	--
KDSL1602-E	Y	--	--	--	Y	--
KDSL1603-E	Y	--	--	--	Y	--
KDSL1604-E	Y	--	--	--	Y	--
KDSL1605-E	Y	--	--	--	Y	--
KDSL1606-E	Y	--	--	--	Y	--
KDSL1607-E	Y	--	--	--	Y	--
KDSL1608-E	Y	--	--	--	Y	--
KDSL1609-I	Y	--	--	--	Y	--
KDSL1610-I	Y	--	--	Y	--	--
KDSL1611-W	Y	--	--	--	Y	--
KDSL1612-E	Y	--	--	--	Y	Y
KDSL2001-E	Y	--	--	--	--	--
KDSL2011-I	Y	Y	--	--	--	Y
KDSL2012-E	Y	Y	--	--	--	Y
KDSL2013-E	Y	--	--	--	--	--
KDSL2014-E	Y	--	--	--	--	--
KDSL2015-E	Y	--	--	--	--	--
KDSL2016-E	Y	--	--	--	--	--
KDSL2030-I	Y	Y	--	--	--	Y
KDSL2031-E	Y	--	--	--	--	Y
KDSL2032-I	Y	Y	--	--	--	Y
KDSL2033-E	Y	--	--	--	--	Y
KDSL2036-E	Y	--	--	--	--	--

Message ID	Output destination					
	Manager log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL2037-I	Y	Y	--	--	--	Y
KDSL2038-E	Y	--	--	--	--	Y
KDSL2040-E	Y	--	--	--	--	Y
KDSL2042-I	Y	Y	--	--	--	Y
KDSL2043-E	Y	--	--	--	--	Y
KDSL2044-E	Y	--	--	--	--	--
KDSL2045-I	Y	Y	--	--	--	--
KDSL2046-I	Y	Y	--	--	--	Y
KDSL2500-E	Y	--	--	--	--	--
KDSL3001-I	Y	Y	--	--	--	Y
KDSL3002-E	Y	--	Y	--	--	--
KDSL3003-E	Y	Y	Y	--	--	--
KDSL3004-E	Y	Y	Y	--	--	--
KDSL3005-W	Y	Y	--	--	--	Y
KDSL3006-E	Y	Y	--	--	--	--
KDSL3007-E	Y	Y	--	--	--	--
KDSL3008-W	Y	Y	--	--	--	--
KDSL3009-E	Y	Y	--	--	--	--
KDSL3010-E	Y	Y	--	--	--	--
KDSL3011-E	Y	Y	--	--	--	--
KDSL3012-W	Y	--	--	--	--	--
KDSL3013-I	Y	Y	--	--	--	--
KDSL3014-W	Y	Y	--	--	--	--
KDSL3015-E	Y	Y	--	--	--	--
KDSL3016-E	Y	Y	--	--	--	--

Message ID	Output destination					
	Manager log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL3017-E	Y	Y	--	--	--	--
KDSL3018-I	Y	Y	--	--	--	--
KDSL3019-E	Y	Y	--	--	--	--
KDSL3020-E	Y	Y	--	--	--	--
KDSL3021-E	Y	Y	--	--	--	--
KDSL3022-W	Y	Y	--	--	--	--
KDSL3030-E	--	--	--	--	--	Y
KDSL3031-E	--	--	--	--	--	Y
KDSL3032-I	Y	--	--	--	--	--
KDSL3033-W	Y	Y	--	--	--	--
KDSL3034-E	Y	Y	--	--	--	--

Legend:

Y: The message is output.

--: The message is not output.

### 17.2.2 Output destinations of JP1/CSC - Manager Remote Option messages

The following table lists the output destination of each JP1/CSC - Manager Remote Option message.

*Table 17-2:* Output destinations of JP1/CSC - Manager Remote Option messages

Message ID	Output destination					
	Remote Option log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL3201-I	Y	--	--	--	--	Y
KDSL3202-E	Y	--	--	--	--	--



Message ID	Output destination					
	Remote Option log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL3203-E	Y	--	--	--	--	--
KDSL3204-E	Y	--	--	--	--	--
KDSL3205-I	Y	--	--	--	--	Y
KDSL3206-W	Y	--	--	--	--	Y
KDSL3207-E	Y	--	Y	--	--	--
KDSL3208-E	Y	--	--	--	--	--
KDSL3209-E	Y	--	--	--	--	--
KDSL3210-E	Y	--	--	--	--	--
KDSL3211-E	Y	--	--	--	--	--
KDSL3212-I	Y	--	--	--	--	--
KDSL3213-I	Y	--	--	--	--	--
KDSL3214-E	Y	--	--	--	--	--
KDSL3215-E	Y	--	--	--	--	--
KDSL3216-E	Y	--	--	--	--	--
KDSL3217-E	Y	--	--	--	--	--
KDSL3218-E	Y	--	--	--	--	--
KDSL3219-I	Y	--	--	--	--	--
KDSL3220-E	Y	--	--	--	--	--
KDSL3221-I	Y	--	--	--	--	--
KDSL3222-E	Y	--	--	--	--	--
KDSL3223-E	Y	--	--	--	--	--
KDSL3224-I	Y	--	--	--	--	--
KDSL3225-I	Y	--	--	--	--	--
KDSL3226-E	Y	--	--	--	--	--
KDSL3301-I	Y	--	--	Y	--	--

Message ID	Output destination					
	Remote Option log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL3302-E	--	--	--	--	Y	--
KDSL3303-E	Y	--	--	--	Y	--
KDSL3304-E	Y	--	--	--	Y	--
KDSL3305-E	Y	--	--	--	Y	--
KDSL3306-E	Y	--	--	--	Y	--
KDSL3307-E	--	--	--	--	Y	--
KDSL3308-E	Y	--	--	--	Y	--
KDSL3309-E	Y	--	--	--	Y	--
KDSL3310-E	Y	--	--	--	Y	--
KDSL3311-E	Y	--	--	--	Y	--
KDSL3312-E	Y	--	--	--	Y	--
KDSL3400-E	--	--	--	--	--	Y
KDSL3401-E	--	--	--	--	--	Y
KDSL3402-E	--	--	--	--	--	Y

Legend:

Y: The message is output.

--: The message is not output.

### 17.2.3 Output destinations of JP1/CSC - Agent messages

The following table lists the output destination of each JP1/CSC - Agent message.

*Table 17-3: Output destinations of JP1/CSC - Agent messages*

Message ID	Output destination					
	Agent log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL5000-I	Y	--	--	--	--	Y

Message ID	Output destination					
	Agent log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL5001-E	Y	--	--	--	--	--
KDSL5002-E	Y	--	--	--	--	--
KDSL5003-E	Y	--	--	--	--	--
KDSL5100-I	Y	--	--	--	--	Y
KDSL5101-W	Y	--	--	--	--	Y
KDSL5102-E	--	--	Y	--	--	--
KDSL5103-E	Y	--	--	--	--	--
KDSL5104-E	Y	--	--	--	--	--
KDSL5105-E <sup>#1</sup>	Y	--	Y	--	--	--
KDSL5106-E	Y	--	--	--	--	--
KDSL5107-E	Y	--	--	--	--	--
KDSL5108-E	Y	--	--	--	--	--
KDSL5109-E	Y	--	--	--	--	--
KDSL5110-E	Y	--	--	--	--	--
KDSL5200-I	Y	--	--	--	--	--
KDSL5201-I	Y	--	--	--	--	Y
KDSL5202-E	Y	--	--	--	--	--
KDSL5203-E	Y	--	--	--	--	--
KDSL5204-I	Y	--	--	--	--	--
KDSL5205-I	Y	--	--	--	--	Y
KDSL5206-E	Y	--	--	--	--	--
KDSL5207-E	Y	--	--	--	--	--
KDSL5208-E	Y	--	--	--	--	--
KDSL5209-E	Y	--	--	--	--	--

Message ID	Output destination					
	Agent log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL5300-E	--	--	--	--	--	Y
KDSL5301-E	--	--	--	--	--	Y
KDSL5302-E	--	--	--	--	--	Y
KDSL5303-E	--	--	--	--	--	Y
KDSL5304-E	--	--	--	--	--	Y
KDSL6000-E	Y	--	--	--	--	--
KDSL6001-E	Y	--	--	--	--	--
KDSL6002-E	Y	--	--	--	--	--
KDSL6003-I	Y	--	--	--	--	--
KDSL6004-E	Y	--	--	--	--	--
KDSL6005-I	Y	--	--	--	--	Y
KDSL6006-E	--	--	--	--	--	Y
KDSL6030-E	Y	--	--	--	--	--
KDSL6032-E	Y	--	--	--	--	--
KDSL6033-W	Y	--	--	--	--	--
KDSL6034-I	Y	--	--	--	--	--
KDSL6035-E	Y	--	--	--	--	--
KDSL6036-I	Y	--	--	--	--	--
KDSL6037-I	Y	--	--	--	--	--
KDSL6038-I	Y	--	--	--	--	--
KDSL6042-E	Y	--	--	--	--	--
KDSL6043-I	Y	--	--	--	--	--
KDSL6060-E	Y	--	--	--	--	--
KDSL6061-E	Y	--	--	--	--	--
KDSL6090-E	Y	--	--	--	--	--

Message ID	Output destination					
	Agent log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL6092-E	Y	--	--	--	--	--
KDSL6093-I	Y	--	--	--	--	--
KDSL6120-I <sup>#2</sup>	Y	--	--	Y	--	Y
KDSL6121-I <sup>#2</sup>	Y	--	--	Y	--	Y
KDSL6122-I <sup>#2</sup>	Y	--	--	Y	--	Y
KDSL6123-E <sup>#2</sup>	--	--	--	--	Y	--
KDSL6124-E <sup>#2</sup>	--	--	--	--	Y	--
KDSL6125-E <sup>#2</sup>	--	--	--	--	Y	--
KDSL6126-E <sup>#2</sup>	Y	--	--	--	Y	--
KDSL6127-E <sup>#2</sup>	Y	--	--	--	Y	--
KDSL6128-E <sup>#2</sup>	Y	--	--	--	Y	--
KDSL6129-E <sup>#2</sup>	Y	--	--	--	Y	--
KDSL6130-E <sup>#2</sup>	Y	--	--	--	Y	--
KDSL6131-E <sup>#2</sup>	Y	--	--	--	Y (not used)	--
KDSL6135-E <sup>#2</sup>	Y	--	--	--	Y	--
KDSL6136-E <sup>#2</sup>	Y	--	--	--	Y	--
KDSL6137-E <sup>#2</sup>	Y	--	--	--	Y	--
KDSL6139-W <sup>#2</sup>	Y	--	--	--	Y	--
KDSL6140-E <sup>#2</sup>	Y	--	--	--	Y	--
KDSL6141-E <sup>#2</sup>	Y	--	--	--	Y	--
KDSL6142-E <sup>#2</sup>	Y	--	--	--	Y	--
KDSL6143-E <sup>#2</sup>	Y	--	--	--	Y	--

Message ID	Output destination					
	Agent log	JP1/IM	Event log	Standard output	Standard error output	Audit log
KDSL6144-E <sup>#2</sup>	Y	--	--	--	Y	--
KDSL6145-E <sup>#2</sup>	Y	--	--	--	Y	--
KDSL6146-E <sup>#2</sup>	--	--	--	--	--	Y
KDSL6147-E <sup>#2</sup>	--	--	--	--	--	Y
KDSL6148-E <sup>#2</sup>	--	--	--	--	--	Y
KDSL6150-E	Y	--	--	--	--	--
KDSL6151-E	Y	--	--	--	--	--
KDSL6152-E <sup>#2</sup>	Y	--	--	--	Y	--
KDSL6180-I	Y (connection history message)	--	--	--	--	Y

## Legend:

Y: The message is output.

--: The message is not output.

## #1

This message is output to either the agent log or the event log.

## #2

Output by a JP1/CSC - Agent RADIUS Component command.

## 17.3 List of JP1/CSC messages

This section lists the messages that have a message ID and that are output by JP1/CSC.

### 17.3.1 List of JP1/CSC - Manager messages

The following table describes and lists the variables in messages that take specific values.

*Table 17-4: Types and descriptions of the variables in messages that take specific values*

Variable	Value	Description
<i>request-source</i>	AIM	Judgment of the security level when AIM updated the inventory.
	PC List window	The administrator performed an operation on the PC List window (evaluation of the security level, message notification, or rejection or permission for network connection for a client).
	cscaction command	The action was implemented by the <i>cscaction</i> command.
	cscjudge command	The security level was judged by the <i>cscjudge</i> command.
	cscnetctrl command	Network connection control performed by the <i>cscnetctrl</i> command.
	Register Permitted PCs window	The administrator performed an operation in the Register Permitted PCs window.
<i>control-type</i>	Permit	Permission to connect the client to the network
	Refuse	Refusal to connect the client to the network
	Refuse in the emergency	Immediate denial of client connection to the network.
<i>action-result</i>	Success	The action (notification to the administrator, notification to the user, or network control) was successful.
	Failure	The action (notification to the administrator, notification to the user, or network control) was not successful.

Variable	Value	Description
	Partial success	The action (notification to the administrator, notification to the user, or network control) was partially successful.
	Not performed	The action (notification to the administrator, notification to the user, or network control) has not been performed yet.
<i>request-contents</i>	Request to judge security level	A request to judge the security level of the client
	Request to add PC information	A request to add information about a new client
	Request to update PC information	A request to update information about the client
	Request to delete PC information	A request to delete information about the client
	Request to control network connection	A request to control client's connection to the network

The messages of JP1/CSC - Manager are as follows:

**(1) Messages regarding JP1/CSC - Manager (0001 to 0999)**

**KDSL0001-I**

Setup of the manager environment was successful.

JP1/CSC - Manager was successfully configured.

(S)

Ends the configuration of JP1/CSC - Manager.

**KDSL0002-E**

An attempt to set up the manager environment has failed.  
Execution permissions are lacking.

JP1/CSC - Manager could not be configured because an unauthorized user attempted the configuration.

(S)

Cancels the configuration of JP1/CSC - Manager.

(O)

Check the user role and reconfigure JP1/CSC - Manager.



**KDSL0004-E**

An attempt to set up the manager environment has failed. A file I/O error occurred. (error code = [error-code])

JP1/CSC - Manager could not be configured because a file I/O error occurred.

(S)

Cancels the configuration of JP1/CSC - Manager.

(O)

Check whether the disk has sufficient free space or an error occurred in the file system. If the problem is not resolved, contact the system administrator.

**KDSL0005-E**

An attempt to set up the manager environment has failed. An internal error occurred. (error code = [error-code])

JP1/CSC - Manager could not be configured because an internal error occurred.

(S)

Cancels the configuration of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0006-E**

An attempt to set up the manager environment has failed. A database access error occurred. (error code = [error-code])

JP1/CSC - Manager could not be configured because a database access error occurred.

(S)

Cancels the configuration of JP1/CSC - Manager.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL0007-E**

An attempt to set up the manager environment has failed. Asset Information Manager is not installed. (error code = [error-code])

The JP1/CSC - Manager environment could not be set up because AIM was not installed.

(S)

Cancels the setup of the JP1/CSC - Manager environment.

(O)

Check whether AIM has been installed correctly.

**KDSL0008-E**

An attempt to set up the manager environment has failed. There is no history information that corresponds to the asset information. (asset information = [*asset-ID*])

The JP1/CSC - Manager environment could not be set up because the history information corresponding to the asset information did not exist.

(S)

Cancels the setup of the JP1/CSC - Manager environment.

(O)

Contact the system administrator.

**KDSL0009-E**

An attempt to set up the manager environment has failed. There is no asset that corresponds to the asset information. (asset information = [*asset-ID*])

The JP1/CSC - Manager environment could not be set up because the asset corresponding to the asset information did not exist.

(S)

Cancels the setup of JP1/CSC - Manager environment.

(O)

Contact the system administrator.

**KDSL0010-I (0x00005400)**

The manager has started.

JP1/CSC - Manager has started.

(S)

Started JP1/CSC - Manager.

**KDSL0011-E**

An attempt to start the manager has failed. Manager setup has not been completed. (error code = [*error-code*])

JP1/CSC - Manager could not be started because JP1/CSC - Manager was not completely set up.

(S)

Cancels the startup of JP1/CSC - Manager.

(O)

Set up JP1/CSC - Manager and then start JP1/CSC - Manager again. If the problem is not resolved, contact the system administrator.

**KDSL0012-E (0x00005401)**

An attempt to start the manager has failed. The communication environment cannot be initialized. (error code = [error-code])

JP1/CSC - Manager could not be started because the communication environment could not be initialized.

(S)

Cancels the startup of JP1/CSC - Manager.

(O)

Check whether the port number specified in the setup window of JP1/CSC - Manager is available on the machine where JP1/CSC - Manager is installed. If the specified port number cannot be used on the machine, set up JP1/CSC - Manager again and specify a port number that can be used on the machine.

**KDSL0013-E (0x00005402)**

An attempt to start the manager has failed. A database access error occurred. (error code = [error-code])

JP1/CSC - Manager could not be started because a database access error occurred.

(S)

Cancels the startup of JP1/CSC - Manager.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL0014-E (0x00005403)**

An attempt to start the manager has failed. An internal error occurred. (error code = [error-code])

JP1/CSC - Manager could not be started because an internal error occurred.

(S)

Cancels the startup of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0015-E (0x00005441)**

An attempt to start the manager has failed. Asset Information Manager is not installed. (error code = [error-code])

JP1/CSC - Manager could not start because AIM was not installed.

(S)

Cancels the startup of JP1/CSC - Manager.

(O)

Check whether AIM is installed correctly.

**KDSL0020-I (0x00005404)**

The manager terminated normally.

JP1/CSC - Manager has ended.

(S)

Ended JP1/CSC - Manager.

**KDSL0021-E (0x00005405)**

An attempt to terminate the manager has failed. A communication error occurred. (error code = [error-code])

A communication error occurred while JP1/CSC - Manager was ending.

(S)

Ends JP1/CSC - Manager.

(O)

Check whether an error occurred in JP1/CSC - Manager.

**KDSL0022-E (0x00005406)**

An attempt to terminate the manager has failed. Manager termination processing timed out. (error code = [error-code])

A timeout error occurred during the end processing of JP1/CSC - Manager.

(S)

Ends JP1/CSC - Manager.

(O)

Check the JP1/CSC - Manager log. Check whether the security level was being judged or an action was being performed while JP1/CSC - Manager was ending.

**KDSL0023-W (0x00005407)**

The manager was forcibly terminated because an error occurred during termination processing.

JP1/CSC - Manager was forcibly ended because an error occurred during the end processing of JP1/CSC - Manager.

(S)

Ends JP1/CSC - Manager.

(O)

Check the JP1/CSC - Manager log. Check whether the security level was being judged or an action was being performed while JP1/CSC - Manager was ending.

**KDSL0024-E (0x00005408)**

An attempt to terminate the manager has failed. A database access error occurred. (error code = [error-code])

A database access error occurred while JP1/CSC - Manager was ending.

(S)

Ends JP1/CSC - Manager.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL0028-E (0x00005409)**

An attempt to terminate the manager has failed. An internal error occurred. (error code = [error-code])

An internal error occurred while JP1/CSC - Manager was ending.

(S)

Ends JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0041-E (0x0000540A)**

An attempt to receive a manager request has failed. A communication error occurred. (error code = [error-code])

The request from JP1/CSC - Manager could not be accepted because a communication error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether an error occurred in JP1/CSC - Manager. Check whether the communication environment of JP1/CSC - Manager is operating normally.

**KDSL0042-E (0x0000540B)**

An attempt to receive a manager request has failed. An internal error occurred. (error code = [error-code])

The request from JP1/CSC - Manager could not be accepted because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0043-E (0x00005452)**

An attempt to receive the manager request has failed. An IP address authentication error occurred. (IP address = *[IP-address]*, error code = *[error-code]*)

The request from JP1/CSC - Manager could not be accepted because an IP address authentication error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check the IP address for the remote option in the Client Security Control - Manager Setup dialog box.

**KDSL0045-W**

A request was discarded because the manager is terminating. (request contents=*[request-reception-date, request-type, request-source]*)

JP1/CSC - Manager discarded the request to end.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check the content of the discarded request in the JP1/CSC - Manager log.

**KDSL0046-E (0x0000540C)**

An attempt to receive a manager request has failed. A database access error occurred. (error code = *[error-code]*)

The request from JP1/CSC - Manager could not be accepted because a database access error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL0047-W**

Network connection control will be skipped because automatic refusal for a network connection is specified to be not executed.

Network connection control will be skipped because **Automatic refusal of network connection** is set to **Do not execute** in the Client Security Control - Manager Setup dialog box.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

In the Client Security Control - Manager Setup dialog box, set **Automatic refusal of network connection** to **Execute**.

**KDSL0050-I (0x0000540D)**

The agent has started. (IP address = [*IP-address*])

JP1/CSC - Agent has started.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0051-W (0x0000540E)**

The agent has terminated. (IP address = [*IP-address*])

JP1/CSC - Agent has ended.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Network control is not possible after JP1/CSC - Agent has ended. Check whether a problem exists even though JP1/CSC - Agent has ended.

**KDSL0052-E (0x0000540F)**

An error occurred with the agent. (IP address = [*IP-address*], error code = [*error-code*])

An error occurred in JP1/CSC - Agent.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Correct the error in JP1/CSC - Agent.

**KDSL0053-E (0x00005410)**

A communication error occurred with the manager. (error code = [*error-code*])

A communication error occurred in JP1/CSC - Manager.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether an error occurred in JP1/CSC - Manager. Check whether the communication between JP1/CSC - Manager and JP1/CSC - Agent is normal.

**KDSL0054-E (0x00005411)**

An internal error occurred with the manager. (error code = [error-code])

An internal error occurred in JP1/CSC - Manager.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0100-I**

A security level judgment will now start. (request source = [request-source], judgment date = [security-level-judgment-date])

Judgment of the client security level will now begin.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0101-I**

A security level judgment has terminated. (request source = [request-source], judgment date = [security-level-judgment-date])

Judgment of the client security level has ended.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0104-I (0x00005412)**

The results of the security level judgment are as follows.  
(request source = [request-source], judgment date = [security-level-judgment-date], number of request PCs = [number-of-PC-units], number of judged PCs = [number-of-PC-units], safe = [number-of-PC-units], caution = [number-of-PC-units], warning = [number-of-PC-units], danger = [number-of-PC-units], unknown = [number-of-PC-units], Not applicable = [number-of-PC-units] )

The result of judgment of the client security level is displayed.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.



**KDSL0106-E (0x00005413)**

An attempt to judge the security level has failed. A database access error occurred. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], error code = [*error-code*])

The client security level could not be judged because a database access error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL0107-E (0x0000544A)**

An attempt to judge a security level has failed. There is no judgment policy. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], policy name = [*policy-name*], asset number = [*asset-number*])

The client security level could not be judged because no judgment policy has been assigned to the client.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

In the JP1/CSC - Manager log file, check whether the corresponding policy has been deleted.

**KDSL0108-E (0x00005415)**

An attempt to judge the security level has failed. An internal error occurred. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], error code = [*error-code*])

The client security level could not be judged because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0109-W**

There is no asset whose security level can be judged. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], asset information = [*asset-ID* or *asset-number*])

No client was found to have target asset information whose security level required judgment.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the asset information has been registered in the asset management database.

**KDSL0110-W**

There is no asset that corresponds to the specified asset number.  
(request source = [*request-source*], judgment date =  
[*security-level-judgment-date*], asset number = [*asset-number*])

There was no asset information with the specified asset number.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the asset information has been registered in the asset management database.

**KDSL0111-W**

Some items cannot be judged because the version of Software Distribution Client installed on the asset to be judged is old.  
(request source = [*request-source*], judgment date =  
[*security-level-judgment-date*], asset number = [*asset-number*])

Some items could not be judged because the version of JP1/Software Distribution Client installed on the target client was out of date.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check the version of JP1/Software Distribution Client installed on the client with the asset number in the message.

**KDSL0112-W**

The program update cannot be judged because MBSA or Windows Update Agent is not installed on the asset to be judged. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], asset number = [*asset-number*])

The security update could not be judged because MBSA or Windows Update Agent has not been set up on the client.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether MBSA or Windows Update Agent is set up on the client indicated by *asset-number* in the message.

**KDSL0113-W**

The security level cannot be judged because no OS information exists on the asset to be judged or the OS is not supported. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], asset number = [*asset-number*])

The security level cannot be judged because OS information for the target client was not found, or the OS is not supported.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the OS information for the client indicated by *asset-number* in the message is registered, and whether the OS is supported.

**KDSL0114-W**

The security level cannot be judged because no asset information exists. (request source = [*request-source*], judgment date = [*security-level-judgment-date*])

The security level could not be judged because the asset information for the target client was not found.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the asset information for the client has been registered.

**KDSL0115-E (0x00005442)**

An attempt to judge the security level has failed. There is no asset that corresponds to the asset information. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], asset number = [*asset-number*])

The security level could not be judged because the asset corresponding to the asset number did not exist.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the asset information has been registered in the asset management

database.

**KDSL0116-W**

Some items cannot be judged because the version of Software Distribution SubManager installed on the asset to be judged is old. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], asset number = [*asset-number*])

Some items could not be judged because the version of JP1/Software Distribution SubManager installed on the target asset was out of date.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check the version of JP1/Software Distribution SubManager installed on the client indicated by *asset-number* in the message.

**KDSL0117-W**

The action will be skipped based on the setting for action execution when the security level is judged. (request source = [*request-source*], judgment date = [*security-level-judgment-date*])

The action will be skipped because the action implementation during security level judgment is specified to be skipped.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

On the **Basic Settings** page of the Client Security Control - Manager Setup dialog box, check the **Action execution** setting under **Security level judgment information**. If you want to implement actions during the security level judgment, change the setting.

**KDSL0118-W**

A security level judgment will be skipped because asset information has not been updated. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], asset number = [*asset-number*])

Security level judgment was skipped because asset information has not been updated.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

On the **Basic Settings** page of the Client Security Control - Manager Setup dialog

box, check the **Perform judgment if asset information is not updated** setting under **Security level judgment information**. If you want to judge security levels for assets whose asset information has not been updated, change the setting.

**KDSL0119-W**

Some items cannot be judged because the version of Software Distribution Manager (relay manager) installed on the asset to be judged is old. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], asset number = [*asset-number*])

Some items could not be judged because the version of Software Distribution Manager (relay manager) installed on the asset was out of date.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check the version of Software Distribution Manager (relay manager) installed on the client indicated by *asset-number* in the message.

**KDSL0120-W**

Some items cannot be judged because the version of Software Distribution Manager or Asset Information Manager is old. (request source = [*request-source*], judgment date = [*security-level-judgment-date*])

Some items could not be judged because the version of Software Distribution Manager or Asset Information Manager was out of date.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Upgrade Software Distribution Manager and Asset Information Manager to version 08-51 or later.

**KDSL0150-E (0x00005416)**

An attempt to add asset information has failed. A database access error occurred. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], error code = [*error-code*])

Asset information could not be added because a database access error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL0151-E (0x00005417)**

An attempt to add asset information has failed. An internal error occurred. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], error code = [*error-code*])

Asset information could not be added because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0152-E (0x00005418)**

An attempt to update asset information has failed. A database access error occurred. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], error code = [*error-code*])

Asset information could not be updated because a database access error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL0153-E (0x00005419)**

An attempt to update asset information has failed. An internal error occurred. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], error code = [*error-code*])

Asset information could not be updated because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0154-E (0x0000541A)**

An attempt to delete asset information has failed. An internal error occurred. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], error code = [*error-code*])

Asset information could not be deleted because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0155-E (0x0000541B)**

An attempt to delete history information has failed. A file I/O error occurred. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], error code = [*error-code*])

The history information could not be deleted because a file I/O error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the disk has sufficient free space or an error occurred in the file system. If the problem is not resolved, contact the system administrator.

**KDSL0156-E (0x00005443)**

An attempt to add asset information has failed. The asset cannot be added because the same asset information exists. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], asset information = [*asset-ID*])

The asset could not be added because the same asset information already exists.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0157-E (0x00005451)**

An attempt to delete asset information has failed. A database access error occurred. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], error code = [*error-code*])

Asset information could not be deleted because a database access error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL0160-I**

Asset information will now be added. (request source = [*request-source*], request reception date = [*request-reception-date*])

Addition of asset information will now begin.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0161-I**

Asset information has been added. (request source =  
[*request-source*], request reception date = [*request-reception-date*])

Addition of asset information has ended.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0162-I**

Asset information will now be updated. (request source =  
[*request-source*], request reception date = [*request-reception-date*])

Update of asset information will now begin.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0163-I**

Asset information has been updated. (request source =  
[*request-source*], request reception date = [*request-reception-date*])

Update of asset information has ended.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0164-I**

Asset information will now be deleted. (request source =  
[*request-source*], request reception date = [*request-reception-date*])

Deletion of asset information will now begin.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0165-I**

Asset information has been deleted. (request source =  
[*request-source*], request reception date = [*request-reception-date*])

Deletion of asset information has ended.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.



**KDSL0166-I**

Detection of asset information deletion will now start. (request source = [*request-source*], request reception date = [*request-reception-date*])

The detection of asset information deletion will now begin.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0167-I**

Detection of asset information deletion has terminated. (request source = [*request-source*], request reception date = [*request-reception-date*])

The detection of asset information deletion has now ended.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0170-E (0x0000541C)**

An attempt to obtain a judgment condition has failed. A communication error occurred. (error code = [*error-code*])

The judgment conditions of the judgment policy could not be acquired because a communication error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether an error occurred in JP1/CSC - Manager. Check whether the communication environment of JP1/CSC - Manager is operating normally.

**KDSL0171-E (0x0000541D)**

An attempt to obtain a judgment condition has failed. An internal error occurred. (error code = [*error-code*])

The judgment conditions of the judgment policy could not be acquired because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0173-E (0x0000541E)**

An attempt to obtain the judgment history has failed. A database access error occurred. (error code = [*error-code*])

The judgment history of the security level could not be acquired because a database access error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL0174-E (0x0000541F)**

An attempt to obtain the judgment history has failed. A file I/O error occurred. (error code = [*error-code*])

The judgment history of the security level could not be acquired because a file I/O error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the disk has sufficient free space or an error occurred in the file system. If the problem is not resolved, contact the system administrator.

**KDSL0175-E (0x00005420)**

An attempt to obtain the judgment history has failed. An internal error occurred. (error code = [*error-code*])

The judgment history of the judgment policy could not be acquired because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0176-E (0x00005421)**

An attempt to register the judgment history has failed. A file I/O error occurred. (error code = [*error-code*])

The judgment history of the security level could not be registered because a file I/O error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the disk has sufficient free space or an error occurred in the file

system. If the problem is not resolved, contact the system administrator.

**KDSL0177-E (0x00005422)**

An attempt to register the judgment history has failed. An internal error occurred. (error code = [error-code])

The judgment history of the security level could not be registered because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0178-E (0x00005423)**

An attempt to delete the judgment history has failed. A file I/O error occurred. (error code = [error-code])

The judgment history of the security level could not be deleted because a file I/O error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the disk has sufficient free space or an error occurred in the file system. If the problem is not resolved, contact the system administrator.

**KDSL0179-E (0x00005424)**

An attempt to delete the judgment history has failed. An internal error occurred. (error code = [error-code])

The judgment history of the security level could not be deleted because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0180-E (0x00005449)**

An attempt to register the judgment history has failed. There is no asset that corresponds to the asset information. (asset information = [asset-ID])

The judgment history for the security level could not be acquired because the asset corresponding to the asset information did not exist.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the asset information has been registered in the asset management database.

**KDSL0191-E (0x00005425)**

An attempt to set up security management has failed. An internal error occurred. (request source = [*request-source*], request reception date = [*request-reception-date*], error code = [*error-code*])

Security management could not be set because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0192-E (0x00005426)**

An attempt to set up security management has failed. A database access error occurred. (request source = [*request-source*], request reception date = [*request-reception-date*], error code = [*error-code*])

Security management could not be set because a database access error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL0193-E (0x00005427)**

An attempt to set up security management has failed. A communication error occurred. (request source = [*request-source*], request reception date = [*request-reception-date*], error code = [*error-code*])

Security management could not be set because a communication error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether an error occurred in JP1/CSC - Manager. Check whether the communication environment of JP1/CSC - Manager is operating normally.

**KDSL0194-I**

The security management settings have been enabled. (request source = [*request-source*], request reception date = [*request-reception-date*])

The security management settings were enabled.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0195-I**

The security management settings have been disabled. (request source = [*request-source*], request reception date = [*request-reception-date*])

The security management settings were disabled.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0196-E (0x00005444)**

An attempt to set up security management has failed. There is no asset that corresponds to the asset information. (request source = [*request-source*], request reception date = [*request-reception-date*], asset information = [*asset-ID*])

Security management could not be set up because the asset corresponding to the asset information did not exist.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the asset information has been registered in the asset management database.

**KDSL0500-I**

An action will now start. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], action date = [*action-date*])

The action will now begin.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0501-I**

An action has terminated. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], action date = [*action-date*])

The action has ended.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0505-I (0x00005428)**

An asset of security level *security-level* has been detected. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], action date = [*action-date*], asset count = [*asset-count*])

An asset of *security-level* was detected.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0510-I (0x00005429)**

The action results are as follows. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], action date = [*action-date*], notice to the administrator = [*action-result*], notice to the user = [*action-result*], network connection control = [*action-result*], user definition action = [*action-result*])

The result of the action is displayed.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0511-I (0x00005472)**

The action results are as follows. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], action date = [*action-date*], notice to the user = [*action-result*])

The result of the action is displayed.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0520-E (0x0000542A)**

An attempt to perform an action has failed. A database access error occurred. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], action date = [*action-date*], error code = [*error-code*])

The action failed because a database access error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL0521-E (0x0000542B)**

An attempt to perform an action has failed. An internal error occurred. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], action date = [*action-date*], error code = [*error-code*])

The action failed because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0522-E (0x0000542C)**

An attempt to register the action results has failed. A database access error occurred. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], action date = [*action-date*], error code = [*error-code*])

The result of the action could not be registered because a database access error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the database is active or an error occurred in the database. All actions were successful.

**KDSL0523-E (0x0000542D)**

An attempt to register the action results has failed. An internal error occurred. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], action date = [*action-date*], error code = [*error-code*])

The result of the action could not be registered because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0524-E (0x00005445)**

An attempt to perform an action has failed. There is no asset that corresponds to the asset information. (request source = [*request-source*], judgment date = [*security-level-judgment-date*], action date = [*action-date*], asset information = [*asset-ID*])

The action could not be performed because the asset corresponding to the asset information did not exist.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the asset information has been registered in the asset management database.

**KDSL0525-E (0x00005446)**

An attempt to register the action results has failed. There is no asset that corresponds to the asset information. (request source = [request-source], judgment date = [security-level-judgment-date], action date = [action-date], asset number = [asset-number])

The action results could not be registered because the asset corresponding to the asset number did not exist.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the asset information has been registered in the asset management database.

**KDSL0526-E (0x0000544B)**

An attempt to perform an action has failed. There is no action policy. (request source = [request-source], judgment date = [security-level-judgment-date], action date = [action-date], policy name = [policy-name], asset number = [asset-number])

No action could be performed because there is no action policy.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Use the JP1/CSC - Manager log file to check whether the relevant policy has been deleted.

**KDSL0527-W**

An action will be skipped because a security level judgment was skipped. (request source = [request-source], judgment date = [security-level-judgment-date], action date = [action-date], asset number = [asset-number])

The action will be skipped because the settings specify that security level judgment is



to be skipped for clients whose asset information has not been updated.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

On the **Basic Settings** page of the Client Security Control - Manager Setup dialog box, check the **Perform judgment if asset information is not updated** setting under **Security level judgment information**. If you want to judge security levels and implement actions for assets whose asset information has not been updated, change the setting.

#### KDSL0550-I

Network connection control will now start. (request source = [request-source], action date = [action-date], control type = [control-type])

Network connection control will now begin.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

#### KDSL0551-I

Network connection control has terminated. (request source = [request-source], action date = [action-date], control type = [control-type])

Network connection control has ended.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

#### KDSL0560-W

Network connection control will be skipped. No MAC addresses are registered. (request source = [request-source], action date = [action-date], control type = [control-type], asset number = [asset-number])

Network connection control is skipped since the MAC address is not registered.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the MAC address of the client with the specified asset number is registered.

**KDSL0561-I**

Network connection control will be skipped. The network connection status and control type are the same. (request source = [request-source], action date = [action-date], control type = [control-type], asset number = [asset-number])

Network connection control is skipped because the network connection status and the control type are the same.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0562-W**

Network connection control will be skipped. The network connection state is refuse in the emergency. (request source = [request-source], action date = [action-date], control type = [control-type], asset number = [asset-number])

Network connection control will be skipped because the network connection status is *Refuse in the emergency*.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Using the network control command (cscnetctrl) or the Client Security Control - Manager Setup dialog box, permit network connections for the client indicated by *asset-number* in the message.

**KDSL0570-E (0x0000542E)**

Network connection control has failed. A communication error occurred. (request source = [request-source], action date = [action-date], control type = [control-type], agent = [agent-IP-address], error code = [error-code])

Network connection control failed because a communication error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the communication environment of JP1/CSC - Manager is operating normally.

**KDSL0571-E (0x0000542F)**

Network connection control has failed. No agents are registered. (request source = [request-source], action date = [action-date], control type = [control-type], error code = [error-code])

Network connection control failed because JP1/CSC - Agent was not registered.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether JP1/CSC - Agent is registered.

#### **KDSL0572-E (0x00005430)**

Network connection control has failed. (request source = [request-source], action date = [action-date], control type = [control-type], MAC address = [PC-MAC-address], agent = [agent-IP-address], error code = [error-code])

Network connection control failed.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether an error occurred in JP1/CSC - Agent.

#### **KDSL0573-E (0x00005431)**

Network connection control has failed. An error occurred with the agent. (request source = [request-source], action date = [action-date], control type = [control-type], agent = [agent-IP-address], error code = [error-code])

Network connection control failed because an error occurred in JP1/CSC - Agent.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether an error occurred in JP1/CSC - Agent.

#### **KDSL0574-W**

An error occurred during network connection control. An error occurred with the agent. (request source = [request-source], action date = [action-date], control type = [control-type], agent = [agent-IP-address], error code = [error-code])

An error occurred during network connection control because an error occurred in JP1/CSC - Agent.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether an error occurred in JP1/CSC - Agent.

**KDSL0575-E (0x00005432)**

Network connection control has failed. An internal error occurred. (request source = [request-source], action date = [action-date], control type = [control-type], error code = [error-code])

Network connection control failed because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0576-E (0x00005433)**

Network connection control has failed. An internal error occurred. (request source = [request-source], action date = [action-date], control type = [control-type], agent = [agent-IP-address], error code = [error-code])

Network connection control failed because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0577-E (0x00005453)**

There is no asset that corresponds to the MAC address, or the IP address and host name. (request source = [request-source], action date = [action-date], control type = [control-type], MAC address = [MAC-address]#, IP address = [IP-address]#, host name = [host-name]#)

Network connection control failed because there is no asset corresponding to the MAC address, or IP address and host name, specified by the network control command (cscnetctrl).

#

- If the command specifies a MAC address, then only a MAC address is output.
- If the command specifies only an IP address, then only an IP address is output.
- If the command specifies only a host name, then only a host name is output.
- If the command specifies both an IP address and host name, then an IP address and host name are output.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether a resource corresponding to the MAC address, or IP address and host name, specified by the network control command (*cscnetctrl*) has been registered in the asset management database.

**KDSL0578-E(0x00005470)**

An attempt to control the network connection has failed. The product to which the agent is linked does not support registration of permitted PCs. (request source = [*request-source*], action date = [*action-date*], control type = [*control-type*], agent = [*agent-IP-address*], error code = *error-code*)

An attempt to control connection to the network has failed because the information for the network control product to which the agent is linked does not support registration of permitted PCs.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check the information for the network control product to which the agent is linked.

**KDSL0600-I**

Message notification will now start. (request source = [*request-source*], action date = [*action-date*])

Transmission of the message will now begin.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0601-I**

Message notification has terminated. (request source = [*request-source*], action date = [*action-date*])

Transmission of the message has ended.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0610-W**

Message notification will be skipped. Software Distribution Client is either not installed or is an old version. (request source = [*request-source*], action date = [*action-date*], asset number = [*asset-number*])

Transmission of the message is skipped because JP1/Software Distribution Client is not installed or JP1/Software Distribution Client before version 07-00 or earlier is installed.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether JP1/Software Distribution Client 07-50 or later is installed in the client with the specified asset number.

#### **KDSL0611-W**

Message notification will be skipped. Software Distribution Client, Software Distribution Manager (relay manager) or Software Distribution SubManager is not installed. (request source = [*request-source*], action date = [*action-date*], asset number = [*asset-number*])

Message notification will be skipped because JP1/Software Distribution Client, Software Distribution Manager (relay manager), or JP1/Software Distribution SubManager is either not installed, or version 07-11 or earlier of the product is installed.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether JP1/Software Distribution Client, Software Distribution Manager (relay manager), or JP1/Software Distribution SubManager is installed in the client indicated by *asset-number*.

#### **KDSL0612-W**

Message notification will be skipped. Software Distribution SubManager version is old. (request source = [*request-source*], action date = [*action-date*], asset number = [*asset-number*])

Message notification will be skipped because JP1/Software Distribution SubManager 07-00 or earlier is installed.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether JP1/Software Distribution SubManager 07-50 or later is installed on the client indicated by *asset-number*.

**KDSL0613-W**

Message notification will be skipped. The PC where Software Distribution SubManager is installed is not a target for action. (request source = [*request-source*], action date = [*action-date*], asset number = [*asset-number*])

Message notification will be skipped. The PC installed Software Distribution SubManager is not a target for action.

Message notification will be skipped because JP1/Software Distribution SubManager is not specified as the target of security level judgment and action.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

In the Client Security Control - Manager Setup dialog box, check whether JP1/Software Distribution SubManager is set as a target for security-level judgment and action.

**KDSL0614-W**

Message notification will be skipped. Software Distribution Manager (relay manager) version is old. (request source = [*request-source*], action date = [*action-date*], asset number = [*asset-number*])

Message notification will be skipped because Software Distribution Manager (relay manager) 07-11 or earlier is installed.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether Software Distribution Manager (relay manager) 07-50 or later is installed on the client indicated by *asset-number*.

**KDSL0615-W**

Message notification will be skipped. The PC where Software Distribution Manager (relay manager) is installed is not a target for action. (request source = [*request-source*], action date = [*action-date*], asset number = [*asset-number*])

Message notification will be skipped because Software Distribution Manager (relay manager) is not specified as a target of security level judgment and action.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

In the Client Security Control - Manager Setup dialog box, check whether Software Distribution Manager (relay manager) is set as a target for security-level judgment and action.

**KDSL0620-E (0x00005434)**

Message notification has failed. Software Distribution Manager is not installed. (request source = [*request-source*], action date = [*action-date*], asset number = [*asset-number*], error code = [*error-code*])

The message could not be sent because JP1/Software Distribution Manager was not installed.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check the installed components of JP1/Software Distribution.

**KDSL0621-E (0x00005435)**

Message notification has failed. Asset Information Manager is not installed. (request source = [*request-source*], action date = [*action-date*], asset number = [*asset-number*], error code = [*error-code*])

The message could not be sent because AIM is not installed.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether AIM is installed correctly.

**KDSL0622-E (0x00005436)**

Message notification has failed. An internal error occurred. (request source = [*request-source*], action date = [*action-date*], asset number = [*asset-number*], error code = [*error-code*])

The message could not be sent because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0623-E (0x00005437)**

Message notification has failed. An internal error occurred. (request source = [*request-source*], action date = [*action-date*], error code = [*error-code*])



The message could not be sent because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0624-E (0x00005447)**

Message notification has failed. A file I/O error occurred.  
(request source = [request-source], action date = [action-date], asset  
number = [asset-number], error code = [error-code])

Message notification has failed because a file I/O error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the disk has sufficient free space or whether an error occurred in  
the file system. If the problem is not resolved, contact the system administrator.

**KDSL0625-E (0x00005448)**

Message notification has failed. An attempt to connect with  
Software Distribution Manager has failed. (request source =  
[request-source], action date = [action-date], asset number =  
[asset-number], error code = [error-code])

Message notification has failed because an attempt to connect with JP1/Software  
Distribution Manager has failed.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether JP1/Software Distribution 07-50 or later is installed and active.  
Also check whether an error occurred in the communication environment.

**KDSL0650-I**

Email notification will now start. (request source =  
[request-source], action date = [action-date])

Transmission of the email will now begin.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0651-I**

Email notification has terminated. (request source =  
[*request-source*], action date = [*action-date*])

Transmission of the email has ended.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0652-I**

Notification to IM will now start. (request source =  
[*request-source*], action date = [*action-date*])

The JP1 event will be sent to JP1/IM.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0653-I**

Notification to IM has terminated. (request source =  
[*request-source*], action date = [*action-date*])

The JP1 event was successfully sent to JP1/IM.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0670-E (0x00005438)**

Email notification has failed. The SMTP service cannot be used.  
(request source = [*request-source*], action date = [*action-date*], asset  
number = [*asset-number*], error code = [*error-code*])

The email could not be sent because the SMTP service was not available.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the SMTP service is operating normally.

**KDSL0671-E (0x00005439)**

Email notification has failed. Asset Information Manager is not  
installed. (request source = [*request-source*], action date =  
[*action-date*], asset number = [*asset-number*], error code = [*error-code*])

The message could not be sent because AIM was not installed.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether AIM is installed correctly.

**KDSL0672-E (0x0000543A)**

Email notification has failed. An internal error occurred.  
(request source = [*request-source*], action date = [*action-date*], asset  
number = [*asset-number*], error code = [*error-code*])

The email could not be sent because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0673-E (0x0000543B)**

Email notification has failed. An internal error occurred.  
(request source = [*request-source*], action date = [*action-date*], error  
code = [*error-code*])

The email could not be sent because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0674-E**

An attempt to notify IM has failed. An internal error occurred.  
(request source = [*request-source*], action date = [*action-date*], error  
code = [*error-code*])

The JP1 event notification could not be sent to JP1/IM because an internal error  
occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0675-E**

An attempt to notify IM has failed. An internal error occurred.  
(request source = [*request-source*], action date = [*action-date*], asset  
number = [*asset-number*], error code = [*error-code*])

The JP1 event notification could not be sent to JP1/IM because an internal error  
occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0676-E**

An attempt to notify IM has failed. The IM linkage option is not specified. (request source = [*request-source*], action date = [*action-date*], error code = [*error-code*])

The JP1 event notification could not be sent to JP1/IM because **Do not notify** was specified for **IM linkage** in the setup of JP1/CSC - Manager.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

To link with JP1/IM, specify **Notify** for **IM linkage** in the setup of JP1/CSC - Manager.

**KDSL0677-E**

An attempt to notify IM has failed. An attempt to connect with IM has failed. (request source = [*request-source*], action date = [*action-date*], asset number = [*asset-number*], error code = [*error-code*])

The JP1 event could not be reported to JP1/IM because an attempt to connect with JP1/IM has failed.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether JP1/IM has started.

**KDSL0680-I**

The action for the user definition will now start. (request source = [*request-source*], action date = [*action-date*])

The user-defined action set in the action policy will now begin.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0681-I**

The action of the user definition has terminated. (request source = [*request-source*], action date = [*action-date*])

The user-defined action set in the action policy has ended.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0682-E (0x00005454)**

The action for the user definition has failed. An internal error occurred. (request source = [*request-source*], action date = [*action-date*], error code = [*error-code*])

The user-defined action failed because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0683-E (0x00005455)**

The action for the user definition has failed. No command is defined in the action policy. (request source = [*request-source*], action date = [*action-date*], action name = [*action-name*], policy name = [*policy-name*], asset number = [*asset-number*], error code = [*error-code*])

The user-defined action could not be performed because the command in the action policy was not found.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check the path specified in the action policy for errors.

**KDSL0684-E (0x00005456)**

The action for the user definition has failed. A file I/O error occurred. (request source = [*request-source*], action date = [*action-date*], action name = [*action-name*], policy name = [*policy-name*], asset number = [*asset-number*], error code = [*error-code*])

The user-defined action could not be performed because a file I/O error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether there is enough free space on the disk. Alternatively, check whether write permission has been set for the `usr` directory in the JP1/CSC - Manager installation directory.

**KDSL0685-E (0x00005457)**

An attempt to execute the command has failed. An internal error occurred. (request source = [*request-source*], action date = [*action-date*], action name = [*action-name*], policy name = [*policy-name*], error code = [*error-code*])

The command could not be performed because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0686-E (0x00005458)**

An attempt to execute command has failed. No command is defined in the action policy. (request source = [*request-source*], action date = [*action-date*], action name = [*action-name*], policy name = [*policy-name*], error code = [*error-code*])

The command could not be performed because the command defined in the action policy was not found.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check the path specified in the action policy for errors.

**KDSL0687-E (0x0000546C)**

The action for the user definition has failed. An internal error occurred. (request source = [*request-source*], action date = [*action-date*], action name = [*action-name*], policy name = [*policy-name*], asset number = [*asset-number*], error code = [*error-code*])

The user-defined action failed because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0750-I**

An action request will now start. (request source = [*request-source*], request reception date = [*request-reception-date*])

An action for the client will now start.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0751-I**

An action request has terminated. (request source = [request-source], request reception date = [request-reception-date])

An action for the client terminated.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0752-I**

Action request contents. (request source = [request-source], request reception date = [request-reception-date], number of request PCs = [number-of-PC-units], number of action PCs = [number-of-PC-units], safe = [number-of-PC-units], caution = [number-of-PC-units], warning = [number-of-PC-units], danger = [number-of-PC-units], unknown = [number-of-PC-units], Not applicable = [number-of-PC-units])

This message displays the contents of the action to be implemented.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0753-W**

Action will be skipped. The judgment result of the asset that corresponds to the asset information is not a target for action. (request source = [request-source], request reception date = [request-reception-date], asset information = [asset-number-or-asset-ID], security level = [security-level])

Actions will be skipped because the judgment result of the security level corresponding to the asset information is *Not yet judged*, *Not applicable*, or *Unknown*.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

**KDSL0754-E(0x00005471)**

An attempt to request an action has failed. There is no asset that corresponds to the asset information. (request source = [request-source], request reception date = [request-reception-date], asset information = [asset-number-or-asset-ID])

An action could not be implemented because there was no asset that corresponds to the asset information.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the asset information has been registered in the asset management database.

**KDSL0755-E(0x0000546E)**

An attempt to request an action has failed. A database access error occurred. (request source = [*request-source*], request reception date = [*request-reception-date*], error code = [*error-code*])

An action could not be implemented because a database access error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL0756-W**

An action cannot be executed because no asset information exists. (request source = [*request-source*], request reception date = [*request-reception-date*])

An action could not be implemented because asset information for the client subject to the action was not found.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the asset information for the client has been registered.

**KDSL0757-W**

There is no asset subject to the action. (request source = [*request-source*], request reception date = [*request-reception-date*], asset information = [*asset-ID-or-asset-number*])

There was no client subject to the action.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the asset information has been registered in the asset management database.

**KDSL0758-W**

There is no asset information that corresponds to the specified asset number. (request source = [*request-source*], request reception date = [*request-reception-date*], asset number = [*asset-number*])



There was no asset information for the client that corresponds to the asset number.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the asset information has been registered in the asset management database.

**KDSL0760-E(0x0000546F)**

An attempt to request an action has failed. An internal error occurred. (request source = [*request-source*], request reception date = [*request-reception-date*], error code = [*error-code*])

An action could not be implemented because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL0800-E**

An attempt to start the manager has failed.

JP1/CSC - Manager could not be started.

(S)

Cancels the startup of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0801-E**

An attempt to terminate the manager has failed.

JP1/CSC - Manager could not be terminated.

(S)

Shuts down JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0802-E**

An attempt to set up the manager environment has failed.

The JP1/CSC - Manager environment could not be configured.

(S)

Cancels the configuration of JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0998-E (0x0000543C)**

An internal error occurred in the manager. (error code =  
[*error-code*])

An internal error occurred in JP1/CSC - Manager.

(S)

Ends JP1/CSC - Manager.

(O)

Contact the system administrator.

**KDSL0999-E (0x0000543D)**

(A message concerning the database)

A message from the database is displayed.

(S)

Check the messages before and after this message.

(O)

See the database documentation and check the content of the message.

**(2) Messages regarding commands (1000 to 1999)**

**KDSL1000-I**

Manager setup terminated normally.

JP1/CSC - Manager is set up.

(S)

Ends the command.

**KDSL1001-E**

An attempt to create client security management information has  
failed.

The client security control information could not be created.

(S)

Ends the command.

(O)

Check whether the setup of Asset Information Manager has been completed and whether the AIM database has sufficient free space.

**KDSL1003-E**

An attempt to set up a manager has failed. Command execution permissions are lacking.

JP1/CSC - Manager could not be set up because the user who executed the command was not authorized to do so.

(S)

Ends the command.

(O)

An administrator role user must execute the command.

**KDSL1004-E**

An attempt to set up a manager has failed.

Setup of JP1/CSC - Manager failed.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL1005-E**

An attempt to set up a manager has failed. Either Asset Information Manager is not installed or it is an unsupported version.

JP1/CSC - Manager could not be set up. JP1/CSC supports AIM 08-00 or later.

(S)

Ends the command.

(O)

Check whether AIM 08-00 or later is installed.

**KDSL1006-E**

An attempt to set up a manager has failed. The World Wide Web Publishing Service is running.

JP1/CSC - Manager could not be set up because the World Wide Web Publishing Service was active.

(S)

Ends the command.

(O)

Check whether the World Wide Web Publishing Service is active or not.

**KDSL1007-E**

An attempt to set up a manager has failed. A database access error occurred.

JP1/CSC - Manager could not be set up because a database access error occurred.

(S)

Ends the command.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL1008-I**

Setup has already been completed.

JP1/CSC - Manager is already set up.

(S)

Ends the command.

**KDSL1050-I**

A security level judgment request has been received.

The security level judgment request was accepted.

(S)

Ends the command.

**KDSL1051-E**

An attempt to judge a security level has failed. A communication error occurred.

The security level could not be judged because a communication error occurred.

(S)

Ends the command.

(O)

Check whether an error occurred in JP1/CSC - Manager. Check whether the communication environment of JP1/CSC - Manager is operating normally.

**KDSL1052-E**

An attempt to judge a security level has failed. A file I/O error occurred.

The security level could not be judged because a file I/O error occurred.

(S)

Ends the command.

(O)

Check whether the disk has sufficient free space or an error occurred in the file system. If the problem is not resolved, contact the system administrator.

**KDSL1053-E**

An attempt to judge a security level has failed. Command execution permissions are lacking.

The security level could not be judged because the user who executed the command was not authorized to do so.

(S)

Ends the command.

(O)

An administrator role user must execute the command.

**KDSL1054-E**

An attempt to judge a security level has failed. Manager setup has not been completed.

The security level could not be judged because the setup of JP1/CSC - Manager was not completed.

(S)

Ends the command.

(O)

Set up JP1/CSC - Manager. If the problem is not resolved, contact the system administrator.

**KDSL1055-E**

An attempt to judge a security level has failed.

The security level could not be judged.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL1056-E**

An attempt to judge a security level has failed. The contents of the asset number file are invalid.

The security level could not be judged because the content of the asset number file was incorrect.

(S)

Ends the command.

(O)

Check whether the content of the asset number file is correct.

**KDSL1057-E**

An attempt to judge a security level has failed. A database access error occurred.

The security level could not be judged because a database access error occurred.

(S)

Ends the command.

(O)

Check whether the database is active or an error occurred in the database, and then try the command again.

**KDSL1058-E**

An attempt to judge a security level has failed. The contents of the search condition file are invalid.

The security level could not be judged because the search condition file contains an error.

(S)

Ends the command.

(O)

Check whether the search condition file is formatted correctly, and then try the command again.

**KDSL1059-W**

The security level cannot be judged because no asset information exists.

The security level could not be judged because there is no asset information corresponding to the search condition in the asset management database.

(S)

Ends the command.

(O)

Check whether the condition specified in the search condition file is correct, and

then try the command again.

**KDSL1060-E**

An attempt to judge a security level has failed. Asset Information Manager is not installed.

The security level could not be judged because AIM is not installed.

(S)

Ends the command.

(O)

Check whether AIM is installed correctly.

**KDSL1080-I**

The policy assignment terminated normally.

Policy assignment has ended.

(S)

Ends the command.

**KDSL1081-E**

An attempt to assign a policy has failed. Command execution permissions are lacking.

Policy assignment was unsuccessful because the user who executed the command was not authorized to do so.

(S)

Ends the command.

(O)

An administrator role user must execute the command.

**KDSL1082-E**

An attempt to assign a policy has failed. Manager setup has not been completed.

Policy assignment was unsuccessful because the setup of JP1/CSC - Manager was not completed.

(S)

Ends the command.

(O)

Set up JP1/CSC - Manager. If the problem is not resolved, contact the system administrator.

**KDSL1083-E**

An attempt to assign a policy has failed. Asset Information Manager is not installed.

Policy assignment was unsuccessful because AIM is not installed.

(S)

Ends the command.

(O)

Check whether AIM is installed correctly.

**KDSL1084-E**

An attempt to assign a policy has failed. A file I/O error occurred.

The policy could not be assigned because a file I/O error occurred.

(S)

Ends the command.

(O)

Check whether the disk has sufficient free space or whether an error occurred in the file system. If the problem is not resolved, contact the system administrator.

**KDSL1085-E**

An attempt to assign a policy has failed. The content of the policy assignment file is invalid. (line number = *[line-number]*)

Policy assignment was unsuccessful because the content of the policy assignment definition file was incorrect.

(S)

Ends the command.

(O)

Check whether the content of the policy assignment definition file is correct.

**KDSL1086-E**

An attempt to assign a policy has failed. A database access error occurred.

Policy assignment was unsuccessful because a database access error occurred.

(S)

Ends the command.

(O)

Check whether the database is active or whether an error occurred in the database,



and then try the command again.

**KDSL1087-E**

An attempt to assign a policy has failed. There is no policy specified for the policy assignment file. (policy name = *[policy-name-specified-in-policy-assignment-definition-file]*)

Policy assignment was unsuccessful because the policy specified in the assignment definition file does not exist.

(S)

Ends the command.

(O)

Check whether the conditions specified in the policy assignment definition file are correct, and then try the command again.

**KDSL1088-W**

There is no asset corresponding to the key word specified for the policy assignment file. (keyword = *[keyword-(group-name-or-asset-number)-specified-in-policy-assignment-definition-file]*)

There is no asset that corresponds to a keyword specified in the policy assignment definition file.

(S)

Resumes the command.

(O)

Check the keywords specified in the policy assignment definition file, and then try the command again.

**KDSL1089-E**

An attempt to assign a policy has failed. There are no assets.

Policy assignment was unsuccessful because there is no corresponding asset information in the resource management database.

(S)

Ends the command.

(O)

Check whether the policy assignment definition file is formatted correctly, and then try the command again.

**KDSL1090-E**

An attempt to assign a policy has failed. A policy specified in the policy assignment file could not be assigned. (policy name = *[policy-name-specified-in-policy-assignment-definition-file]*)

Policy assignment was unsuccessful because a policy that could not be assigned was specified in the policy assignment definition file.

(S)

Ends the command.

(O)

Review the policy names in the policy assignment definition file, and then try the command again.

**KDSL1091-E**

An attempt to assign a policy has failed.

Policy assignment was unsuccessful for a reason not covered by messages KDSL1081-E to KDSL1090-E.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL1110-I**

The policy import terminated normally.

The policy has been imported.

(S)

Ends the command.

**KDSL1111-E**

An attempt to import the policy has failed. Command execution permissions are lacking.

The policy could not be imported because the user who executed the command was not authorized to do so.

(S)

Ends the command.

(O)

An administrator role user must execute the command.

**KDSL1112-E**

An attempt to import the policy has failed. Manager setup has not been completed.

The policy could not be imported because the setup of JP1/CSC - Manager was not completed.

(S)

Ends the command.

(O)

Set up JP1/CSC - Manager. If the problem is not resolved, contact the system administrator.

**KDSL1113-E**

An attempt to import the policy has failed. Asset Information Manager is not installed.

The policy could not be imported because AIM is not installed.

(S)

Ends the command.

(O)

Check whether AIM is installed correctly.

**KDSL1114-E**

An attempt to import the policy has failed. A file I/O error occurred.

The policy could not be imported because a file I/O error occurred.

(S)

Ends the command.

(O)

Check whether the disk has sufficient free space or whether an error occurred in the file system. If the problem is not resolved, contact the system administrator.

**KDSL1115-E**

An attempt to import the policy has failed. The content of the anti-virus product policy import file is invalid. (line number = [*line-number*])

The policy could not be imported because the content of the policy import file for anti-virus products was incorrect.

(S)

Ends the command.

(O)

Check whether the content of the policy import file for anti-virus products is correct.

**KDSL1116-E**

An attempt to import the policy has failed. A database access error occurred.

The policy could not be imported because a database access error occurred.

(S)

Ends the command.

(O)

Check whether the database is active or whether an error occurred in the database.

**KDSL1117-W**

There is no judgment policy name specified for the anti-virus product policy import file. (judgment policy name = [judgment-policy-name])

The judgment policy specified in the policy import file for anti-virus products does not exist.

(S)

Resumes the command.

(O)

Check whether the content of the policy import file for anti-virus products is correct.

**KDSL1118-W**

The information to be updated to the anti-virus product policy import file is not specified. (line number = [line-number])

The information to use to update the policy import file for anti-virus products was not specified.

(S)

Resumes the command.

(O)

Check whether the content of the policy import file for anti-virus products is correct.

**KDSL1119-W**

An attempt to update the policy specified in the policy import file for the anti-virus product failed. (judgment policy name = [judgment-policy-name])

The policy could not be imported because the specified policy name could not be updated.

(S)

Resumes the command.

(O)

Review the specified policy name, and then try the command again.

**KDSL1120-E**

An attempt to import the policy has failed.

The policy could not be imported for a reason not covered by messages KDSL1111-E to KDSL1119-W.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL1130-I**

The policy import terminated normally. (policy name = *[policy-name]*)

The policy import terminated normally.

(S)

Ends the command.

**KDSL1131-E**

An attempt to import the policy failed. A file I/O error occurred. (policy name = *[policy-name]*)

The policy could not be imported because a file I/O error occurred.

(S)

Ends the command.

(O)

- Check whether the path and access permissions for the policy import file are correct.
- Check whether the disk has sufficient free space or whether an error occurred in the file system. If the problem is not resolved, contact the system administrator.

**KDSL1132-E**

An attempt to import the policy failed. A database access error occurred. (policy name = *[policy-name]*)

The policy could not be imported because a database access error occurred.

(S)

Ends the command.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL1133-E**

An attempt to import the policy failed. No policy name is specified. (policy name = [*policy-name*])

The specified judgment policy was not found.

(S)

Ends the command.

(O)

Review the specified policy name, and then try the command again.

**KDSL1134-E**

An attempt to import the policy failed. The specified policy cannot be updated. (policy name = [*policy-name*])

The policy could not be imported because the specified policy could not be updated.

(S)

Ends the command.

(O)

Review the specified policy name, and then try the command again.

**KDSL1135-E**

An attempt to import the policy failed. The content of the policy import file is invalid. (policy name = [*policy-name*], line number = [*line-number*], item number = [*item-number*])

The policy could not be imported because the contents of the policy import file were invalid.

(S)

Ends the command.

(O)

Check whether the contents of the policy import file are correct.

**KDSL1136-E**

An attempt to import the policy failed. A required section of the policy import file is not specified. (policy name = [*policy-name*], section name = [*section-name*])

The policy could not be imported because the section was not specified in the policy import file.

(S)

Ends the command.

(O)

Check whether the contents of the policy import file are correct.

#### **KDSL1137-E**

An attempt to import the policy failed. A required parameter ID of the policy import file is not specified. (policy name = *[policy-name]*, section name = *[section-name]*, parameter ID = *[parameter-ID]*, item name = *[item-name]*)

The policy could not be imported because the parameter ID was not specified in the policy import file.

(S)

Ends the command.

(O)

Check whether the contents of the policy import file are correct.

#### **KDSL1138-E**

An attempt to import the policy failed. The content specified for a line in the policy import file is the same as for another line. (policy name = *[policy-name]*, line number = *[line-number]*)

The policy could not be imported because a line that has the same contents has already been specified in the policy import file.

(S)

Ends the command.

(O)

Check whether the contents of the policy import file are correct.

#### **KDSL1139-E**

An attempt to import the policy failed. The number of conditions for each item does not match the number of specified conditions. (policy name = *[policy-name]*, line number = *[line-number]*)

The policy could not be imported because the number of conditions specified for each item is not the same for the items.

(S)

Ends the command.

(O)

Check whether the contents of the policy import file are correct.

**KDSL1140-E**

An attempt to import the policy failed. Conditions are duplicated within the specified conditions. (policy name = *[policy-name]*, line number = *[line-number]*)

The policy could not be imported because the same condition was specified more than once.

(S)

Ends the command.

(O)

Check whether the contents of the policy import file are correct.

**KDSL1141-E**

An attempt to import the policy failed. The judgment options of the group and judgment items do not match. (policy name = *[policy-name]*, line number = *[line-number]*)

The policy could not be imported because the group judgment option and the item judgment option do not match.

(S)

Ends the command.

(O)

Check whether the contents of the policy import file are correct.

**KDSL1142-E**

An attempt to import the policy failed. The values of the judgment options of the group are not the same within the same group. (policy name = *[policy-name]*, group name = *[group-name]*)

The policy could not be imported because the values of the group judgment options are different within the group.

(S)

Ends the command.

(O)

Check whether the contents of the policy import file are correct.



**KDSL1143-E**

An attempt to import the policy failed. The judgment options of the group and judgment items are not the same within the same group. (policy name = [*policy-name*], group name = [*group-name*])

The policy could not be imported because the group judgment option and the item judgment option are different in the group.

(S)

Ends the command.

(O)

Check whether the contents of the policy import file are correct.

**KDSL1144-E**

An attempt to import the policy failed. The combination of judgment conditions is invalid. (policy name = [*policy-name*], line number = [*line-number*])

The policy could not be imported because conflicting conditions were specified.

(S)

Ends the command.

(O)

Check whether the contents of the policy import file are correct.

**KDSL1145-E**

An attempt to import the policy failed. The property comparison conditions are invalid. (policy name = [*policy-name*], line number = [*line-number*])

The policy could not be imported because the value of the comparison condition for the specified property was incorrect.

(S)

Ends the command.

(O)

Check whether the contents of the policy import file are correct.

**KDSL1200-I**

PC list information has been output.

PC list information has been output.

(S)

Ends the command.

**KDSL1201-E**

An attempt to output PC list information has failed. A file I/O error occurred.

PC list information could not be output because a file I/O error occurred.

(S)

Ends the command.

(O)

Check whether the path access permissions for the output destination folder of PC list information are correct.

**KDSL1202-E**

An attempt to output PC list information has failed. Command execution permissions are lacking.

PC list information could not be output because the user who executed the command was not authorized to do so.

(S)

Ends the command.

(O)

An administrator role user must execute the command.

**KDSL1203-E**

An attempt to output PC list information has failed. Manager setup has not been completed.

PC list information could not be output because JP1/CSC - Manager setup has not been completed.

(S)

Ends the command.

(O)

Set up JP1/CSC - Manager and then try the command again.

**KDSL1204-E**

An attempt to output PC list information has failed. The format of the security level judgment date is invalid.

PC list information could not be output because the format of the security level judgment date was invalid.

(S)

Ends the command.

(O)

Check whether the format of the security level judgment date is correct, and then try the command again.

**KDSL1205-W**

An attempt to output PC list information has failed. No PC list information matches the conditions.

PC list information could not be output because the PC list information to be output was not found.

(S)

Ends the command.

(O)

Check the security level judgment date in the JP1/CSC - Manager log file. Alternatively, check whether there is an asset that belongs to the group specified in the search condition file.

**KDSL1206-E**

An attempt to output PC list information has failed. A database access error occurred.

PC list information could not be output because a database access error occurred.

(S)

Ends the command.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL1207-E**

An attempt to output PC list information has failed. The judgment history cannot be obtained.

PC list information could not be output because the judgment history could not be obtained.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL1208-E**

An attempt to output PC list information has failed. There are no assets.

PC list information could not be output because no assets for which output was

possible were not found.

(S)

Ends the command.

(O)

Check whether the asset information has been registered in the asset management database.

**KDSL1209-E**

An attempt to output PC list information has failed. Asset Information Manager is not installed.

PC list information could not be output because AIM is not installed.

(S)

Ends the command.

(O)

Check whether AIM has been installed correctly.

**KDSL1210-E**

An attempt to output PC list information has failed. The contents of the search condition file are invalid.

PC list information could not be output because the contents of the search condition file are invalid.

(S)

Ends the command.

(O)

Check whether the search condition file is formatted correctly, and then try the command again

**KDSL1220-E**

An attempt to output PC list information has failed.

PC list information could not be output.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL1250-I**

An action request has been received.

An action request has been received.

(S)

Ends the command.

#### **KDSL1251-E**

An attempt to execute an action has failed. A communication error occurred.

An action could not be implemented because a communication error occurred.

(S)

Ends the command.

(O)

Check whether an error occurred in JP1/CSC - Manager. Also check whether the communication environment of JP1/CSC - Manager is operating normally.

#### **KDSL1252-E**

An attempt to execute an action has failed. A file I/O error occurred.

An action could not be implemented because a file I/O error occurred.

(S)

Ends the command.

(O)

Check whether the disk has sufficient free space or whether an error occurred in the file system. If the problem is not resolved, contact the system administrator.

#### **KDSL1253-E**

An attempt to execute an action has failed. Command execution permissions are lacking.

An action could not be implemented because the user who executed the command was not authorized to do so.

(S)

Ends the command.

(O)

An administrator role user must execute the command.

#### **KDSL1254-E**

An attempt to execute an action has failed. Manager setup has not been completed.

An action could not be implemented because JP1/CSC - Manager setup has not been

completed.

(S)

Ends the command.

(O)

Set up JP1/CSC - Manager. If the problem is not resolved, contact the system administrator.

**KDSL1256-E**

An attempt to execute an action has failed. The contents of the asset number file are invalid.

An action could not be implemented because the contents of the asset number file are invalid.

(S)

Ends the command.

(O)

Check whether the contents of the asset number file are valid.

**KDSL1257-E**

An attempt to execute an action has failed. A database access error occurred.

An action could not be implemented because a database access error occurred.

(S)

Ends the command.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL1258-E**

An attempt to execute an action has failed. The contents of the search condition file are invalid.

An action could not be implemented because the contents of the search condition file are invalid.

(S)

Ends the command.

(O)

Check whether the search condition file is formatted correctly, and then try the command again.

**KDSL1259-W**

An action cannot be executed because no asset information exists.

An action could not be implemented because asset information that meets the condition was not found in the asset management database.

(S)

Ends the command.

(O)

Check whether the asset that meets the condition exists in the asset management database, and then try the command again.

**KDSL1260-E**

An attempt to execute an action has failed. Asset Information Manager is not installed.

An action could not be implemented because AIM was not installed.

(S)

Ends the command.

(O)

Check whether AIM has been installed correctly.

**KDSL1261-E**

An attempt to execute an action has failed. There is no action policy name specified.

An action could not be implemented because the specified action policy name was not found.

(S)

Ends the command.

(O)

Check the action policy name, and then try the command again.

**KDSL1262-E**

An attempt to execute an action has failed. A specified action policy name could not be assigned.

An action could not be implemented because the specified action policy name could not be assigned.

(S)

Ends the command.

(O)

Check the action policy name, and then try the command again.

**KDSL1270-E**

An attempt to execute an action has failed.

An action could not be implemented.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL1300-I**

Storage of statistics terminated normally.

The statistics have been stored.

(S)

Ends the command.

**KDSL1301-E**

Storage of statistics has failed. Command execution permissions are lacking.

Statistics could not be stored because the user who executed the command was not authorized to do so.

(S)

Ends the command.

(O)

An administrator role user must execute the command.

**KDSL1302-E**

Storage of statistics has failed. Manager setup has not been completed.

Statistics could not be stored because the setup of JP1/CSC - Manager was not completed.

(S)

Ends the command.

(O)

Set up JP1/CSC - Manager. If the problem is not resolved, contact the system administrator.



**KDSL1303-E**

Storage of statistics has failed. Asset Information Manager is not installed.

Statistics could not be stored because AIM is not installed.

(S)

Ends the command.

(O)

Check whether AIM is installed correctly.

**KDSL1304-E**

Storage of statistics has failed. A database access error occurred.

Statistics could not be stored because a database access error occurred.

(S)

Ends the command.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL1305-E**

Storage of statistics has failed. There is no PC security information in the asset management database.

Statistics could not be stored because there was no PC security information in the asset management database.

(S)

Ends the command.

(O)

Check whether there is PC security information in the asset management database.

**KDSL1310-E**

Storage of statistics has failed.

Statistics could not be stored.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL1350-I**

Statistics have been output.

Statistics have been output.

(S)

Ends the command.

**KDSL1351-E**

Output of statistics has failed. A file I/O error occurred.

Statistics could not be output because a file I/O error occurred.

(S)

Ends the command.

(O)

Check whether the path and access permissions for the output destination folder of the statistics are correct.

**KDSL1352-E**

Output of statistics has failed. Command execution permissions are lacking.

Statistics could not be output because the user who executed the command was not authorized to do so.

(S)

Ends the command.

(O)

An administrator role user must execute the command.

**KDSL1353-E**

Output of statistics has failed. Manager setup has not been completed.

Statistics could not be output because JP1/CSC - Manager setup has not been completed.

(S)

Ends the command.

(O)

Set up JP1/CSC - Manager and then try the command again.

**KDSL1354-E**

Output of statistics has failed. A database access error occurred.

Statistics could not be output because a database access error occurred.

(S)

Ends the command.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL1355-E**

Output of statistics has failed. The contents of the search condition file are invalid.

Statistics could not be output because the contents of the search condition file are invalid.

(S)

Ends the command.

(O)

Check whether the search condition file is formatted correctly, and then try the command again.

**KDSL1356-W**

Output of statistics has failed. No group belongs to the specified group or level.

Statistics could not be output because no group belongs to the specified group or level.

(S)

Ends the command.

(O)

Check whether the asset information has been registered in the asset management database. Alternatively, check whether any assets belong to the group specified in the search condition file.

**KDSL1357-E**

Output of statistics has failed. Asset Information Manager is not installed.

Statistics could not be output because AIM is not installed.

(S)

Ends the command.

(O)

Check whether AIM has been installed correctly.

**KDSL1358-W**

Output of statistics has failed. No statistics matches the conditions.

Statistics could not be output because no applicable statistics exist.

(S)

Ends the command.

(O)

In the JP1/CSC - Manager log file, check the date and time when the statistics storage command (cscstorecount) was executed. Alternatively, check whether any assets belong to the group specified in the search condition file.

**KDSL1359-E**

Output of statistics has failed. The format of the start or end date for totals is invalid.

Statistics could not be output because the start date or end date for totals was formatted incorrectly.

(S)

Ends the command.

(O)

Check whether the start date or end date for totals are formatted correctly, and then try the command again.

**KDSL1370-E**

Output of statistics has failed.

Statistics could not be output.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL1450-I**

The update of patch information terminated normally.

The patch information was updated.

(S)

Ends the command.

**KDSL1451-E**

The update of patch information has failed. Command execution permissions are lacking.

Patch information could not be updated because the user who executed the command was not authorized to do so.

(S)

Ends the command.

(O)

An administrator role user must execute the command.

**KDSL1452-E**

The update of patch information has failed. Manager setup has not been completed.

Patch information could not be updated because the setup of JP1/CSC - Manager was not completed.

(S)

Ends the command.

(O)

Set up JP1/CSC - Manager, and then try the command again.

**KDSL1453-E**

The update of patch information has failed. Asset Information Manager is not installed.

Patch information could not be updated because AIM is not installed.

(S)

Ends the command.

(O)

Check whether AIM is installed correctly.

**KDSL1454-E**

The update of patch information has failed. Software Distribution Manager is not installed.

Patch information could not be updated because JP1/Software Distribution Manager was not installed.

(S)

Ends the command.

(O)

Check whether Software Distribution Manager is installed.

**KDSL1455-E**

The update of patch information has failed. The version of Software Distribution Manager is old.

Patch information could not be updated because Software Distribution Manager 08-02 or earlier is installed.

(S)

Ends the command.

(O)

Check whether Software Distribution Manager 08-10 or later is installed.

**KDSL1456-E**

The update of patch information has failed. A database access error occurred.

Patch information could not be updated because a database access error occurred.

(S)

Ends the command.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL1457-E**

The update of patch information has failed. A file I/O error occurred for the patch information file.

Patch information could not be updated because a file I/O error occurred.

(S)

Ends the command.

(O)

Check whether the path and access permissions for the output destination folder of the patch information file are correct.

**KDSL1458-E**

The update of patch information has failed. The contents of the patch information file are invalid.

Patch information could not be updated because the patch information file contains an error.

(S)

Ends the command.

(O)

Check whether the patch information file is formatted correctly, and then try the command again.

**KDSL1459-E**

The update of patch information has failed. A file I/O error occurred for the patch information management file.

Patch information could not be updated because a file I/O error occurred in the patch information management file.

(S)

Ends the command.

(O)

Check whether the path and access permissions for the output destination folder of the patch information management file are correct.

**KDSL1460-E**

The update of patch information has failed. The contents of the patch information management file are invalid.

Patch information could not be updated because the patch information management file contains an error.

(S)

Ends the command.

(O)

Check whether the patch information management file is formatted correctly, and then try the command again.

**KDSL1461-E**

The update of patch information has failed. A file I/O error occurred for the patch information update condition file.

Patch information could not be updated because a file I/O error occurred in the patch information update condition file.

(S)

Ends the command.

(O)

Check whether the path and access permissions for the output destination folder of the patch information update condition file are correct.

**KDSL1462-E**

The update of patch information has failed. The contents of the patch information update condition file are invalid. (line number = [*line-number*])

Patch information could not be updated because the patch information update condition file contains an error.

(S)

Ends the command.

(O)

Check whether the patch information update condition file is formatted correctly, and then try the command again.

**KDSL1463-E**

The update of patch information has failed. There is no judgment policy specified. (judgment policy name = [*judgment-policy-name*])

The patch information update command could not be executed because the specified judgment policy does not exist.

(S)

Ends the command.

(O)

Check the name of the judgment policy, and then try the command again.

**KDSL1464-E**

The update of patch information has failed. The specified policy cannot be assigned. (judgment policy name = [*judgment-policy-name*])

The patch information update command could not be executed because the specified judgment policy could not be assigned.

(S)

Ends the command.

(O)

Check the name of the judgment policy, and then try the command again.

**KDSL1465-I**

None of the information in the patch information file is subject to updating.

None of the patch information in the patch information file was subject to updating.

(S)

Ends the command.



**KDSL1466-I**

The patch information file has not been updated.

The patch information file had not been updated.

(S)

Ends the command.

**KDSL1467-E**

The update of patch information has failed. The version of MSXML is old.

Patch information could not be updated because MSXML version 4.0 or earlier is installed.

(S)

Ends the command.

(O)

Check whether MSXML 4.0 Service Pack 2 or MSXML 6.0 is installed.

**KDSL1468-W**

The judgment policy cannot be updated because patch information is invalid. (article ID number = [*article-ID-number*])

Patch information could not be updated because the patch information contains an error.

(S)

Ends the command.

(O)

Set the relevant patch information in the Definition of Mandatory Security Updates dialog box.

**KDSL1469-E**

The update of patch information has failed.

Patch information could not be updated.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL1500-I**

The policy export terminated normally. (policy name = [*policy-name*])

The policy export terminated normally.

(S)

Ends the command.

**KDSL1501-E**

An attempt to export the policy failed. You do not have command execution permissions.

The policy could not be exported because the user who executed the command was not authorized to do so.

(S)

Ends the command.

(O)

A user with administrator privileges must execute the command.

**KDSL1502-E**

An attempt to export the policy failed. Manager setup is incomplete.

The policy could not be exported because JP1/CSC - Manager setup had not been completed.

(S)

Ends the command.

(O)

Set up JP1/CSC - Manager. If the problem is not resolved, contact the system administrator.

**KDSL1503-E**

An attempt to export the policy failed. Asset Information Manager is not installed.

The policy could not be imported because AIM was not installed.

(S)

Ends the command.

(O)

Check whether AIM is installed correctly.

**KDSL1504-E**

An attempt to export the policy failed. A file I/O error occurred. (policy name = [*policy-name*])

The policy could not be exported because a file I/O error occurred.

(S)

Ends the command.

(O)

Check whether the path and access permissions for the output folder of the policy export file are correct.

**KDSL1505-E**

An attempt to export the policy failed. A database access error occurred. (policy name = [*policy-name*])

The policy could not be exported because a database access error occurred.

(S)

Ends the command.

(O)

Check whether the database is active or whether an error occurred in the database.

**KDSL1506-E**

An attempt to export the policy failed. No policy name is specified. (policy name = [*policy-name*])

The specified judgment policy was not found.

(S)

Ends the command.

(O)

Review the specified policy name, and then try the command again.

**KDSL1507-E**

An attempt to export the policy failed.

The policy could not be exported.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL1600-I**

Network information maintenance terminated normally.

Network information maintenance terminated normally.

(S)

Ends the command.

**KDSL1601-E**

Network information maintenance failed. You do not have command execution permissions.

Maintenance of the network information could not be performed because the user who executed the command was not authorized to do so.

(S)

Ends the command.

(O)

A user with administrator privileges must execute the command.

**KDSL1602-E**

Network information maintenance failed. Manager setup is incomplete.

Maintenance of the network information could not be performed because JP1/CSC - Manager setup had not been completed.

(S)

Ends the command.

(O)

Set up JP1/CSC - Manager, and then try the command again.

**KDSL1603-E**

Network information maintenance failed. Asset Information Manager is not installed.

Maintenance of the network information could not be performed because AIM was not installed.

(S)

Ends the command.

(O)

Check whether AIM is installed.

**KDSL1604-E**

Network information maintenance failed. A file I/O error occurred.

Maintenance of the network information could not be performed because a file I/O error occurred.

(S)

Ends the command.

(O)

Check whether the path and access permissions for the output destination folder are correct.

#### **KDSL1605-E**

Network information maintenance failed. The content of the file defining MAC addresses that are not to be removed is invalid.  
(line number = [*line-number*])

Maintenance of the network information could not be performed because the definition file of MAC addresses not subject to deletion contains an error.

(S)

Ends the command.

(O)

Check whether the contents of the definition file of MAC addresses not subject to deletion are correct, and then try the command again.

#### **KDSL1606-E**

Network information maintenance failed. A database access error occurred.

Maintenance of the network information could not be performed because a database access error occurred.

(S)

Ends the command.

(O)

Check whether the database is active, and then try the command again.

#### **KDSL1607-E**

Network information maintenance failed. No network control product is installed. (product name = [*product-name*]#)

Maintenance of the network information could not be performed because the network control product was not installed.

#

JP1/NM - Manager

(S)

Ends the command.

(O)

Check whether the network control product is installed.

**KDSL1608-E**

Network information maintenance failed. An error was detected in the network control product. (error code = [*error-code*])

Maintenance of the network information could not be performed because an error was detected in the network control product.

(S)

Ends the command.

(O)

Check whether the network control linkage is configured correctly or whether an error occurred in the network control product.

**KDSL1609-I**

The network information subject to maintenance was not found.

The network information subject to maintenance was not found.

(S)

Ends the command.

**KDSL1610-I**

A MAC address was removed from the list of permitted devices. (MAC address = [*MAC-address*])

The MAC address was removed from the list of permitted devices.

(S)

Ends the command.

**KDSL1611-W**

An attempt to remove a MAC address from the list of permitted devices failed. (MAC address = [*MAC-address*], error code = [*error-code*])

The MAC address could not be removed from the list of permitted devices.

(S)

Ends the command.

(O)

Check whether an error occurred in the network control product.

**KDSL1612-E**

Network information maintenance failed.

Maintenance of the network information could not be performed.

(S)

Ends the command.

(O)

Contact the system administrator.

**(3) Messages regarding the execution of operations on the Policy Management window (2000 to 2999)**

**KDSL2001-E**

An internal error occurred while a policy was being changed or obtained. (error code = [error-code])

An internal error occurred when the security policy was being changed or acquired.

(S)

Outputs the message and cancels the processing in the Policy Management window.

(O)

Contact the system administrator.

**KDSL2011-I (0x0000543E)**

*user-ID* logged in.

The user indicated in the message logged in to the Policy Management Login window of JP1/CSC.

(S)

Outputs the message and continues the processing in the Policy Management window.

**KDSL2012-E (0x0000543F)**

*user-ID* failed to log in.

The user indicated in the message failed to log in to the Policy Management Login window of JP1/CSC.

(S)

Outputs the message and cancels the processing in the Policy Management window.

(O)

Check whether the user ID, the password, and the user role are correct.

**KDSL2013-E**

A database access error occurred in the Policy Management window. (error code = [error-code])

A database access error occurred in the Policy Management window.

(S)

Outputs the message and cancels the processing in the Policy Management window.

(O)

Check whether the database is active or an error occurred in the database.

**KDSL2014-E**

An I/O error occurred in the policy file. (error code = [error-code])

An I/O error occurred in the security policy file.

(S)

Outputs the message and cancels the processing in the Policy Management window.

(O)

Check whether the disk has sufficient free space or an error occurred in the file system. If the problem is not resolved, contact the system administrator.

**KDSL2015-E**

Asset Information Manager is not installed. (error code = [error-code])

AIM is not installed.

(S)

Outputs the message and cancels the processing in the Policy Management window.

(O)

Check whether AIM is installed correctly.

**KDSL2016-E**

An internal error occurred in the Policy Management window. (error code = [error-code])

An internal error occurred in the Policy Management window.

(S)

Outputs the message and cancels the processing in the Policy Management window.

(O)

Contact the system administrator.



**KDSL2030-I (0x0000544C)**

The *policy-type* policy was registered. (policy name = [*policy-name*])

The judgment policy or the action policy was registered.

(S)

Outputs the message and continues the processing in the Policy Management window.

**KDSL2031-E**

An attempt to register the *policy-type* policy has failed. (policy name = [*policy-name*])

The judgment policy or the action policy could not be registered.

(S)

Outputs the message and cancels the processing in the Policy Management window.

(O)

Contact the system administrator.

**KDSL2032-I (0x0000544D)**

The *policy-type* policy was assigned. (policy name = [*policy-name*], assignment unit = [*assignment-unit*], assignment number = [*assignment-number*])

The judgment policy or the action policy was assigned.

(S)

Outputs the message and continues the processing in the Policy Management window.

**KDSL2033-E**

An attempt to assign the *policy-type* policy has failed. (policy name = [*policy-name*], assignment unit = [*assignment-unit*])

The judgment policy or the action policy could not be assigned.

(S)

Outputs the message and cancels the processing in the Policy Management window.

(O)

Contact the system administrator.

**KDSL2036-E**

An attempt to obtain *policy-type* policy has failed. (policy name = [*policy-name*])

The judgment policy or the action policy could not be acquired.

(S)

Outputs the message and cancels the processing in the Policy Management window.

(O)

Contact the system administrator.

**KDSL2037-I (0x00005440)**

*policy-type* policy has been changed. (policy name = [*policy-name*])

The judgment policy or the action policy was changed.

(S)

Outputs the message and continues the processing in the Policy Management window.

**KDSL2038-E**

An attempt to change *policy-type* policy has failed. (policy name = [*policy-name*])

The judgment policy or the action policy could not be changed.

(S)

Outputs the message and cancels the processing in the Policy Management window.

(O)

Contact the system administrator.

**KDSL2040-E**

An attempt to update the *policy-type* policy name has failed. (policy name = [*policy-name*])

The name of the judgment policy or action policy could not be changed.

(S)

Outputs the message and cancels the processing in the Policy Management window.

(O)

Contact the system administrator.

**KDSL2042-I (0x0000544E)**

The *policy-type* policy was deleted. (policy name = [*policy-name*])

The judgment policy or the action policy was deleted.

(S)

Outputs the message and continues the processing in the Policy Management window.

**KDSL2043-E**

An attempt to delete the *policy-type* policy has failed. (policy name = [*policy-name*])

The judgment policy or the action policy could not be deleted.

(S)

Outputs the message and cancels the processing in the Policy Management window.

(O)

Contact the system administrator.

**KDSL2044-E**

An attempt to delete the *policy-type* policy has failed. The policy is assigned. (policy name = [*policy-name*])

The policy has already been assigned and cannot be deleted.

(S)

Outputs the message and cancels the processing in the Policy Management window.

(O)

Contact the system administrator.

**KDSL2045-I (0x0000544F)**

The default policy was assigned to the assets where the *policy-type* policy [*policy-name*] is assigned.

The default policy has been assigned to the asset to which the *policy-type* policy *policy-name* was assigned.

(S)

Outputs the message and continues the processing in the Policy Management window.

**KDSL2046-I (0x00005450)**

The *policy-type* policy name was changed. (before change = [*policy-name-before*], after change = [*policy-name-after*])

The name of the judgment policy or the action policy was changed.

(S)

Outputs the message and continues the processing in the Policy Management

window.

**KDSL2500-E**

Manager setup has not been completed. (error code = [error-code])

Setup of JP1/CSC - Manager has not been completed yet.

(S)

Cancels the processing in the Client Security Control - Manager Setup dialog box or in the Policy Management window.

(O)

Execute the `cscsetup` command to set up JP1/CSC - Manager, and then start operation of the Client Security Control - Manager Setup dialog box or the Policy Management window. If the problem is not resolved, contact the system administrator.

**(4) Messages regarding linkage with JP1/CSC - Manager Remote Option (3000 to 3199)**

**KDSL3001-I (0x00005459)**

The remote service has started.

JP1/CSC - Manager Remote Option has started.

(S)

Started JP1/CSC - Manager Remote Option.

**KDSL3002-E**

An attempt to start the remote service has failed. Manager setup has not been completed. (error code = [error-code])

JP1/CSC - Manager Remote Option could not be started because JP1/CSC - Manager was not completely set up.

(S)

Cancels the startup of JP1/CSC - Manager Remote Option.

(O)

Set up JP1/CSC - Manager and then start JP1/CSC - Manager Remote Option again. If the problem is not resolved, contact the system administrator.

**KDSL3003-E (0x0000545A)**

An attempt to start the remote service has failed. The communication environment cannot be initialized. (error code = [error-code])

JP1/CSC - Manager Remote Option could not be started because the communication environment could not be initialized.

(S)

Cancels the startup of JP1/CSC - Manager Remote Option.

(O)

Check whether the port number specified in the Client Security Control - Manager Setup dialog box is available. If the port number cannot be used, specify a port number that can be used and reconfigure the JP1/CSC - Manager environment.

**KDSL3004-E (0x0000545B)**

An attempt to start the remote service has failed. An internal error occurred. (error code = [error-code])

JP1/CSC - Manager Remote Option could not be started because an internal error occurred.

(S)

Cancels the startup of JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3005-W (0x0000545C)**

The remote service terminated normally.

JP1/CSC - Manager Remote Option has terminated.

(S)

JP1/CSC - Manager Remote Option has terminated.

**KDSL3006-E (0x0000545D)**

An attempt to terminate the remote service has failed. A communication error occurred. (error code = [error-code])

A communication error occurred when JP1/CSC - Manager Remote Option was ending.

(S)

Ends JP1/CSC - Manager Remote Option.

(O)

Check whether an error occurred in JP1/CSC - Manager.

**KDSL3007-E (0x0000545E)**

An attempt to terminate the remote service has failed. The remote service termination processing timed out. (error code = [error-code])

A timeout error occurred during the end processing of JP1/CSC - Manager Remote Option.

(S)

Ends JP1/CSC - Manager Remote Option.

(O)

Check the JP1/CSC - Manager log. Check whether a policy was being updated while JP1/CSC - Manager Remote Option was ending.

**KDSL3008-W (0x0000545F)**

The remote service was forcibly terminated because an error occurred during termination processing.

JP1/CSC - Manager Remote Option was forcibly ended because an error occurred during the end processing of JP1/CSC - Manager Remote Option.

(S)

Ends JP1/CSC - Manager Remote Option.

(O)

Check the JP1/CSC - Manager log. Check whether a policy was being updated while JP1/CSC - Manager Remote Option was ending.

**KDSL3009-E (0x00005460)**

An attempt to terminate the remote service has failed. An internal error occurred. (error code = [error-code])

An internal error occurred while JP1/CSC - Manager Remote Option was ending.

(S)

Ends JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3010-E (0x00005461)**

An attempt to receive the remote option request has failed. A communication error occurred. (error code = [error-code])

The request from JP1/CSC - Manager Remote Option could not be accepted because a communication error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

(O)

Check whether an error occurred in JP1/CSC - Manager. Check whether the communication environment of JP1/CSC - Manager is operating normally.

**KDSL3011-E (0x00005462)**

An attempt to receive the remote option request has failed. An internal error occurred. (error code = [*error-code*])

The request from JP1/CSC - Manager Remote Option could not be accepted because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3012-W**

A request was discarded because the remote service is terminating. (content of request = [*content-of-request*])

JP1/CSC - Manager Remote Option discarded the request because it was ending.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

(O)

Check the content of the discarded request in the JP1/CSC - Manager log.

**KDSL3013-I (0x00005463)**

The remote option has started. (IP address = [*IP-address*])

JP1/CSC - Manager Remote Option has started.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

**KDSL3014-W (0x00005464)**

The remote option has terminated. (IP address = [*IP-address*])

JP1/CSC - Manager Remote Option has ended.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

**KDSL3015-E (0x00005465)**

An error occurred with the remote option. (IP address = [*IP-address*], error code = [*error-code*])

An error occurred in JP1/CSC - Manager Remote Option.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

(O)

Correct the error in JP1/CSC - Manager Remote Option.

**KDSL3016-E (0x00005466)**

A communication error occurred with the remote service. (error code = [error-code])

A communication error occurred in JP1/CSC - Manager Remote Option.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

(O)

Check whether an error occurred in JP1/CSC - Manager. Check whether the communication between JP1/CSC - Manager and JP1/CSC - Manager Remote Option is normal.

**KDSL3017-E (0x00005467)**

An internal error occurred with the remote service. (error code = [error-code])

An internal error occurred in JP1/CSC - Manager Remote Option.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3018-I (0x00005468)**

The policy has been updated.

The judgment policy was updated.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

**KDSL3019-E (0x00005469)**

An attempt to update the policy has failed. (error code = [error-code])

The judgment policy could not be updated.



(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3020-E (0x0000546A)**

An attempt to send a message to the remote option has failed. A communication error occurred. (error code = [error-code])

The message could not be sent to JP1/CSC - Manager Remote Option because a communication error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3021-E (0x0000546B)**

An attempt to send a message to the remote option has failed. An internal error occurred. (error code = [error-code])

The message could not be sent to JP1/CSC - Manager Remote Option because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3022-W (0x0000546D)**

A request was received from an unregistered remote option. (IP address = [IP-address])

A request was received from a remote management server not registered with JP1/CSC - Manager.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

(O)

Register the IP address of the remote option in the Client Security Control - Manager Setup dialog box.

**KDSL3030-E**

An attempt to start a remote service has failed.

JP1/CSC - Manager Remote Option could not be started because an attempt to start the remote service of JP1/CSC - Manager failed.

(S)

Cancels the startup processing of JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3031-E**

An attempt to terminate a remote service has failed.

JP1/CSC - Manager Remote Option could not be terminated because an attempt to terminate the remote service of JP1/CSC - Manager failed.

(S)

Terminates JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3032-I**

Anti-virus product information has been updated. (renewal date = [*renewal-date*], updated information = [*updated-information*], asset number = [*asset-number*])

Anti-virus product information has been updated.

(S)

Outputs the message and continues the remote service processing.

**KDSL3033-W (0x00005473)**

Acquisition of the anti-virus product information failed. No inventory information exists for the asset number. (asset number = [*asset-number*])

The anti-virus product information could not be acquired because there was no inventory information for the asset number.

(S)

Outputs the message and continues the remote service processing.

(O)

Check the automatic update information in the JP1/CSC - Manager Setup dialog box.

**KDSL3034-E (0x00005474)**

An attempt to automatically update the anti-virus product failed. A database access error occurred. (error code = [error-code])

The anti-virus product information could not be updated because a database access error occurred.

(S)

Outputs the message and continues the remote service processing.

(O)

Check whether the database is active.

### 17.3.2 List of JP1/CSC - Manager Remote Option messages

This subsection lists the messages of JP1/CSC - Manager Remote Option.

**KDSL3201-I**

Setup of the remote option environment was successful.

JP1/CSC - Manager Remote Option was successfully configured.

(S)

Ends the configuration for JP1/CSC - Manager Remote Option.

**KDSL3202-E**

An attempt to set up the remote option environment has failed. Execution permissions are lacking.

JP1/CSC - Manager Remote Option could not be configured because an unauthorized user attempted the configuration.

(S)

Cancels the configuration of JP1/CSC - Manager Remote Option.

(O)

Check the user role and reconfigure JP1/CSC - Manager Remote Option.

**KDSL3203-E**

An attempt to set up the remote option environment has failed. A file I/O error occurred. (error code = [error-code])

JP1/CSC - Manager Remote Option could not be configured because an I/O error occurred.

(S)

Cancels the configuration of JP1/CSC - Manager Remote Option.

(O)

Check whether the disk has sufficient free space or whether an error occurred in the file system. If the problem is not resolved, contact the system administrator.

**KDSL3204-E**

An attempt to set up the remote option environment has failed.  
An internal error occurred. (error code = [error-code])

JP1/CSC - Manager Remote Option could not be configured because an internal error occurred.

(S)

Cancels the configuration of JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3205-I**

The remote option has started.

JP1/CSC - Manager Remote Option has started.

(S)

Started JP1/CSC - Manager Remote Option.

**KDSL3206-W**

The remote option has terminated.

JP1/CSC - Manager Remote Option has ended.

(S)

Ended JP1/CSC - Manager Remote Option.

**KDSL3207-E**

An attempt to start the remote option has failed. Remote option setup has not been completed. (error code = [error-code])

JP1/CSC - Manager Remote Option could not be started because JP1/CSC - Manager Remote Option was not completely set up.

(S)

Cancels the startup of JP1/CSC - Manager Remote Option.

(O)

Set up JP1/CSC - Manager Remote Option and then start it again. If the problem is not resolved, contact the system administrator.

**KDSL3208-E**

An attempt to start the remote option has failed. The communication environment cannot be initialized. (error code = [error-code])

JP1/CSC - Manager Remote Option could not be started because the port number specified during setup was not available.

(S)

Cancels the startup of JP1/CSC - Manager Remote Option.

(O)

Check whether the port number specified in the Client Security Control - Manager Remote Option Setup dialog box is available. If the port number cannot be used, specify a port number that can be used and reconfigure JP1/CSC - Manager Remote Option.

**KDSL3209-E**

An attempt to start the remote option has failed. An error occurred during a module call to the anti-virus product information acquisition. (error code = [error-code])

JP1/CSC - Manager Remote Option could not be started because an error occurred during a call to the anti-virus product information acquisition module.

(S)

Cancels the startup of JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3210-E**

An attempt to start the remote option has failed. An internal error occurred. (error code = [error-code])

JP1/CSC - Manager Remote Option could not be started because an internal error occurred.

(S)

Cancels the startup of JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3211-E**

An attempt to terminate the remote option has failed. An internal error occurred. (error code = [error-code])

An internal error occurred when JP1/CSC - Manager Remote Option was ending.

(S)

Ends JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3212-I**

The policy update request for the anti-virus product will now start.

JP1/CSC - Manager Remote Option will send a request to update the judgment policy of the anti-virus product.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

**KDSL3213-I**

The policy update request for the anti-virus product will now end.

JP1/CSC - Manager Remote Option has finished sending a request to update the judgment policy of the anti-virus product.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

**KDSL3214-E**

An attempt to connect with the remote service has failed. (error code = [*error-code*])

Failed to establish connection to JP1/CSC - Manager Remote Option.

(S)

Outputs the message and continues the startup processing of JP1/CSC - Manager Remote Option.

(O)

Check whether an error occurred in JP1/CSC - Manager. Check whether the communication between JP1/CSC - Manager and JP1/CSC - Manager Remote Option is normal.

**KDSL3215-E**

An attempt to send a message to the remote service has failed. A communication error occurred. (error code = [*error-code*])

The message could not be sent to JP1/CSC - Manager Remote Option because a communication error occurred.

(S)

Outputs the message and terminates JP1/CSC - Manager Remote Option, or continues processing if JP1/CSC - Manager Remote Option is requesting a policy update of the anti-virus product.

(O)

Check whether an error occurred in JP1/CSC - Manager. Check whether the communication between JP1/CSC - Manager and JP1/CSC - Manager Remote Option is normal.

#### **KDSL3216-E**

An attempt to request a policy update of the anti-virus product has failed. An internal error occurred. (error code = [error-code])

JP1/CSC - Manager Remote Option could not request a policy update of the anti-virus product because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

#### **KDSL3217-E**

Error notification for the remote option has failed. An internal error occurred. (error code = [error-code])

Error notification for JP1/CSC - Manager Remote Option failed because an internal error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

#### **KDSL3218-E**

An internal error occurred with the remote option. (error code = [error-code])

An internal error occurred in JP1/CSC - Manager Remote Option.

(S)

Outputs the message and ends JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3219-I**

The anti-virus product information has not been changed.

There were no changes to the anti-virus product information.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

**KDSL3220-E**

An attempt to request a policy update for the anti-virus product has failed. An attempt to authenticate the IP address of the remote service has failed.

A request to update the judgment policy of the anti-virus product failed because the IP address for JP1/CSC - Manager Remote Option could not be authenticated.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

(O)

Check the IP address of the remote option in the Client Security Control - Manager Setup dialog box.

**KDSL3221-I**

The policy update for the anti-virus product was successful.  
(updated information = [updated-information])

The judgment policy of the anti-virus product was updated successfully.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

**KDSL3222-E**

An attempt to update the policy for the anti-virus product has failed. An error occurred in the remote option. (error code = [error-code])

The policy of the anti-virus product could not be updated because an error occurred in JP1/CSC - Manager Remote Option.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

(O)



Contact the system administrator.

**KDSL3223-E**

An attempt to start the remote option has failed. The anti-virus product is not installed. (anti-virus product name = [anti-virus-product-name])

JP1/CSC - Manager Remote Option could not be started because an anti-virus product is not installed.

(S)

Cancels the startup of JP1/CSC - Manager Remote Option.

(O)

Check whether the anti-virus product specified in the Client Security Control - Manager Remote Option Setup dialog box has been installed.

**KDSL3224-I**

The anti-virus product information has been updated. (renewal date = [renewal-date], updated information = [updated-information])

Information about the anti-virus product was updated.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

**KDSL3225-I**

The anti-virus product information has been sent. (renewal date = [renewal-date], updated information = [updated-information])

Information about the anti-virus product was sent to JP1/CSC - Manager.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

**KDSL3226-E**

A file I/O error occurred in the remote option. (error code = [error-code])

Information about the anti-virus product could not be updated because a file I/O error occurred in JP1/CSC - Manager Remote Option.

(S)

Outputs the message and continues processing of JP1/CSC - Manager Remote Option.

(O)

Check whether the disk has sufficient free space or an error occurred in the file system. If the problem is not resolved, contact the system administrator.

**KDSL3301-I**

The network connection control request was executed.

JP1/CSC - Manager Remote Option has sent a network connection control request.

(S)

Ends the command.

**KDSL3302-E**

An attempt to control the network connection has failed. Command execution permissions are lacking.

JP1/CSC - Manager Remote Option could not control network connections because the user who executed the command was not authorized to do so.

(S)

Ends the command.

(O)

An administrator role user must execute the command.

**KDSL3303-E**

An attempt to control the network connection has failed. The MAC address format is invalid.

JP1/CSC - Manager Remote Option could not control network connections because the specified MAC address was formatted incorrectly.

(S)

Ends the command.

(O)

Check the MAC address format, and then try the command again.

**KDSL3304-E**

An attempt to control the network connection has failed. The IP address format is invalid.

JP1/CSC - Manager Remote Option could not control network connections because the specified IP address was formatted incorrectly.

(S)

Ends the command.

(O)

Check the IP address format, and then try the command again.

**KDSL3305-E**

An attempt to control the network connection has failed. The host name length is invalid.

JP1/CSC - Manager Remote Option could not control network connections because the specified host name is the wrong length.

(S)

Ends the command.

(O)

Check the length of the host name, and then try the command again.

**KDSL3306-E**

An attempt to control the network connection has failed. A file I/O error occurred.

JP1/CSC - Manager Remote Option could not control network connections because an I/O error occurred.

(S)

Ends the command.

(O)

Check whether the disk has sufficient free space or whether an error occurred in the file system. If the problem is not resolved, contact the system administrator.

**KDSL3307-E**

An attempt to control the network connection has failed. Setup has not been completed.

JP1/CSC - Manager Remote Option could not control network connections because JP1/CSC - Manager Remote Option was not completely set up.

(S)

Ends the command.

(O)

Set up JP1/CSC - Manager Remote Option and then try the command again. If the problem is not resolved, contact the system administrator.

**KDSL3308-E**

An attempt to control the network connection has failed. The contents of the network connection control list file are invalid. (line number = [*line-number*])

JP1/CSC - Manager Remote Option could not control network connections because the content of the network connection control list was incorrect.

(S)

Ends the command.

(O)

Check whether the content of the network connection control list is correct.

**KDSL3309-E**

An attempt to control the network connection has failed. A communication error occurred.

JP1/CSC - Manager Remote Option could not control network connections because a communication error occurred.

(S)

Ends the command.

(O)

Check whether an error occurred in JP1/CSC - Manager. Check whether the communication between JP1/CSC - Manager and JP1/CSC - Manager Remote Option is normal.

**KDSL3310-E**

An attempt to control the network connection has failed. An attempt to authenticate the IP address with the manager failed.

JP1/CSC - Manager Remote Option could not control network connections because the IP address of JP1/CSC - Manager could not be authenticated.

(S)

Ends the command.

(O)

Check whether the port number specified in the Client Security Control - Manager Remote Option Setup dialog box is available. If the port number cannot be used, specify a port number that can be used and reconfigure the JP1/CSC - Manager Remote Option environment.

**KDSL3311-E**

An attempt to control the network connection has failed. An error occurred in the manager.

JP1/CSC - Manager Remote Option could not control network connections because an error occurred in JP1/CSC - Manager.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL3312-E**

An attempt to control the network connection has failed. An internal error occurred.

JP1/CSC - Manager Remote Option could not control network connections because an internal error occurred.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL3400-E**

An attempt to start the remote option has failed.

JP1/CSC - Manager Remote Option could not be started.

(S)

Cancels the startup processing of JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3401-E**

An attempt to terminate the remote option has failed.

JP1/CSC - Manager Remote Option could not be shut down.

(S)

Terminates JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

**KDSL3402-E**

An attempt to set up the remote option environment has failed.

JP1/CSC - Manager Remote Option could not be configured.

(S)

Cancels the configuration of JP1/CSC - Manager Remote Option.

(O)

Contact the system administrator.

### 17.3.3 List of JP1/CSC - Agent messages

This subsection lists the messages of JP1/CSC - Agent.

#### **(1) Messages regarding JP1/CSC - Agent (5000 to 5999)**

##### **KDSL5000-I**

Setup of the agent environment was successful.

JP1/CSC - Agent was successfully configured.

(S)

Ends the configuration of JP1/CSC - Agent.

##### **KDSL5001-E**

An attempt to set up the agent environment has failed. Execution permissions are lacking.

JP1/CSC - Agent could not be configured because an unauthorized user attempted the configuration.

(S)

Cancels the configuration of JP1/CSC - Agent.

(O)

Check the user role and reconfigure JP1/CSC - Agent.

##### **KDSL5002-E**

An attempt to set up the agent environment has failed. A file I/O error occurred. (error code = [error-code])

JP1/CSC - Agent could not be configured because a file I/O error occurred.

(S)

Cancels the configuration of JP1/CSC - Agent.

(O)

Check whether the disk has sufficient free space or an error occurred in the file system. If the problem is not resolved, contact the system administrator.

##### **KDSL5003-E**

An attempt to set up the agent environment has failed. An internal error occurred. (error code = [error-code])

JP1/CSC - Agent could not be configured because an internal error occurred.

(S)

Cancels the configuration of JP1/CSC - Agent.

(O)

Contact the system administrator.

**KDSL5100-I**

The agent has started.

JP1/CSC - Agent has started.

(S)

Started JP1/CSC - Agent.

**KDSL5101-W**

The agent has terminated.

JP1/CSC - Agent has ended.

(S)

Ended JP1/CSC - Agent.

**KDSL5102-E**

An attempt to start an agent has failed. Agent setup has not been completed. (error code = [error-code])

JP1/CSC - Agent could not be started because it was not completely set up.

(S)

Cancels the startup processing of JP1/CSC - Agent.

(O)

Complete the setup of JP1/CSC - Agent and then start it again. If the problem is not resolved, contact the system administrator.

**KDSL5103-E**

An attempt to start an agent has failed. The communication environment cannot be initialized. (error code = [error-code])

JP1/CSC - Agent could not be started because the port number specified during setup was not available.

(S)

Cancels the startup processing (JP1/CSC - Agent).

(O)

Check whether the port number specified in the setup window of JP1/CSC - Agent is available. If the port number cannot be used, specify a port number that can be used and reconfigure JP1/CSC - Agent.

**KDSL5104-E**

An attempt to start an agent has failed. An error occurred during a module call to the network control product. (error code = [error-code])

JP1/CSC - Agent could not be started because an error occurred during the call to a module of the network control product.

(S)

Cancels the startup processing of JP1/CSC - Agent.

(O)

Contact the system administrator.

**KDSL5105-E**

An attempt to start an agent has failed. An internal error occurred. (error code = [*error-code*])

JP1/CSC - Agent could not be started because an internal error occurred.

(S)

Cancels the startup processing of JP1/CSC - Agent.

(O)

Contact the system administrator.

**KDSL5106-E**

An attempt to terminate an agent has failed. An internal error occurred. (error code = [*error-code*])

An internal error occurred when JP1/CSC - Agent was ending.

(S)

Ends JP1/CSC - Agent.

(O)

Contact the system administrator.

**KDSL5107-E**

An attempt to connect with a manager has failed. (error code = [*error-code*])

Failed to establish connection to JP1/CSC - Manager.

(S)

Outputs the message and continues the startup processing of JP1/CSC - Agent.

(O)

Check whether an error occurred in JP1/CSC - Manager. Check whether the communication between JP1/CSC - Manager and JP1/CSC - Agent is normal.

**KDSL5108-E**

An attempt to send a message to a manager has failed. A communication error occurred. (error code = [*error-code*])



The message could not be sent to JP1/CSC - Manager because a communication error occurred in JP1/CSC - Agent.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

(O)

Check whether an error occurred in JP1/CSC - Manager. Check whether the communication between JP1/CSC - Manager and JP1/CSC - Agent is normal.

#### **KDSL5109-E**

An attempt to receive a request from a manager has failed. (error code = [error-code])

The request from JP1/CSC - Manager could not be accepted.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

(O)

You do not need to take any action for this message.

#### **KDSL5110-E**

An attempt to start an agent has failed. Software Distribution Manager is either not installed or is an old version. (error code = [error-code])

JP1/CSC - Agent could not be started because JP1/Software Distribution Manager was not installed or the version was old.

(S)

Cancels the startup processing of JP1/CSC - Agent.

(O)

Check whether JP1/ Software Distribution Manager 08-10 or later is installed.

#### **KDSL5200-I**

A network connection refusal request to the network control product will now start.

JP1/CSC - Agent will send a network connection rejection request to the network control product.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

#### **KDSL5201-I**

A network connection refusal request to the network control product has terminated.

JP1/CSC - Agent sent a network connection rejection request to the network control product.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

**KDSL5202-E**

An attempt to request a network connection refusal to the network control product has failed. An error was detected in the network control product. (error code = [*error-code*])

JP1/CSC - Agent could not send a network connection rejection request to the network control product because an error was detected in the network control product.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

(O)

Check whether an error occurred in the network control product.

**KDSL5203-E**

An attempt to request network connection refusal to the network control product has failed. An internal error occurred. (error code = [*error-code*])

JP1/CSC - Agent could not send a network connection rejection request to the network control product because an internal error occurred in JP1/CSC - Agent.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

(O)

Contact the system administrator.

**KDSL5204-I**

A network connection permission request to the network control product will now start.

JP1/CSC - Agent will send a network connection permission request to the network control product.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

**KDSL5205-I**

A network connection permission request to the network control product has terminated.

JP1/CSC - Agent sent a network connection permission request to the network control

product.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

#### **KDSL5206-E**

An attempt to request network connection permission to the network control product has failed. An error was detected in the network control product. (error code = [error-code])

JP1/CSC - Agent could not send a network connection permission request to the network control product because an error was detected in the network control product.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

(O)

Check whether an error occurred in the network control product.

#### **KDSL5207-E**

An attempt to request network connection permission to the network control product has failed. An internal error occurred. (error code = [error-code])

JP1/CSC - Agent could not send a network connection permission request to the network control product because an internal error occurred in JP1/CSC - Agent.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

(O)

Contact the system administrator.

#### **KDSL5208-E**

An attempt to request a network connection refusal to the network control product has failed. A file I/O error occurred. (error code = [error-code])

JP1/CSC - Agent could not send a network connection rejection request to the network control product because a file I/O error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

(O)

Contact the system administrator.

**KDSL5209-E**

An attempt to request network connection permission to the network control product has failed. A file I/O error occurred. (error code = [error-code])

JP1/CSC - Agent could not send a network connection permission request to the network control product because a file I/O error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

(O)

Contact the system administrator.

**KDSL5300-E**

An attempt to start an agent has failed.

JP1/CSC - Agent could not be started.

(S)

Cancels the startup processing of JP1/CSC - Agent.

(O)

Contact the system administrator.

**KDSL5301-E**

An attempt to terminate an agent has failed.

JP1/CSC - Agent could not be shut down.

(S)

Terminates JP1/CSC - Agent.

(O)

Contact the system administrator.

**KDSL5302-E**

An attempt to set up the agent environment has failed.

JP1/CSC - Agent could not be configured.

(S)

Cancels the configuration of JP1/CSC - Agent.

(O)

Contact the system administrator.

**KDSL5303-E**

An attempt to request network connection refusal from the network control product has failed.

JP1/CSC - Agent could not send a network connection rejection request to the network control product.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

(O)

Contact the system administrator.

**KDSL5304-E**

An attempt to request network connection permission from the network control product has failed.

JP1/CSC - Agent could not send a network connection permission request to the network control product.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

(O)

Contact the system administrator.

**(2) Messages regarding quarantine system operation (6000 to 6200)****KDSL6000-E**

An attempt to update the connection control list has failed. A file I/O error occurred. (MAC address = [MAC-address], error code = [error-code])

The connection control list could not be updated because a file I/O error occurred.

(S)

Outputs the message and ends processing of JP1/CSC - Agent.

(O)

Check whether the disk has sufficient free space or whether an error occurred in the file system.

**KDSL6001-E**

An attempt to search the connection control list has failed. A file I/O error occurred. (MAC address = [MAC-address], error code = [error-code])

The connection control list could not be searched because a file I/O error occurred.

(S)

Outputs the message and cancels processing of JP1/CSC - Agent.

(O)

Check whether the disk has sufficient free space or whether an error occurred in the file system.

**KDSL6002-E**

An attempt to search the connection control list has failed. An internal error occurred. (error code = [*error-code*])

The connection control list could not be searched because an internal error occurred in JP1/CSC - Agent.

(S)

Outputs the message and cancels processing of JP1/CSC - Agent.

(O)

Contact the system administrator.

**KDSL6003-I**

There is no MAC address in the connection control list. (MAC address = [*MAC-address*])

The MAC address was not found in the connection control list.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

(O)

Check the MAC address as required, and register it in the list manually.

**KDSL6004-E**

An attempt to update the connection control list has failed. An internal error occurred. (error code = [*error-code*])

The connection control list could not be updated because an internal error occurred in JP1/CSC - Agent.

(S)

Outputs the message and cancels processing of JP1/CSC - Agent.

(O)

Contact the system administrator.

**KDSL6005-I**

The connection control list has been updated.

The connection control list was updated.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

**KDSL6006-E**

An attempt to update the connection control list has failed.

The connection control list could not be updated.

(S)

Outputs the message and cancels processing of JP1/CSC - Agent.

(O)

Contact the system administrator.

**KDSL6030-E**

An attempt to confirm the connection status has failed. A file I/O error occurred. (MAC address = [*MAC-address*], error code = [*error-code*])

The connection status could not be confirmed because a file I/O error occurred.

(S)

Outputs the message and continues processing of JP1/CSC - Agent, connecting the client to the quarantined network or rejecting the network connection according to the JP1/CSC - Agent settings.

(O)

Check whether the disk has sufficient free space or whether an error occurred in the file system.

**KDSL6032-E**

An attempt to confirm the connection status has failed. An internal error occurred. (error code = [*error-code*])

The connection status could not be confirmed because an internal error occurred in JP1/CSC - Agent.

(S)

Outputs the message and continues processing of JP1/CSC - Agent, connecting the client to the quarantined network or rejecting the network connection according to the JP1/CSC - Agent settings.

(O)

Contact the system administrator.

**KDSL6033-W**

An attempt to confirm the connection status has failed. There is no MAC address. (MAC address = [*MAC-address*])

The connection status could not be confirmed because *MAC-address* was not found in

the connection control list.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

**KDSL6034-I**

The authentication request has been received. (MAC address = [MAC-address])

An authentication request for *MAC-address* was received.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

**KDSL6035-E**

The authentication server is not set correctly. The VLAN is not set. (MAC address = [MAC-address])

The VLAN cannot be set because the authentication server has not been set up correctly for use with Microsoft IAS.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

(O)

The attribute that specifies VLAN-related information is missing from the RADIUS protocol. See *13.2.2 Setting up an authentication server*, and review the settings of the authentication server.

**KDSL6036-I**

Connection to the normal network will now be performed. (MAC address = [MAC-address])

*MAC-address* will be connected to the normal network.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

**KDSL6037-I**

Connection to the quarantined network will now be performed. (MAC address = [MAC-address])

*MAC-address* will be connected to the quarantined network.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

**KDSL6038-I**

Connection to the refused network will now be performed. (MAC address = [MAC-address])



*MAC-address* will be rejected for network connection.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

#### **KDSL6042-E**

There is no MAC address in the communication packet.

There is no MAC address in the communication packet.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

#### **KDSL6043-I**

Connection to the unauthenticated network will now be performed.  
(MAC address = [*MAC-address*])

The client with the indicated MAC address will be connected to the unauthenticated network.

(S)

Outputs the message and continues processing of JP1/CSC - Agent.

#### **KDSL6060-E**

An attempt to save the connection history has failed. A file I/O error occurred. (MAC address = [*MAC-address*], connection destination = [Quarantined, Rejected, or Normal])

The connection history for *MAC-address* could not be saved because a file I/O error occurred.

(S)

Outputs the message and continues processing.

(O)

Check whether the disk has sufficient free space or whether an error occurred in the file system.

#### **KDSL6061-E**

An attempt to save the connection history has failed. An internal error occurred. (MAC address = [*MAC-address*], connection destination = [Quarantined, Rejected, or Normal], error code = [*error-code*])

The connection history for *MAC-address* could not be saved because a file I/O error occurred in JP1/CSC - Agent.

(S)

Outputs the message and continues processing, connecting the client to the

quarantined network or denying the network connection according to the JP1/  
CSC - Agent settings.

(O)

Contact the system administrator.

**KDSL6090-E**

The message notification has failed. An internal error occurred.  
(IP address = *[IP-address]*, message = *[message]*, error code =  
*[error-code]*)

Message *message* could not be sent to *IP-address* because of an internal error in JP1/  
CSC - Agent.

(S)

Outputs the message and continues processing.

(O)

Contact the system administrator.

**KDSL6092-E**

The message notification has failed. (command = *[command]*)

The message could not be sent.

(S)

Outputs the message and continues processing.

**KDSL6093-I**

The message notification was successful. (IP address =  
*[IP-address]*, message = *[message]*)

The message *message* was sent to *IP-address*.

(S)

Outputs the message and continues processing.

**KDSL6120-I**

Importing terminated normally.

The connection control list was imported.

(S)

Ends the command.

**KDSL6121-I**

Exporting terminated normally.

The connection control list was exported.

(S)

Ends the command.

**KDSL6122-I**

Deletion of the asset information terminated normally.

The MAC address was deleted from the connection control list.

(S)

Ends the command.

**KDSL6123-E**

An attempt to import has failed. Execution permissions are lacking.

The connection control list could not be imported because the user who executed the command was not authorized to do so.

(S)

Ends the command.

(O)

An administrator role user must execute the command.

**KDSL6124-E**

An attempt to export has failed. Execution permissions are lacking.

The connection control list could not be exported because the user who executed the command was not authorized to do so.

(S)

Ends the command.

(O)

An administrator role user must execute the command.

**KDSL6125-E**

An attempt to delete asset information has failed. Execution permissions are lacking.

The MAC address could not be deleted from the connection control list because the user who executed the command was not authorized to do so.

(S)

Ends the command.

(O)

An administrator role user must execute the command.

**KDSL6126-E**

An attempt to import has failed. A file I/O error occurred.  
(error code = [*error-code*])

The connection control list could not be imported because a file I/O error occurred.

(S)

Ends the command.

(O)

Check whether the import file exists, and then try the command again.

**KDSL6127-E**

An attempt to export has failed. A file I/O error occurred.  
(error code = [*error-code*])

The connection control list could not be exported because a file I/O error occurred.

(S)

Ends the command.

(O)

Check the export file, and then try the command again.

**KDSL6128-E**

An attempt to delete asset information has failed. A file I/O error occurred. (error code = [*error-code*])

The MAC address could not be deleted from the connection control list because a file I/O error occurred.

(S)

Ends the command.

(O)

Check whether the MAC address list file exists, and then try the command again.

**KDSL6129-E**

An attempt to import has failed. The file format is invalid.

The connection control list could not be imported because the import file was formatted incorrectly.

(S)

Ends the command.

(O)

Check the formatting of the import file, and then try the command again.

**KDSL6130-E**

An attempt to export has failed. The file format is invalid.  
The connection control list could not be imported because the export file was formatted incorrectly.

(S)

Ends the command.

(O)

Check the formatting of the export file, and then try the command again.

**KDSL6131-E**

An attempt to delete asset information has failed. The file format is invalid.

The MAC address could not be deleted from the connection control list because the MAC address list file was formatted incorrectly.

(S)

Ends the command.

(O)

Check the formatting of the MAC address list file, and then try the command again.

**KDSL6135-E**

An attempt to import has failed. The agent is running.

The connection control list could not be imported because the command was executed while the JP1/CSC - Agent service was running.

(S)

Ends the command.

(O)

Stop the JP1/CSC - Agent service, and then try the command again.

**KDSL6136-E**

An attempt to delete asset information has failed. The agent is running.

The MAC address could not be deleted from the connection control list because the command was executed while the JP1/CSC - Agent service was running.

(S)

Ends the command.

(O)

Stop the JP1/CSC - Agent service, and then try the command again.

**KDSL6137-E**

An attempt to delete asset information has failed. The Internet Authentication Service or the Network Policy Server is running.

The MAC address could not be deleted from the connection control list because the command was executed while the Microsoft Internet Authentication Service or Network Policy Server service was running.

(S)

Ends the command.

(O)

Stop the Microsoft Internet Authentication Service or Network Policy Server service, and then try the command again.

**KDSL6139-W**

An attempt to delete asset information has failed. The MAC address is not in the connection control list. (MAC address = [MAC-address])

MAC-address could not be deleted because it was not in the connection control list.

(S)

Ends the command.

(O)

Specify a MAC address that is in the connection control list.

**KDSL6140-E**

An attempt to import has failed. An internal error occurred. (error code = [error-code])

The connection control list could not be imported because an internal error occurred in JP1/CSC - Agent.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL6141-E**

An attempt to export has failed. An internal error occurred. (error code = [error-code])

The connection control list could not be exported because an internal error occurred in JP1/CSC - Agent.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL6142-E**

An attempt to delete asset information has failed. An internal error occurred. (error code = [*error-code*])

The MAC address could not be deleted from the connection control list because an internal error occurred in JP1/CSC - Agent.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL6143-E**

An attempt to delete asset information has failed. The MAC address format is invalid. (MAC address = [*MAC-address*])

The specified MAC address was formatted incorrectly and could not be deleted from the connection control list.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL6144-E**

An attempt to export has failed. There is no connection control list.

There is no connection control list to export.

(S)

Outputs the message and cancels processing.

(O)

Create a connection control list, and then try the command again.

**KDSL6145-E**

An attempt to delete asset information has failed. There is no connection control list.

The asset information could not be deleted because there is no connection control list.

(S)

Outputs the message and cancels processing.

(O)

Create a connection control list, and then try the command again.

**KDSL6146-E**

An attempt to import has failed.

The connection control list could not be imported.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL6147-E**

An attempt to export has failed.

The connection control list could not be exported.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL6148-E**

An attempt to delete asset information has failed.

The asset information could not be deleted from the connection control list.

(S)

Ends the command.

(O)

Contact the system administrator.

**KDSL6150-E**

Initialization has failed. A file I/O error occurred. (error code = [*error-code*])

JP1/CSC - Agent could not be initialized because a file I/O error occurred.

(S)

Outputs the message and cancels processing.

(O)



Contact the system administrator.

**KDSL6151-E**

Initialization has failed. An internal error occurred. (error code = [*error-code*])

JP1/CSC - Agent could not be initialized because an internal error occurred.

(S)

Outputs the message and cancels processing.

(O)

Contact the system administrator.

**KDSL6152-E**

Setup has not been completed.

JP1/CSC - Agent was not completely set up.

(S)

Outputs the message and cancels processing.

(O)

Set up JP1/CSC - Agent.

**KDSL6180-I**

*date, MAC-address, IP-address, connection-destination, VLAN-ID*

A connection history message appears.


(S)

Outputs the message and continues processing.

## 17.4 List of messages in the Client Security Management window

This section explains how the user must respond to the messages output to the Client Security Management window of AIM.

On the message dialog boxes, message levels are indicated using icons:

- Danger: 
- Warning: 
- Information: 

### 17.4.1 Action messages in the PC List window

When you perform one of the following operations in the PC List window, an action message appears:

- To judge the security level  
Click the **Judge** button.
- To send a warning message  
Click the **Message** button.
- To permit network connection  
Click the **Permit** button.
- To reject network connection  
Click the **Refuse** button.
- To enable security management  
Click the **Valid** button.
- To disable security management  
Click the **Invalid** button.
- To output the judgment and action history to a CSV file  
Click the **History CSV** button.

The following tables list the action messages that may be displayed when you perform one of the above operations in the PC List window.

**(1) To judge the security level**

The following table lists the action messages that may be displayed when you click the **Judge** button to judge the security level:

*Table 17-5: Action messages that may be displayed when you judge the security level*

No.	Message	Message level	Action to be taken
1	Judgment of the security level for the specified PC was executed.	Information	No action is required.
2	An attempt to judge the security level failed because Client Security Control - Manager has not started.	Danger	Start JP1/CSC - Manager and re-execute the operation.
3	An attempt to judge the security level failed because an error occurred with Client Security Control - Manager.	Danger	Contact the system administrator.

**(2) To send a warning message**

When you click the **Message** button, the Warning Notification window appears. The following table lists the action messages that may be displayed when you click the **Notify** button in the Warning Notification window to send a warning message to a client user:

*Table 17-6: Action messages that may be displayed when you send a warning message*

No.	Message	Message level	Action to be taken
1	A warning message was sent to the specified PC.	Information	No action is required.
2	An attempt to send a warning message failed because Client Security Control - Manager has not started.	Danger	Start JP1/CSC - Manager and re-execute the operation.
3	An attempt to send a warning message failed because an error occurred with Client Security Control - Manager.	Danger	Contact the system administrator.

**(3) To permit a network connection**

The following table lists the action messages that may be displayed when you click the **Permit** button to permit a client to connect to the network:

*Table 17-7:* Action messages that may be displayed when you permit a network connection

No.	Message	Message level	Action to be taken
1	Network connection permission was performed for the specified PC.	Information	No action is required.
2	An attempt to permit a network connection failed because Client Security Control - Manager has not started.	Danger	Start JP1/CSC - Manager and re-execute the operation.
3	An attempt to permit a network connection failed because an error occurred with Client Security Control - Manager.	Danger	Contact the system administrator.

**(4) To reject a network connection**

The following table lists the action messages that may be displayed when you click the **Refuse** button to reject a client permission to connect to the network:

*Table 17-8:* Action messages that may be displayed when you reject a network connection

No.	Message	Message level	Action to be taken
1	Network connection refusal was performed for the specified PC.	Information	No action is required.
2	An attempt to refuse a network connection failed because Client Security Control - Manager has not started.	Danger	Start JP1/CSC - Manager and re-execute the operation.
3	An attempt to refuse a network connection failed because an error occurred with Client Security Control - Manager.	Danger	Contact the system administrator.

**(5) To enable security management**

The following table lists the action messages that may be displayed when you click the **Valid** button to enable the security management for a client:

*Table 17-9:* Action messages that may be displayed when you enable security management

No.	Message	Message level	Action to be taken
1	Security management of the specified PC has been enabled.	Information	No action is required.
2	An attempt to enable security management failed because Client Security Control - Manager has not started.	Danger	Start JP1/CSC - Manager and re-execute the operation.
3	An attempt to enable security management failed because a database access error occurred with Client Security Control - Manager.	Danger	Start the AIM database and re-execute the operation.
4	An attempt to enable security management failed because an error occurred with Client Security Control - Manager.	Danger	Contact the system administrator.

**(6) To disable security management**

The following table lists the action messages that may be displayed when you click the **Invalid** button to disable the security management for a client:

*Table 17-10:* Action messages that may be displayed when you disable security management

No.	Message	Message level	Action to be taken
1	Security management of the specified PC has been disabled.	Information	No action is required.
2	An attempt to disable security management failed because Client Security Control - Manager has not started.	Danger	Start JP1/CSC - Manager and re-execute the operation.

No.	Message	Message level	Action to be taken
3	An attempt to disable security management failed because a database access error occurred with Client Security Control - Manager.	Danger	Start the AIM database and re-execute the operation.
4	An attempt to disable security management failed because an error occurred with Client Security Control - Manager.	Danger	Contact the system administrator.

**(7) To output the judgment and action history to a CSV file**

The following table lists the action messages that may be displayed when you click the **History CSV** button to output the judgment and action history to a CSV file:

*Table 17-11:* Action messages that may be displayed when you output the judgment and action history to a CSV file

No.	Message	Message level	Action to be taken
1	The judgment and action history of the specified PC has been output as a CSV file.	Information	No action is required.
2	An attempt to obtain the judgment and action history of the specified PC has failed.	Danger	Contact the system administrator.

## 17.4.2 Error messages in the PC Security Level Details window

This subsection describes the error messages that may be displayed in the PC Security Level Details window.

**(1) Error messages in the PC Security Level Details window**

The following table lists the error messages that may be displayed in the PC Security Level Details window when you click an asset number anchor on the PC List window:

*Table 17-12:* Error messages that may be displayed in the PC Security Level Details window

No.	Message	Message level	Action to be taken
1	An attempt to obtain asset information for the specified PC has failed.	Warning	Check whether the specified asset is deleted. If the asset is not deleted, contact the system administrator.
2	An attempt to obtain security information for the specified PC has failed.	Danger	Contact the system administrator.

**(2) Error messages in the Security Updates Details window**

The following table lists the error messages that may be displayed in the Security Updates Details window:

*Table 17-13:* Error messages that may be displayed in the Security Updates Details window

No.	Message	Message level	Action to be taken
1	An attempt to obtain asset information for the specified PC has failed.	Warning	Check whether the specified asset is deleted. If the asset is not deleted, contact the system administrator.
2	An attempt to obtain security information for the specified PC has failed.	Danger	Contact the system administrator.
3	An attempt to obtain security update information failed because Client Security Control - Manager has not started.	Danger	Start JP1/CSC - Manager and re-execute the operation.
4	An attempt to obtain security update information failed because a database access error occurred with Client Security Control - Manager.	Danger	Start the AIM database and re-execute the operation.
5	An attempt to obtain security update information failed because an error occurred with Client Security Control - Manager.	Danger	Contact the system administrator.

**(3) Error messages in the Anti-Virus Products Details window**

The following table lists the error messages that may be displayed in the Anti-Virus Products Details window:

*Table 17-14:* Error messages that may be displayed in the Anti-Virus Products Details window

No.	Message	Message level	Action to be taken
1	An attempt to obtain asset information for the specified PC has failed.	Warning	Check whether the specified asset is deleted. If the asset is not deleted, contact the system administrator.
2	An attempt to obtain security information for the specified PC has failed.	Danger	Contact the system administrator.
3	An attempt to obtain anti-virus product information failed because Client Security Control - Manager has not started.	Danger	Start JP1/CSC - Manager and re-execute the operation.
4	An attempt to obtain anti-virus product information failed because a database access error occurred with Client Security Control - Manager.	Danger	Start the AIM database and re-execute the operation.
5	An attempt to obtain anti-virus product information failed because an error occurred with Client Security Control - Manager.	Danger	Contact the system administrator.

**(4) Error messages in the Prohibited Software Details window**

The following table lists the error messages that may be displayed in the Prohibited Software Details window:

*Table 17-15:* Error messages that may be displayed in the Prohibited Software Details window

No.	Message	Message level	Action to be taken
1	An attempt to obtain asset information for the specified PC has failed.	Warning	Check whether the specified asset is deleted. If the asset is not deleted, contact the system administrator.



No.	Message	Message level	Action to be taken
2	An attempt to obtain security information for the specified PC has failed.	Danger	Contact the system administrator.
3	An attempt to obtain prohibited software information failed because Client Security Control - Manager has not started.	Danger	Start JP1/CSC - Manager and re-execute the operation.
4	An attempt to obtain prohibited software information failed because a database access error occurred with Client Security Control - Manager.	Danger	Start the AIM database and re-execute the operation.
5	An attempt to obtain prohibited software information failed because an error occurred with Client Security Control - Manager.	Danger	Contact the system administrator.

**(5) Error messages in the Mandatory Software Details window**

The following table lists the error messages that may be displayed in the Mandatory Software Details window:

*Table 17-16:* Error messages that may be displayed in the Mandatory Software Details window

No.	Message	Message level	Action to be taken
1	An attempt to obtain asset information for the specified PC has failed.	Warning	Check whether the specified asset is deleted. If the asset is not deleted, contact the system administrator.
2	An attempt to obtain security information for the specified PC has failed.	Danger	Contact the system administrator.
3	An attempt to obtain mandatory software information failed because Client Security Control - Manager has not started.	Danger	Start JP1/CSC - Manager and re-execute the operation.

No.	Message	Message level	Action to be taken
4	An attempt to obtain mandatory software information failed because a database access error occurred with Client Security Control - Manager.	Danger	Start the AIM database and re-execute the operation.
5	An attempt to obtain mandatory software information failed because an error occurred with Client Security Control - Manager.	Danger	Contact the system administrator.

**(6) Error messages in the User Definition Details window**

The following table lists the error messages that may be displayed in the User Definition Details window.

*Table 17-17:* Error messages that may be displayed in the User Definition Details window

No.	Message	Message level	Action to be taken
1	An attempt to obtain asset information for the specified PC has failed.	Warning	Check whether the specified asset is deleted. If the asset is not deleted, contact the system administrator.
2	An attempt to obtain security information for the specified PC has failed.	Danger	Contact the system administrator.
3	An attempt to obtain user definition information failed because Client Security Control - Manager has not started.	Danger	Start JP1/CSC - Manager and re-execute the operation.
4	An attempt to obtain user definition information failed because a database access error occurred with Client Security Control - Manager.	Danger	Start the AIM database and re-execute the operation.

No.	Message	Message level	Action to be taken
5	An attempt to obtain user definition information failed because an error occurred with Client Security Control - Manager.	Danger	Contact the system administrator.

**(7) Error messages in the PC Security Settings Details window**

The following table lists the error messages that may be displayed in the PC Security Settings Details window:

*Table 17-18:* Error messages that may be displayed in the PC Security Settings Details window

No.	Message	Message level	Action to be taken
1	An attempt to obtain asset information for the specified PC has failed.	Warning	Check whether the specified asset has been deleted. If the asset has not been deleted, contact the system administrator.
2	An attempt to obtain security information for the specified PC has failed.	Danger	Contact the system administrator.
3	An attempt to obtain PC security settings information failed because Client Security Control - Manager has not started.	Danger	Start JP1/CSC - Manager and re-execute the operation.
4	An attempt to obtain PC security settings information failed because a database access error occurred with Client Security Control - Manager.	Danger	Start the AIM database and re-execute the operation.
5	An attempt to obtain PC security settings information failed because an error occurred with Client Security Control - Manager.	Danger	Contact the system administrator.

**(8) Error messages in the Judgment and Action History window**

The following table lists the error messages that may be displayed in the Judgment and Action History window:

*Table 17-19: Error messages that might be displayed in the Judgment and Action History window*

No.	Message	Message level	Action to be taken
1	An attempt to obtain asset information for the specified PC has failed.	Warning	Check whether the specified asset is deleted. If the asset is not deleted, contact the system administrator.
2	An attempt to obtain the judgment and action history for the specified PC has failed.	Danger	Contact the system administrator.

**17.4.3 Messages in the Register Permitted PCs window**

The following table lists the messages that may be displayed in the Register Permitted PCs window:

*Table 17-20: Messages that may be displayed in the Register Permitted PCs window*

No.	Message	Message level	Action to be taken
1	Network connection permission was performed for the specified PC.	Information	No action is required.
2	An attempt to permit a network connection failed because the MAC address was invalid.	Warning	Check the format of the file containing the list of permitted PCs and re-execute the operation.
3	A MAC address does not exist in the permitted-PC list file.	Warning	Check the path for the file containing the list of permitted PCs and the format of the file, and re-execute the operation.
4	An attempt to permit a network connection failed because Client Security Control - Manager has not started.	Danger	Start JP1/CSC - Manager and re-execute the operation.

No.	Message	Message level	Action to be taken
5	An attempt to permit a network connection failed because an error occurred with Client Security Control - Manager.	Danger	Contact the system administrator.

#### 17.4.4 Error message in the Evaluation Result List window

The following table shows the error message that may be displayed in the Evaluation Result List window.

*Table 17-21:* Error message that may be displayed in the Evaluation Result List window

No.	Message	Message level	Action to be taken.
1	An attempt to obtain an evaluation result for security countermeasures has failed.	Danger	Contact the system administrator.

#### 17.4.5 Error message in the Statistics List window

The following table shows the error message that may be displayed in the Statistics List window.

*Table 17-22:* Error message that may be displayed in the Statistics List window

No.	Message	Message level	Action to be taken
1	An attempt to obtain statistics has failed.	Danger	Contact the system administrator.

#### 17.4.6 Error message in the Statistics Graph Display window

The following table shows the error message that may be displayed in the Statistics Graph Display window.

*Table 17-23:* Error message that may be displayed in the Statistics Graph Display window

No.	Message	Message level	Action to be taken
1	A graph cannot be drawn in this environment.	Warning	Install Office Web Component on the management terminal.

### 17.4.7 Error message in the Statistics Details window

The following table shows the error message that may be displayed in the Statistics Details window.

*Table 17-24:* Error message that may be displayed in the Statistics Details window

No.	Message	Message level	Action to be taken
1	An attempt to obtain statistics details has failed.	Danger	Contact the system administrator.

### 17.4.8 Error message in the Statistics Details Graph Display window

The following table shows the error message that may be displayed in the Statistics Details Graph Display window.

*Table 17-25:* Error message that may be displayed in the Statistics Details Graph Display window

No.	Message	Message level	Action to be taken
1	A graph cannot be drawn in this environment.	Warning	Install Office Web Component on the management terminal.

## Chapter

---

# 18. Troubleshooting

---

This chapter describes the actions to be taken if a problem occurs during the operation of the client security control system.

- 18.1 Troubleshooting procedure
- 18.2 Data that must be collected if a problem occurs
- 18.3 Common problems and their solutions
- 18.4 Backup and restoration

---

## 18.1 Troubleshooting procedure

---

This section describes the procedure for resolving a problem that might occur in the client security control system.

To resolve a problem that occurs in the client security control system:

1. Check the error message.

If an error message appears while you are using the Client Security Management window or the Policy Management window:

Check the error message displayed in the window.

If an error occurs while you are entering a command or after you enter a command:

Check the standard output message.

Other cases:

If JP1/CSC has sent a JP1 event notification to JP1/IM, check whether an error message from JP1/CSC was output to JP1/IM.

In addition, check whether an error message was output to the log files created by JP1/CSC - Manager and JP1/CSC - Agent.

2. Determine the cause of the problem and check the action to be taken. Take the specified action.

For details about how to read the error messages displayed in a processing results window, the causes of problems, and the actions to be taken, see *17. Messages*.

For details about the causes of the error messages that are output while you are entering a command or after you enter a command, and the actions to be taken, see the description of the standard output message for the applicable command in *15. Commands*.

3. If the problem is not resolved or if an internal error or a communication error occurs, collect the required data and take the appropriate action.

For details about how to collect data, see *18.2 Data that must be collected if a problem occurs*.



## 18.2 Data that must be collected if a problem occurs

This section describes the troubleshooting data you must collect if a problem occurs in the client security control system.

If an internal error or a communication error occurs in the client security control system or if the problem is not resolved even after you perform an appropriate action, collect the following troubleshooting data and let the administrator handle the problem. If the administrator cannot resolve the problem, the administrator must contact the person in charge at Hitachi or a Hitachi sales representative and ask for assistance.

### 18.2.1 Data for resolving problems in JP1/CSC - Manager

The following table lists the data to be collected for resolving problems in JP1/CSC - Manager and how to collect the data:

*Table 18-1: Data for resolving problems in JP1/CSC - Manager*

Data for resolving problems	How to collect
Logs	Copy the files in the following folder: <i>JP1/CSC - Manager-installation-folder\log</i>
Trace information file	Copy the files in the following folder: <i>JP1/CSC - Manager-installation-folder\trace</i>
Internal management information	Copy the files in the following folders: <ul style="list-style-type: none"> <li><i>JP1/CSC - Manager-installation-folder\dat</i></li> <li><i>JP1/CSC - Manager-installation-folder\spool</i></li> <li><i>JP1/CSC - Manager-installation-folder\db</i></li> </ul>
Definition information	Copy the files in the following folder: <i>JP1/CSC - Manager-installation-folder\conf</i>

### 18.2.2 Data for resolving problems in JP1/CSC - Manager Remote Option

The following table lists the data to be collected for resolving problems in JP1/CSC - Manager Remote Option and how to collect the data:

*Table 18-2: Data for resolving problems in JP1/CSC - Manager Remote Option*

Data for resolving problems	How to collect
Logs	Copy the files in the following folder: <i>JP1/CSC - Manager-Remote-Option-installation-folder\log</i>
Trace information file	Copy the files in the following folder: <i>JP1/CSC - Manager-Remote-Option-installation-folder\trace</i>
Definition information	Copy the files in the following folder: <i>JP1/CSC - Manager-Remote-Option-installation-folder\conf</i>

### 18.2.3 Data for resolving problems in JP1/CSC - Agent

The following table lists the data to be collected for resolving problems in JP1/CSC - Agent and how to collect the data:

*Table 18-3: Data for resolving problems in JP1/CSC - Agent*

Data for resolving problems	How to collect
Logs	Copy the files in the following folder: <i>JP1/CSC - Agent-installation-folder\log</i>
Trace information file	Copy the files in the following folder: <i>JP1/CSC - Agent-installation-folder\trace</i>
Definition information	Copy the files in the following folder: <ul style="list-style-type: none"> <li><i>JP1/CSC - Agent-installation-folder\conf</i></li> <li><i>JP1/CSC - Agent-installation-folder\radius\conf</i></li> </ul>

### 18.2.4 Data for resolving problems in JP1/Software Distribution and AIM

If a problem occurs in the client security control system, you must also collect troubleshooting data in JP1/Software Distribution and AIM.

- For the data that needs to be collected in JP1/Software Distribution and Asset Information Manager Subset Component of JP1/Software Distribution Manager, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 2*, for Windows systems.
- For the data that needs to be collected in Asset Information Manager, see the manual *Job Management Partner 1/Asset Information Manager Administrator's*

*Guide.*

## 18.3 Common problems and their solutions

This section describes the leading causes of problems in the client security control system, and how to resolve them.

The following table lists the leading causes and solutions for problems that occur in the client security control system.

*Table 18-4:* Causes and solutions for problems in the client security control system

Problem	Cause	Solution
When judging the security level of a client, the security level is judged as Unknown for all judgment items.	Software inventory information has not been collected from JP1/Software Distribution Client.	<p>Use one of the following methods to provide software inventory information about JP1/Software Distribution Client:</p> <ul style="list-style-type: none"> <li>• Provide inventory information from the client In the client setup window of JP1/Software Distribution, on the <b>System Conditions</b> page, select the <b>When the system is changed, inventory information is notified to Higher System</b> check box.<sup>#1</sup></li> <li>• Provide inventory information from the manager In JP1/Software Distribution Manager, execute the <b>Get software information from client</b> job with <b>Search all software</b> specified.<sup>#2</sup></li> </ul>
JP1/CSC - Manager setup fails, and the following message is output to the log file: KDSL1001-E An attempt to create client security management information has failed	The AIM database (Embedded RDB <sup>#3</sup> ) has insufficient capacity.	Create an AIM database that has a capacity of at least 101 MB. <sup>#4</sup>

Problem	Cause	Solution
The number of assets in the Device List of AIM does not match the number of assets displayed when <b>PC Security Level Management</b> is selected.	There are two potential causes: <ul style="list-style-type: none"> <li>• Inventory was taken by executing a task.</li> <li>• The Asset Information Synchronous Service service was started while the JP1/CSC - Manager service was stopped.</li> </ul>	Execute the <code>cscsetup</code> command. <sup>#5</sup>

#1

For details about the client setup windows for JP1/Software Distribution, see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows Systems.

Note that this solution requires JP1/Software Distribution Client to be upgraded after the settings have been changed. If you do not want to upgrade JP1/Software Distribution Client, take action as described in *Provide inventory information from the manager*.

#2

For details about the *Get software information from client* job, see the manual *Job Management Partner 1/Software Distribution Administrator's Guide Volume 1*, for Windows Systems.

#3

The Embedded RDB is an embedded relational database provided by Asset Information Manager.

#4

For details about the AIM database, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

#5

For details about the `cscsetup` command, see *cscsetup (sets up JP1/CSC - Manager)* in 15. *Commands*.

## 18.4 Backup and restoration

If the system stops operating due to failures such as a disk failure, the data used in JP1/CSC may be lost. To prepare for such unexpected situations, you must periodically back up some files.

The following table lists the files that must be backed up:

*Table 18-5: Files that must be backed up*

Product	Type	Folder name
JP1/CSC - Manager <sup>#</sup>	Definition information	<i>JP1/CSC - Manager-installation-folder\conf</i>
	Internal management information	<i>JP1/CSC - Manager-installation-folder\dat</i>
		<i>JP1/CSC - Manager-installation-folder\db</i>
		<i>JP1/CSC - Manager-installation-folder\spool</i>
	Audit log information	<i>JP1/CSC - Manager-installation-folder\log</i>
JP1/CSC - Manager Remote Option	Definition information	<i>JP1/CSC - Manager-Remote-Option-installation-folder\conf</i>
	Audit log information	<i>JP1/CSC - Manager-Remote-Option-installation-folder\log</i>
JP1/CSC - Agent <sup>#</sup>	Definition information	<i>JP1/CSC - Agent-installation-folder\conf</i>
		<i>JP1/CSC - Agent-installation-folder\radius\conf</i>
	Internal management information	<i>JP1/CSC - Agent-installation-folder\radius\dat</i>
	Audit log information	<i>JP1/CSC - Agent-installation-folder\log</i>

#

If a cluster system is used, *JP1/CSC - Manager-installation-folder* is the shared disk specified during setup of JP1/CSC - Manager, and *JP1/CSC - Agent-installation-folder* is the shared disk path specified during setup of JP1/CSC - Agent.

If a problem occurs, restore the backup files to their original folder.

JP1/CSC uses the asset management database of AIM. For details about how to back

up the database, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.





---

# Appendixes

---

- A. List of Files
- B. List of Port Numbers
- C. List of Processes
- D. Operation on a Cluster System
- E. Estimating Required Disk Capacity
- F. Audit Log Output
- G. Version Changes
- H. Glossary

## A. List of Files

This appendix lists by program the files used for JP1/CSC.

### A.1 List of files for JP1/CSC - Manager

The following table lists the files used for JP1/CSC - Manager.

*Table A-1: List of files for JP1/CSC - Manager*

File contents	Folder name	File name
Manager log file	<i>JP1/CSC - Manager-installation-folder\log</i>	<i>cscmlogn.log<sup>#</sup></i>

#

*n* indicates the log file number from 1 to 999. **Number of log files** can be specified during JP1/CSC - Manager setup, and is 10 by default. For details about how to specify **Number of log files**, see 5.4.3 *Setting up JP1/CSC - Manager*.

### A.2 List of files for JP1/CSC - Manager Remote Option

The following table lists the files used for JP1/CSC - Manager Remote Option.

*Table A-2: List of files for JP1/CSC - Manager Remote Option*

File contents	Folder name	File name
Remote Option log file	<i>JP1/CSC - Manager-Remote-Option-installation-folder\log</i>	<i>cscmrlogn.log<sup>#</sup></i>

#

*n* indicates the log file number from 1 to 999. **Number of log files** can be specified during JP1/CSC - Manager Remote Option setup, and is 10 by default. For details about how to specify **Number of log files**, see 5.5.3 *Setting up JP1/CSC - Manager Remote Option*.

### A.3 List of files for JP1/CSC - Agent

The following table lists the files used for JP1/CSC - Agent.

*Table A-3: List of files for JP1/CSC - Agent*

File contents	Folder name	File name
Agent log file	<i>JP1/CSC - Agent-installation-folder\log</i>	<i>cscalogn.log<sup>#</sup></i>

#

*n* indicates the log file number from 1 to 999. **Number of log files** can be specified during JP1/CSC - Agent setup, and is 10 by default. For details about how to specify **Number of log files**, see the description of JP1/CSC - Agent setup in 13. *Setting Up a Quarantine System*.

## A.4 List of sample definition files

The client security control system provides samples of definition files.

The following table lists the types of sample files and their import destinations or associated command arguments.

*Table A-4:* Types of sample files and their import destinations or associated command arguments

No.	Type of sample file	File name	Judgment item or registered data	Import destination
1	Definition file for excluded security updates	ExUpPgm_sample.csv	<b>Security updates</b>	Definition of Excluded Security Updates dialog box
2	Definition file for mandatory security updates	NeedUpPgm_sample.csv	<b>Security updates</b>	<b>Patch</b> page of the Definition of Mandatory Security Updates dialog box
3	Definition file for mandatory service packs	NeedUpSP_sample.csv	<b>Security updates</b>	<b>Service Pack</b> page of the Definition of Mandatory Security Updates dialog box
4	Anti-virus product definition file	VirusMeasure_sample.csv	<b>Anti-virus products</b>	Edit Judgment Policy (Anti-virus Product) window
5	Prohibited software definition file	UnjustSoft_sample.csv	<b>Prohibited software</b>	Edit Judgment Policy (Prohibited Software) window
6	Mandatory software definition file	NeedSoft_sample.csv	<b>Mandatory software</b>	Edit Judgment Policy (Mandatory Software) window
7	User definition file	UserDefJudge_sample.csv	<b>User definition</b>	Edit Judgment Policy (User Definition) window

No.	Type of sample file	File name	Judgment item or registered data	Import destination
8	Mail address definition file	MailAddress_sample.csv	Email address to be notified	Settings for Email Address dialog box
9	Patch update condition file	cscpatchcond_sample.txt	Conditions for updating patch information	The -f option of the judgment policy update command for security updates (cscpatchupdate)
10	Excluded user definition file	cscm_excluder.conf_sample.txt	User accounts to be excluded	None

*Note:*

Sample definition files must be customized based on the security objectives before they are imported.

The sample files are stored in the following location:

*JPI/CSC - Manager-installation-folder\sample*

**(1) Sample of a definition file for excluded security updates**

The following shows a sample of a definition file for excluded security updates:

```
"ExpUpProgram", "01-001", "111111" . . . (a)
"ExpUpProgram", "02-002", "222222" . . . (b)
```

**Legend:**

(a): Example when the update number MS01-001 is set

(b): Example when the update number MS02-002 is set

The sample contains the following settings.

No.	Item	Set value for (a)	Set value for (b)
1	Parameter ID	ExpUpProgram	
2	Update number	MS01-001	MS02-002

No.	Item	Set value for (a)	Set value for (b)
3	Article ID number	KB111111	KB222222

For details about the definition file for excluded security updates, see *16.2.3 Definition file of excluded security updates*.

## (2) Sample of a definition file for mandatory security updates

The following shows a sample of a definition file for mandatory security updates.

```
"NeedUpProgram", "01-001", "111111", "0000", "0", "0", "", "0", "200", "", "" . . . (a)
"NeedUpProgram", "02-002", "222222", "0019", "1", "0", "", "0", "300", "", "" . . . (b)
"NeedUpProgram", "03-003", "333333", "0017", "1", "1", "6.0", "1", "400", "", "" . . . (c)
"NeedUpProgram", "04-004", "444444", "0017", "1", "99", "1.0.0", "0", "400", "SoftwareA", "1" . . . (d)
```

Legend:

(a): Example when **OS for mandatory security updates** is set to **All OSs**

(b): Example when **OS for mandatory security updates** is not set to **All OSs**

(c): Example when **Product name for mandatory security updates** is set to **Microsoft Internet Explorer**

(d): Example when **Product name for mandatory security updates** is set to any other product

The sample contains the following settings.

No.	Item	Set value for (a)	Set value for (b)	Set value for (c)	Set value for (d)
1	Parameter ID	NeedUpProgram			
2	Update number	MS01-001	MS02-002	MS03-003	MS04-004
3	Article ID number	KB111111	KB222222	KB333333	KB444444
4	OS for mandatory security updates	All OSs	Windows Server 2003 (32bit)	Windows Server 2003, Enterprise Edition	Windows Server 2003, Enterprise Edition

No.	Item	Set value for (a)	Set value for (b)	Set value for (c)	Set value for (d)
5	OS service pack for mandatory security updates	No specification	Service Pack 1	Service Pack 1	Service Pack 1
6	Product name for mandatory security updates	No specification	No specification	Microsoft Internet Explorer	Other products
7	Product version for mandatory security updates	No specification	No specification	6.0	1.0.0
8	Product service pack for mandatory security updates	No specification	No specification	Service Pack 1	No specification
9	Security level	Caution	Warning	Danger	Danger
10	Product name for mandatory security updates	(Not applicable)	(Not applicable)	(Not applicable)	SoftwareA
11	Comparison condition	(Not applicable)	(Not applicable)	(Not applicable)	Match all the words

For details about the definition file for mandatory security updates, see *16.2.4 Definition file for mandatory security updates*.

### (3) Sample of a definition file for mandatory service packs

The following shows a sample of a definition file for mandatory service packs.

```
"NeedUpServicePackOS", "0017", "1", "0", "300"      . . . (a)
"NeedUpServicePackProduct", "1", "6.0", "1", "1", "0000", "0", "300" . . . (b)
```

Legend:

(a): Example when an OS service pack is defined

(b): Example when a product service pack is defined

The sample contains the following settings.

(a): Example when an OS service pack is defined

No.	Item	Value set for (a)
1	Parameter ID	NeedUpServicePackOS
2	OS	Windows Server 2003
3	OS service pack	Service Pack 1
4	OS service pack condition	Include only service packs that match <b>OS service pack</b> .
5	Security level	Warning

(b): Example when a product service pack is defined

No.	Item	Value set for (b)
1	Parameter ID	NeedUpServicePackProduct
2	Product name	Microsoft Internet Explorer
3	Product version	6.0
4	Product service pack	Service Pack 1
5	Product service pack condition	Include all service packs other than <b>Product service pack</b> .
6	OS	All OSs
7	OS service pack	No specification
8	Security level	Warning

For details about the definition file for mandatory service packs, see *16.2.5 Definition file for mandatory service packs*.

#### (4) **Sample of an anti-virus product definition file**

The following shows a sample of an anti-virus product definition file.

```
"VirusProduct","Virus Software1","","","","0","400"      . . . (a)
"VirusProduct","Virus Software2","9.0.3.1000","61.2.1.10","20060918.018","1","400" . . . (b)
```

Legend:

(a): Example when only whether the anti-virus product has been installed is judged

(b): Example when all items are judged

The sample contains the following settings.

No.	Item	Value set for (a)	Value set for (b)
1	Parameter ID	VirusProduct	
2	Anti-virus product name	Virus Software1	Virus Software2
3	Product version	No specification	9.0.3.1000
4	Engine version	No specification	61.2.1.10
5	Virus definition file version	No specification	20060918.018
6	Determine that PCs with no resident anti-virus products are at risk	Do not judge residency.	Judge residency.
7	Security level	Danger	Danger

For details about the anti-virus product definition file, see *16.2.6 Anti-virus products definition file*.

#### (5) Sample of a prohibited software definition file

The following shows a sample of a prohibited software definition file.

```
"UnjustSoftware","Software","","0000","200"      . . . (a)
"UnjustSoftware","SoftwareA","2.0.0","0000","400","1" . . . (b)
```

Legend:

(a): Example when a comparison condition is omitted

(b): Example when a comparison condition is set



The sample contains the following settings.

No.	Item	Value set for (a)	Value set for (b)
1	Parameter ID	UnjustSoftware	
2	Software name	Software	SoftwareA
3	Version	No specification	2.0.0
4	OS	All OSs	All OSs
5	Security level	Caution	Danger
6	Comparison condition	Match part of the words <sup>#</sup>	Match all the words

#

*Match part of the words* is assumed because no comparison condition has been specified.

For details about the prohibited software definition file, see *16.2.7 Prohibited software definition file*.

#### (6) Sample of a mandatory software definition file

The following shows a sample of a mandatory software definition file.

```
"NeedSoftware", ""SoftwareA"", ""0000", "200", "SoftwareA" . . . (a)
"NeedSoftware", ""SoftwareA"", ""SoftwareB"", ""0670", "0700"", ""0000", "200", "Software" (b)
```

Legend:

(a): Example when one software product is set in one group

(b): Example when multiple software products are set in one group

The sample contains the following settings.

No.	Item	Value set for (a)	Value set for (b)	
1	Parameter ID	NeedSoftware		
2	Software name	SoftwareA	SoftwareA	SoftwareB
3	Version	No specification	0670	0700
4	OS	All OSs	All OSs	
5	Security level	Caution	Caution	

No.	Item	Value set for (a)	Value set for (b)
6	Group name	SoftwareA	Software

For details about the mandatory software definition file, see *16.2.8 Mandatory software definition file*.

### (7) Sample of a user definition file

The following shows a sample of a user definition file.

```
"UserDefJudge","Power-saving CPU","""Hardware asset information""","""Hardware asset
information""","""CPU""","CPU""","""8""","8""","""28694""","28695""","""4""","4""","200"
```

The sample contains the following settings.

No.	Item	Set value	
1	Parameter ID	UserDefJudge	
2	Judgment item name	Power-saving CPU	
3	Class	Hardware information	Hardware information
4	Property	CPU	CPU
5	Comparison condition	Do not match.	Do not match.
6	Comparison value	28694	28695
7	Treatment when value is not set for property	Treat the security level as unknown.	Treat the security level as unknown.
8	Security level	Caution	

For details about the user definition file, see *16.2.9 User definition file*.

### (8) Sample of a mail address definition file

The following shows a sample of a mail address definition file.

```
manager-a@company.jp
manager-b@company.jp
```

The sample contains the following settings.

No.	Item	Set value
1	Email address	manager-a@company.jp manager-b@company.jp

For details about the mail address definition file, see *16.3 Mail address definition file*.

### (9) Sample of a patch update condition file

The following shows a sample of a patch update condition file.

```
Patch_Release_Start=2007/03/01
#Patch_Release_End=2008/03/31
Patch_Release_Period=0
Patch_Product=0
Patch_Class=0
Patch_OS=0
Patch_Serious=0
Patch_Update_Cond=0
Patch_Version=0
Patch_Delay=0
Patch_Emergency=400
Patch_Importance=400
Patch_Warning=300
Patch_Caution=200
Patch_Nothing=200
```

The sample contains the following settings.

No.	Item	Set value
1	Release date (start)	2007/03/01
2	Release date (end)	None specified <sup>#</sup>
3	Release period	0
4	Product type	All (OS and software products)
5	Class	All
6	Target OS	All
7	Severity rating	All
8	Update condition	Only patches added since last execution
9	Processing dependent on patch information file version.	Do not process the file.
10	Update delay time	0

No.	Item	Set value
11	Security level setting (critical)	Danger
12	Security level setting (important)	Danger
13	Security level setting (moderate)	Warning
14	Security level setting (low)	Caution
15	Security level setting (unspecified)	Caution

#

Lines beginning with a hash symbol (#) are treated as comments.

For details about the patch update condition file, see *16.11 Patch update condition file*.

#### (10) Sample of an excluded user definition file

The following shows a sample of an excluded user definition file.

```
;exclude userid list
user1
user2
```

The sample contains the following settings.

No.	Item	Set value
1	User account name	user1 user2

For details about the excluded user definition file, see *16.19 Excluded user definition file*.

## B. List of Port Numbers

This appendix lists the port numbers used by JP1/CSC and the direction in which data passes through the firewall.

### B.1 Port numbers

The following table lists the port numbers used by JP1/CSC.

*Table B-1: Port numbers used by JP1/CSC*

Port number	Protocol	Description
22340	TCP	The port number that JP1/CSC - Manager uses to receive requests such as judgment and action requests.
22345	TCP	The port number that JP1/CSC - Agent uses to receive network control requests.
22351	TCP	The port number that JP1/CSC - Manager uses to receive automatic policy update requests for the anti-virus product.

### B.2 Direction in which data passes through the firewall

The following table describes the direction in which data passes through the firewall.

*Table B-2: Direction in which data passes through the firewall*

Programs that must be set in the firewall	Port number/protocol	Direction in which data passes through the firewall
JP1/CSC - Manager, JP1/CSC - Agent, and JP1/CSC - Manager Remote Option	22340/tcp	<ul style="list-style-type: none"> <li>JP1/CSC - Agent =&gt; JP1/CSC - Manager</li> <li>JP1/CSC - Manager Remote Option =&gt; JP1/CSC - Manager</li> </ul>
JP1/CSC - Manager and JP1/CSC - Agent	22345/tcp	JP1/CSC - Manager => JP1/CSC - Agent
JP1/CSC - Manager and JP1/CSC - Manager Remote Option	22351/tcp	JP1/CSC - Manager Remote Option => JP1/CSC - Manager

Legend:

$A \Rightarrow B$ : Indicates that data passes from  $A$  through the firewall to  $B$ .

## C. List of Processes

The following lists the process names for JP1/CSC.

### (1) List of JP1/CSC - Manager processes

Table C-1: List of JP1/CSC - Manager processes

Process name	Function
cscmaccept.exe	Manager process
cscmsvc.exe	Manager service
cscmrssvc.exe	Remote service

### (2) List of JP1/CSC - Manager Remote Option processes

Table C-2: List of JP1/CSC - Manager Remote Option processes

Process name	Function
cscmrsvsvc.exe	Virus definition information monitoring service

### (3) List of JP1/CSC - Agent processes

Table C-3: List of JP1/CSC - Agent processes

Process name	Function
cscanetcon.exe	Network control process

---

## D. Operation on a Cluster System

---

JP1/CSC - Manager and JP1/CSC - Agent can be run on a cluster system. This appendix explains how to set up and run these programs on a cluster system.

*Note:*

JP1/CSC - Manager Remote Option cannot be used on a cluster system.

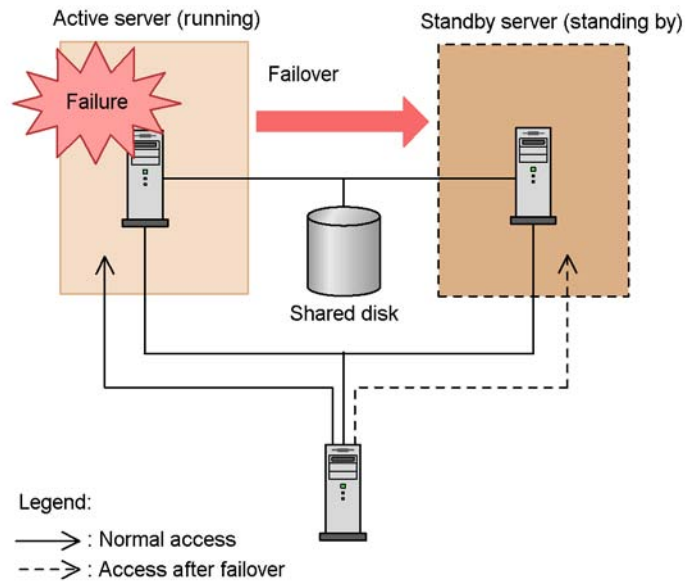
### D.1 Cluster system overview

#### (1) Overview

A cluster system is designed to achieve high availability (HA), and consists of an active server, which performs processing, and a standby server, which takes processing over when a failure occurs. This is called an *active-standby configuration*. This improves availability, since processing is carried over from the active server to the standby server when an error occurs, preventing operations from stopping. This operation of carrying over during a failure is called *failover*.

The software that controls an overall cluster system is called *cluster software*. Cluster software can monitor whether or not a system is operating normally, and perform failover when an error is detected, to prevent operation from stopping. The following figure gives an overview of a cluster system.

*Figure D-1: Cluster system overview*



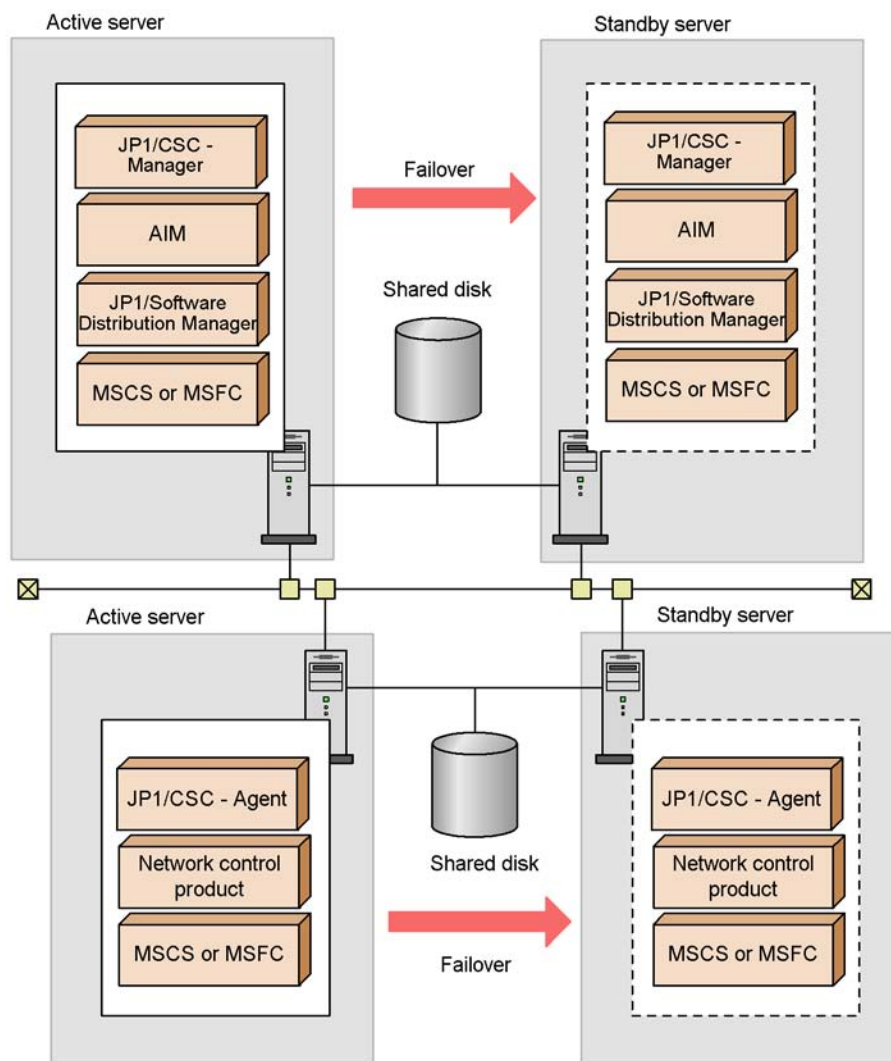
## **(2) Cluster system configuration**

JP1/CSC - Manager and JP1/CSC - Agent can be run on an active-standby cluster system. By running these programs on a cluster system, procedures can be carried over from the active server to the standby server when a server failure occurs, allowing client security management to continue.

The following figure shows a configuration for running JP1/CSC - Manager and JP1/CSC - Agent on a cluster system.



Figure D-2: Example cluster system configuration



It is also possible to run only JP1/CSC - Manager or only JP1/CSC - Agent on a cluster system.

## D.2 Prerequisites and supported operations

### (1) Prerequisites

The following table explains the prerequisites for running JP1/CSC - Manager and JP1/CSC - Agent on a cluster system.

Table D-1: Prerequisites

Component	Prerequisites
OS and required software	<p>OS</p> <p>Windows Server 2003, Enterprise Edition or Windows Server 2008 Enterprise</p> <p>OS cluster software</p> <p>Microsoft Cluster Server (MSCS) or Windows Server Failover Cluster (WSFC)</p>
Servers	Two servers in a cluster configuration
Network	<ul style="list-style-type: none"> <li>• A logical IP address can be used for communication when communication is lost due to a problem in the cluster software or for some other reasons.</li> <li>• Correspondence between host names and IP addresses is not changed by cluster software or name servers during JP1/CSC - Manager operation.</li> <li>• The LAN board corresponding to the host name has the highest priority in the network binding settings, with no other LAN boards of higher priority.</li> </ul>
Shared disk	<ul style="list-style-type: none"> <li>• Failover can be performed from the active server to the standby server.</li> <li>• The shared disk must be allocated before starting JP1/CSC<sup>#1</sup>.</li> <li>• The shared disk must not be deallocated while JP1/CSC<sup>#1</sup> is active.</li> <li>• Exclusion control is performed so that invalid usage does not exist from multiple servers.</li> <li>• Contents written to files are guaranteed even when failover occurs.</li> <li>• Failover can be performed forcibly even when the shared disk is being used by another process.</li> <li>• Recovery measures when a shared disk error is detected is controlled by the cluster software, and is transparent to JP1/CSC<sup>#1</sup>. If JP1/CSC<sup>#1</sup> needs to be started or stopped during the recovery process, the start/stop execution request must be issued from the cluster software.</li> </ul>
Logical IP address	<ul style="list-style-type: none"> <li>• Communication is performed using an address that can be carried over.</li> <li>• The logical IP address must be assigned before starting JP1/CSC<sup>#1</sup>.</li> <li>• The logical IP address must not be deallocated while JP1/CSC<sup>#1</sup> is active.</li> <li>• Recovery measures when a network error is detected is controlled by the cluster software, and is transparent to JP1/CSC<sup>#1</sup>. If JP1/CSC<sup>#1</sup> needs to be started or stopped during the recovery process, the start/stop execution request must be issued from the cluster software.</li> </ul>
AIM <sup>#2</sup>	<ul style="list-style-type: none"> <li>• AIM must also be configured for operation in the cluster system.</li> <li>• JP1/CSC - Manager must be set up so that failover is performed after AIM failover is completed.</li> </ul>

#1

Refers to *JP1/CSC - Manager* when running JP1/CSC - Manager on a cluster system, or to *JP1/CSC - Agent* when running JP1/CSC - Agent on a cluster system.

#2

The prerequisites for AIM are unnecessary when running only JP1/CSC - Agent on a cluster system.

**(2) Supported operations**

When JP1/CSC - Manager is run on a cluster system, only operations for JP1/CSC - Manager itself are supported.

When JP1/CSC - Agent is run on a cluster system, only operations for JP1/CSC - Agent itself are supported.

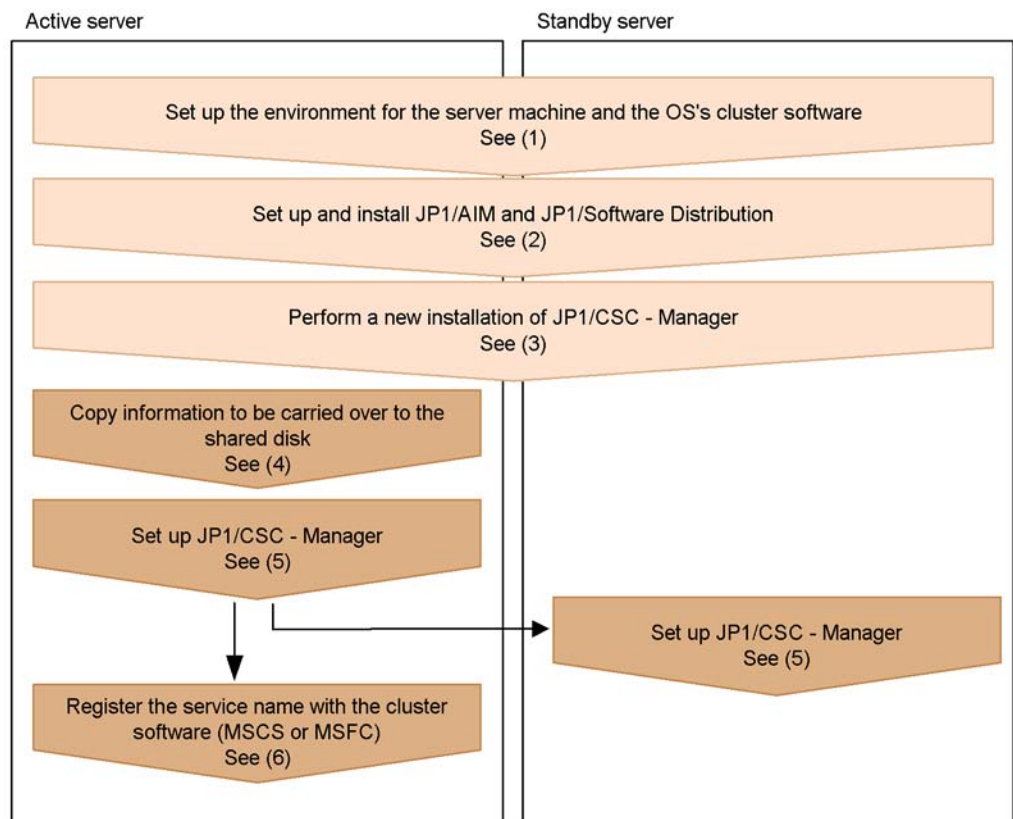
Cluster environment (shared disks and logical IP addresses) control depends on cluster software control. Therefore, if the prerequisites listed in *Table D-1 Prerequisites* are not satisfied, or problems occur with cluster environment control, check the cluster software and OS.

**D.3 Installing and setting up JP1/CSC - Manager**



This section explains how to install and set up a new installation of JP1/CSC - Manager to be run in a cluster system.

The following figure shows the procedures for installation and setup. Setup of the cluster environment for the OS, JP1/Software Distribution, and AIM must be completed and logical IP addresses must be usable before you can set up JP1/CSC - Manager for operation in the cluster system.

*Figure D-3: Procedures for JP1/CSC - Manager installation and setup (new installation)*



Legend:

-  : Tasks to perform on both the active server and standby server
-  : Tasks to perform on either the active server or standby server

### **(1) Setting up the environment for the server machine and OS cluster software**

To set up the environment, perform the following on the active server and standby server:

- Set up the server machine.
- Install and set up the OS cluster software.
- Prepare the shared disk and logical IP address.

For details about installing and setting up the cluster software, see the cluster software

documentation.

## **(2) Installing and setting up JP1/Software Distribution and AIM**

Install and set up JP1/Software Distribution and AIM to run in the cluster environment. For details about installing and setting up JP1/Software Distribution (and Asset Information Manager Subset Component of JP1/Software Distribution Manager), see the manual *Job Management Partner 1/Software Distribution Setup Guide*, for Windows systems. For details about installing and setting up Asset Information Manager, see the manual *Job Management Partner 1/Asset Information Manager Planning and Setup Guide*.

## **(3) Performing a new installation of JP1/CSC - Manager**

Install JP1/CSC - Manager on the local disk of both the active server and standby server. If you did not choose the automatic setup option during installation, restart the system after installation is completed. When the system has restarted, stop the World Wide Web Publishing Service and execute the `cscsetup` command.

## **(4) Copying information carried over to the shared disk (for the active server only)**

An administrator manually copies the following JP1/CSC - Manager installation folders to the shared disk path specified during setup.

*Table D-2: Folders copied to the shared disk*

Contents	Copy source	Copy destination
Environment settings information	<i>JP1/CSC - Manager-installation-folder</i> \conf	<i>shared-disk-path</i> \conf
Policy file	<i>JP1/CSC - Manager-installation-folder</i> \dat	<i>shared-disk-path</i> \dat
Policy import execution file (manual)	<i>JP1/CSC - Manager-installation-folder</i> \spool	<i>shared-disk-path</i> \spool
History file	<i>JP1/CSC - Manager-installation-folder</i> \db	<i>shared-disk-path</i> \db
Log file	<i>JP1/CSC - Manager-installation-folder</i> \log	<i>shared-disk-path</i> \log

Legend:

*installation-folder* indicates the installation folder for JP1/CSC - Manager.

The default installation folder for JP1/CSC - Manager is as follows (when the OS is installed under C:\):

For Windows Server 2003 (x64):

C:\Program Files(x86)\HITACHI\jplnetmcscm

For other OSs:

C:\Program Files\HITACHI\jplnetmcscm

### (5) Setting up JP1/CSC - Manager

Set up JP1/CSC - Manager on the active server first, and then on the standby server.

JP1/CSC - Manager can be set up from the Client Security Control - Manager Setup dialog box. For the items in the **Basic Settings** page, **Agent** page, and **Remote Option** page, set the same information for the active server and standby server.

For details about setting up JP1/CSC - Manager, see 5.4.3 *Setting up JP1/CSC - Manager*.

#### ■ Active server

Choose the **Basic settings** page in the Client Security Control - Manager Setup dialog box, and set the following items for **Cluster information**.

Table D-3: Setup items for Cluster information (active server)

Setup item	Description
Cluster environment	Be sure to specify Use.
Logical IP address	Specify the logical IP address of the cluster system. This item is required.
Logical host	This item is optional. For JP1/IM linkage, specify the name of the logical host when messages are sent to the event server on the logical host. For details about the logical host name, see the manual <i>Job Management Partner 1/Base User's Guide</i> .
Shared disk	Specify the shared disk path of the cluster system. JP1/CSC - Manager creates on the shared disk information carried over to the standby server. This item is required.

#### ■ Standby server

In the Client Security Control - Manager Setup dialog box, set the same information as for the active server in the items in the **Basic Settings** page, **Agent** page, and **Remote Option** page.

### (6) Registering service names in the cluster software (for the active server only)

In the cluster software (MSCS or WSFC), register the names of the JP1/CSC - Manager services that you want to be able to fail over. If a remote management server is configured in the system, also register the name of the remote service. The services

whose names are registered in the cluster software are as follows.

Product name	Service name	Resource type	Description
JP1/CSC - Manager	JP1_NETM_CSCM	Generic service	Name of JP1/CSC - Manager service
	JP1_NETM_CSCM_RS	Generic service	Name of remote service

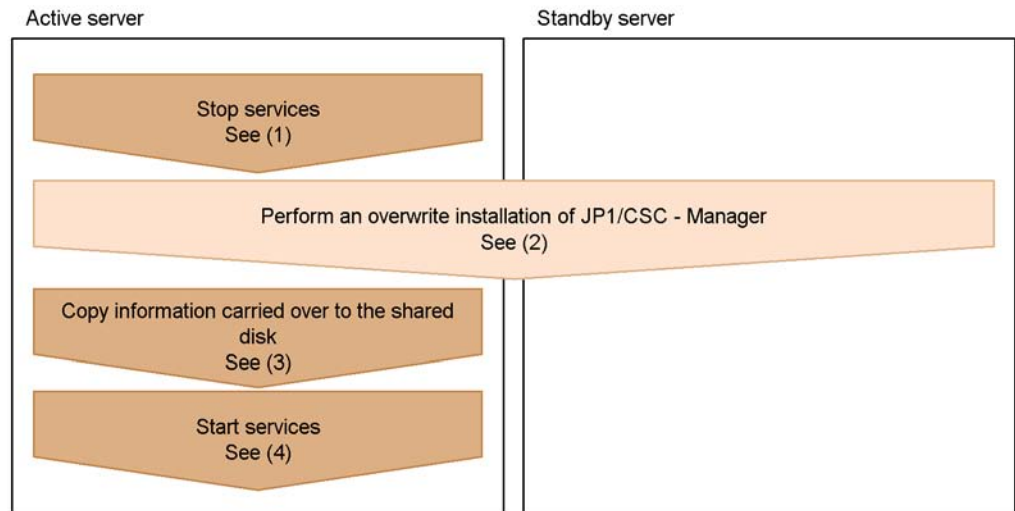
For details about how to register service names, see the MSCS or WSFC documentation. When registering service names, note the following:

- Have the service carried over from the active server to the standby server, with the IP address and shared disk used.
- Have the JP1/CSC - Manager service also fail over when the AIM service is failed over.
- Once the logical IP address and shared disk can be used, set JP1/CSC - Manager to start. Also set JP1/CSC - Manager to stop in the reverse order from how it starts.



#### D.4 Performing an overwrite installation of JP1/CSC - Manager

This section explains how to perform an overwrite installation of JP1/CSC - Manager in a cluster system.

The following figure shows the procedures for an overwrite installation of JP1/CSC - Manager.

*Figure D-4: Procedures for overwrite installation of JP1/CSC - Manager*

Legend:

-  : Tasks to perform on both the active server and standby server
-  : Tasks to perform on the active server only

### **(1) Stop services**

Make sure that the resources registered in the cluster software (MSCS or WSFC) are offline, and then stop the following services:

- JP1\_NETM\_CSCM
- JP1\_NETM\_CSCM\_RS

For details about how to stop services, see the MSCS or WSFC documentation.

### **(2) Perform an overwrite installation of JP1/CSC - Manager**

Perform an overwrite installation of JP1/CSC - Manager on the active server and standby server. If you did not choose the automatic setup option during installation, restart the system after installation is completed. When the system has restarted, stop the World Wide Web Publishing Service and execute the `cscsetup` command. For details about the procedures for performing an overwrite installation, see 5.4.1(2) *Performing an overwrite installation of JP1/CSC - Manager*.



### (3) Copying information carried over to the shared disk (for the active server only)

An administrator manually copies the following folders and files in the JP1/CSC - Manager installation folder to the shared disk path specified during setup.

Table D-4: Folders and files to copy to the shared disk

Contents	Source	Destination
Environment settings information	JP1/CSC - Manager-installation-folder\conf\cscmenv.conf	shared-disk-path\conf\cscmenv.conf
	JP1/CSC - Manager-installation-folder\conf\cscmenvname.conf	shared-disk-path\conf\cscmenvname.conf
	JP1/CSC - Manager-installation-folder\conf\cscmpolimportcmd.conf	shared-disk-path\conf\cscmpolimportcmd.conf
Policy files	JP1/CSC - Manager-installation-folder\dat\action\00000001	shared-disk-path\dat\action\0000001
	JP1/CSC - Manager-installation-folder\dat\action\00000002	shared-disk-path\dat\action\0000002
	JP1/CSC - Manager-installation-folder\dat\judge\00000001	shared-disk-path\dat\judge\0000001
	JP1/CSC - Manager-installation-folder\dat\judge\00000002	shared-disk-path\dat\judge\0000002

### (4) Start services

Make sure that the resources registered in the cluster software (MSCS or WSFC) are online, and then start the following services:

- JP1\_NETM\_CSCM
- JP1\_NETM\_CSCM\_RS

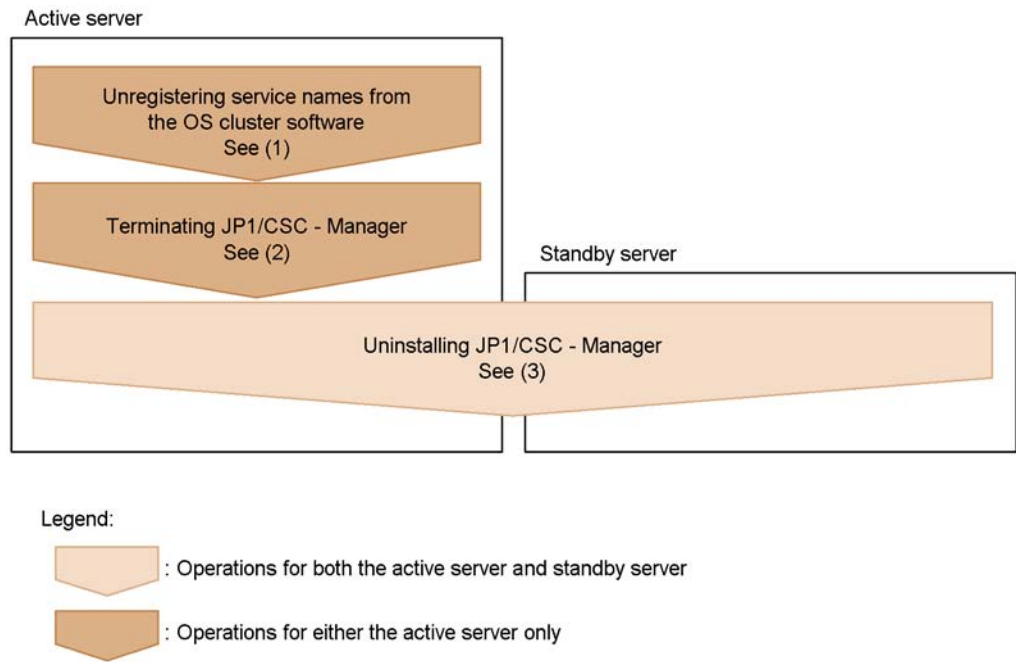
For details about how to start services, see the MSCS or WSFC documentation.

## D.5 Uninstalling JP1/CSC - Manager

This section explains how to uninstall JP1/CSC - Manager from a cluster system.

The following diagram shows the procedures for uninstalling JP1/CSC - Manager.

*Figure D-5: Procedures for uninstalling JP1/CSC - Manager*



**(1) Unregistering a service name from the OS cluster software (for the active server only)**

Unregister the JP1/CSC - Manager service names from the OS cluster software. If a remote management server is configured in the system, also unregister the name of the remote service. For details about unregistering JP1/CSC - Manager service names, see the cluster software documentation.

**(2) Terminating JP1/CSC - Manager (for the active server only)**

On the active server, terminate JP1/CSC - Manager. The administrator terminates the Client Security Control - Manager service from the service controller. If a remote management server is configured in the system, also unregister the remote service JP1/CSC - Manager Remote Service.

Note that if JP1/CSC - Manager is set to be started automatically when the OS starts up, JP1/CSC - Manager will terminate automatically when the management server shuts down.

For the setup required to start JP1/CSC - Manager automatically, see *5.4.4 Setting up JP1/CSC - Manager and the remote service to start automatically*.

**(3) Uninstalling JP1/CSC - Manager**

Uninstall JP1/CSC - Manager from the active server and standby server. For details about the uninstallation procedures, see *5.4.2 Uninstalling JP1/CSC - Manager*.

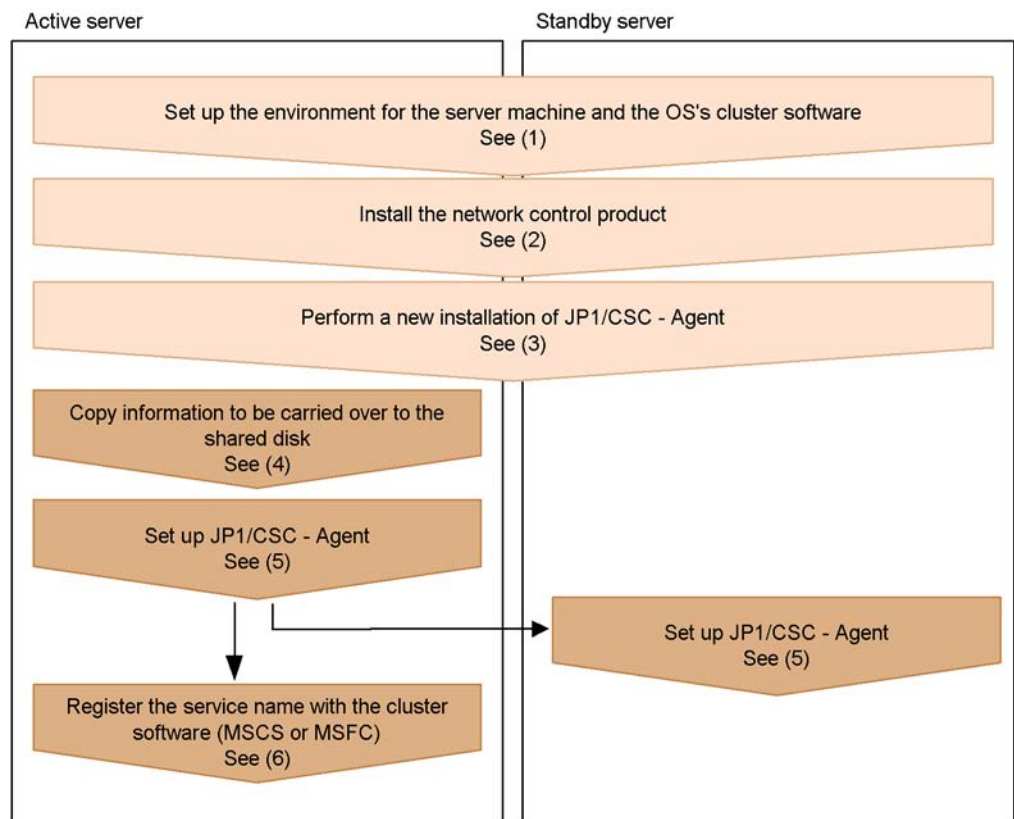
After uninstallation, manually delete the files created on the shared disk.

**D.6 Installing and setting up JP1/CSC - Agent**



This section explains how to install and set up a new installation of JP1/CSC - Agent to be run in a cluster system.

The following figure shows the procedures for installation and setup. Setup of the cluster environment for the OS and configuration of the network control product must be completed and logical IP addresses must be usable before you can set up JP1/CSC - Agent for operation in the cluster system.

*Figure D-6: Procedures for JP1/CSC - Agent installation and setup (new installation)*



Legend:

-  : Tasks to perform on both the active server and standby server
-  : Tasks to perform on either the active server or standby server

### **(1) Setting up the environment for the server machine and OS cluster software**

To set up the environment, perform the following on the active server and standby server:

- Set up the server machine.
- Install and set up the OS cluster software.
- Prepare the shared disk and logical IP address.

For details about installing and setting up the cluster software, see the cluster software

documentation.

## **(2) Installing a network control product**

Install and set up a network control product to run in the cluster environment. For details about installing a network control product, see the documentation for the particular network control product.

## **(3) Performing a new installation of JP1/CSC - Agent**

Install JP1/CSC - Agent on the local disk of both the active server and standby server.

## **(4) Copying information carried over to the shared disk (for the active server only)**

An administrator manually copies the following JP1/CSC - Agent installation folders to the shared disk path specified during setup.

*Table D-5: Folders copied to the shared disk*

Contents	Copy source	Copy destination
Environment settings information	<i>JP1/CSC - Agent-installation-folder</i> \conf	<i>shared-disk-path</i> \conf
Log file	<i>JP1/CSC - Agent-installation-folder</i> \log	<i>shared-disk-path</i> \log
RADIUS settings information	<i>JP1/CSC - Agent-installation-folder</i> \radius\conf	<i>shared-disk-path</i> \radius\conf
RADIUS log file	<i>JP1/CSC - Agent-installation-folder</i> \radius\log	<i>shared-disk-path</i> \radius\log
RADIUS connection control list	<i>JP1/CSC - Agent-installation-folder</i> \radius\dat	<i>shared-disk-path</i> \radius\dat

Legend:

*installation-folder* indicates the installation folder for JP1/CSC - Agent. The default installation folder for JP1/CSC - Agent is as follows (when the OS is installed under C:\):

For Windows Server 2003 (x64):

C:\Program Files(x86)\HITACHI\jplnetmcsca

For other OSs:

C:\Program Files\HITACHI\jplnetmcsca

**(5) Setting up JP1/CSC - Agent**

Set up JP1/CSC - Agent on the active server first, and then on the standby server.

JP1/CSC - Agent can be set up from the Client Security Control - Agent Setup dialog box. For the items in the Client Security Control - Agent setup dialog box, set the same information for the active sever and standby server.

The procedure for setting up JP1/CSC - Agent differs according to the linked network control product. For details, see *13. Setting Up a Quarantine System*.

■ Active server

Choose the **Basic Settings** page in the Client Security Control - Agent Setup dialog box, and set the following items for **Cluster information**.

*Table D-6: Setup items for Cluster Information (active server)*

Setup item	Description
Cluster environment	Be sure to specify Use.
Logical IP address	Specify the logical IP address of the cluster system. This item is required.
Shared disk	Specify the shared disk path of the cluster system. JP1/CSC - Agent creates on the shared disk information carried over to the standby server. This item is required.

■ Standby server

In the items in the Client Security Control - Agent Setup dialog box, set the same information as for the active server.

**(6) Registering a service name in the cluster software (for the active server only)**

In the cluster software (MSCS or WSFC), register the name of the JP1/CSC - Agent service that you want to be able to fail over. The name of the service is as follows:

Service name	Resource type
JP1_NETM_CSCA	Generic service

For details about how to register service names, see the MSCS or WSFC documentation. When registering service names, note the following:

- Have the service carried over from the active server to the standby server, with the IP address and shared disk used.
- Have the JP1/CSC - Agent service also fail over when the network control product is failed over.
- Set JP1/CSC - Agent to start once the logical IP address and shared disk can be

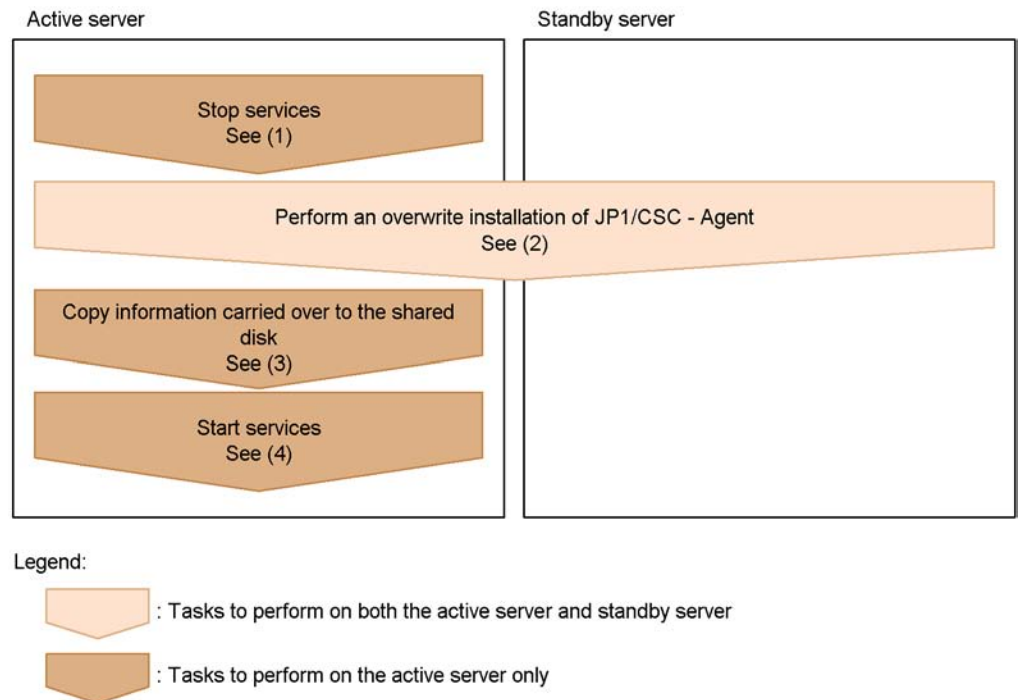
used. Also set JP1/CSC - Agent to stop in the reverse order from how it starts.

## D.7 Performing an overwrite installation of JP1/CSC - Agent

This section explains how to perform an overwrite installation of JP1/CSC - Agent in a cluster system.

The following figure shows the procedures for an overwrite installation of JP1/CSC - Agent.

*Figure D-7: Procedures for overwrite installation of JP1/CSC - Agent*



### (1) Stop services

Make sure that the resources registered in the cluster software (MSCS or WSFC) are offline, and then stop the following service:

- JP1\_NETM\_CSCA

For details about how to stop services, see the MSCS or WSFC documentation.

### (2) Perform an overwrite installation of JP1/CSC - Agent

Perform an overwrite installation of JP1/CSC - Agent on the active server and standby server. For details about the procedures for performing an overwrite installation, see 5.7.1(2) *Performing an overwrite installation of JP1/CSC - Agent*.

**(3) Copying information carried over to the shared disk (for the active server only)**

An administrator manually copies the following files in the JP1/CSC - Agent installation folder to the shared disk path specified during setup.

*Table D-7: Files to copy to the shared disk*

Contents	Source	Destination
Environment settings information	<i>JP1/CSC - Agent-installation-folder</i> \conf\cscaenv.conf	<i>shared-disk-path</i> \conf\cscaenv.conf
	<i>JP1/CSC - Agent-installation-folder</i> \conf\cscaenvname.conf	<i>shared-disk-path</i> \conf\cscaenvname.conf
RADIUS settings information	<i>JP1/CSC - Agent-installation-folder</i> \radius\conf\cscrenv.conf	<i>shared-disk-path</i> \radius\conf\cscrenv.conf
	<i>JP1/CSC - Agent-installation-folder</i> \radius\conf\cscrenvname.conf	<i>shared-disk-path</i> \radius\conf\cscrenvname.conf

**(4) Start services**

Make sure that the resources registered in the cluster software (MSCS or WSFC) are online, and then start the following service:

- JP1\_NETM\_CSCA

For details about how to start services, see the MSCS or WSFC documentation.

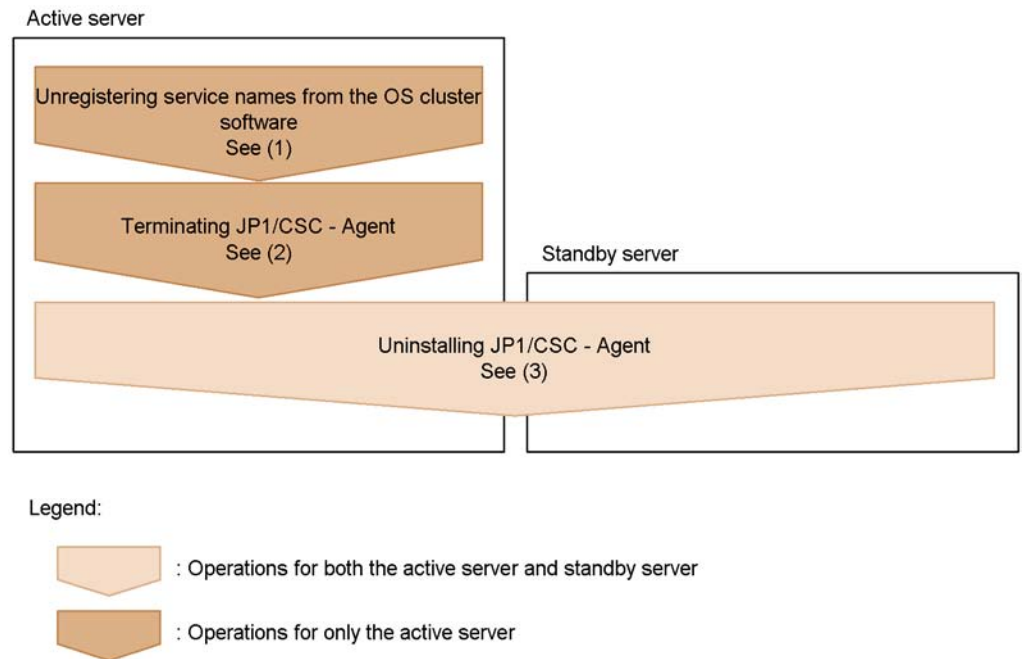
**D.8 Uninstalling JP1/CSC - Agent**

This section explains how to uninstall JP1/CSC - Agent from a cluster system.

The following diagram shows the procedures for uninstalling JP1/CSC - Agent.



Figure D-8: Procedures for uninstalling JP1/CSC - Agent



**(1) Unregistering a service name from the OS cluster software (for the active server only)**

Unregister the JP1/CSC - Agent service names from the OS cluster software. For details about how to do this, see the cluster software documentation.

**(2) Terminating JP1/CSC - Agent (for the active server only)**

On the active server, terminate JP1/CSC - Agent. The administrator terminates the Client Security Control - Agent service from the service controller.

Note that if JP1/CSC - Agent is set to be started automatically when the OS starts up, JP1/CSC - Agent will terminate automatically when the management server shuts down.

For the setup required to start JP1/CSC - Agent automatically, see 5.7.4 *Setting up JP1/CSC - Agent to start automatically*.

**(3) Uninstalling JP1/CSC - Agent**

Uninstall JP1/CSC - Agent from both the active and standby servers. For details about the uninstallation procedures, see 5.7.2 *Uninstalling JP1/CSC - Agent*.

After uninstallation, manually delete the files created on the shared disk.

## D.9 Operation during failover

### (1) When failover is performed

The following are examples of when to perform failover for JP1/CSC - Manager and JP1/CSC - Agent. Whether to perform failover in each situation must be set by the administrator.

- When a JP1/CSC - Manager is terminated on the NT service
- When a hardware failure occurs
- When an OS failure occurs
- When power is cut
- When a network failure occurs
- When a failure occurs in AIM (JP1/CSC - Manager only)

### (2) Administrator operations after failover

The administrator must perform the following operations when a failover occurs.

#### (a) JP1/CSC - Manager

Because JP1/CSC - Manager is started on the standby server, a message reporting JP1/CSC - Manager startup is output to the log.

The following table lists the operations that the administrator must perform if failover occurs during processing.

*Table D-8: Administrator operations after failover (JP1/CSC - Manager)*

Processing being performed during failover	Operation performed by the administrator
Security level judgment	Use the JP1/CSC - Manager log file to check whether security level judgment has finished. If processing has not finished, perform security level judgment again. <sup>#1</sup>
Action implementation	Use the JP1/CSC - Manager log file to check whether the action has finished. If processing has not finished, implement the action again. <sup>#2</sup>
Operations on a window	If failover occurred during operation of a window (Security Policy Management window, Setup window, or Client Security Management window), use the JP1/CSC - Manager log file to check whether the operation has finished. If it has not, perform the operation again.

#1

To check whether or not the security level judgment has finished, check the messages output to the log file to indicate the start and end of security level

judgment. If a start message from JP1/CSC - Manager was output between the start and end messages for security level judgment, processing has not finished.

#2

To check whether or not the action has finished, check the messages output to the log file to indicate the start and end of the action. If a start message from JP1/CSC - Manager was output between the start and end messages for the action, processing has not finished.

### (b) JP1/CSC - Agent

Because JP1/CSC - Agent is started on the standby server, a message reporting JP1/CSC - Agent startup is output to the log.

The following table lists the operations that the administrator must perform if a failover occurs during processing.

*Table D-9: Administrator operations after failover (JP1/CSC - Agent)*

Processing being performed during failover	Operation performed by the administrator
Action implementation	Use the JP1/CSC - Manager log file to check whether the action has finished. If processing has not finished, implement the action again. #
Operation in the Setup window	If a failover occurred while an operation was being performed in the Setup window, use the JP1/CSC - Agent log file to check whether the operation has finished. If it has not, perform the operation again.

#

To check whether the action has finished, review the messages output to the log file to indicate the start and end of the action. If a start message from JP1/CSC - Manager was output between the start and end messages for the action, processing has not finished.

### (3) Precautions

Keep the following in mind when performing operation on a cluster system:

- If the JP1/CSC<sup>#</sup> service cannot start or stop, a JP1/CSC<sup>#</sup> process may still be running. In this situation, restart the system.
- Startup control (NT service) cannot be used for operations that run on the logical IP address of the cluster system. To control JP1/CSC<sup>#</sup> startup on a cluster system, use the cluster software.
- When running JP1/CSC<sup>#</sup> on a cluster system, do not enable JP1/CSC<sup>#</sup> to start automatically.

#### D. Operation on a Cluster System

#

- Refers to *JP1/CSC - Manager* when running JP1/CSC - Manager on a cluster system.
- Refers to *JP1/CSC - Agent* when running JP1/CSC - Agent on a cluster system.

## E. Estimating Required Disk Capacity

This appendix explains how to estimate the disk capacity used by JP1/CSC.

### E.1 Disk capacity used by JP1/CSC - Manager

This section explains the disk capacity used by the files and database of JP1/CSC - Manager.

#### (1) Disk capacity used by files

The following table describes the disk capacity used by each file.

Table E-1: Disk capacity used by each file

No.	Type	Type of judgment policy	Formula for estimating disk capacity (in megabytes)
1	Fixed file		235 <sup>#1</sup>
2	Log file		$(a \times b / 1,024) \times 2^{\#2}$
3	Judgment history	Security update <b>Latest security updates</b> is specified.	$(200 + 82 \times e) \times c \times d / (1,024 \times 1,024)$
4		Security update <b>Specify security updates</b> is specified.	$((200 + 280 \times f) \times c \times d + (200 + 280 \times g) \times c \times d) / (1,024 \times 1,024)$
5		Anti-virus products	$(36 + 1,170 \times h + 1,160 \times i) \times c \times d / (1,024 \times 1,024)$
6		Prohibited software	$(38 + 450 \times j) \times c \times d / (1,024 \times 1,024)$
7		Mandatory software	$(38 + 707 \times k) \times c \times d / (1,024 \times 1,024)$
8		User definition	$(50 + 320 \times l + 1,436 \times m) \times c \times d / (1,024 \times 1,024)$
9		PC security settings	$6,144 \times t \times c \times d / (1,024 \times 1,024)$
10	Judgment policy files		$(12,428 + 544 \times (e + g) + 296 \times f + 1,552 \times h + 592 \times j + 940 \times k + 55 \times l + 1,020 \times m) \times n / (1,024 \times 1,024)$
11	Action policy files		$(307,200 + 360 \times o) \times p / (1,024 \times 1,024)$
12	Product name definition file		$256 \times r / (1,024 \times 1,024)$

No.	Type	Type of judgment policy	Formula for estimating disk capacity (in megabytes)
13	User-defined actions	Temporary file when <b>Pass the asset information to the command</b> is selected. <sup>#3</sup>	$2,500 \times c / (1,024 \times 1,024)$
14		Temporary file when <b>Pass the judgment result to the command</b> and either <b>Summary</b> or <b>Details</b> are selected. <sup>#3</sup>	$160 \times c / (1,024 \times 1,024)$
15		Temporary file (security updates), when <b>Pass the judgment result to the command</b> and <b>Details</b> are selected. <sup>#3</sup>	$(272 \times g + 150 \times q + 270 \times f) \times c / (1,024 \times 1,024)$
16		Temporary file (anti-virus products), created when <b>Pass the judgment result to the command</b> and <b>Details</b> are selected. <sup>#3</sup>	$142 \times c / (1,024 \times 1,024)$
17		Temporary file (prohibited software), created when <b>Pass the judgment result to the command</b> and <b>Details</b> are selected. <sup>#3</sup>	$770 \times j \times c / (1,024 \times 1,024)$
18		Temporary file (mandatory software), created when <b>Pass the judgment result to the command</b> and <b>Details</b> are selected. <sup>#3</sup>	$1,280 \times k \times c / (1,024 \times 1,024)$
19		Temporary file (user definition), created when <b>Pass the judgment result to the command</b> and <b>Details</b> are selected. <sup>#3</sup>	$642 \times l \times c / (1,024 \times 1,024)$
20	Temporary file created when an HTML message is previewed in the Edit Action Policy window		$33,000 \times s / (1,024 \times 1,024)$
21	Audit log file		17

Legend:

$a$ : Number of log files (default is 10)

- b*: Log file size (in kilobytes, with a default of 1,024)
- c*: Number of assets
- d*: Number of history preservation generations (default is 20)
- e*: Number of excluded patches defined in the judgment policy
- f*: Number of service packs defined in the judgment policy
- g*: Number of patches defined in the judgment policy
- h*: Number of anti-virus products installed on the asset
- i*: Number of anti-virus products defined in the judgment policy
- j*: Number of prohibited software applications defined in the judgment policy
- k*: Number of mandatory software applications defined in the judgment policy
- l*: Number of user-defined judgment items defined in the judgment policy
- m*: Number of user-defined judgment conditions defined in the judgment policy
- n*: Number of judgment policies
- o*: Number of email addresses defined in the action policy
- p*: Number of action policies
- q*: Number of OS service packs defined in the judgment policy
- r*: Number of product name definitions (default is an empty file)
- s*: Number of Edit Action Policy windows opened
- t*: Number of PC security setting judgment items defined in the judgment policy

#1

11 (size needed for installation) + 224 (trace within the product)

#2

The values of *a* and *b* can be changed from the JP1/CSC - Manager setup window. For details about the JP1/CSC - Manager setup window, see *5.4.3 Setting up JP1/CSC - Manager*.

#3

Item set in the **Action for the user definition** area of the Edit Action Policy window. For details about this window, see *6.10 Setting an action for each security level*.

## (2) Database disk capacity

The following is a formula to estimate the disk capacity used by the database, in

megabytes.

$$(188 + 24,280 \times c + (2,996 \times d) \times c + 194 \times (6 + n + p)) \times 1.5 + 4,060 \times (u + 1) \times v / (1,024 \times 1,024) + 50$$

Legend:

*c*: Number of assets

*d*: Number of history preservation generations (default is 20)

*n*: Number of judgment policies

*p*: Number of action policies

*u*: Number of groups registered in AIM

*v*: Number of days on which the statistics storage command (*cscstorecount*) was executed

In consideration of the database block size and index area, the estimate is multiplied by 1.5.

## E.2 Disk capacity used by JP1/CSC - Manager Remote Option

This section explains the disk capacity required for the files used by JP1/CSC - Manager Remote Option.

Table E-2: Disk capacity used by each file

No.	Type	Formula for estimating disk capacity (in megabytes)
1	Fixed file	51 <sup>#1</sup>
2	Log file	$a \times b / 1,024$ <sup>#2</sup>
3	Audit log file	17

Legend:

*a*: Number of log files (default is 10)

*b*: Log file size (in kilobytes, with a default of 1,024)

#1

3 (size needed for installation) + 48 (trace within the product)

#2

The values of *a* and *b* can be changed from the Client Security Control - Manager Remote Option Setup dialog box. For details about setting up JP1/CSC - Manager Remote Option, see 5.5 *Installing and setting up JP1/CSC - Manager Remote Option*.



### E.3 Disk capacity used by JP1/CSC - Agent

This section explains the disk capacity used by the files used by JP1/CSC - Agent.

For the amount of disk space required for JP1/CSC - Agent linked to an authentication server, see *Table E-4*.

*Table E-3: Disk capacity used by each file*

No.	Type	Formula for estimating disk capacity (in megabytes)
1	Fixed file	37 <sup>#1</sup>
2	Log file	$a \times b / 1,024^{\#2}$
3	Audit log file	17

Legend:

*a*: Number of log files (default is 10)

*b*: Log file size (in kilobytes, with a default of 1,024)

#1

5 (size needed for installation) + 32 (trace within the product)

#2

The values of *a* and *b* can be changed from the JP1/CSC - Agent setup window. For details about setting up JP1/CSC - Agent, see the description in *13. Setting Up a Quarantine System*.

#### ■ Amount of disk space required for JP1/CSC - Agent linked to an authentication server

The following table lists the amount of disk space required for the files used by JP1/CSC - Agent linked to an authentication server.

*Table E-4: Disk capacity used by each file (for authentication server linkage)*

No.	Type	Formula for estimating disk capacity (in megabytes)
1	Fixed file	101 <sup>#1</sup>
2	Log file	$a \times b / 1,024^{\#2}$
3	Connection history file	$c \times d / 1,024^{\#2}$
4	Connection control list file	$e \times 16 / (1,024 \times 1,024)$

No.	Type	Formula for estimating disk capacity (in megabytes)
5	Audit log file	17

Legend:

*a*: Number of log files (default is 10)

*b*: Log file size (in kilobytes, with a default of 1,024)

*c*: Number of connection history files (default is 100)

*d*: Connection history file size (in kilobytes, with a default of 1,024)

*e*: Number of assets

#1

5 (size needed for installation) + 96 (trace within the product)

#2

The values of *a*, *b*, *c*, and *d* can be changed from the Client Security Control - Agent Setup dialog box. For details about setting up JP1/CSC - Agent, see the description in *13. Setting Up a Quarantine System*.

## F. Audit Log Output

This section describes the information output to the JP1/CSC audit log.

### F.1 Event types output to the audit log

The following table lists the types of events that are output to the audit log, and the triggers that cause JP1/CSC to output the information. The events output to the audit log are classified according to their event type.

*Table F-1: Types of event output to audit log*

Event type	Description	Trigger for output by JP1/CSC
StartStop	An event indicating that a software product has started or stopped.	A log entry relating to a service starting or stopping is output when: <ul style="list-style-type: none"> <li>• A service is started</li> <li>• A service fails to start</li> <li>• A service is stopped</li> <li>• A service terminates abnormally</li> </ul>
Authentication	An event indicating that authentication of a CSC administrator or CSC user succeeded or failed.	A log entry relating to users logging in or out from various windows is output when: <ul style="list-style-type: none"> <li>• A user logs in successfully</li> <li>• A login attempt fails</li> <li>• A user logs out</li> </ul>
ConfigurationAccess	An event indicating that a CSC administrator executed a permitted operation, and the operation completed normally or failed.	A log entry relating to attempts to modify definitions, policies, or the connection control list is output when: <ul style="list-style-type: none"> <li>• A product definition is modified successfully</li> <li>• An attempt to modify a product definition fails</li> </ul>

Event type	Description	Trigger for output by JP1/CSC
ContentAccess	An event indicating that an attempt was made to access security data managed by CSC, and the attempt succeeded or failed.	A log entry relating to attempts to access the security information managed by CSC is output when: <ul style="list-style-type: none"> <li>• A policy is modified successfully</li> <li>• An attempt to modify a policy terminates abnormally</li> <li>• Security management information is accessed successfully</li> <li>• An attempt to access security information fails</li> <li>• The connection control list is modified successfully</li> <li>• An attempt to modify the connection control list fails</li> </ul>
ManagementAction	An event indicating an action executed as a result of judgment or action based on a security policy.	A log entry relating to the result of judgment or action is output.

## F.2 Audit log save format

This section describes the file format used when saving audit logs.

The following table lists the names of the files to which each product outputs audit log information.

*Table F-2: Audit log file names and output destinations*

Product name	File name	Output destination
JP1/CSC - Manager	jplnetmcscauditlog*.log <sup>#</sup>	<i>JP1/CSC - Manager-installation-folder\log</i>
JP1/CSC - Manager Remote Option	jplnetmcsmauditlog*.log <sup>#</sup>	<i>JP1/CSC - Manager Remote Option-installation-folder\log</i>
JP1/CSC - Agent	jplnetmcscauditlog*.log <sup>#</sup>	<i>JP1/CSC - Agent-installation-folder\log</i>

#

In place of the asterisk (\*), a number from 1 to 15 is appended to all but the latest log file. When the size of the latest log file reaches 1,024 bytes, the file is renamed from *file-name.log* to *file-name1.log* and a new file is created. The numbers appended to the existing log files are incremented by one with each new file. When the number of log files exceeds 16, the log files are deleted in order from the oldest file.

Example: jplnetmcscmauditlog.log  
 jplnetmcscmauditlog1.log  
 jplnetmcscmauditlog2.log

### F.3 Audit log output format

The following describes the output format, output destination, and output items of an audit log. An example of audit log output is also shown.

#### (1) Output format

An audit log consists of the string CALFHM, indicating that the information is formatted as an audit log, followed by the revision number of the audit log, and finally the relevant output items.

The following figure shows the output format of an audit log.

*Figure F-1: Output format of audit log*

CALFHM X.X, output-item-1 = value-1, output-item-2 = value-2, ..., output-item-n = value-n

#### (2) Output destination

For details about the output destinations for audit logs, see Table *F-2 Audit log file names and output destinations*.

#### (3) Output items

The items in an audit log fall into the following two categories:

- Common output items  
Items common to all JP1 products that output audit logs.
- Fixed output items  
Items that specific JP1 products can output in audit logs.

##### (a) Common output items

The following table lists the values output as common output items, and the content of each item.

Table F-3: Common output items in audit logs

No.	Output item		Value	Content
	Item name	Output attribute name		
1	Common specification identifier	--	CALFHM	An ID indicating that the information is formatted as an audit log
2	Common specification revision number	--	X.X	The revision number used to manage the audit log
3	Sequence number	seqnum	<i>sequence-number</i>	The sequence number of the audit log record
4	Message ID	msgid	KDSLxxx-x	The message ID from the product
5	Date and time	date	YYYY-MM-DDThh:mm:ss.sssTZD <sup>#</sup>	The time (including timezone) when the audit log was output
6	Generated program name	progid	JP1/CSC	The name of the program where the event occurred

No.	Output item		Value	Content
	Item name	Output attribute name		
7	Generated component name	compid	Component name <ul style="list-style-type: none"> <li>• Manager Manager program</li> <li>• Policy Policy Management window</li> <li>• ManagerSetup Manager Setup window</li> <li>• AgentSetup Agent Setup window</li> <li>• RemoteOptionSetup Remote Option Setup window</li> <li>• Command A command</li> <li>• Agent Agent program</li> <li>• RemoteOption Remote option program</li> </ul>	The name of the component where the event occurred
8	Generated process ID	pid	<i>process-ID</i>	The ID of the process associated with the event
9	Generated location	ocp:ip 4 or ocp:host	<i>IP-address-or-host-name-of-audit-log management-server</i>	The IP address or host name of the audit log management server where the event occurred
10	Event type	ctgry	<ul style="list-style-type: none"> <li>• StartStop</li> <li>• Authentication</li> <li>• ConfigurationAccess</li> <li>• ContentAccess</li> <li>• ManagementAction</li> </ul>	The category to which the event output to the audit log belongs
11	Event result	result	<ul style="list-style-type: none"> <li>• Success The event was successful.</li> <li>• Failure The event was a failure.</li> <li>• Occurrence There is no distinction between success or failure for the event.</li> </ul>	The result of the event

No.	Output item		Value	Content
	Item name	Output attribute name		
12	Subject identification information	subj:uid or subj:euid	<ul style="list-style-type: none"> <li>• subj:uid JP1/AIM user</li> <li>• subj:euid OS user (Administrator)</li> </ul>	Identification information for the user who caused the event

Legend:

--: None.

#

T is a delimiter between the date and time.

ZD specifies the timezone. One of the following is output:

+hh:mm: Indicates a timezone *hh:mm* ahead of UTC.

-hh:mm: Indicates a timezone *hh:mm* behind UTC.

z: Indicates a timezone equivalent to UTC.

#### (b) Fixed output items

The following table lists the values output as fixed output items, and the content of each item.

Table F-4: Fixed output items in audit logs

No.	Output item		Value	Content
	Item name	Output attribute name		
1	Object information	obj	<ul style="list-style-type: none"> <li>• SecurityInfo Judgment result information</li> <li>• Policy Policy information</li> <li>• Config Configuration file</li> <li>• NetworkControlList Network control list file</li> </ul>	The name of the object



No.	Output item		Value	Content
	Item name	Output attribute name		
2	Action information	op	<ul style="list-style-type: none"> <li>Start</li> <li>Stop</li> <li>Login</li> <li>Logout</li> <li>Refer</li> <li>Add</li> <li>Update (includes create)</li> <li>Delete</li> </ul>	The action that generated the event
3	Permissions information #	auth	<ul style="list-style-type: none"> <li>JP1/AIM permissions</li> <li>OS permissions</li> </ul>	The AIM permission is output as the permission for JP1 products. Administrator permission is output as the OS permission.
4	Origin of request	from:ipv4	<i>IP-address-of-request-origin</i>	The IP address of the client using the Web browser
5	Message	msg	A message with any content.	A message describing the nature of the event

#

This item is not output if the user has inadequate permission or permission information cannot be acquired.

#### **(4) Example of audit log output**

The following shows an example of the audit logs output in the process of updating policy information in JP1/CSC - Manager and performing security level judgment.

In this example, the following tasks took place:

1. Started JP1/CSC - Manager.
2. Performed user authentication.
3. Updated policy information.
4. Performed security level judgment.

## 5. Stopped JP1/CSC - Manager.

The audit logs are as follows:

Figure F-2: Content of audit logs

Operation 1	CALFHM 1.0, seqnum=1, msgid=KDSL0010-I, date=2008-05-12T08:53:51.568-07:00, progid=JP1/CSC, compid=Manager, pid=3440, ocp:ipv4=192.168.0.10, ctgry=StartStop, result=Success, subj:uid=Administrator, op=Start, auth=Administrator, msg="The manager has started."
Operation 2	CALFHM 1.0, seqnum=1, msgid=KDSL2011-I, date=2008-05-12T16:54:13.609-07:00, progid=JP1/CSC, compid=Policy, pid=3476, ocp:ipv4=192.168.0.10, ctgry=Authentication, result=Success, subj:uid=csc_admin, op=Login, auth=csc_admin, msg="csc_admin logged in."
Operation 3	CALFHM 1.0, seqnum=2, msgid=KDSL2037-I, date=2008-05-12T16:55:16.560-07:00, progid=JP1/CSC, compid=Policy, pid=3476, ocp:ipv4=192.168.0.10, ctgry=ContentAccess, result=Success, subj:uid=csc_admin, obj=Policy, op=Update, auth=csc_admin, msg="Judgment policy has been changed. (policy name = [(Default policy)])"
Operation 4	CALFHM 1.0, seqnum=1, msgid=KDSL0104-I, date=2008-05-12T16:57:08.351-07:00, progid=JP1/CSC, compid=Manager, pid=3460, ocp:ipv4=192.168.0.10, ctgry=ManagementAction, result=Occurrence, subj:uid=Administrator, auth=Administrator, msg="The results of the security level judgment are as follows. (request source = [AIM], judgment date = [2008/05/12 16:57:07], number of request PCs = [1], number of judged PCs = [1], safe = [0], caution = [1], warning = [0], danger = [0], unknown = [0], Not applicable = [0])" CALFHM 1.0, seqnum=2, msgid=KDSL0510-I, date=2008-05-12T16:57:08.421-07:00, progid=JP1/CSC, compid=Manager, pid=3460, ocp:ipv4=192.168.0.10, ctgry=ManagementAction, result=Occurrence, subj:uid=Administrator, auth=Administrator, msg="The action results are as follows. (request source = [AIM], judgment date = [2008/05/12 16:57:07], action date = [2008/05/12 16:57:08], notice to the administrator = [Unimplemented], notice to the user = [Success], network connection control = [Unimplemented], user definition action = [Unimplemented])"
Operation 5	CALFHM 1.0, seqnum=2, msgid=KDSL0020-I, date=2008-05-13T00:03:04.184-07:00, progid=JP1/CSC, compid=Manager, pid=3440, ocp:ipv4=192.168.0.10, ctgry=StartStop, result=Success, subj:uid=Administrator, op=Stop, auth=Administrator, msg="The manager terminated normally."

## F.4 Configuration for outputting audit logs

The following describes the settings required to output audit logs from JP1/CSC.

### (1) Configuring JP1/CSC - Manager to output audit logs

To configure JP1/CSC - Manager to output audit logs, in the JP1/CSC - Manager setup dialog box, set **Audit log** to **Output**.

For details about the setup procedures for JP1/CSC - Manager, see *5.4.3 Setting up JP1/CSC - Manager*.

### (2) Configuring JP1/CSC - Manager Remote Option to output audit logs

To configure JP1/CSC - Manager Remote Option to output audit logs, in the JP1/CSC - Manager Remote Option setup dialog box, set **Audit log** to **Output**.

For details about the setup procedures for JP1/CSC - Manager Remote Option, see *5.5.3 Setting up JP1/CSC - Manager Remote Option*.

**(3) Configuring JP1/CSC - Agent to output audit logs**

To configure JP1/CSC - Agent to output audit logs, in the JP1/CSC -Agent setup dialog box, set **Audit log** to **Output**.

The setup procedures for JP1/CSC - Agent differ according to the network control product to which the agent is linked. For details, see *13. Setting Up a Quarantine System*.

---

## G. Version Changes

---

This appendix describes changes between versions.

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

- In a quarantine system linked to Job Management Partner 1/Network Monitor, **MAC address and IP address** is now a specifiable format for the permitted-devices list to be registered in JP1/Network Monitor.
- A quarantine system linked to an authentication server that uses IEEE 802.1X or MAC authentication in a static VLAN environment can now be set up.
- One-byte alphanumeric characters can now be used to specify the update number and article ID number of security updates in the Policy Management window.
- The following message has been added to the JP1/CSC - Agent messages:  
KDSL6043-I

### **(2) Changes in version 08-50**

- PC security settings can now be defined in judgment policies, to judge whether there are any settings on the client PC that may lead to a reduced security level.
- Statistics representing trends in the status of security measures on a group-by-group basis can now be checked in the Client Security Management window.  
  
The results of a search for statistics can be displayed as a graph or output to a CSV file.
- The `cscpatchupdate` command for automatically updating patch information for judgment policies relating to security updates has been added.
- For a user-defined judgment item with the judgment condition **Do not match**, you can now set more than one judgment condition relating to the same property, enabling judgment of such aspects as whether the client is running a power-saving CPU.
- When using the feature to automatically update judgment policies relating to anti-virus products, a grace period can now be set to impose a delay between the acquisition of the latest information about the anti-virus product and the automatic update of the judgment policy definition.
- Security level judgment can now be skipped for clients whose inventory information has not been updated since the last time their security level was judged.
- Windows Server 2008 has been added as an operating system that supports JP1/

CSC. Accordingly, Network Policy Server has been added as a required program for an authentication server using IEEE 802.1X authentication. Also, Windows Server Failover Cluster has been added as cluster software that can be used to run JP1/CSC in a cluster system.

- Windows 2000 has been removed from the list of operating systems that support JP1/CSC - Manager and JP1/CSC - Agent.
- Windows Vista has been added as an operating system that supports JP1/CSC - Manager Remote Option.
- JP1/Software Distribution Manager (relay manager) has been added to the judgment items for mandatory software.
- Products by F-Secure and Microsoft have been added to the antivirus products for which judgment policies can be updated to the latest definitions.
- Version 08-51 has been added to the supported versions of JP1/Software Distribution Client.
- The operation history of JP1/CSC can now be output as audit log information.
- When including judgment results for PCs in a notification message, you can specify whether to display the judgment results at the beginning or end of the message.
- The `cscstorecount` command for storing statistics in the management database about the status of security measures for groups has been added.
- When the number of assets judged to be at a particular security level exceeds 3,000, the list of PCs at that security level is split over multiple emails.
- Windows Server 2008 has been added as an operating system that can be subjected to judgment and action policies.
- The `cscexportcount` command for outputting statistics for specified groups to a CSV file from a variety of perspectives has been added.
- The following messages have been added to the JP1/CSC - Manager messages:  
KDSL0118-W, KDSL0119-W, KDSL0120-W, KDSL0527-W, KDSL0614-W,  
KDSL0615-W, KDSL0800-E, KDSL0801-E, KDSL0802-E, KDSL1300-I,  
KDSL1301-E, KDSL1302-E, KDSL1303-E, KDSL1304-E, KDSL1305-E,  
KDSL1310-E, KDSL1350-I, KDSL1351-E, KDSL1352-E, KDSL1353-E,  
KDSL1354-E, KDSL1355-E, KDSL1356-W, KDSL1357-E, KDSL1358-W,  
KDSL1359-E, KDSL1370-E, KDSL1450-I, KDSL1451-E, KDSL1452-E,  
KDSL1453-E, KDSL1454-E, KDSL1455-E, KDSL1456-E, KDSL1457-E,  
KDSL1458-E, KDSL1459-E, KDSL1460-E, KDSL1461-E, KDSL1462-E,  
KDSL1463-E, KDSL1464-E, KDSL1465-I, KDSL1466-I, KDSL1467-E,  
KDSL1468-W, KDSL1469-E, KDSL3030-E, KDSL3031-E

- The following messages have been added to the JP1/CSC - Manager Remote Option messages:  
KDSL3224-I, KDSL3225-I, KDSL3226-E, KDSL3400-E, KDSL3401-E, KDSL3402-E
- The following messages have been added to the JP1/CSC - Agent messages:  
KDSL5300-E, KDSL5301-E, KDSL5302-E, KDSL5303-E, KDSL5304-E, KDSL6006-E, KDSL6146-E, KDSL6147-E, KDSL6148-E
- The following message relating to JP1/CSC - Manager has been changed:  
KDSL0611-W
- The following message relating to JP1/CSC - Agent has been changed:  
KDSL6137-E
- A list of leading causes and solutions for problems that occur in the client security control system has been added.
- Estimations of the disk capacity required for JP1/CSC - Manager, JP1/CSC - Manager Remote Option, and JP1/CSC - Agent have been changed.

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

- The `cscexportplist` command that outputs PC list information (asset information and judgment results for clients) to a CSV file has been added.
- The `cscaction` command that implements actions for specified clients has been added. An item (**Action execution**) that specifies whether or not to skip the action during security level judgment has been added in the JP1/CSC - Manager Setup window.
- The description of using a quarantine system linked to JP1/Software Distribution (AMT Linkage facility) has been added.
- The following products from McAfee have been added to the anti-virus products that can automatically update the judgment policies to the latest definitions.
  - McAfee VirusScan Enterprise 8.5i(32bit)
  - McAfee VirusScan Enterprise 8.5i(64bit)
- Version 08-10 has been added to the versions of JP1/Software Distribution Client that support the functionality.
- HTML format has been added as the format of a message to be sent to a client.
- The method of setting up Asset Information Manager Subset Component of JP1/Software Distribution Manager has been changed.
- The method of setting up Asset Information Manager has been changed.

- An item (**Customize judgment results**) has been added in the Client Security Control - Manager Setup dialog box. This item specifies the security level that is used if the specified patch information is not found in the list of installed software or unapplied patch information during security update judgment.
- An item (**Message notification information**) has been added in the Client Security Control - Manager Setup dialog box. This item specifies whether or not to include Safe and Not applicable in the judgment results displayed in the message.
- Operability of the Policy Management window has been improved as follows:
  - Double-clicking an item in a list opens the window corresponding to the item.
  - Multiple items in a list can be selected and deleted.
  - During import of definition information, import is canceled if the file to be imported contains no information (empty file).
  - During export of definition information, the **Export** button is disabled if the definition has not been registered in the dialog box for setting the policies.
  - Scroll bars have been provided on the right of the **Text of notification email** and **Body text of notification message** list boxes for an action policy.
- Samples of definition files for judgment policies and action policies have been provided.
- Characters representing a product name can now be entered in the definition of security updates (patch information) for a judgment policy. An item (**Comparison condition**) has been added to the setting items.
- **Product name for mandatory security updates** and **Comparison condition** have been added to the items in the definition file for mandatory security updates for the judgment policy definition file. 99 (Other products) has been added to the values that can be set in the list of products.
- A product name definition file for registering a product name in the combo box has been added.
- **All** has been added to the selection of service packs in the definition of security updates for a judgment policy.
- 100 (all) has been added to the list of service packs used for the judgment policy definition file.
- An item for the comparison condition of software names has been added in the prohibited software definition for a judgment policy.
- An item (**Comparison condition**) has been added to the judgment policy definition file.

- The **Import** and **Export** buttons have been added in the Setting for mail address dialog box so that the email addresses of the administrator can be added from a CSV file.
- A mail address definition file used for defining the email address of the administrator has been added.
- Sample files of mail address definition files have been added.
- The following OS types have been added in the setting values used in each judgment policy definition file.
  - Windows Vista Enterprise
  - Windows Vista Ultimate
  - Windows Vista
- The following messages have been added to the JP1/CSC - Manage messages.  
KDSL0117-W, KDSL0578-E, KDSL0750-I, KDSL0751-I, KDSL0752-I, KDSL0753-W, KDSL0754-E, KDSL0755-E, KDSL0756-W, KDSL0757-W, KDSL0758-W, KDSL0760-E, KDSL1200-I, KDSL1201-E, KDSL1202-E, KDSL1203-E, KDSL1204-E, KDSL1205-W, KDSL1206-E, KDSL1207-E, KDSL1208-E, KDSL1209-E, KDSL1210-E, KDSL1220-E, KDSL1250-I, KDSL1251-E, KDSL1252-E, KDSL1253-E, KDSL1254-E, KDSL1256-E, KDSL1257-E, KDSL1258-E, KDSL1259-W, KDSL1260-E, KDSL1261-E, KDSL1262-E, KDSL1270-E
- The following messages have been changed to the JP1/CSC - Manage messages.  
KDSL0045-W, KDSL0613-W
- The following messages have been added to the JP1/CSC - Agent messages.  
KDSL5110-E, KDSL5208-E, KDSL5209-E
- Estimation of the disk capacity required for JP1/CSC - Manager and JP1/CSC - Agent has been changed.

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

- A remote management server (JP1/CSC - Manager Remote Option) has been added for linking JP1/CSC - Manager to another system.
- Judgment policies about anti-virus products (from Trend Micro, Symantec, or McAfee) can be updated automatically to the latest definitions.
- The `cscnetctrl` command for controlling network connections when using a quarantine system has been added.
- JP1/CSC - Agent can now be used on a cluster system.
- The network control product NetMonitor, linked to JP1/CSC when configuring



and operating a quarantine system, has been changed to JP1/NM.

- Asset Information Manager Subset Component of JP1/Software Distribution Manager can now be used to configure and operate a management server. The job categories in AIM that can be executed by a CSC administrator have also been changed.
- Administrators can define user-specific asset information (user definitions) in a judgment policy.
- Administrators can define user-defined actions (implemented by user-specified command) in an action policy.
- Windows have been added for customizing the email sent to the administrator and the message sent to the client when an action execution condition is set and the client's security level is judged *Safe*.
- An option (**Execute the action when the security level changes**) has been added to enable execution of a specified action only when the security level changes to *Safe* from another security level. Items for customizing **Mail notification (execution conditions)** and **Message notification (execution conditions)** have been added to the Edit Action Policy window.
- When a client is removed from the network, its network connections can now be denied automatically.
- A quarantine system can be configured and operated by linking JP1/CSC to a network control product (JP1/NM or an IEEE 802.1X authentication server).
- WUA is now supported by JP1/Software Distribution Client as a tool for detecting unapplied Windows security updates. WUA has been added as an optional client product.
- Administrators can now define multiple judgment policies and action policies.
- Administrators can now specify a number of consecutive days or a number of consecutive times as an action execution condition in an action policy. An item for setting the consecutive days/times count method has been added to the Client Security Control - Manager Setup dialog box.
- Judgment policies and action policies can now be assigned to clients.
- A Manage Judgment Policy dialog box has been added for managing judgment policies.
- Judgment item names are now displayed in the title bar of the Edit Judgment Policy window.
- An item for determining whether JP1/Software Distribution SubManager is installed has been added to the judgment items for mandatory software.
- A Manage Action Policy dialog box for managing action policies has been added.

- Windows have been added for customizing the email sent to the administrator and the message sent to the client when an action execution condition has been set.
- Display conditions can be set for the clients listed in the PC list tree view of the Policy Management main window.
- The `cscassign` command for assigning judgment policies and action policies to clients has been added.
- A new option (`-k`) option has been added to the security level judgment command (`cscjudge`) to enable clients in a particular group to be specified as judgment targets.
- The `cscexport` command for exporting a connection control list when using a quarantine system has been added.
- The `cscrdelete` command for deleting specified client information from a connection control list when using a quarantine system has been added.
- The `cscimport` command for importing a connection control list when using a quarantine system has been added.
- A chapter describing the definition files used in running a client security control system has been added.

The following definition files have been added:

- Asset number file
- Search condition file
- Policy assignment definition file
- Import file
- MAC address list file
- The following files have been added as definition files:
  - Policy import file for anti-virus products
  - Policy import execution file (manual)
- The following JP1/CSC - Manager messages have been added:

KDSL0043-E, KDSL0047-W, KDSL0116-W, KDSL0157-E, KDSL0166-I, KDSL0167-I, KDSL0526-E, KDSL0562-W, KDSL0577-E, KDSL0611-W, KDSL0612-W, KDSL0613-W, KDSL0680-I, KDSL0681-I, KDSL0682-E, KDSL0683-E, KDSL0684-E, KDSL0685-E, KDSL0686-E, KDSL0687-E, KDSL0107-E, KDSL1057-E, KDSL1058-E, KDSL1059-W, KDSL1060-E, KDSL1080-I, KDSL1081-E, KDSL1082-E, KDSL1083-E, KDSL1084-E, KDSL1085-E, KDSL1086-E, KDSL1087-E, KDSL1088-W, KDSL1089-E, KDSL1090-E, KDSL1091-E, KDSL1110-I, KDSL1111-E, KDSL1112-E,

KDSL1113-E, KDSL1114-E, KDSL1115-E, KDSL1116-E, KDSL1117-W, KDSL1118-W, KDSL1119-W, KDSL1120-E, KDSL2030-I, KDSL2031-E, KDSL2032-I, KDSL2033-E, KDSL2040-E, KDSL2042-I, KDSL2043-E, KDSL2044-E, KDSL2045-I, KDSL2046-I

KDSL3001-I, KDSL3002-E, KDSL3003-E, KDSL3004-E, KDSL3005-W, KDSL3006-E, KDSL3007-E, KDSL3008-W, KDSL3009-E, KDSL3010-E, KDSL3011-E, KDSL3012-W, KDSL3013-I, KDSL3014-W, KDSL3015-E, KDSL3016-E, KDSL3017-E, KDSL3018-I, KDSL3019-E, KDSL3020-E, KDSL3021-E, KDSL3022-W

- Messages about JP1/CSC - Manager Remote Option (messages 3200 to 3400) have been added.
- The following JP1/CSC - Manager messages have been changed:  
KDSL0112-W, KDSL0113-W, KDSL2033-E, and KDSL0510-I
- Messages about using a quarantine system (messages 6000 to 6200) have been added to the JP1/CSC - Agent messages.
- Error messages displayed in the User Definition Details window have been added to the messages displayed in the PC Security Level Details window.
- The installation folder path for JP1/CSC - Manager and JP1/CSC - Agent has been added for Windows Server 2003 (x64).
- An explanation about estimating the disk capacity required by JP1/CSC - Manager Remote Option has been added.
- An explanation about estimating the disk capacity required by JP1/CSC - Manager and JP1/CSC - Agent has been added.
- The manual has been reorganized as shown in the following table.

3020-3-G25-10(E)	3020-3-L31(E)
--	Part 1. Overview
1. Overview	1. Overview
--	Part 2. Functionality
--	2. Client Security Control System Functionality
--	3. Client Security Control System Configuration
--	Part 3. System Design and Setup
2. Considerations for Installing and Operating a Client Security Control System	4. Considerations for Installing and Operating a Client Security Control System

<b>3020-3-G25-10(E)</b>	<b>3020-3-L31(E)</b>
3. Installation and Setup	5. Installation and Setup
4. Managing Security Policies	6. Managing Security Policies
--	Part 4. System Operation
5. Managing Inventory Information	7. Managing Inventory Information
6. Monitoring Clients	8. Monitoring Clients
7. Dealing with Security Risks	9. Dealing with Security Risks
8. Auditing Security	10. Auditing Security
--	11. Linking to JP1/IM <sup>#</sup>
--	Part 5. Quarantine Systems
9. Linking to NetMonitor	12. Overview of Quarantine Systems
10. Using the Quarantine System	13. Setting Up a Quarantine System
	14. Operating a Quarantine System
11. Linking to Other JP1 Products	--
--	Part 6. Reference
12. Commands	15. Commands
--	16. Definition Files
13. Messages	17. Messages
14. Troubleshooting	18. Troubleshooting
Appendixes	Appendixes

## Legend:

--: No corresponding part or chapter.

#

Chapter 11 in 3020-3-G25-10(E) was renamed as Chapter 9 in 3020-3-L31(E).

---

## H. Glossary

---

**action execution condition**

A condition for implementing an action. The condition may be either a consecutive number of days or a consecutive number of times. When an action execution condition is set for a security level, the action is implemented when that security level is unchanged in successive judgments for the specified number of days or times.

**action policy**

A policy to implement an action based on a client security level. An administrator can use the Edit Action Policy window to set action policies. Based on the security level, warning messages can be sent to client users, and client network connections can be denied.

**administrator**

A CSC administrator responsible for client security management or an Asset Information Manager administrator who manages asset information.

**AMT Linkage facility**

*See JP1/Software Distribution (AMT Linkage facility).*

**anti-virus product**

A product that guards PCs from viruses, restoring files infected with viruses and recovering computers to their state before infection. The anti-virus products managed by a client security control system are those supported by JP1/Software Distribution.

**asset information**

Information for managing hardware and software in a company.

**Asset Information Manager**

A program that centrally manages IT assets such as hardware information and software information, in the asset management database. The client inventory information collected by JP1/Software Distribution is managed in the asset management database.

**Asset Information Manager Subset Component of JP1/Software Distribution Manager**

A component of JP1/Software Distribution Manager, providing centralized management of IT assets such as hardware information and software information in an asset management database. The client inventory information collected by JP1/Software Distribution is managed in the asset management database.

**asset management database**

The database in which asset information is stored. This database is managed by AIM.

**asset number**

A number used to identify each asset. This is chosen by the user. On a client security control system, this number is the basic unit for client management.

**asset number file**

A file containing asset numbers for clients whose security levels are to be judged. This is used when the security level judgment command is executed.

**audit log**

A log that is output as part of an audit trail of internal controls. An audit log includes information about who executed what operation, at what time. The information can be used to review and evaluate the internal controls of the system.

**authentication server**

A server required for authenticating clients; also called a RADIUS server. An authentication server uses either IEEE 802.1X authentication, which authenticates a user based on a user ID and a password, or MAC authentication, which authenticates a client based on a MAC address.

When a quarantine system is linked to an authentication server, the authentication server both authenticates clients and instructs the switch to control network connections from clients based on the connection control list.

JP1/CSC - Agent and either Microsoft IAS or Network Policy Server must be installed on the authentication server.

**client**

A PC that is connected to the network and managed by the client security control system.

**client security control system**

A system for managing client security measures, realized by the programs JP1/CSC, AIM, and JP1/Software Distribution. A client security control system can be used to manage client asset information, monitor clients, and deal with security risks.

**Client Security Management window**

The Web browser interface for monitoring clients and registering permitted PCs. The Client Security Management window is opened from the initial window of AIM.

**cluster system**

A cluster system is one that consists of multiple linked server systems running as one, to facilitate continued operation when a failure occurs. When a failure occurs on the

server performing operations (active), processing can be carried over to a standby server (standby). Note that *cluster system* can also refer to load distribution functionality via parallel processing, but in this manual, it refers to functionality to prevent interruption in operations via system switching.

**connection control list**

A list of network connection control actions performed by JP1/CSC - Manager in a quarantine system linked to an authentication server. Client access to the network is controlled according to this list.

The connection control list is managed by JP1/CSC - Agent. It contains registered information about client network connections (permitted or denied), MAC addresses, and IP addresses.

**CSC administrator**

A user with the administrator role for JP1/CSC. CSC administrators can perform tasks such as monitoring clients in the Client Security Management window of AIM, and setting security policies in the JP1/CSC Security Policy Management window.

**CSC user**

A user with the user role for JP1/CSC. CSC users can use some of the functionality provided by the Client Security Management window of AIM.

**Customize Job windows**

Functionality to control the processing that can be executed from each operation window, according to the user role. The elements in each operation window (buttons, search conditions, and editable items) depend on the user role.

**excluded user definition file**

A file containing user accounts that are to be excluded from the password-related judgment in the PC security settings.

**export file**

An output file used when exporting a connection control list by the `cscexport` command.

Export files are text files in CSV format.

**form**

This refers to the content (settings for showing/hiding button and search conditions) of the settings customized for each operation window of the Job window. Forms are set in each operation window, and multiple settings can be performed for one operation window.

## **group**

Asset information managed by AIM.

In the Policy Management main window in JP1/CSC - Manager, the group tree view in the left pane shows the hierarchy of groups in which clients are managed.

## **IEEE 802.1X**

A standard that defines the user authentication protocol on a network. Users connecting to the network are checked by user ID or password to determine whether they are legitimate users, and only authenticated users are permitted access. Authentication requires an IEEE 802.1X-compliant network device (switch, for example), a RADIUS server (authentication server), and supplicant.

## **import file**

A text file in CSV format, used when importing a connection control list by the `cscimport` command.

## **inventory information**

Information needed for client management, such as the hardware usage for the client and types of software installed on the client. Inventory information is collected by JP1/Software Distribution, and is managed in an asset management database by AIM.

## **IT assets**

This refers to the hardware information and software information about the IT devices, software, and network environment for the various PCs in the company.

## **JP1/Base**

A program that provides the event service. This controls the start order for services, and sends and receives JP1 events. JP1/Base is a prerequisite product for JP1/IM.

## **JP1/CSC - Agent**

A program that receives instructions from JP1/CSC - Manager when client network control is performed, and directs actions to the linked network control product.

## **JP1/CSC - Manager**

A program for managing client security. It judges client security levels according to previously defined judgment policies, based on inventory information in the asset management database. As a result of the judgment, actions are implemented according to the security level.

## **JP1/CSC - Manager Remote Option**

A program that supports client security management in the remote environment when the JP1/CSC system is configured with a remote management server linked to a remote system, such as a model system for anti-virus products. This program also links with



anti-virus products installed on the remote management server to automatically update judgment policies and control network connections from another system.

### **JP1/IM**

A program that provides integrated monitoring of distributed systems. JP1/IM links to JP1/CSC, to notify administrators of JP1 events occurring on a client security control system, and to provide a platform for operations to understand and investigate problem areas.

### **JP1/NM**

A program that monitors and manages client network connections. JP1/NM consists of JP1/NM - Manager, which provides integrated management of network connection control, and JP1/NM, which monitors clients on a subnetwork basis.

### **JP1/Software Distribution - Asset Information Manager Subset Component of JP1/Software Distribution Manager**

*See Asset Information Manager Subset Component of JP1/Software Distribution Manager.*

### **JP1/Software Distribution (AMT Linkage facility)**

A JP1/Software Distribution facility that, when a computer compatible with AMT is used as a client, uses the AMT packet control functionality to control client connections to the network.

### **JP1/Software Distribution Client**

A program that collects client inventory information, and sends it to JP1/Software Distribution Manager.

### **JP1/Software Distribution Manager**

A program that uses a network to distribute software and manage clients by means of batch processes. It manages client inventory information collected from JP1/Software Distribution Client.

### **JP1/Software Distribution Manager (relay manager)**

A program for assisting with remote installation and setup in a large-scale network or in a configuration with numerous clients. This product works as a relay system for JP1/Software Distribution Manager.

### **JP1/Software Distribution SubManager**

A program that relays remote installations, to perform setup on large-scale networks, and when numerous clients exist.

### **JP1 event**

Information sent to JP1/Base when a client security level changes on a client security

control system. JP1 events are managed by the JP1/Base event service.

### **judgment item**

An item to judge a client security level, such as the application status of client security updates and installation of anti-virus products. An administrator sets a judgment policy for each judgment item.

The following types of judgment items exist:

- Security update
- Anti-virus product
- Prohibited software
- Mandatory software
- PC security settings
- User definition

### **judgment policy**

A policy to judge a client security level. An administrator edits judgment policies in the Edit Judgment Policy window or by using the judgment policy update command (`cscpolimport`).

### **judgment policy information file**

A text file used for importing judgment policies by using the `cscpolimport` command. When the `cscpolexport` command is executed, an export file that has the same format as this file is output.

### **MAC address list file**

A file used to delete information about multiple clients from a connection control list in JP1/CSC - Agent. Deletion is performed as a batch operation using the asset deletion command (`cscrdelete`). The MAC address list file contains the MAC addresses of the clients whose information is to be deleted.

### **management server**

A server that manages client inventory information and client security measures. JP1/CSC - Manager, AIM, and JP1/Software Distribution Manager are installed on the management server.

### **mandatory software**

Software that is required to be installed on a client.

### **MBSA**

A Microsoft tool to implement security audits for Windows products. It can manage Windows security updates (patches and service packs) not applied to a client.

**Microsoft Internet Authentication Service**

The Internet authentication service provided in Windows Server 2003 as a standard component for authenticating clients. When a quarantine system linked to an authentication server is set up, this product is required on the authentication server.

**monitoring server**

A server configured when running a quarantine system linked with JP1/NM.

The monitoring server controls client network connections based on instructions from the management server.

**NetMonitor**

A program to monitor and manage client network connections. This consists of NetMonitor/Manager, which provides integrated management of network connection control, and NetMonitor, which monitors clients on each sub-network.

**network control product**

A product that links to JP1/CSC - Agent, providing functionality to refuse or permit client network connections.

**network control server**

This is set up to control client network connections. JP1/CSC - Agent and a network control product are installed on a network control server.

**Network Policy Server**

The network policy server provided in Windows Server 2008 as a standard component for authenticating clients. When a quarantine system linked to an authentication server is set up, this product is required on the authentication server.

**non-Software Distribution host**

This refers to a device on a network, on which JP1/Software Distribution has not been installed.

**number of consecutive days**

An action execution condition. The set action is implemented when the security level is unchanged in successive judgments for the specified number of days. This value can be set separately for each action.

**number of consecutive times**

An action execution condition. The set action is implemented when the client's security level is unchanged in successive judgments for the specified number of times. This value can be set separately for each action.

**patch information file**

A file containing information used to acquire patches from Microsoft's servers. This file is required to automatically update judgment policies relating to security updates. Patch information files are collected by Job Management Partner 1/Software Distribution, and updated to reflect the patches being offered by Microsoft.

**policy assignment definition file**

A file used when executing the policy assignment command (`cscassign`). The recipients and names of the policies to be assigned are defined in this file.

**Policy Management window**

A generic name for the windows and dialog boxes for managing security policies.

**prohibited software**

Software that is not used for company operations, or may expose clients and networks to risk when installed.

**quarantine system**

A system that permits clients previously disconnected from the network due to a high security risk level to be reconnected to the network after the latest security measures are implemented.

**quarantined network**

A network (VLAN) in which security measures are implemented on clients when JP1/CSC - Agent is linked to an authentication server in a dynamic VLAN environment. The quarantined network is set up with a switch that supports IEEE 802.1X authentication.

Clients without adequate security can be connected to the quarantined network, enabling security measures to be implemented online.

**RADIUS server**

A server required for authenticating clients when IEEE 802.1X or MAC authentication is used.

This server is required when a quarantine system is linked to an authentication server.

In this manual, a RADIUS server is called an authentication server.

**remote installation**

Functionality to transfer and install packaged software from JP1/Software Distribution Manager to a client.

**remote management server**

A system that supports judgment policy management and client security measures on

a management server when JP1/CSC is linked with a remote system, such as a model system for anti-virus products. JP1/CSC - Manager Remote Option must be installed on the remote management server.

**search condition file**

A file used in the -k option of the security level judgment command (`cscjudge`), action command (`cscaction`), PC list information output command (`cscexportplist`), and statistics output command (`cscexportcount`) to specify a target group for command execution. The file defines the name of the group to which the command applies.

**search host**

Functionality to detect devices connected to the network from JP1/Software Distribution Manager, and to collect host information.

**security level**

A level that indicates the risk of client security measures. Security levels are set in the Edit Judgment Policy window. The following types of security level exist:

- **Danger**
- **Warning**
- **Caution**
- **Safe**

**security policy**

A generic name for judgment policies and action policies. These are rules that set judgment and action conditions for client security levels.

**Security Policy Management windows**

A generic name for the Policy Management window, Edit Judgment Policy window and Edit Action Policy window.

**security update**

A program to strengthen functionality and correct bugs in an OS or application. This term applies to patch and service pack information.

**statistics**

Information that summarizes the status of security measures over time for individual groups. Using the Client Security Management window, an administrator can monitor trends in the status of security measures for each group in the form of evaluation points, countermeasure usage, and other information.

**supplicant**

Software required on the client in order to authenticate users by using IEEE 802.1x authentication. This software is required when using a quarantine system that is linked to an authentication server by using IEEE 802.1x authentication.

JP1/CSC supports only a supplicant installed in Windows as standard. The Windows standard supplicant is installed in Windows 2000 (SP4 or later), Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, and Windows 7.

**treatment server**

A server required for setting up a quarantine system linked to JP1/Network Monitor or an authentication server.

A treatment server maintains communication with clients that have been disconnected from the network because they pose a security risk. This allows security measures to be implemented on the clients in an online environment.

**unauthenticated network**

A network required for implementing security measures on clients when JP1/CSC - Agent is linked to an authentication server in a static VLAN environment. Connection to the unauthenticated network is controlled by a switch that supports either IEEE 802.1X or MAC authentication.

Clients for which security measures have not been fully implemented are first connected to the unauthenticated network, where the needed security measures can be implemented online.

**WUA**

A Microsoft tool for implementing security audits on Windows products. WUA can be used to manage Windows security updates (patches and service packs) that have not been applied on the client. In addition to OS security updates, WUA can manage software security updates for Microsoft Office and other applications.

---

# Index

---

## A

- abbreviations for products iii
- access list settings
  - authentication server linkage 561
- acronyms vi
- action 7
  - execution condition (glossary) 1035
  - user definition 449
- action execution 144
- action implementation 40
  - by network control command (cscnetctrl) 56
- action implementation method 438
  - by administrator 438
  - by security level judgment results 438
- action implementing 54
- action items tree view 337
- action messages
  - displayed when you disable security management 955
  - displayed when you enable security management 955
  - displayed when you judge security level 953
  - displayed when you output judgment and action history to CSV file 956
  - displayed when you permit network connection 954
  - displayed when you reject network connection 954
  - displayed when you send warning message 953
  - in PC List window 952
- action policy 43, 198, 1035
  - assigning 376
  - consideration 111
  - copying 340
  - creating 334
  - default policy 332
  - deleting 339
  - functionality 48
  - initial policy 333
  - managing 332
  - renaming 339
- action types 439
- active server 996, 1004
- active-standby configuration 989
- Add Agent Information window 150
- Add Remote Option Information window 152
- adding
  - anti-virus product information 250
  - detailed mandatory software information 275
  - information about excluded security update 221
  - mandatory software information 274
  - patch information 229
  - prohibited software information 264
  - service pack information 238
- adding to network
  - new client (JP1/NM linkage) 595
  - new client (JP1/Software Distribution (AMT Linkage facility) linkage) 655
- administrator 1035
- administrator notification email
  - editing 353
- agent communication environment information
  - authentication server linkage 552
  - JP1/NM linkage 537
  - JP1/Software Distribution linkage (AMT linkage facility) 575
- agent log 808
- agent log file 976
- Agent tab 141
- all job categories 175
- AMT Linkage facility 1035
  - setting up for quarantine system linked to 130
- anti-virus product 41, 43, 97, 146, 1035
  - adding information 250
  - automatic update of judgment policies 46
  - changing information 252

- deleting information 253
  - editing judgment policy 247
  - exporting information 255
  - importing information 254
  - policy import file 260, 777
  - remote management server 94
  - updating security policies automatically (features) 12
- Anti-Virus Products Details window 416
- Anti-Virus Products page 166
- Anti-Virus Products tab 163
- asset information 1035
  - file 737
  - user-specific 41
- Asset Information Manager 77, 1035
  - installing 133
  - setting up 133
- Asset Information Manager Subset Component of JP1/Software Distribution Manager 77
  - glossary 1035
- asset management database 41, 1036
- asset number 412, 1036
  - file 678, 731, 1036
- assigning
  - jobs that CSC user can use 183
- assigning to clients
  - security policy 119
- at addition of asset information 143
- at update of asset information 143
- audit log 147, 166, 808
  - configuration for output 1024
  - glossary 1036
  - output event types 1017
  - output format 1019
  - outputting 1017
  - save format 1018
- audit log file
  - JP1/CSC - Agent 1015
  - JP1/CSC - Manager Remote Option 1014
- audit log file (authentication server linkage)
  - JP1/CSC - Agent 1016
- audit log information 147, 166, 537, 552, 576
- auditing security 451, 452
- authentication interval 557, 560
- authentication process
  - authentication server linkage (using IEEE 802.1X authentication in dynamic VLAN environment) 604
  - authentication server linkage (using MAC authentication in static VLAN environment) 619
- authentication server 78, 500
  - glossary 1036
  - quarantine system 503
  - setting up (authentication server linkage) 547
  - system configuration containing multiple 520
- authentication server linkage
  - adding new client to network 639
  - authentication server setup 547
  - command for managing connection control list 638
  - editing connection control list 638
  - fixed file (JP1/CSC - Agent) 1015
  - implementing security measures 638
  - information registered in connection control list 634
  - installing JP1/Software Distribution Client (relay system) 563
  - inter-VLAN communication settings 560
  - log file (JP1/CSC - Agent) 1015
  - managing connection control list 634
  - managing network connection histories for clients 645
  - notes on network connection control based on connection control list 637
  - operation that can be performed on Basic Settings page 550
  - operation that can be performed on IAS page 553
  - permitting network connection 567
  - quarantine system operation 603
  - quarantine system setup 545
  - removing clients after operation has started 643
  - setting security policy 567
  - setting up client 563
  - setting up environment before operation can be started 567



- setting up JP1/Software Distribution Client 563
  - setting up JP1/Software Distribution Client (relay system) 563
  - setting up treatment server 563
  - tasks during quarantine system operation 632
  - when connection control list is updated 636
- authentication server linkage (IEEE 802.1X authentication in dynamic VLAN environment)
  - isolation process 608
- authentication server linkage (MAC authentication in static VLAN environment)
  - isolation process 623
  - recovery process 626
  - treatment process 624
- authentication server linkage (using IEEE 802.1X authentication in dynamic VLAN environment)
  - authentication process 604
  - inspection process 604
- authentication server linkage (using MAC authentication in static VLAN environment)
  - authentication process 619
  - inspection process 619
- authentication server linkage in dynamic VLAN environment
  - example of operating quarantine system (IEEE 802.1X authentication) 603
- authentication server linkage in static VLAN environment
  - example of operating quarantine system (MAC authentication) 618
- automatic logon 293
- automatic policy update 167
  - information 167
- automatic update (judgment policies for anti-virus products) 46
  - grace period 46
- automatic update (judgment policies for security updates) 44
- Automatic updates for anti-virus products page 153
- Automatic updates for anti-virus products tab 141
- automatically obtaining
  - client inventory information 392
  - inventory information 389

- inventory information from JP1/Software Distribution Manager, setup 131, 133
- automatically reporting
  - inventory information to AIM 130

## B

- backup and restoration 972
- basic configuration
  - authentication server linkage 515
  - JP1/NM linkage 509
  - JP1/Software Distribution (AMT Linkage facility) linkage 524
  - system configuration 64
- Basic Settings page
  - items that can be displayed and set (authentication server linkage) 551
  - items that can be displayed and set (JP1/Network Monitor linkage) 536
  - operation (authentication server linkage) 550
  - operation (JP1/Network Monitor linkage) 535
  - use with JP1/CSC - Manager Remote Option 164
- Basic Settings tab 140
  - JP1/CSC - Manager Remote Option 163

## C

- caution 52
- changing
  - anti-virus product information 252
  - detailed mandatory software information 276
  - information about excluded security update 222
  - mandatory software information 278
  - patch information 233
  - prohibited software information 265
  - service pack information 240
- checking
  - countermeasure usage for each judgment item 478
  - detailed information for anti-virus product 416
  - detailed information for client 412

- detailed information for mandatory software 420
  - detailed information for PC security settings 422
  - detailed information for prohibited software 418
  - detailed information for security update 413
  - detailed information for user definition 424
  - device details for client 426
  - history of judgments and actions for client 426
- class list
  - for user-defined judgments 318
- client 66, 71, 1036
  - adding to network (authentication server linkage) 639
  - assigning security policies 49
  - denying network connection (usage example) 18
  - distributing security update programs and definition files (usage example) 20
  - implementing security measures (authentication server linkage) 638
  - implementing security measures (JP1/NM linkage) 593
  - implementing security measures (JP1/Software Distribution (AMT Linkage facility) linkage) 655
  - judging security levels (features) 6
  - listing (usage example) 22
  - managing network connection histories (authentication server linkage) 645
  - prerequisite programs 81
  - searching for 402
  - security audit (features) 8
  - setting up 95
  - setting up (authentication server linkage) 563
  - setting up (JP1/NM linkage) 541
  - viewing history of judgments and actions (usage example) 23
  - warning message notification (usage example) 16
- client inventory information
  - automatically obtaining 392
- client network connections
  - controlling 445
- Client Security Control - Agent Setup dialog box
  - items that can be set (authentication server linkage) 549
  - settings (JP1/Software Distribution (AMT Linkage facility) linkage) 575
- Client Security Control - Manager Remote Option Setup dialog box 162
- Client Security Control - Manager Setup dialog box 139
- client security control system 2, 1036
  - configuration 63
  - lifecycle 122
  - overall configuration 38
  - overview 2
  - typical uses 16
- client security level
  - judging 431
- client security level management 40
- Client Security Management window 58, 175, 1036
  - implementing actions 55
  - list of messages 952
  - network connection control 445
- client user notification message
  - editing 362
- client's history of judgments and actions as CSV file
  - outputting 430
- cluster environment 145
- cluster information 145
  - authentication server linkage 552
  - JP1/NM linkage 537
  - JP1/Software Distribution linkage (AMT linkage facility) 575
- cluster software 989
- cluster system 1036
  - configuration 990
  - new installation and setup of JP1/CSC - Agent 1001
  - new installation and setup of JP1/CSC - Manager 993
  - operating on 90
  - overview 989

- overwrite installation of JP1/CSC - Agent 1005
  - overwrite installation of JP1/CSC - Manager 997
  - uninstalling JP1/CSC - Agent 1006
- command for deleting client information from connection control list 695
- commands 659
  - assigning security policies to clients 667
  - controlling network connections 681
  - cscaction 664
  - cscassign 192, 667
  - cscexportcount 669
  - cscexportplist 674
  - cscjudge 192
  - cscjudge (judges security levels) 678
  - cscnetctrl 56, 446, 681
  - cscnwmaintenance 684
  - cscpatchupdate 192, 686
  - cscpollexport 690
  - cscpolimport 692
  - cscrdelete 695
  - cscrexport 697
  - cscrimport 699
  - cscsetup (sets up JP1/CSC - Manager) 700
  - cscstorecount 192, 701
  - deleting specified client from connection control list 695
  - detail 662
  - directory 662
  - exporting connection control list 697
  - exporting judgment policies 690
  - for executing user-defined action 703
  - implementing actions for specified client 664
  - importing connection control list 699
  - list 660
  - maintaining list of permitted devices 684
  - network connection control 446
  - outputting PC list information 674
  - outputting statistics relating to security measure statuses 669
  - storing statistics on status of security measures 701
  - updating judgment policies 260
  - updating judgment policy settings 692
  - updating patch information for judgment policies relating to security updates 686
- configuration
  - quarantine system 88
- connection control list
  - command for exporting 697
  - command for importing 699
  - editing (authentication server linkage) 638
  - file (authentication server linkage) 1015
  - glossary 1037
  - information registered in connection control list (authentication server linkage) 634
  - management command (authentication server linkage) 638
  - managing (authentication server linkage) 634
  - notes on network connection control (authentication server linkage) 637
  - when connection control list is updated (authentication server linkage) 636
- connection history file (authentication server linkage) 1015
- connection information for refused asset 555
- connection information for unregistered asset 555
- controlling
  - client network connections 445
  - network connection 446
- conventions
  - abbreviations for products iii
  - acronyms vi
  - diagrams vii
  - fonts and symbols viii
  - KB, MB, GB and TB ix
  - version numbers x
- countermeasure usage 10
  - formula for calculating 469
- countermeasure usage for each judgment item
  - checking 478
- counting consecutive days and times 350
- creating
  - CSC user 179
- CSC administrator 1037
  - role 176
  - user 179

CSC administrators and CSC users  
     creating 174  
 CSC user 1037  
     creating 179  
     creating new user role 181  
     registering 187  
 cscanetcon.exe 988  
 cscassign command 192, 667  
 cscexportcount command 669  
 cscjudge command 192  
 cscmaccept.exe 988  
 cscmpolimport.dat file 259  
 cscmrssvc.exe 988  
 cscmrsvs.exe process 988  
 cscmsvc.exe 988  
 cscnetctrl command 681  
 cscpatchupdate command 192, 686  
 cscrdelete command 695  
 cscexport command 697  
 cscimport command 699  
 CSCSendMessage folder 373  
 cscstorecount command 192, 701  
 CSV output  
     statistics 480  
     statistics for specific groups 480  
     statistics for specific judgment items 483  
 CSV Output window 454  
 customize 337  
 Customize Job windows 1037  
 Customize Job Windows window 189  
 customize judgment results (anti-virus products) 144  
 customize judgment results (security updates) 144

## D

danger 52  
 data for resolving problems  
     AIM 968  
     JP1/CSC - Agent 968  
     JP1/CSC - Manager 967  
     JP1/CSC - Manager Remote Option 967  
     JP1/Software Distribution 968  
 data that must be collected if problem occurs 967  
 days since password was updated 291  
 default policy

    action policy 332  
     judgment policy 205  
 defining  
     patch information 228  
     service pack information 236  
 definition file 705  
     anti-virus products 720  
     excluded security updates 715  
     list of sample files 977  
     mandatory security updates 716  
     mandatory service packs 718  
     mandatory software 723  
     prohibited software 722  
 definition file of MAC addresses not subject to  
 deletion 803  
 definition information 967, 968  
     JP1/CSC - Manager Remote Option 968  
 deleting  
     anti-virus product information 253  
     asset information 146  
     detailed mandatory software information 277  
     information about excluded security  
     update 224  
     mandatory software information 280  
     patch information 234  
     prohibited software information 266  
     service pack information 241  
 designing  
     system configuration 86  
 detailed device information  
     preventing update processing 189  
 detailed information  
     checking for anti-virus product 416  
     checking for client 412  
     checking for mandatory software 420  
     checking for PC security settings 422  
     checking for prohibited software 418  
     checking for security update 413  
     checking for user definition 424  
 detailed mandatory software information  
     adding 275  
     changing 276  
     deleting 277  
 detecting

- non-Software Distribution clients 389, 390
  - security updates not applied to client 396
  - unapplied security updates 389
- detecting non-Software Distribution clients
  - setting up 133
- Device Details dialog box 189
- device details for client
  - checking 426
- diagram conventions vii
- dialog boxes
  - Client Security Control - Manager Remote Option Setup 162
  - Device Details 189, 426
  - Manage Action Policy 332
  - Manage Judgment Policy 205
  - Settings for Email Address 343
- disabling
  - security management 432
  - security management for client 432
- display position of judgment results 146
- displaying as graph
  - statistics 485
  - statistics for specific groups 485
  - statistics for specific judgment items 488
- Drive encryption by BitLocker 308

## E

- Edit Action Policy window 342
  - setting action for security level 342
- Edit Judgment Policy (Judgments for anti-virus products) window 247
- Edit Judgment Policy (Judgments for mandatory software) window 270
- Edit Judgment Policy (Judgments for PC security settings) window 284
- Edit Judgment Policy (Judgments for prohibited software) window 262
- Edit Judgment Policy (Judgments for security updates) window 216
- Edit Judgment Policy (Judgments for user definition) window 309
- edit view 211, 337
- editing
  - administrator notification email 353
  - anti-virus product judgment policy 247
  - client user notification message 362
  - mandatory software judgment policy 270
  - PC security setting judgment policy 284
  - prohibited software judgment policy 262
  - security update judgment policy 216
- email
  - sender address 360
  - sending to administrators 448
  - transmission unit 360
- email sender address 147
- enabling
  - security management 433
  - security management for client 432
- error messages
  - displayed in Anti-Virus Products Details window 958
  - displayed in Judgment and Action History window 962
  - displayed in Mandatory Software Details window 959
  - displayed in PC Security Level Details window 956, 957
  - displayed in PC Security Settings Details window 961
  - displayed in Prohibited Software Details window 958
  - displayed in Security Updates Details window 957
  - displayed in User Definition Details window 960
  - Statistics Details Graph Display window 964
  - Statistics Details window 964
  - Statistics Graph Display window 963
  - Statistics List window 963
- estimating
  - used disk capacity 1011
- Evaluation Condition Input window 458
- evaluation point 457
- Evaluation Result List window 461
  - error message 963
- evaluation results for each group 462
- evaluation results for each user 464
- event ID 806

## Index

event log 808  
excluded user definition file 801  
export file (glossary) 1037  
exporting  
    anti-virus product information 255  
    information about excluded security update 225  
    mandatory software information 282  
    patch information 236  
    prohibited software information 267  
    service pack information 241  
extend update time 168

## F

failover 989  
file  
    Remote Option log 976  
firewall  
    direction in which data passes through 987  
fixed file 1011, 1015  
    JP1/CSC - Agent (authentication server linkage) 1015  
    JP1/CSC - Manager Remote Option 1014  
font conventions viii  
form 1037  
format  
    of command explanation 662  
    of message 806  
    of message explanation 806  
    of output messages 806  
formula for evaluation point score 457  
functionality  
    action policy 48  
    assigning security policies to clients 49  
    judgment policy 43  
    overview 38

## G

GB meaning ix  
glossary  
    excluded user definition file 1037  
    judgment policy information file 1040  
group (glossary) 1038  
Guest account settings 287

GUI buttons that CSC users can use  
    limiting 184

## H

history information 145  
history of judgments and actions as CSV file  
    outputting 434  
history of judgments and actions for client  
    checking 426  
History of Judgments and Actions window 427

## I

IAS page  
    items that can be displayed and set (authentication server linkage) 555  
    operation (authentication server linkage) 553  
IEEE 802.1X  
    glossary 1038  
IEEE 802.1X authentication server linkage  
    recovery process 612  
    treatment process 610  
IM linkage 145, 494  
IM linkage information 145  
implementing action 54  
    according to security level (features) 7  
    after all security level judgments have been made 27  
    as result of administrator instruction 55  
    as result of security level judgment 54  
    by action command (cscaction) 57  
    by network control command (cscnetctrl) 56  
    from Client Security Management window 55  
import file 782  
    glossary 1038  
importing  
    anti-virus product information 254  
    information about excluded security update 224  
    mandatory software information 281  
    patch information 235  
    prohibited software information 267  
    service pack information 241  
information about excluded security update

- adding 221
    - changing 222
    - deleting 224
    - exporting 225
    - importing 224
  - information of IT assets 2
  - initial policy
    - action policy 333
    - judgment policy 206
  - inspection process
    - authentication server linkage (using IEEE 802.1X authentication in dynamic VLAN environment) 604
    - authentication server linkage (using MAC authentication in static VLAN environment) 619
    - JP1/Software Distribution (AMT Linkage facility) linkage 648
    - using quarantine support facility (JP1/NM linkage) 580
    - without using quarantine support facility (JP1/NM linkage) 587
  - installation and setup 126
    - JP1/CSC - Manager Remote Option 158
  - installing
    - anti-virus products link with automatic judgment policy updating 99
    - Asset Information Manager 133
    - JP1/CSC - Agent 171
    - JP1/CSC - Agent (authentication server linkage) 548
    - JP1/CSC - Agent (JP1/NM linkage) 533
    - JP1/CSC - Agent (JP1/Software Distribution (AMT Linkage facility) linkage) 573
    - JP1/CSC - Manager 135
    - JP1/CSC - Manager Remote Option 158
    - JP1/NM 540
    - JP1/NM - Manager 532
    - JP1/Software Distribution Client (relay system) 576
    - JP1/Software Distribution Client (relay system) (authentication server linkage) 563
    - JP1/Software Distribution Client (relay system) for JP1/NM linkage 541
    - JP1/Software Distribution Manager 129
    - Microsoft Internet Authentication Service (authentication server linkage) 547
    - Network Policy Server (authentication server linkage) 547
  - inter-VLAN communication settings (authentication server linkage) 558, 560
  - internal management information 967
  - inventory information 41, 1038
    - automatically obtaining 389
    - management 40
    - managing 386
    - update automatic judgment 51
  - IP address 165
    - registering with JP1/NM (non-client devices) 542
  - isolation process
    - authentication server linkage (IEEE 802.1X authentication in dynamic VLAN environment) 608
    - authentication server linkage (MAC authentication in static VLAN environment) 623
    - JP1/Software Distribution (AMT Linkage facility) linkage 650
    - using quarantine support facility (JP1/NM linkage) 582
    - without using quarantine support facility (JP1/NM linkage) 588
  - IT asset information
    - integrated management (features) 4
  - IT assets 1038
- ## J
- job menus
    - PC Security Level Management 58
    - Security Counter-Measure Evaluation 58
  - jobs that CSC user can use
    - assigning 183
  - JP1 event 494, 1039
  - JP1/Base 1038
  - JP1/CSC
    - linkage with network control products 500
  - JP1/CSC - Agent 78, 1038

- audit log file 1015
- audit log file (authentication server linkage) 1016
- connection control list file (authentication server linkage) 1015
- connection history file (authentication server linkage) 1015
- data for resolving problems 968
- fixed file (authentication server linkage) 1015
- installing 171
- installing (authentication server linkage) 548
- installing (JP1/NM linkage) 533
- installing (JP1/Software Distribution (AMT Linkage facility) linkage) 573
- JP1\_NETM\_CSCA (generic service) 1004
- list of files 976
- list of processes 988
- log file (authentication server linkage) 1015
- new installation and setup (cluster system) 1001
- overwrite installation (cluster system) 1005
- setting up 173
- setting up (authentication server linkage) 548
- setting up (JP1/NM linkage) 533
- setting up (JP1/Software Distribution (AMT Linkage facility) linkage) 573
- setting up to start automatically 173
- uninstallation (cluster system) 1006
- uninstalling 173
- used disk capacity 1015
- JP1/CSC - Agent messages
  - list 932
- JP1/CSC - Manager 77, 1038
  - data for resolving problems 967
  - installing 135
  - JP1\_NETM\_CSCM (generic service) 997
  - JP1\_NETM\_CSCM\_RS (generic service) 997
  - list of files 976
  - list of processes 988
  - manager service 988
  - new installation and setup (cluster system) 993
  - operation on cluster system 989
  - overwrite installation (cluster system) 997
  - remote service 988
  - setting up 139
  - setting up for automatic start 156
  - uninstalling 138
  - used disk capacity 1011
- JP1/CSC - Manager and remote service
  - setting up for automatic start 156
- JP1/CSC - Manager messages
  - list 829
- JP1/CSC - Manager Remote Option 77
  - audit log file 1014
  - cscmrsvcs.exe process 988
  - data for resolving problems 967
  - definition information 968
  - fixed file 1014
  - glossary 1038
  - installation and setup 158
  - installing 158
  - list of files 976
  - list of messages 921
  - list of processes 988
  - log 968
  - log file 1014
  - message output destinations 822
  - messages regarding linkage 914
  - Remote Option log file 976
  - setting up 162
  - trace information file 968
  - uninstalling 162
  - used disk capacity 1014
  - virus definition information monitoring service 988
- JP1/CSC messages
  - list 829
- JP1/IM 14, 1039
  - linkage 14, 494
- JP1/IM integrated console 494
- JP1/Network Monitor linkage
  - operation that can be performed on Basic Settings page 535
  - operation that can be performed on NM page 538
- JP1/NM 500



- glossary 1039
- installing 540
- quarantine system 501
- registering IP addresses of non-client devices 542
- setting up 540
- stopping monitoring 542
- JP1/NM - Manager
  - installing 532
  - Integrated Management window 532
  - setting up 532
- JP1/NM linkage
  - adding new clients to network 595
  - client setup 541
  - creating permitted-PC list file 597
  - environment setup 541
  - implementing security measures 593
  - inspection process (using quarantine support facility) 580
  - inspection process (without using quarantine support facility) 587
  - installing JP1/Software Distribution Client (relay system) 541
  - isolation process (using quarantine support facility) 582
  - isolation process (without using quarantine support facility) 588
  - judging security levels 544
  - monitoring server setup 540
  - network control server setup 532
  - operation with quarantine support facility 580
  - operation without quarantine support facility 580
  - permitting network connections 543
  - quarantine support facility usage 580
  - quarantine system operation 580
  - quarantine system setup 530
  - recovery process (using quarantine support facility) 585
  - recovery process (without using quarantine support facility) 591
  - registering permitted PCs 596, 598
  - removing clients after startup 600
  - setting security policies 544
  - setting up JP1/Software Distribution Client 541
  - setting up JP1/Software Distribution Client (relay system) 541
  - starting monitoring 543
  - tasks during quarantine system operation 592
  - treatment process (using quarantine support facility) 583
  - treatment process (without using quarantine support facility) 589
  - treatment server setup 540
  - windows for registering permitted PCs 596
  - without using quarantine support facility 587
- JP1/Software Distribution
  - Asset Information Manager Subset Component of JP1/Software Distribution Manager 77
  - Asset Information Manager Subset Component of JP1/Software Distribution Manager (glossary) 1039
- JP1/Software Distribution (AMT Linkage facility) 1039
  - confirming system setup 573
- JP1/Software Distribution (AMT Linkage facility) linkage
  - adding new clients to network 655
  - implementing security measures 655
  - inspection process 648
  - isolation process 650
  - judging security levels 577
  - management and network control server setup 572
  - quarantine system operation 648
  - quarantine system setup 572
  - quarantine system usage examples 648
  - recovery process 652
  - removing client after startup 655
  - setting security policy 577
  - tasks during quarantine system operation 654
  - treatment process 651
  - treatment server setup 576
- JP1/Software Distribution Client 1039
  - functionality limitations by version 95
  - installing 170

- setting up 170
    - setting up (authentication server linkage) 563
    - setting up (JP1/NM linkage) 541
  - JP1/Software Distribution Client (relay system)
    - installing (authentication server linkage) 563
    - installing (JP1/NM linkage) 541
    - installing (JP1/Software Distribution (AMT Linkage facility) linkage) 576
    - setting up (authentication server linkage) 563
    - setting up (JP1/NM linkage) 541
    - setting up (JP1/Software Distribution (AMT Linkage facility) linkage) 576
  - JP1/Software Distribution Manager 77, 1039
    - collecting MAC addresses 542
    - installing 129
    - setting up 129
  - JP1/Software Distribution Manager (relay manager)
    - glossary 1039
  - JP1/Software Distribution SubManager 1039
  - JP1\_NETM\_CSCA (generic service) 1004
  - JP1\_NETM\_CSCM (generic service) 997
  - JP1\_NETM\_CSCM\_RS (generic service) 997
  - judging
    - client security level 431
    - security levels 51
  - judgment
    - by administrator 51
    - history 1011
    - item 43, 1040
    - items tree view 216
    - performing by latest security updates 220
    - performing by specified security updates 226
  - judgment items tree view 211
  - judgment level
    - judgment result file 739
  - judgment policy 43, 198, 1040
    - assigning 374
    - automatic update (anti-virus products) 46
    - automatic update (security updates) 44, 243
    - consideration 107
    - copying 214
    - creating 207
    - default policy 205
    - definition file import destination 709
    - deleting 213
    - editing 209
    - editing judgment policy 309
    - functionality 43
    - initial policy 206
    - managing 205
    - renaming 213
    - update command 260
    - updating manually or automatically (anti-virus products) 256
  - judgment policy information file 786
  - judgment policy update command for security updates 192
  - judgment result
    - (anti-virus product) file 744
    - (mandatory software) file 747
    - (PC security settings) file 749
    - (prohibited software) file 746
    - (security updates) file 742
    - (summary) file 740
    - (user definition) file 748
- ## K
- KB meaning ix
- ## L
- lifecycle
    - client security control system 122
  - limiting
    - GUI buttons that CSC users can use 184
  - linkage
    - JP1/IM 14
    - network control product (features) 13
    - quarantine system 501
  - linked product information 168
  - list of classes 714
  - list of files 976
    - JP1/CSC - Agent 976
    - JP1/CSC - Manager 976
    - JP1/CSC - Manager Remote Option 976
  - list of messages
    - JP1/CSC - Manager Remote Option 921
  - list of OS types 710
  - list of processes 988

- JP1/CSC - Agent 988
- JP1/CSC - Manager 988
- list of products 713
- list of security levels 713
- list of service packs 713
- log 967, 968
  - JP1/CSC - Manager Remote Option 968
- log file 1011, 1015
  - JP1/CSC - Agent (authentication server linkage) 1015
  - JP1/CSC - Manager Remote Option 1014
- log file size 145, 166
- log information 145, 166
  - authentication server linkage 552
  - JP1/NM linkage 537
  - JP1/Software Distribution linkage (AMT linkage facility) 575
- logical host 145
- logical IP address 145

## M

- MAC address
  - collecting from JP1/Software Distribution Manager 542
  - list file 695, 784
  - list file (glossary) 1040
- mail address definition file 728
- mail notification information 147
- Manage Action Policy dialog box 332
- Manage Judgment Policy dialog box 205
- management and network control server
  - setting up (JP1/Network Distribution (AMT Linkage facility) linkage) 572
- management server 65, 70, 1040
  - prerequisite programs 80
  - setting up 92
- management terminal 66, 71
  - prerequisite programs 80
  - setting up 92
- manager communication environment information
  - authentication server linkage 551
- manager communication environment information 143, 165
  - JP1/NM linkage 536
  - JP1/Software Distribution linkage (AMT linkage facility) 575
- manager log 808
  - file 976
- manager service 988
- managing
  - inventory information 386
  - security policy 43
- mandatory software 43, 1040
  - adding information 274
  - changing information 278
  - deleting information 280
  - editing judgment policy 270
  - exporting information 282
  - importing information 281
- Mandatory Software Details window 420
- maximum connection time 561
- MB meaning ix
- MBSA 77, 96, 1040
- message notification information 146, 556
- message notification job
  - checking execution results 373
- message output destinations
  - JP1/CSC - Manager Remote Option 822
- messages 805
  - displayed in Register Permitted PCs window 962
  - explanation format 806
  - format 806
  - in Register Permitted PCs window 962
  - list of Client Security Management window 952
  - list of output destinations 808
  - notification by action policy 440
  - notification by administrator 440
  - output format 806
  - regarding commands 872
  - regarding execution of operations on Policy Management window 909
  - regarding JP1/CSC - Agent 932
  - regarding JP1/CSC - Manager 830
  - regarding linkage with JP1/CSC - Manager Remote Option 914
  - regarding quarantine system operation 939

- sending to client users 440
  - setup to delete results of notification message jobs 130
- method for counting number of consecutive days and times 144
- Microsoft Internet Authentication Service
  - glossary 1041
  - installing 547
  - setting up 547
- Microsoft Internet Explorer 77
- monitoring interval 167
- monitoring server
  - glossary 1041
  - setting up (JP1/NM linkage) 540

**N**

- name 168
- NetMonitor 1041
- network configuration
  - authentication server linkage 518, 561
- network connection
  - automatically refusal 146
  - controlling 446, 681
  - controlling by action policy 445
  - controlling by administrator 445
  - controlling by command 446
  - managing histories (authentication server linkage) 645
  - permitting (authentication server linkage) 567
  - permitting (JP1/NM linkage) 543
- network connection control
  - by cscnetctrl command 446
  - from Client Security Management window 445
  - list file 780
- network control device
  - setting up (dynamic VLAN environment) 557
  - setting up (static VLAN environment) 560
- network control product 78, 1041
  - linkage to build and run quarantine system (features) 13
  - linkage with JP1/CSC 500
- network control product information

- agent communication environment information 552
  - JP1/NM linkage 537
  - JP1/Software Distribution linkage (AMT linkage facility) 575
- network control server 78, 1041
  - setting up (JP1/NM linkage) 532
- Network Policy Server
  - glossary 1041
  - installing 547
  - setting up 547
- network, addition to
  - new client (authentication server linkage) 639
- new client
  - adding to network (JP1/NM linkage) 595
  - adding to network (JP1/Software Distribution (AMT Linkage facility) linkage) 655
- new installation
  - JP1/CSC - Agent (cluster system) 1001
  - JP1/CSC - Manager (cluster system) 993
- NM page
  - items that can be displayed and set (JP1/Network Monitor linkage) 539
  - operation (JP1/Network Monitor linkage) 538
- non-Software Distribution clients
  - detecting 389, 390
- non-Software Distribution host 1041
- notes
  - network connection control based on connection control list (authentication server linkage) 637
- notification message to client user
  - example 442
- notification method 147
- notification of action execution results 145
- notification of security level judgment results 145
- number of consecutive days (glossary) 1041
- number of consecutive times (glossary) 1041
- number of history preservation generations 145
- number of log files 145, 166

**O**

- operation during failover 1008

- output destinations
  - JP1/CSC - Agent messages 824
  - JP1/CSC - Manager messages 808
- outputting
  - client's history of judgments and actions as CSV file 430
  - history of judgments and actions as CSV file 434
  - PC list information to file 25
  - results of estimation to CSV file 465
  - search results of clients to file 453
- overview
  - automatic update of judgment policies for anti-virus products 46
  - automatic update of judgment policies for security updates 44
  - cluster system 989
  - functionality 38
  - quarantine process 499
  - quarantine system 497
  - quarantine system linked to authentication server 503
  - quarantine system linked to JP1/NM 501
  - quarantine system linked to JP1/Software Distribution (AMT Linkage facility) 506
  - quarantine systems by linked product 501
- overwrite installation
  - JP1/CSC - Agent (cluster system) 1005
  - JP1/CSC - Manager (cluster system) 997
- P**
- password protection 306
- passwords that never expire 290
- patch information
  - adding 229
  - changing 233
  - defining 228
  - deleting 234
  - exporting 236
  - importing 235
- patch information file
  - glossary 1042
  - setup for acquiring 132
- patch update condition file 763
- PC list information 59
- PC list information file 751
- PC List window 409
  - action messages 952
- PC Search window 402, 453
- PC Security Level Details window 412
  - error messages 956
- PC Security level management 59
- PC security settings 43
  - defining account items 286
  - defining anonymous connection items 296
  - defining automatic update items 302
  - defining drive encryption 307
  - defining firewall items 300
  - defining logon items 292
  - defining password items 288
  - defining screensaver items 304
  - defining service items 298
  - defining share items 294
  - editing judgment policy 284
  - error messages displayed in Details window 961
- PC Security Settings Details window 422
- Perform judgment if asset information is not updated 144
- periodic judgment 51
- permitted-device information 539
- permitted-PC list file 596
  - creating (JP1/NM linkage) 597
- policy assignment command 192
- policy assignment definition file 667, 734
  - glossary 1042
- policy import execution file (manual) 779
- Policy Management main window 199
  - menus 203
- Policy Management window
  - glossary 1042
- policy update information 146
- port number 166, 987
  - list 987
- port number for receiving automatic policy update requests 143
- port number for receiving requests 143
- port number used for automatic policy update 166

- power-on password 293
- prerequisite OS
  - for linking to authentication server 522
  - for linking to JP1/NM 512
- prerequisite programs
  - client 81
  - management server 80
  - management terminal 80
  - remote management server 80
- procedures for setting task in Scheduled Tasks 192
- process
  - cscmrvc.exe 988
  - JP1/CSC - Manager Remote Option 988
  - manager service 988
  - remote service 988
  - virus definition information monitoring service 988
- product configuration 77
- product name definition file 729
- prohibited software 43, 1042
- Prohibited Software Details window 418
- prohibited software information
  - adding 264
  - changing 265
  - deleting 266
  - exporting 268
  - importing 267
- prohibited software judgment policy
  - editing 262
- property list (for user-defined judgments) 318

## Q

- quarantine support facility
  - quarantine system (JP1/NM linkage) 580
  - quarantine system operation without (JP1/NM linkage) 580
- quarantine system 498, 1042
  - basic configuration (authentication server linkage) 515
  - basic configuration (JP1/NM linkage) 509
  - basic configuration (JP1/Software Distribution (AMT Linkage facility) linkage) 524
  - building and running (features) 13
  - messages regarding operation 939

- network configuration (authentication server linkage) 518
- non-usage examples (JP1/NM linkage) 587
- operating (authentication server linkage) 603
- operating (JP1/NM linkage) 580
- operating (JP1/Software Distribution (AMT Linkage facility) linkage) 648
- overview 497
- overview (authentication server linkage) 503
- overview (JP1/NM linkage) 501
- overview (linked to JP1/Software Distribution (AMT Linkage facility)) 506
- overview by linked product 501
- setting up 98
- setting up (authentication server linkage) 545
- setting up (JP1/NM linkage) 530
- setting up (JP1/Software Distribution (AMT Linkage facility) linkage) 572
- system configuration 72
- tasks during operation (authentication server linkage) 632
- tasks during operation (JP1/NM linkage) 592
- tasks during operation (JP1/Software Distribution (AMT Linkage facility) linkage) 654
- usage examples (authentication server linkage in dynamic VLAN environment) 603
- usage examples (authentication server linkage in static VLAN environment) 618
- usage examples (JP1/NM linkage) 580, 587
- usage examples (JP1/Software Distribution (AMT Linkage facility) linkage) 648

- quarantine system setup
  - authentication server linkage 545
  - JP1/NM linkage 530
  - JP1/Software Distribution (AMT Linkage facility) linkage 572
- quarantined network (glossary) 1042

## R

- RADIUS server (glossary) 1042
- recovery process

- authentication server linkage (MAC authentication in static VLAN environment) 626
  - IEEE 802.1X authentication server linkage 612
  - JP1/Software Distribution (AMT Linkage facility) linkage 652
  - using quarantine support facility (JP1/NM linkage) 585
  - without using quarantine support facility (JP1/NM linkage) 591
  - Register Permitted PCs
    - window 596
  - Register Permitted PCs window
    - messages 962
  - registering
    - CSC user 187
  - registering permitted PCs
    - JP1/NM linkage 596, 598
    - window transition (JP1/NM linkage) 596
  - remote installation 1042
  - remote management server 71, 77
    - anti-virus product 94
    - glossary 1042
    - prerequisite programs 80
    - setting up 94
    - system configuration 69, 87
  - Remote Option log 808
  - Remote Option log file 976
  - Remote Option page 151
  - Remote Option tab 141
  - remote service 988
  - removing clients
    - authentication server linkage 643
    - JP1/NM linkage 600
    - JP1/Software Distribution (AMT Linkage facility) linkage 655
  - required products
    - for linking to authentication server 522
    - for linking to JP1/NM 512
  - required products and prerequisite OS
    - for linking to authentication server 522
    - for linking to JP1/NM 512
  - for linking to JP1/Software Distribution (AMT facility) 526
  - Restriction of anonymous connections 297
  - result notification information 145
- ## S
- safe 52
  - "Safe" or "Not applicable" results 146
  - sample
    - anti-virus product definition file 981
    - definition file for excluded security updates 978
    - definition file for mandatory security updates 979
    - definition file for mandatory service packs 980
    - mandatory software definition file 983
    - patch update condition file 985
    - prohibited software definition file 982
    - user definition file 984
  - sample of
    - excluded user definition file 986
  - screensaver settings 305
  - search condition file 664, 674, 678, 732
    - glossary 1043
  - search host 390, 1043
  - search results
    - outputting as CSV file 453
  - searching
    - statistics 471
    - statistics for specific groups 471
  - security audit
    - features 8
  - Security Control - Agent Setup dialog box
    - pages (JP1/Network Monitor linkage) 534
  - Security Counter-Measure Evaluation 60
  - security level 6, 51, 1043
    - client 52
    - each judgment condition 52
    - each judgment item 52
    - guides for judgment standards 104
    - implementing appropriate actions (features) 7
    - judging 51
    - judging (features) 6

- judging (JP1/NM linkage) 544
  - judging (JP1/Software Distribution (AMT Linkage facility) linkage) 577
  - judgment command 192
  - judgment method 52
  - judgment trigger 51
- security level factor 457
- security level judgment 40
- security level judgment information 143
- security management
  - disabling 432
  - enabling 433
- security management for client
  - enabling and disabling 432
- security measures
  - authentication server linkage 638
  - gauging trends 469
  - JP1/NM linkage 593
  - JP1/Software Distribution (AMT Linkage facility) linkage 655
- security policy 1043
  - assigning 49
  - assigning to clients 119, 374
  - assigning to clients (command) 667
  - automatic update (features) 11, 12
  - consideration 104
  - management 40
  - managing 43
  - setting 198
  - setting (authentication server linkage) 567
  - setting (JP1/NM linkage) 544
  - setting (JP1/Software Distribution (AMT Linkage facility) linkage) 577
- Security Policy Management window 175, 1043
- security updates 43, 1043
  - automatic update of judgment policies 44
  - editing judgment policy 216
  - updating security policies automatically (features) 11
- Security Updates Details window 413
- service
  - JP1\_NETM\_CSCA 1004
  - JP1\_NETM\_CSCM 997
  - JP1\_NETM\_CSCM\_RS 997
  - service pack information
    - adding 238
    - changing 240
    - defining 236
    - deleting 241
    - exporting 242
    - importing 241
  - Set Display Conditions dialog box 379
  - setting display conditions 379
  - setting up
    - action for each security level 342
    - Asset Information Manager 133
    - client 95
    - for acquiring patch information files 132
    - for deleting results of notification message jobs 130
    - for reporting inventory information to AIM automatically 130
    - JP1/CSC - Agent 173
    - JP1/CSC - Agent (authentication server linkage) 548
    - JP1/CSC - Agent (cluster system) 1001
    - JP1/CSC - Agent (JP1/NM linkage) 533
    - JP1/CSC - Agent (JP1/Software Distribution (AMT Linkage facility) linkage) 573
    - JP1/CSC - Manager (cluster system) 993
    - JP1/CSC - Manager Remote Option 162
    - JP1/NM 540
    - JP1/NM - Manager 532
    - JP1/Software Distribution Client (authentication server linkage) 563
    - JP1/Software Distribution Client (JP1/NM linkage) 541
    - JP1/Software Distribution Client (relay system) (authentication server linkage) 563
    - JP1/Software Distribution Client (relay system) for JP1/NM linkage 541
    - JP1/Software Distribution Client (relay system) for JP1/Software Distribution (AMT Linkage facility) linkage 576
    - JP1/Software Distribution Manager 129
    - management server 92
    - management terminal 92



- Microsoft Internet Authentication Service (authentication server linkage) 547
  - Network Policy Server(authentication server linkage) 547
  - quarantine system 98
  - remote management server 94
  - scrapping clients 131
  - task in Scheduled Tasks 192
  - Windows standard supplicant (authentication server linkage) 565
  - setting up environment
    - JP1/NM linkage 541
    - JP1/Software Distribution (AMT Linkage facility) linkage 576
  - setting up environment before operation can be started
    - authentication server linkage 567
  - setting up for automatic start
    - JP1/CSC - Manager and remote service 156
    - virus definition information monitoring service 168
  - setting up to start automatically
    - JP1/CSC - Agent 173
  - settings for Windows automatic updates 303
  - shared disk 145
  - shared folder settings 295
  - Software Distribution information 145
  - Software Distribution Manager (relay manager) 146
  - Software Distribution SubManager 145
  - standard error output 808
  - standard output 808
  - standby server 996, 1004
  - starting monitoring (JP1/NM linkage) 543
  - statistical data 10
  - statistics 58, 61
    - displaying as graph 485
    - features 10
    - glossary 1043
    - outputting to CSV file 480
    - searching 471
    - storing 470
  - Statistics Details Graph Display window
    - error message 964
  - Statistics Details window
    - error message 964
  - statistics for specific groups
    - displaying as graph 485
    - outputting as CSV file 480
    - searching 471
  - statistics for specific judgment items
    - displaying as graph 488
    - outputting as CSV file 483
  - Statistics Graph Display window
    - error message 963
  - statistics information 147
  - Statistics List window
    - error message 963
  - statistics output file 769
  - statistics storage command 192
  - status of security measures
    - evaluating on clients 457
    - searching for evaluation results 458
    - viewing trends (features) 10
  - status of unnecessary services 299
  - stopping monitoring (JP1/NM linkage) 542
  - storing
    - statistics 470
  - supplicant
    - glossary 1044
    - setting up (authentication server linkage) 565
  - symbol conventions viii
  - system configuration 64
    - basic configuration 64, 86
    - containing multiple authentication servers 520
    - design considerations 84
    - designing 86
    - large-scale system 87
    - quarantine system 72
    - remote management server 69
    - with remote management server 87
  - system installation
    - items to consider 84
- ## T
- task in Scheduled Tasks
    - setting 192
  - tasks during operation

- quarantine system (authentication server linkage) 632
  - quarantine system (JP1/NM linkage) 592
  - quarantine system (JP1/Software Distribution (AMT Linkage facility) linkage) 654
  - TB meaning ix
  - trace information file 967, 968
    - JP1/CSC - Manager Remote Option 968
  - treatment process
    - authentication server linkage (MAC authentication in static VLAN environment) 624
    - IEEE 802.1X authentication server linkage 610
    - JP1/Software Distribution (AMT Linkage facility) linkage 651
    - using quarantine support facility (JP1/NM linkage) 583
    - without using quarantine support facility (JP1/NM linkage) 589
  - treatment server
    - glossary 1044
    - setting up (authentication server linkage) 563
    - setting up (JP1/Network Distribution (AMT Linkage facility) linkage) 576
    - setting up (JP1/NM linkage) 540
  - troubleshooting 965
    - common problems and solutions 970
    - procedure 966
- ## U
- unapplied security updates
    - detecting 389
  - unauthenticated network
    - glossary 1044
  - uninstalling
    - JP1/CSC - Agent 173
    - JP1/CSC - Agent (cluster system) 1006
    - JP1/CSC - Manager 138
    - JP1/CSC - Manager Remote Option 162
  - usage examples
    - JP1/NM quarantine support facility 580
    - quarantine system (authentication server linkage in dynamic VLAN environment) 603
    - quarantine system (authentication server linkage in static VLAN environment) 618
    - quarantine system (JP1/Software Distribution (AMT Linkage facility) linkage) 648
    - without using JP1/NM quarantine support facility 587
  - used disk capacity
    - estimating 1011
    - JP1/CSC - Agent 1015
    - JP1/CSC - Manager 1011
    - JP1/CSC - Manager Remote Option 1014
  - user definition 43
    - adding judgment condition 313
    - adding judgment item 311
    - changing judgment condition 322
    - changing judgment item 327
    - classes and properties specifiable in judgments 318
    - command execution for actions 351
    - command for executing action 703
    - deleting judgment condition 324
    - deleting judgment item 329
    - editing judgment policy 309
    - error messages displayed in Details window 960
    - example of setting judgment condition 324
    - executing actions 449
    - exporting judgment items 330
    - file 724
    - importing judgment items 330
  - User Definition Details window 424
  - user definition judgment 147
  - user roles
    - Asset Information Manager administrator 174
    - CSC administrator 174
    - CSC user 174
- ## V
- version number conventions x
  - virus definition information monitoring service 988
    - setting up for automatic start 168
  - vulnerable passwords 289

**W**

- warning 52
- windows
  - setting up standard supplicant (authentication server linkage) 565
- Windows firewall settings 301
- Windows security update 41
- work flow from installation to starting operation 36
- WUA 78, 96
  - glossary 1044